MASTERARBEIT

ANALYSE DER USERAKZEPTANZ IN WEBBASIERENDEN SINGLE SIGN ON LÖSUNGEN

ausgeführt am

Studiengang
Informationstechnologien und Wirtschaftsinformatik

Von: Gabriel-Antonio Furthmaier
Personenkennzeichen: 1610320041

Graz, am 19. März 2018 .....

Unterschrift

EHRENWÖRTLICHE ERKLÄRUNG

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die benutzten Quellen wörtlich zitiert sowie inhaltlich entnommene Stellen als solche kenntlich gemacht habe.

.....

Unterschrift

DANKSAGUNG

Ich möchte mich an alle Personen bedanken, die mich in den letzten Jahren unterstützt haben. Besonderen Dank gilt meinen Pflegeeltern, ohne deren Unterstützung ich nie die Möglichkeit gehabt hätte, eine dermaßen gute Ausbildung zu genießen, um schlussendlich am Campus02 berufsbegleitend studieren zu können. 22 Jahre ist es nun her, als damals ein 5-jähriger Junge mit seinen zwei älteren Brüder von den nettesten, hilfsbereitesten und großherzigsten Menschen aufgenommen wurde. Seit dieser Zeit ist viel Gutes passiert und deshalb geht ein großer Dank an diese zwei besonderen Menschen.

Jede Person, die sich schon einmal berufsbegleitend weitergebildet hat, sei es durch diverse Kurse oder durch ein Studium, weiß, wie groß die Herausforderung sein kann, sein Privatleben mit der Ausbildung vereinbaren zu lassen. Um das einigermaßen gut bewerkstelligen zu können, braucht man gute Freunde, die auch in schwierigen Zeiten zu einem stehen. Glücklicherweise kann ich mich auf Patrick, Christopher und Kevin verlassen und weiß, dass sie mich auch auf meinem weiteren Weg unterstützen werden.

Des Weiteren möchte ich mich bei meinem Betreuer Günther Zwetti für seine Unterstützung bei meiner Masterarbeit bedanken. Ein großer Dank geht auch an alle Professoren und Mitarbeiter der Fachhochschule Campus 02 für die spannenden letzten 2 Jahre. Ob Big Data, Data Warehouse, General Management, E-Service Engineering oder R Programmierung, ich habe jede Lehrveranstaltung genossen und habe einiges für die Zukunft mitnehmen können.

Auch beruflich habe ich mich während der Zeit weiterentwickelt und arbeite nun als Applikationsentwickler bei der Merkur Versicherung AG. Ich hoffe, dass ich mich im beruflichen Umfeld sowohl fachlich als auch persönlich weiterentwickeln darf.

Abschließend möchte ich die Danksagung mit einem Zitat von Konfuzius beenden, der die letzten zwei berufsbegleitenden Jahre sehr gut auf den Punkt bringt:

Der Weg ist das Ziel
(Konfuzius)

KURZFASSUNG

Die vorliegende Masterarbeit soll Unternehmen ansprechen, die planen, eine Single Sign On Lösung in ihrem Unternehmen zu etablieren. Damit das Authentifizierungsverfahren im Unternehmen von den Mitarbeitern auch genutzt wird, muss eine starke Akzeptanz zwischen den Nutzern und einer Single Sign On Lösungen gegeben sein. Aus diesem Grund werden im Theorieteil Faktoren der Benutzerakzeptanz aus dem Technology Acceptance Model 3 herausgearbeitet, welche im Speziellen für die Akzeptanz von Single Sign On Lösungen zutreffend sind. Die empirische Forschung besteht dabei aus zwei Teilen, in denen einerseits eine Umfrage erstellt und andererseits die Zusammenhänge zwischen den herausgearbeiteten Faktoren und der Benutzerakzeptanz auf Signifikanz geprüft werden.

Die Auswertung der Umfrage im Rahmen dieser Masterarbeit zeigt dabei einen starken Zusammenhang zwischen der IT-Affinität und der Einstellung des Nutzers gegenüber einer Single Sign On Lösung auf die Benutzerakzeptanz.

Eine ebenfalls im Rahmen dieser Arbeit erstellte Fallstudie zeigt, dass Single Sign On Technologien im Privatbereich noch keinen großen Anklang finden und dass auch die Vertrauenswürdigkeit des Identity Provider keinen Einfluss auf die Benutzerakzeptanz von Single Sign On Lösungen hat.

Abschließend werden Maßnahmenvorschläge erstellt, um die Akzeptanz von Single Sign On sowohl in Unternehmen als auch im Privatbereich zu steigern.

ABSTRACT

This master‘s thesis is intended to address companies who are planning to establish a single sign-on solution in their company. The acceptance between users and a single sign-on solution must be given to ensure that the authentication method will be used.

For this reason, the theory section outlines factors of user acceptance from the technology acceptance model 3, which are especially applicable to the acceptance of single sign-on solutions. The empirical research consisted of 2 parts, in which on the one hand a survey has been created and on the other hand the correlation between the outcoming factors and the user acceptance has been checked for significance.

The survey has been found that the user's IT affinity and attitude towards a single sign-on solution has a major impact on user acceptance.

In addition, a case study outlines that the single sign-on technology is still not very popular in the private sector and it has been found that the trustworthiness of the identity provider has no impact on the user acceptance of single sign-on solutions.

Finally, proposed measures has been developed to increase the acceptance of single sign on in business and private sector.

INHALTSVERZEICHNIS

1 MOTIVATION

Da jeder Internetnutzer in Zukunft eine Fülle von Identitätsdaten zu verwalten hat, werden Single-Sign-On-Technologien stark an Bedeutung gewinnen. Stehen heute noch die einfache Bedienbarkeit und der Schutz gegen einfache Phishingangriffe im Vordergrund der Entwicklungen, so müssen diese Systeme, da sie ein lohnendes Angriffsziel darstellen, auch gegen komplexere Angriffe geschützt werden. (Borges et al. 2011)

Die Prognose aus dem Buch ,,Identitätsdiebstahl und Identitätsmissbrauch im Internet“ im Jahr 2011 zeigt, dass Single Sign On eine große Zukunft vorausgesagt wurde. Seit dieser Zeit hat die Relevanz von Single Sign On stetig zugenommen und die Applikationen, welche Single Sign On implementiert haben, haben sich vervielfacht. Jedoch wurde schon damals auf komplexe Angriffe hingewiesen, die uns heute vor großen Herausforderungen stellen.

Aus Sicherheitsgründen wird es im beruflichen und privaten Alltag immer wichtiger, dass man sich verschiedenste Passwörter merken muss. Man wird somit von der Vielzahl an Passwörter überflutet und behilft sich im schlimmsten Fall damit, diese auf einem Post-it zu notieren, um es aufgrund der leichten Auffindbarkeit auf den Computerbildschirm oder auf die Tastatur zu heften.

30% aller Mitarbeiter schreiben ihre Passwörter in irgendeiner Form auf und stellen damit ein Sicherheitsrisiko für sich selbst und für Firmen dar. (Insights For Professionals 2017)

Um dieses Risiko zu minimieren oder sogar zu eliminieren, kann eine Technologie eingesetzt werden, mit der jeder IT-affine User bewusst oder schon einmal unbewusst in Berührung gekommen ist.

Es ist vielen IT-affinen User schon aufgefallen, dass es bei diversen Apps die Möglichkeit besteht, sich über ein eigenes Konto bei Dritten wie Facebook, Twitter oder Google Plus anzumelden, ohne sich nochmals bei der Anwendung selbst legitimieren zu müssen.

Der Mechanismus, der dahintersteckt und somit das bequeme Anmelden ohne erneuerte Legitimierung ermöglicht, wird ,,Single Sign On“ genannt.

Immer mehr Unternehmen statten Ihre Applikationen mit Single-Sign On Lösungen aus, da sie erkannt haben, dass die Bereitstellung solcher Lösungen langfristig die Rentabilität des Unternehmens verbessert.

Erstrangig können ,,Help Desk“ Kosten durch Wegfall von Passwort Anfragen reduziert werden und die Kundenzufriedenheit durch Vereinfachung des Anmeldeprozesses erhöht werden.

Da sich die Benutzer weniger Passwörter merken müssen und die Verwaltung von Passwörter gänzlich wegfällt, wird zudem die Arbeitsproduktivität gesteigert.

Des Weiteren sind die Mitarbeiter durch die Reduktion der Komplexität gewillter, die Sicherheitsrichtlinien einzuhalten und somit bleiben Investitionen in Sicherheitsvorkehrungen und Sicherheitsmechanismen rentabel und erhalten. (John Carl Villanueva 2014)

Auch im privaten Umfeld ist ,,Single Sign On“ nicht mehr wegzudenken. Anstatt, dass sich Personen bei jeder Anwendung separat anmelden müssen, können sie ihr Konto aus bekannten Plattformen, wie Facebook, Twitter oder Google Plus verwenden, um sich zu legitimieren.

Dennoch muss abgegrenzt werden, wann eine bequeme Einmalanmeldung aus Sicherheitsgründen sinnvoll ist. Nicht in allen Branchen ist es wünschenswert und ratsam, ,,Single Sign On“-Lösungen zu implementieren. Deshalb erfolgt Im Zuge des elektronischen Zahlungsverkehrs die Authentifizierung des Benutzers bei jeder Transaktion, um zu gewährleisten, dass keine Dritten Zugriff auf die sensiblen Daten eines Benutzers erhalten und somit die Sicherheit vor Datendiebstahl und Datenmanipulation zu 100% garantiert ist. (Michael Strecker 2010)

Ein weiterer Grund, warum die Akzeptanz von Single Sign On Lösungen noch nicht in allen Unternehmen erreicht wurde, ist dass die Authentifizierung an einer Stelle von Statten geht und bei erfolgreichen Angriffen, Benutzerdaten von verschiedensten Anwendungen von Angreifern ausgespäht werden können. Fällt zudem der Server aus, der für das Identitymanagement zuständig ist, dann kann sich ein User bei keiner Applikation mehr anmelden. In Fachkreisen spricht man von ,,Single-Point-of-Failure“.

Weiters zu beachteten ist, dass besonders im Privatbereich sensible Daten von Benutzer an Drittanbieter weitergegeben werden. Aus diesem Grund müssen Drittanbieter garantieren, dass mit den gewonnen Daten vertrauenswürdig umgegangen wird und Dritten nicht zugänglich gemacht wird. (Matthew Davis 2013)

Zusammenfassend ist somit zusagen, einerseits erhöht die Technologie ,,Single Sign On“ den Nutzungskomfort bei Applikationsanmeldungen, andererseits birgt die Nutzung einer solchen Technologie einige Risiken.

Interessant wäre es zu wissen, ob sich Nutzer deren genannten Risiken bewusst sind und ob somit das Sicherheitsbewusstsein der Nutzer Einfluss auf die Benutzerakzeptanz von Webapplikationen hat.

Da nach reichlicher Recherche in keiner mir bekannten öffentlich publizierten Arbeit die Benutzerakzeptanz im Umfeld von ,,Single Sign On“ Technologien beleuchtet wurde, soll diese Arbeit diese Lücke schließen und Unternehmen dabei helfen, die Einflussfaktoren auf die Benutzerakzeptanz von Single Sign On Lösungen zu kennen. Weiters sollen mit Hilfe dieser Arbeit Maßnahmen abgeleitet werden können, um die Benutzerakzeptanz von Single Sign On unter Berücksichtigung der abhängigen Faktoren zu verbessern.

Zunächst wird diese Arbeit einen guten Überblick über die aktuell verfügbaren „Single Sign On“ Standards geben. Im Speziellen wird auf die Authentifikation-Standards SAML 2.0 und auf Open ID eingegangen, deren Implementierungsansätze beschrieben und Bezug genommen, wie diese Standards mit den Webservice-Protokollen SOAP und REST interagieren.

Im letzten Teil der Theorie sollen abschließend Userakzeptanz Modelle, wie das ,,Technology Acceptance Model“ betrachtet werden und Faktoren herausgearbeitet werden, die die Benutzerakzeptanz der User beeinflussen oder stören.

Im Rahmen der empirischen Untersuchung wird zunächst ein Fragebogen berufstätigen Personen zur Beantwortung vorgelegt und die Ergebnisse auf Basis der herausgearbeiteten Faktoren analysiert.

Anschließend soll anhand einer Feldstudie ersichtlich sein, welche Benutzer die SSO Lösung als Anmeldeverfahren verwenden und welche Benutzer sich auf traditionellen Weg anmelden.

Im Zuge der Feldstudie werden Webapplikationen und Apps, aus den verschiedensten Bereichen in die Evaluierung aufgenommen, um weitere Einflussgrößen für die Ergebnisdarlegung zu gewinnen.

Durch einen gewählten quantitativen Methodenmix bestehend aus Fragebogenauswertung einer Umfrage und einer Fallstudie ist es schließlich möglich, den Zusammenhang zwischen Userakzeptanz und den einzelnen unabhängigen Faktoren zu messen und zu bewerten.

1.1 Abgrenzung des Themas

Diese Arbeit soll nicht alle Single Sign On Technologien im Detail durchleuchten und auch keine detaillierten Implementierungsansätze für die in der Arbeit besprochenen Technologien parat haben. Im Theorieteil wird deshalb nur ein Überblick über die gängigen Single Sign On Lösungen wie Kerberos, LAP und Shibboleth gegeben, aber nicht auf technische Implementierungen eingegangen, da diese nicht zur Beantwortung der Forschungsfrage beitragen.

Da sich die Arbeit auf die Benutzerakzeptanz von webbasierenden Single Sign On Lösungen konzentriert, werden die webbasierenden Single Sign On Standards SAML 2.0 und Open ID im Detail betrachtet. Auch bei der Erstellung des Fragebogens und der Fallstudie wird der Fokus auf die genannten Technologien gesetzt.

Des Weiteren wird auf detaillierte Begriffsdefinitionen der Protokolle HTTP, TCP/IP, REST und SOAP verzichtet. Diese Definitionen sollten bei Bedarf in weiterführender Literatur nachgeschlagen werden.

Auch bei der Theorie des Technology Acceptance Model wird nur auch jene Inhalte eingegangen, die benötigt werden, um relevante Faktoren für die Beantwortung der Forschungsfrage, zu erhalten.

2 FORSCHUNGSFRAGE UND HYPOTHESE

Der Abschnitt Forschungsfrage und Hypothese soll das konkrete Zielvorhaben dieser Arbeit festigen und es sollen Annahmen aufgestellt werden, welche später in der Arbeit verifiziert bzw. falsifiziert werden.

2.1 Forschungsfrage

Wie bereits in der Einleitung erwähnt, soll diese Arbeit den Zusammenhang zwischen der Benutzerakzeptanz und deren Einflussgrößen im Umfeld von webbasierenden Single Sign On Lösungen evaluieren. Im Zuge dieser Arbeit soll folgende Frage beantwortet werden:

Aufgrund welcher Einflussgrößen der Userakzeptanz werden webbasierende SSO Lösungen der direkten Anmeldung über die jeweilige Webanmeldung vorgezogen?

2.2 Hypothese

Nachfolgend sind 4 Alternativhypothesen und 4 Nullhypothesen angeführt. Die jeweiligen 4 H1-Hypothesen, die in dieser Arbeit empirisch geprüft werden, stellen einen Zusammenhang zwischen Benutzerakzeptanz und einer konkreten Einflussgröße dar. Die H0 Hypothese widerlegt die H1 Hypothese und sollte im besten Fall im Zuge der empirischen Untersuchung falsifiziert werden.

H1: Je höher das Sicherheitsbewusstsein der Nutzer, umso geringer ist die Benutzerakzeptanz gegenüber Single Sign On Lösungen.

H0: Das Sicherheitsbewusstsein wirkt sich nicht auf die Benutzerakzeptanz von Single Sign On Lösungen aus.

H1: Je höher die Vertrauenswürdigkeit der Nutzer gegenüber des Identity Providers, umso höher ist die Benutzerakzeptanz gegenüber Single Sign On Lösungen.

H0: Die Vertrauenswürdigkeit des Identity Providers wirkt sich nicht auf die Benutzerakzeptanz von Single Sign On Lösungen aus.

H1: Je höher die IT-Affinität der Nutzer ist, umso höher ist die Akzeptanz gegenüber Single Sign On Lösungen.

H0: Die IT-Affinität wirkt sich nicht auf die Akzeptanz von Single Sign On Lösungen aus.

H1: Je positiver die Einstellung der Nutzer gegenüber Single Sign On ist, umso höher ist die Akzeptanz, die Lösung zu nutzen.

H0: Die Einstellung hat keinen Einfluss auf die Akzeptanz von Single Sign On Lösungen.

2.3 Ziel

Die Einflussgrößen, wie das Sicherheitsbewusstsein der Nutzer, die Vertrauenswürdigkeit der Nutzer gegenüber eines Identity Providers, die IT-Affinität und die Einstellung der Nutzer gegen über einer Single Sign On Lösungen werden durch bestehende Benutzerakzeptanzmodelle herausgearbeitet. Ob weitere Faktoren als die genannten, Einfluss auf die Benutzerakzeptanz haben, wird sich bei der Faktorenanalyse und in weitere Folge bei der Evaluierung zeigen. Welchen Effekt diese Einflussgrößen auf die Benutzerakzeptanz haben und ob die genannten Größen überhaupt mit der Benutzerakzeptanz korrelieren, wird sich im Rahmen dieser Masterarbeit herausstellen.

Ziel dieser Masterarbeit ist es, dass die gewonnen Erkenntnisse auf verschiedene webbasierende SSO Lösungen anwendbar sind und sich daher nicht nur auf eine Anwendung beschränken.

Unternehmen erfahren anhand dieser Masterarbeit, welche Faktoren der Userakzeptanz in Bezug auf Single Sign On Lösungen relevant sind. Aufgrund dessen ist es IT Unternehmen möglich, ihre Umsätze zu steigern und die Zufriedenheit der Benutzer bzw. der Kunden zu erhöhen. Da die Sicherheit bei Anmeldungsprozessen eine sehr große Rolle spielt und diese gewährleistet werden muss, ist es interessant zu wissen, wie der Benutzer selbst über die Sicherheit bei einer bequemen Anmeldemöglichkeit über Single Sign On denkt.

Ein weiteres Ziel dieser Arbeit sollte es sein, dass Unternehmen aus den Erkenntnissen der empirischen Untersuchung, geeignete Maßnahmen für ihre Zwecke ableiten können. Andererseits sollte jedem Leser ein Einblick über Single Sign On Lösungen ermöglicht werden, um selbst kritisch oder positiv über diese Technologie urteilen zu können.

3 PRINZIPEN VON SINGLE SIGN ON

Es gibt verschiedenste Möglichkeiten sich bei Anwendungen zu legitimieren. Sei es durch Legitimierung durch Passwort und Benutzername, durch digitale Signatur, durch ein ausgestelltes Zertifikat, durch Smartcards oder durch biometrische Schlüssel.

Alle erwähnten Legitimierungsmöglichkeiten haben eines gemeinsam: Sie müssen bei jedem Anmeldungsprozess von neuem vorgelegt werden, um die Authentizität der Benutzer zu bestätigen.

Eine Möglichkeit, um den Legitimierungsprozess der Nutzer bei unterschiedlichsten Systemen zu vereinfachen, ist das zur Verfügung stellen einer Single Sign On Lösung auf der Anbieterseite und das Nutzen dieser Technologie auf der Konsumentenseite. (Cryptas 2017)

3.1 Definition von SSO

Die Open Group, ein neutrales IT-Konsortium, dass aus mehr aus 500 Mitgliedern besteht und für die Entwicklung von neuen Industriestandards der Unix-Betriebssysteme zuständig ist, hat SSO wie folgt definiert: (Pearson 2017)

> *Single sign-on (SSO) is mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords. Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable but difficult to implement. (OpenGroup 2010)*

Die Aussage der Open Group beschreibt kurz und knapp den Sinn und Zweck von SSO. Dem Benutzer soll es möglich sein, bei einmaliger Authentisierung Zugriff auf verschiedenste Systeme zu erhalten. Somit soll der Komfort, durch den Wegfall der Legitimierungen bei den einzelnen Systemen, erhöht werden. Weiterführend soll SSO menschliche Fehler reduzieren, welche maßgeblich für System- und Entwicklungsfehler in der Praxis sind. Einerseits weist die OG darauf hin, dass Single Sign On Lösungen erwünscht sind, andererseits sind diese auch nicht einfach zu implementieren. Das soll ein Hinweis darauf sein, dass man bei der Entwicklung und Implementierung solcher Lösungen auf verschiedenste Problemfelder trifft. Probleme können während der Implementierungsphase folgende sein:

- unzureichende Sicherheit,
- erheblicher organisatorische Aufwand durch Kontenzusammenlegung und zentraler Benutzerdatenbank,
- erhöhter Ressourcenaufwand durch Kauf eines Servers (z.B Kerberos)
- kein gänzliches Vertrauen durch die Mitarbeiter und fehlendes Commitment der Geschäftsführung

(Sandro Wefel 2012)

3.2 Vor- und Nachteile von Single Sign On

Wie schon in der Einleitung erwähnt gibt es einige Vorteile, die für den Einsatz einer Single Sign On Technologie sprechen und einige Nachteile, die dagegensprechen. Bei Einführung einer Single Sign On Lösung muss man sich dessen bewusst sein und abwägen können, ob solch eine Lösung im eigenem unternehmerischen Kontext nach Abwägung der unten genannten Vor- und Nachteile sinnvoll ist.

3.2.1 Vorteile

Produktivitätsgewinn und Zeitersparnis: Durch die nur einmalige Authentisierung des Users bei diversen Anwendungen wird Zeit gespart und diese gewonnene Zeit kann für andere Tätigkeiten verwendet werden. (Michel Smidt 2016)

Verbesserung der Rentabilität der Unternehmen: Da der Help-Desk aufgrund laufender Anfragen bezüglich Zurücksetzung von Passwörter entlastet wird, werden Ressourcen für andere wertschöpfende Tätigkeiten frei. (Michel Smidt 2016)

Sicherheitsgewinn für Unternehmen: Der Sicherheitsgewinn wird durch die einmalige Übermittlung der Daten an den Authentifizierungsdienst geschaffen. (Michel Smidt 2016)

Geringer administrativer Aufwand: Der administrative Aufwand bei der Aktualisierung der Authentifizierungsdatenbank ist um einiges überschaubarer, da bei einer Benutzeränderung nur an einer Stelle was geändert werden muss. (Michel Smidt 2016)

Vermeidung von unsicheren Passwörter: User neigen dazu, bei den Vielzahl an benutzten Konten, dasselbe Passwort bei jeder Anwendung zu verwenden oder ein unsicheres Passwort zu verwenden, welches sich leicht merken lässt. Durch Single Sign On kann ein robustes und sicheres Passwort verwendet werden. (Mike Decrescenzo 2014)

Reduzierung von Pishing Attacken: Da die Anmeldedaten nur mehr an einer Stelle eingegeben werden müssen, ist es für Angreifer schwieriger an diese Anmeldedaten zu gelangen. Die Überprüfung der Sicherheitsstandards fällt um einiges leichter, da SSL-Zertifikate und URL nur an einer Stelle kontrolliert werden müssen. (Prowse 2014)

Sicherheitsbewusstere Mitarbeiter: Mitarbeiter sind durch den gewonnenen Komfort gewillter Sicherheitsrichtlinien und Sicherheitsvorkehrungen einzuhalten. (Langer 2016)

Wegfall der Synchronisation von Passwörter: Bei bereits vorhandenen Passwortdatenbanken bei unterschiedlichen Diensten wird als erster Schritt versucht, die einzelnen Passwörter abzugleichen. Das kann Server übergreifend nur mit erheblichen Aufwand durchgeführt werden. (Pröhl 2011)

Kundenbezug durch Single Sign On: Durch den Wegfall von separaten Konten, wird der Kunden auf jeder Plattform gleich angesprochen und das kann von einem Kunden positiv wahrgenommen werden. (Canor Cahill 2008)

3.2.2 Nachteile

Single Point of Failure: Wenn der Server ausfällt, welcher die Benutzerdaten enthält, dann ist es einem Benutzer nicht mehr möglich, sich an einem seiner gewünschten Systemen anzumelden. (Christopher Perry 2016)

Anmeldung nur über SSO möglich: Wenn ein Anbieter nur Anmeldungen über SSO ermöglicht, dann verliert er jene Kunden, welche nicht bei den Drittanbietern angemeldet sind. (Academic 2017)

Rückverfolgbarkeit durch den SSO Anbieter: Ein SSO Anbieter, wie Facebook kann die Abfolge von Seitenaufrufen mitverfolgen. Das heißt Facebook sieht, wie oft eine App benutzt wurde. (AGNIESZKA CZERNIK 2016)

Weitergabe von Informationen an Webseiten-Betreiber: Um SSO zu ermöglichen, müssen auch Informationen vom SSO Anbieter an den Applikationsbetreiber weitergeben werden, die jedoch vom jeweiligen Betreiber vertraulich behandelt werden sollten. Es ist jedoch gängige Praxis, dass Informationen weitergegeben werden, welche über die Legitimierung hinausgehen. (AGNIESZKA CZERNIK 2016)

Offengelegte Systeme bei Angriff: Ist ein Angriff erfolgreich, dann erhält der Angreifer Zugriff auf alle Systeme, mit den sicher der Benutzer über SSO anmelden kann. (Andreas Neumann 2017)

Zugriffsberechtigungen werden nicht festgelegt: Die Single Sign On Technologie berücksichtigt in ihrer Grundform nur die Authentifizierung der Benutzer und regelt nicht die Berechtigungen der einzelnen Benutzer bei den angemeldeten Systemen. (Andrew Hindle 2014)

Single Sign Off nicht aktiviert: Ist Single Sign Off nicht implementiert, dann bleibt der User solange beim jeweiligen System angemeldet bis die Sitzung abläuft. (Romain Péchayre 2015)

3.3 Lösungskonzepte von Single Sign On

Es gibt die verschiedensten Lösungskonzepte, wie Single Sign On Lösungen umgesetzt werden können. Wenn über das Thema SSO gesprochen wird, dann ist meistens von einer Protallösung oder einem Ticketingsystem die Rede, wo sich Benutzer bei einer autorisierten Stelle über einen Server authentifizieren. Nichtsdestotrotz gibt es weitere nicht so gängige SSO Konzepte wie die Medienlösung oder die lokale Lösung. Nachfolgend sind die einzelnen Lösungskonzepte in ihrer Grundform beschrieben.

3.3.1 Medienlösung

Die Medienlösung ist einer der selten aufkommenden SSO Lösungskonzepte in der Praxis. Über ein Medium werden Credentials, wie ein Sicherheitstoken oder ein Passwort übertragen. Die Anwendungen für den gesamten Arbeitsplatz stehen für die Mitarbeiter ohne weiter notwendige

Authentifizierungspflicht zur Verfügung. Als Medium für die eindeutige Identifikation der Benutzer können der

- drahtlose Schlüssel (Bluetooth-Token),
- ein Schlüssel mit Kontaktübertragung (USB, 1wire) oder
- eine Schlüsseleingabe über Tastatureingabe.

dienen.

(Bitium 2017)

3.3.2 Portallösung

Bei erstmaligen Einloggen bei einem Portal authentisiert sich der Benutzer beim Server und ist zugleich bei allen Applikationen angemeldet, welche vom Portal betrieben werden. Zugleich werden auch die Berechtigungen des Benutzers für die einzelnen Applikationen vergeben. Bei Webanwendungen ist die Umsetzung mit HTTP-Cookies möglich ohne Sicherheitsrisiken einzugehen, da die Applikationen von der gleichen Domäne betrieben werden. (Shivakumar 2016)

3.3.3 Ticketingsystem

Das Ticketingsystem ist ein sehr verbreiteter Lösungsansatz um SSO Lösungen umzusetzen. Es wird ein Authentisierungsdienst eingesetzt, welcher den User für die ausgestellte Dauer eines Tickets für verschiedenste Systeme authentifiziert. Ein Authentisierungsdienst wie Kerberos besitzt ein Key Distribution Center, dass für die Authentisierung der Benutzer verantwortlich ist und SSO Funktionalitäten unterstützt. (Pröhl 2011)

3.3.4 Lokale Lösung

Die trivialste Lösung ist es die Credentials automatisch in der Eingabemaske für jede Anwendung befüllen zu lassen. Bei jedem Einstieg des Benutzers werden somit die vertraulichen Informationen in der Eingabemaske vorbelegt. Um nun zu vermeiden, dass die Eingabemasken gefälscht werden und um zu garantieren, dass die vertraulichen Informationen an keine Dritten gelangen, müssen Informationen wie Aufrufpfade, Erstelldatum abgefragt werden.

Unteranderem können die Credentials

- in einer verschlüsselten Datei,
- auf einer Chipkarte,
- auf einem Verzeichnisdienst,
- auf einem Single Sign On Server im Netzwerk oder
- auf einer Datenbank

zur Verwendbarkeit abgelegt sein, damit der Benutzer sich die Passwörter bei nicht selbst mehr merken muss. Bei dieser Lösung muss auf die Sicherheit der gespeicherten Passwörter besonders viel Wert gelegt werden, damit diese nicht Dritte entschlüsseln und missbrauchen können.(La Parisien 2017)

3.4 Webbasierender Single Sign On Workflow

Es gibt zahlreiche webbasierende SSO Lösungen, sowie offene Protokolle, welche eine reibungslose Authentifizierung und zumeist auch Autorisierung der Benutzer gewährleisten. Die an der Kommunikation beteiligen Parteien, der Kommunikationsablauf zwischen den einzelnen Parteien, sowie die Interaktionen zwischen Client und Browser ähneln sich bei jeder webbasierenden SSO Lösung. Exemplarisch soll hier ein webbasierender SSO Workflow dargestellt werden, der abstrahiert und generalisiert die Prozessschritte innerhalb einer SSO Lösung darstellt.

3.4.1 Parteien

Es gibt zahlreiche Akteure, die im Zuge der Authentifizierung eines Benutzers bei einem Server miteinander kommunizieren. Nachfolgend sind die beteiligten Parteien angeführt, welche für die reibungslose Interaktion in einer SSO Lösung unerlässlich sind.

User: Der User möchte nach Eingabe von den Credentials Zugriff auf die gewünschten Systeme erhalten.

Web Browser: Der User navigiert im Browser um auf die Applikation zugreifen zu können.

Service Provider: Ein Service Provider kommuniziert mit dem Identity Provider, ob die Authentifikation erfolgreich war und ermöglicht es, dass der User auf die Ressourcen zugreifen kann.

Identity Provider: Der Identity Provider authentifiziert den Benutzer und gewährt bei Erfolg über den Service Provider Zugriff auf die gewünschten Applikationen.

Applikation: Die Applikation stellt mit ihren Funktionalitäten Ressourcen dar, auf die der User zugreifen möchte.

3.4.2 Prozessschritte innerhalb einer SSO Lösung

Abbildung 1 zeigt die Prozessschritte, welche nötig sind, damit ein User Zutritt zur gewünschten Anwendung erhält. Das in UML modellierte Prozessdiagramm zeigt die Aktivitäten, welche von den Akteuren User, Service Provider und Identity Provider durchgeführt werden müssen, damit schlussendlich der Benutzer erfolgreich bei der gewünschten Applikation angemeldet ist. Im Grunde lässt sich der gesamte Kommunikationsablauf zwischen User, Service Provider und Identity Provider in 9 Teilschritten beschreiben. Wie schon erwähnt gilt dieser ,,Single Sign On Workflow“ nur als Überblick um in das Thema Fuß fassen zu können. Genauer auf den

Informationsaustausch zwischen den einzelnen Parteien wird eingegangen, wenn die Protokolle OpenID und SAML 2.0 in den Folgekapiteln behandelt werden.

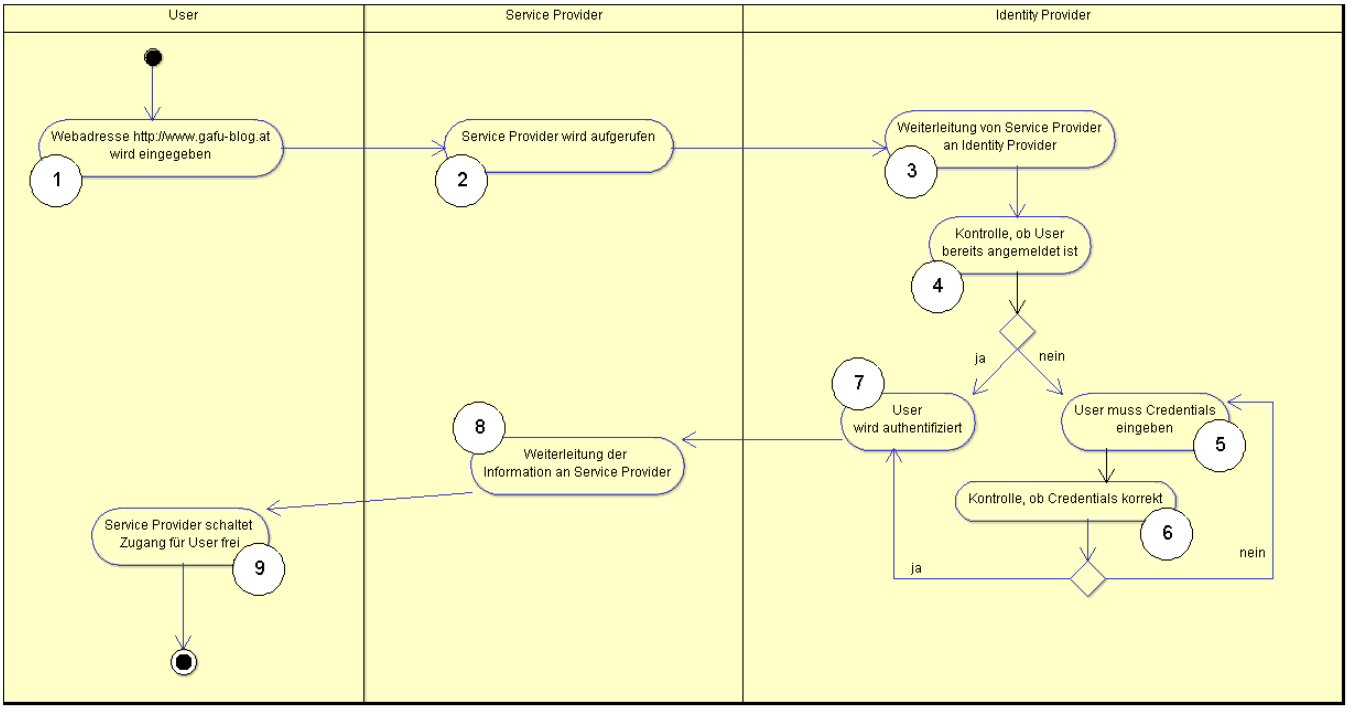

Abbildung 1: Single Sign On Workflow (Socialcast 2017)

1) **Webadresse wird eingegeben:** Der User gibt über einen Browser die Webadresse ein, um Zugang zur Applikation zu erhalten.
2) **Service Provider wird aufgerufen:** Bei Eingabe der URL wird der Service Provider der Anwendung aufgerufen.
3) **Weiterleitung von Service Provider an Identity Provider:** Um die Identität des Benutzers zu bestätigen, leitet der Service Provider auf die Webadresse des Identity Providers um.
4) **Kontrolle, ob User bereits angemeldet ist:** Der Identity Provider kontrolliert, ob der Benutzer bereits angemeldet ist.
5) **User muss Credentials eingeben:** Ist er nicht angemeldet, muss der Benutzer seine vertraulichen Daten, wie Usererkennung und Passwort eingeben.
6) **Kontrolle, ob eingegebenen Credentials korrekt sind:** Daraufhin kontrolliert der Identity Provider, ob die Credentials mit den Daten in der Passwortdatenbank übereinstimmen.
7) **User wird authentifiziert:** Ist der Benutzer bereits angemeldet oder sind die eingegebenen Credentials korrekt, dann wird seine Identität bestätigt.
8) **Weiterleitung der Informationen an Service Provider:** Der Service Provider erhält vom Identity Provider die Info, dass der Benutzer vertrauenswürdig ist.

9) **Service Provider schaltet Zugang für User frei:** Da der Service Provider nun weiß, dass der Benutzer erfolgreich beim Identity Provider authentifiziert hat, erhält dieser Zugang zur Anwendung.

4 SSO TECHNOLOGIEN

Dieses Kapitel soll einen kurzen Überblick über die aktuell relevanten Technologien in der Praxis geben, welche SSO unterstützen. Besonders wird auf die webbasierenden Standards SAML 2.0 und OpenID eingegangen, welche auf verschiedensten Webapplikationen und mobilen Applikationen Verwendung finden.

4.1 Kerberos

Kerberos hat sich in den letzten Jahren auf den verschiedensten IT-Umgebungen, sei es auf einer Windows, Linux oder Apple Umgebung, als Authentisierungsdienst etabliert und hat sich seit jeher stark verbreitet. Für den Zugriff auf einen Dienst, werden Tickets erstellt, die für eine bestimmte Zeitspanne gültig sind.

Kerberos kennt als Teilnehmer

- den Client,
- den Dienst und
- das Key Distribution Center (KDC),

die im Anmeldeprozess miteinander interagieren.

Der KDC besteht aus den Authentification Service (AS), welcher für die Ticketerzeugung, für die Clientanfragen, sowie der Erzeugung der kryptographischen Session Keys zuständig ist. Zusätzlich beinhaltet der KDC eine Datenbank, welche die Langzeitschlüssel für die Verschlüsselung und Entschlüsselung von Nachrichten, enthält. Um die Sicherheit und Vertraulichkeit der Kommunikation zwischen den einzelnen Parteien zu gewährleisten, werden kryptographische Verschlüsselungsverfahren eingesetzt.

Kerberos unterteilt Umgebungen noch in organisatorische Einheiten, auch Realm genannt. Diese Realms bestehen wiederum aus Principals, welche Dienste oder Clients sein können. Da die Kommunikation zwischen den unterschiedlichen Realms möglich ist, wird die Single Sign On Funktionalität unter Kerberos unterstützt und gefördert.

Die Abbildung 2 illustriert das einstufige Kerberos-Verfahren und gibt einen Einblick über den Informationsaustausch zwischen den oben genannten Parteien.

(Pröhl 2011)

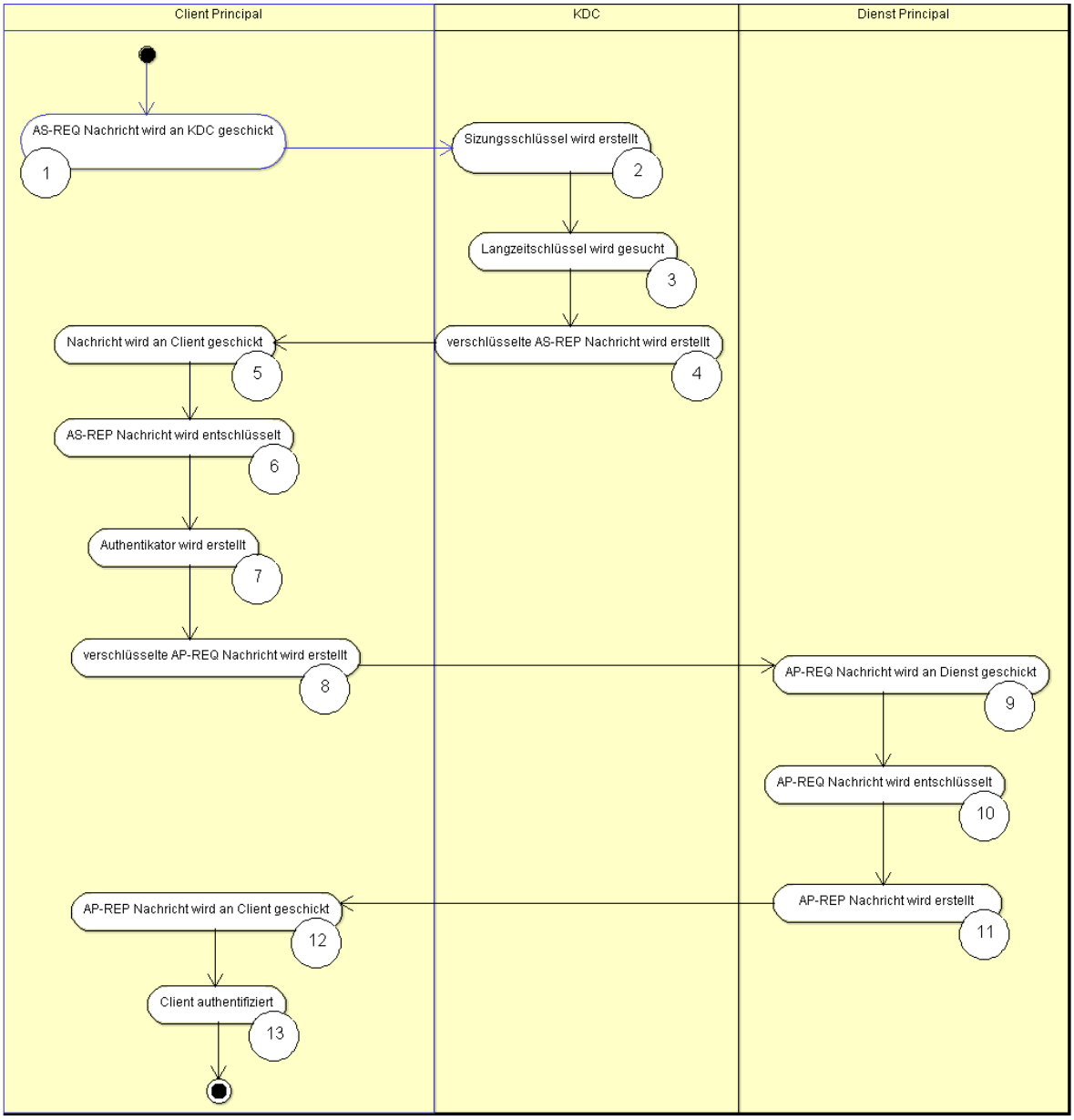

Abbildung 2: Kerberos Prozessworkflow (eigene Abbildung)

1) **AS-REQ Nachricht wird an KDC geschickt:** Client schickt Anfrage an KDC und diese Authentification Service Request Nachricht enthält den Principal-Namen des Clients und den Principal-Namen des Dienstes.
2) **Sitzungsschlüssel wird erstellt:** Es wird ein zufälliger Sitzungsschlüssel für Client und Dienst generiert, welche die Nachricht identifiziert.
3) **Langzeitschlüssel wird gesucht:** In der KDC Datenbank wird der Langzeitschlüssel von Client und Dienst gesucht, um die Nachricht zu verschlüsseln.
4) **Verschlüsselte AS-REP Nachricht wird erstellt**: Die AS-REP Nachricht, bestehend aus Client-Teil und Ticket wird mit dem Langzeitschlüssel verschlüsselt. Der Client-Teil enthält

den Principal Name des Dienstes und den Session Key. Das Ticket wiederum enthält den Principal Name des Clients und den dazugehörigen Session Key.

5) **Nachricht wird an Client geschickt:** Die AS-REP Nachricht wird zur weiteren Verarbeitung an den Client zugeschickt.
6) **AS-REP Nachricht wird entschlüsselt:** Der Client entschlüsselt die AS-REP Nachricht mit dem ihm bekannten Langezeitschlüssel. Dadurch ist dem Client der notwendige Session Key bekannt.
7) **Authentifikator wird erstellt:** Ein verschlüsselter Zeitstempel wird mit dem Client Principal Name in eine Nachricht verpackt und mit dem Sitzungsschlüssel verschlüsselt.
8) **Verschlüsselte AP-REQ Nachricht wird erstellt:** Die AP-REQ Nachricht besteht aus einem Ticket und dem Authentifikator . Das Ticket ist nach dem Versand vom KDC zum Client unverändert geblieben. Der Authentifikator wurde wie bereits erwähnt, auf Basis des Client-Teils erstellt.
9) **AP-REQ Nachricht wird an Dienst geschickt:** Diese Nachricht wird an den Dienst geschickt, um den Authentisierungsvorgang abzuschließen.
10) **AP-REQ Nachricht wird entschlüsselt:** Mit dem vom Dienst bekannten Langzeitschlüssel wird das Ticket in der AP-REQ Nachricht entschlüsselt. Der enthaltene Sessionkey dient dazu, um den Authentifikator zu entschlüsseln.
11) **AP-REP Nachricht wird erstellt:** Wenn der Sessionkey und der Zeitstempel vom Dienst als richtig befunden wurde, erstellt der Dienst eine Application Service Reply Nachricht, welche wiederum einen Authentifikator enthält.
12) **AP-REP Nachricht wird an Client geschickt:** Diese Nachricht dient dazu um das Service zu authentifizieren und wird dem Client zur Überprüfung geschickt.
13) **Client und Dienst authentifiziert:** Nachdem der Client, den Authentifikator entschlüsselt hat und als richtig befunden hat, sind sowohl Client und Dienst eindeutig identifiziert worden. Somit hat der User die Berechtigung auf den Dienst zuzugreifen.

(Pröhl 2011)

4.2 Liberty Alliance Project

Das Liberty Alliance Projekt bietet einen Single Sign On Standard für Webapplikationen an, welche aus einem Webservices Framework (ID-WSF) und Service Interface Specifications (ID-SIS) besteht und einen sicheren Identitätsaustausch zwischen verschiedenen Domänen ermöglicht.

ID-WSF baut auf verschiedenen bereits existierenden Standards wie SAML, WS-Security und WS-Adressing auf, jedoch erweitert ID-WSF diese, um Funktionalitäten in Bezug auf Privatsphäre, Sicherheit und Verwaltung von identitätsrelevanten Informationen.

Im Gegenzug spezifiziert und definiert ID-SIS die Syntax und Semantik der versendeten identitätsbezogenen Nachrichten, wie Geolocation, Anwesenheit oder Profilattribute.

Da die Kommunikation zwischen den einzelnen Akteuren im Liberty Allicance Projekt über Webservices gehandhabt wird, kennt LAP noch weitere 2 Akteure.

Web Service Consumer (WSC): Der Webservice Konsument fordert Informationen beim Webservice-Provider an oder ruft zu Verfügung gestellte Funktionen beim Service Provider auf.

Web Service Provider (WSP): Der Webservice Anbieter stellt das Webservice für den Webservice-Konsumenten zur Verfügung. (Oracle 2017)

4.2.1 Spezifizierte Webservices in LAP

Die ID-WSF Spezifikation unterscheidet zwischen eine Reihe von Webservicearten, die jedoch nicht alle bei einer SSO Lösung im Einsatz sein müssen.

Discovery Service (DS): Der Discovery Service stellt sicher, dass der WSC bei Versendung einer Anfrage den WSP mit der passenden Userkennung findet. Dazu ist jedoch die einmalige Registrierung des Webservices beim Discovery Service notwendig.

Identity Mapping Service (IMS): Der Identity Mapping Service ist ein Webservice, der die Zuordnung von Benutzeridentitäten zwischen verschiedenen Domänen ermöglicht. Notwendig wird solch ein Webservice, wenn Anbieter zum Austausch von Identitäten aus Sicherheitsgründen Pseudonyme verwenden.

Interaction Service (IS): Wenn die Zustimmung eines Benutzers auf identitätsbezogene Inhalte benötigt wird, dann vermittelt der Interaction Service zwischen Anbieter und Benutzer. Ein konkretes Beispiel wäre, wenn ein Benutzer über eine gewollte Änderung seines Inhaltes von einem anderen Benutzer via SMS informiert wird und seine Zustimmung verlangt wird, um den Autorisierungsprozess abschließen zu können.

People Service (PS): Ist ein spezielles Webservice, das ermöglicht Beziehungen im sozialen Netzwerk zu verwalten und zu erhalten.

Authentification Service (AS): Der Authentification Service stellt die Authentifizierung des Client beim Identity Provider sicher und ermöglicht es dem Client sich beim Service Anbieter anzumelden.

Single Sign On Service (SSOS): Dieses Webservice unterstützt die Authentisierung verschiedenster Clients beim Anbieter ohne sich erneut anzumelden zu müssen. (Canor Cahill 2008)

4.2.2 Bootstrapping

Der Überführungsprozess von einer Single Sign On Umgebung zu einer Webservice Umgebung wird Bootstrapping genannt. Der Service Provider wird dabei zum Webservice Konsument und

benötigt notwendige Informationen, welche er über generierte Tokens erhält, um gezielte Anfragen an den Webservice Anbieter zu senden.

Das ID-WSF stellt für das Bootstrapping das Profil ID-WSF ERP, welches aus SAML Assertionen besteht, zur Verfügung, um den Discovery Service aufzurufen. (Misra et al. 2010)

4.2.3 Kommunikationsworkflow in LAP

Um die Prozessschritte, die mit der Verwendung des Standards LAP anfallen, anschaulich darzustellen, wird angenommen, dass sich ein Benutzer auf MyTrips.com einloggt. MyTrips.com interagiert über Single Sign On mit MyCalendar.com. Daher ist ein erneutes Einloggen nicht mehr notwendig.

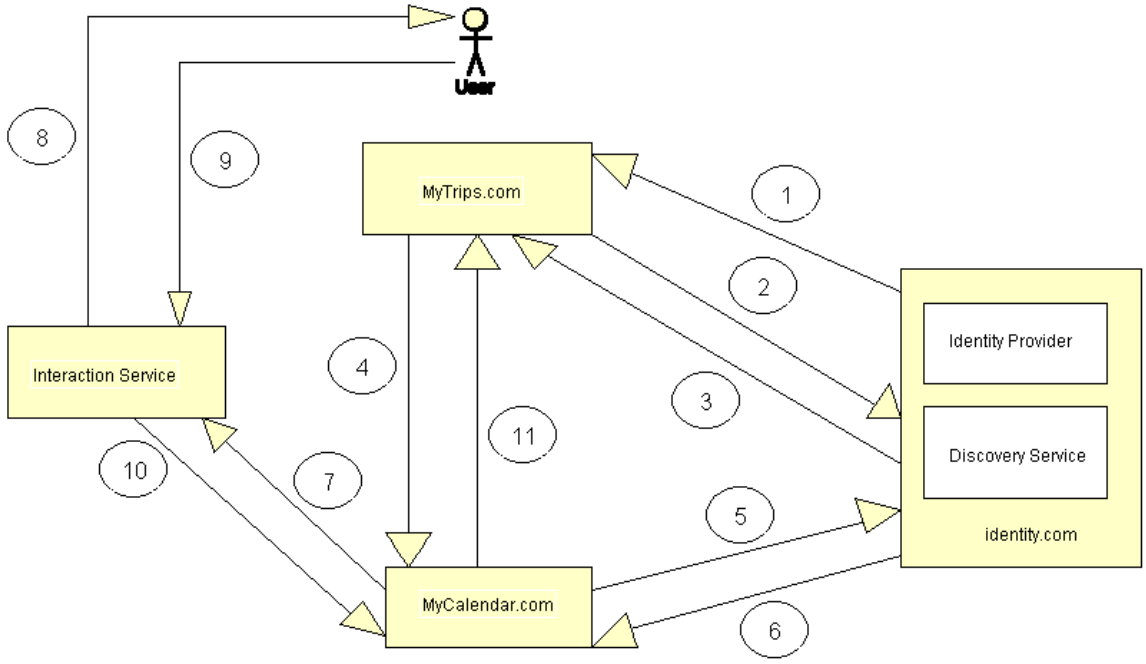

Abbildung 3: LAP Prozessworkflow (Canor Cahill 2008)

1) **Authentifizierung durch Identity Provider:** User loggt sich über MyTrips.com an und bucht einen Urlaub. Der Identity Provider schickt eine SAML 2 Assertion zu MyTrips.com, welche den Bootstrap ID-WSF endpoint reference (EPR) enthält. Der EPR besteht aus einem Sicherheits- und Identitätstoken.
2) **MyTrips.com schickt Anfrage an Discovery Service:** Da MyTrips.com auf das Service MyCalendar.com zugreifen möchte, schickt MyTrips.com eine Anfrage an den Discovery Service um die Usererkennung für MyCalendar.com zu erhalten.
3) **Discovery Service schickt ID-WSF ERP an MyTrips.com:** Der ID-WSF enthält wiederum Sicherheits- und Identitätstoken. Der Sicherheitstoken, kann aus einem SAML Token, der den User spezifiziert, sowie aus einem Token bestehen, der My.Trips.com

spezifiziert. Der ID-WSF ERP kann nach Weiterleitung an MyCalender.com, vom MyCalender.com verwendet werden, um weitere Services aufzurufen.

4) **MyTrips.com schickt Anfrage an MyCalendar.com:** MyTrips.com schickt den ID-WSF ERP an MyCalendar.com und zusätzlich eine Nachricht, ob beim gewünschten Buchungsdatum, Termine frei sind.
5) **MyCalendar.com braucht Einwilligung vom User:** MyCalendar.com schickt eine Nachricht mit dem ERP an den Discovery Service, um Zugriff auf den Interaction Service zu erhalten.
6) **Discovery Service schickt ID-WSF ERP an MyCalender.com:** Discovery Service versendet an MyCalender.com wiederum ein ID-WS ERP, um einen sicheren Nachrichtenaustausch zu gewährleisten.
7) **MyCalendar.com ruft Interaction Service auf:** Der Interaction Service ist dafür zuständig, dass er dem User über eine SMS eine Anfrage zur Einwilligung schickt.
8) **Interaction Service schickt SMS an User:** Ob MyTrips.com die Antwort auf seine Anfrage erhält, hängt davon ab ob der User einwilligt.
9) **User antwortet mit Bestätigung:** Mit passender Antwort auf die SMS, wird die Nachricht für MyTrips.com freigegeben.
10) **Interactive Service antwortet an MyCalendar.com:** MyCalendar.com enthält die Antwort vom Interactive Service, dass der User die Anfrage bestätigt hat.
11) **MyCalendar.com schickt Information an MyTrips.com:** MyCalendar.com antwortet schlussendlich auf die Anfrage von MyTrips.com und gibt die Kalenderinformation preis.

(Canor Cahill 2008)

4.3 Shibboleth

Shibboleth ist eine webbasierende Single-Sign On Lösung, die auf SAML basiert und die es ermöglicht von seiner Heimatumgebung auf Dienste unterschiedlicher Anbieter zuzugreifen. (Shibboleth 2017)

Shibboleth wird bereits in zahlreichen Frameworks von Unternehmen eingesetzt und hat sich als Single Sign Lösung etabliert.

Die Abbildung 4 zeigt abstrahiert den Prozessworkflow zwischen den bereits bekannten Parteien Identity Provider, User und Service Provider. Interessant ist, dass bei Single Sign On Lösungen, welche mit Shibboleth umgesetzt werden, Cookies verwendet werden können, um einen Session Code oder die geschützte Ressource selbst zu speichern. Das Risiko, dass diese Daten von 3 Dritten gelesen werden können, wird dadurch abgesichert, dass Pseudo-Namen bei der Speicherung der Cookies verwendet werden. (Scott Cantor 2012)

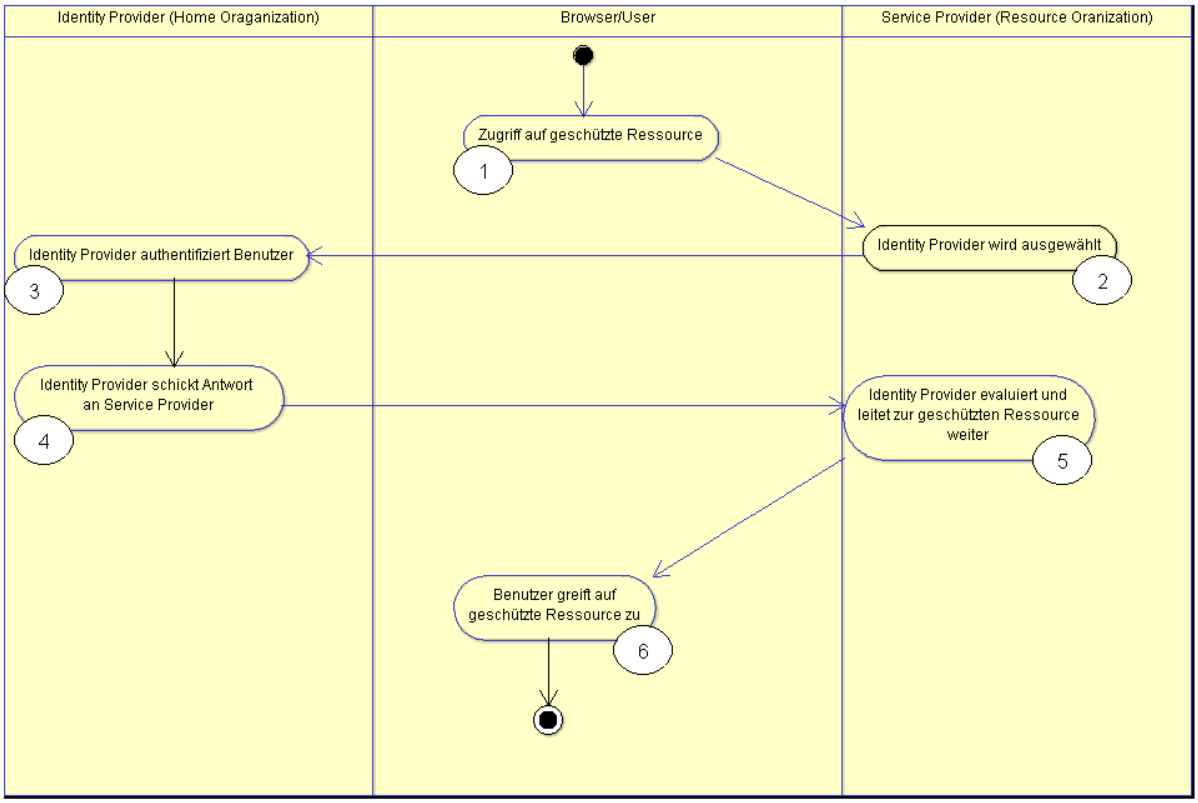

Abbildung 4: Shibboleth Prozessworkflow (Scott Cantor 2012)

Die Interaktion zwischen den beteiligten Parteien im Zuge des Authentifizierungsprozesses der Shibboleth SSO Lösung kann in 6 Schritten unterteilt werden.

1) **Benutzer versucht auf geschützte Ressource zuzugreifen:** Der Service Provider fängt den Zugriff des Benutzers ab. Die geschützte Ressource kann in der Server-Konfiguration festgelegt werden.
2) **Service Provider wählt Identity Provider aus:** Ein Sessioninitiator stoßt den Prozess der Authentifikation an und legt fest, bei welchem Identity Provider der User registriert ist. Eine weitere Möglichkeit ist es, dass sich der Sessioninitiator eines Discovery Service behilft um den Identity Provider festzustellen. Zusätzlich kann noch ein Cookie, das „relay state“ genannt wird, vom Service Provider abgespeichert werden, welche die angeforderte Original Ressource enthält.
3) **Identity Provider authentifiziert Benutzer:** Eine Authentifizierungsanfrage vom Service Provider an den Identity Provider wird verschickt. Die Anfrage wird vom Service Provider über den Browser durchgeschleust und gelangt schließlich zum Identity Provider. Der Identity Provider sieht nach, ob der Service Provider vertraulich ist und entscheidet, ob der User authentifiziert werden kann. Der Identity Provider liest bei Bedarf, das erstellte Cookie des Service Providers aus und erstellt ein eigenes um den Fortschritt der Authentifizierung messen zu können.

4) **Identity Provider schickt Antwort an Service Provider:** Es hängt vom SAML Profil ab, welche Informationen zum Service Provider geschickt werden und wie sie verpackt werden. Für die Sammlung und Transformation der Daten ist der Attribute Resolver und für das endgültige Verpacken und komprimieren der Informationen der Attribute Filter zuständig. Der Attribute Resolver encodiert die Daten aus Sicherheitsgründen und die Nachrichten werden schlussendlich über eine SAML Assertion verschickt, welche wiederum verschlüsselt ist.
5) **Service Provider evaluiert und leitet zu geschützten Ressource weiter:** Der Service Provider entschlüsselt und decodiert die SAML-Nachricht des Identity Provider. Ist alles in Ordnung, wird eine neue User Session erstellt, nachdem die Daten extrahiert und verarbeitet wurden. Die Überführung der Daten aus der SAML Assertion in Sessiondaten, wird mit den Shibboleth Elementen AttributeExtractor und AtrributeFilter erreicht. Um nun auf die ursprüngliche Ressource zuzugreifen, kann die URL aus dem „relay state“ Cookie ausgelesen werden oder aus der Nachricht des Identity Providers ausgelesen werden, wenn diese mitgeschickt wurde. Abschließend wird vom Service Provider nochmals ein Cookie erstellt, welche den Session Code enthält, um den Browser mit der erstellten Sitzung jederzeit zuordnen zu können.
6) **Benutzer greift auf geschützte Ressource zu:** Der Browser wird nun auf die geschützte Ressource weitergeleitet. Der Session Code wird aus dem Cookie ausgelesen und der Benutzer ist authentifiziert.

(Nate Klingenstein 2017)

4.4 SAML 2.0

SAML 2.0 ist ein XML basierter Sicherheitsstandard für Authentifizierung und Autorisierung in Single Sign On Lösungen, welcher zurzeit in vielen Unternehmen im Einsatz ist. Einer der namhaften Unternehmen, welche SAML 2.0 für die Authentifizierung von User und Autorisierung von Ressourcen im Einsatz hat, ist Google. Google tritt meistens als Identity Provider auf und jegliche Webanwendung, welcher als Service Provider fungiert, kann den User über ein Google Konto authentifizieren lassen. (Jed Breinholt 2017)

SAML 2.0 spezifiziert im Grunde, welche Informationen über den Benutzer übermittelt werden sollen, jedoch nicht, wie sie übermittelt werden. Diese Aufgabe übernehmen unter anderem Transportprotokolle wie SOAP, TCP/IP.

SAML wurde von OASIS im Jahr 2002 entwickelt und wurde im September 2005 von SAML 2.0 abgelöst. Zurzeit wird an einer neuen Version SAML 2.1 gearbeitet. In SAML 2.1 sollen Erweiterungen direkt in die Spezifikation eingepflegt werden, die über die Jahre zusätzlich zu SAML 2.0 entwickelt wurden. Zusätzlich sollen unsaubere Implementierungen bereinigt werden und der Standard SAML 2.0 wird nach Einführung der neuen Version 2.1 erhalten bleiben. (OASIS 2017)

4.4.1 Arten der SAML Authentifizierung

Grundsätzlich wird zwischen den Workflows Identity Provider Initiated und Service Provider Initiated unterschieden. Der Hauptunterschied zwischen den Kommunikationsabläufen liegt darin, dass sich beim Identity Provider Initiated Workflow, der User direkt beim Identity Provider ohne Mithilfe des Service Providers anmelden kann.

4.4.2 Identity Provider Initiated

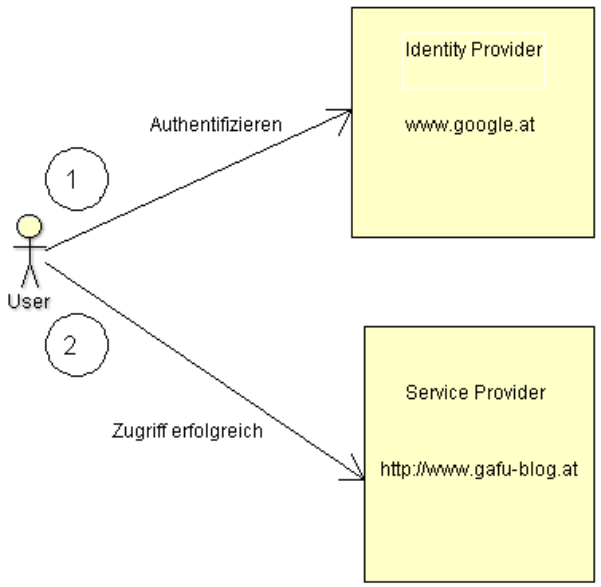

Abbildung 5: Identity Provider Initiated (Sadiq 2016)

1) **Authentifizieren:** Der Benutzer authentisiert sich beim Identity Provider ohne jemals eine Anfrage an den Service Provider zu stellen.
2) **Zugriff erfolgreich:** Authentifiziert der Identity Provider den Benutzer, dann kann sich der Benutzer beim Service Provider anmelden.

4.4.3 Service Provider Initiated

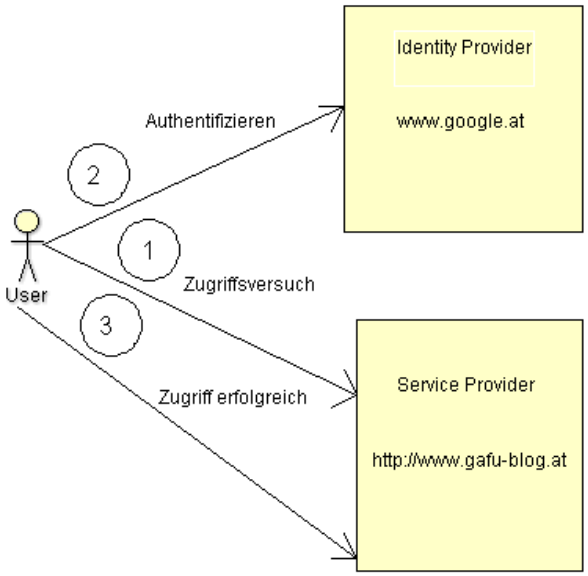

Abbildung 6: Service Provider Initiated (Sadiq 2016)

1) **Zugriffsversuch:** Der Benutzer versucht sich beim Service Provider anzumelden.
2) **Authentifizieren:** Der Service Provider leitet den Benutzer über den Browser zum Identity Provider weiter. Der Identity Provider identifiziert den Benutzer und authentifiziert diesen.
3) **Zugriff erfolgreich:** Der Benutzer hat nun Zugriff auf die Ressourcen des Service Providers.

(Sadiq 2016)

4.4.4 SAML Komponenten

Die SAML Architektur besteht aus den Komponenten Assertion, Protokoll, Binding und Profil.

1) **Assertion:** Die SAML Assertion wird zur Kommunikation zwischen User und Identity Provider verwendet. Die Assertion enthält Informationen über den Benutzer und spezifiziert im Falle eines Autorisierung-Statement, welche Berechtigungen der Benutzer beim Service Provider erhält.
2) **Protokoll:** Die Protokolle definieren in Form eines XML Schemas, wie SAML Assertionen erhalten und gesendet werden.
3) **Binding:** Damit das SAML Protokoll auch verschickt werden kann, muss das SAML Protokoll mit den untergeordneten Transportprotokollen wie SOAP oder HTTP zusammenarbeiten.

4) **Profil:** Profile definieren, wie Assertionen, Protokolle und Bindings miteinander kombiniert werden müssen, um eine sicherheitsgestützte Kommunikation durch SAML 2.0 zwischen den Parteien zu gewährleisten.

(Michel Smidt 2016)

4.4.5 Assertion

Eine SAML Assertion enthält alle notwendigen Informationen eines Benutzers, um diesen authentifizieren zu lassen und diesen den Zutritt zum gewünschten System zu gewähren. Der Identity Provider erstellt eine SAML Assertion und übermittelt diese Aussage dem Service Provider, der aufgrund dieser Aussage entscheidet, ob der User Zutritt zur Applikation erhält oder nicht.

Die SAML Assertion kann 3 verschiedene Aussagen übermitteln. Es wird zwischen den Aussagen Authentification statement, Attribute statement und Authorization decision statement unterschieden.

1) **Authentification statement:** Das Authentification statement wird vom Identity Provider oder von der Partei, welche den Benutzer erfolgreich authentifiziert hat, erstellt. Die Aussage enthält Information über den Ersteller der Assertion, über die authentifizierte Person, über die Gültigkeitsdauer der Assertion und weitere authentifizierungsbezogene Informationen.
2) **Attribute statement:** Das Attribute Statement enthält spezifische Details über den Benutzer. Das könnten ein Benutzerstatus, ein Kreditlimit oder der Anzeigename des Benutzers sein.
3) **Authorization decision statement:** Mit dem Authorization decision statement wird festgelegt, welche Berechtigungen der Benutzer nach der Anmeldung erhält.

(Carol Geyer 2007)

4.4.6 Protokoll

Die Protokolle definieren Regeln, wie die Kommunikation zwischen den einzelnen Parteien aussieht. Es gibt für die verschiedensten Anwendungsfälle ein XML-basiertes verschlüsseltes Protokoll. Laut SAML 2.0 Spezifikation wird zwischen den unten angeführten Protokollen unterschieden:

1) **Assertion Query und Request Protocol:** Durch das Assertion Query und Request Protocol lassen sich existierende Assertionen ansprechen. Während beim Request Protocol die bereits vorhandenen Assertionen mit einer ID abfragen lassen, können mit dem Query Protocol neue und bereits existierende Assertionen auf Basis des Statement Typs und des Empfängers der Assertionen abgefragt werden.
2) **Authentification Request Protocol:** Das Authentification Request Protocol wird verwendet, wenn der Service Provider nach der Assertion des Benutzers beim Identity

Provider anfragt. Das Web Browser SSO Profil benutzt dieses Protokoll, wenn der Benutzer über den Browser vom Service Provider zum Identity Provider für die Authentifizierung weitergeleitet wird.

3) **Artifact Resolution Protocol**: Unter Artifact versteht man in SAML 2.0 einen kleinen, fix vorgegebenen Wert, der die Referenz auf eine Assertion abbildet. Erhält der Service Provider ein Artifact, dann benutzt der Service Provider das Artifact Resolution Protocol, um den Identity Provider um die Auflösung der Referenz des Artifacts zu bitten. Damit erhält der Service Provider die eigentliche Nachricht vom Identity Provider. Das Artifact selbst wird über das HTTP Protokoll zum Service Provider verschickt, während die Auflösungsanfrage und -antwort über das SOAP Protokoll von Statten geht.
4) **Name Identifier Management Protocol:** Dieses Protokoll kann sowohl vom Service Provider, als auch vom Identity Provider benutzt werden. Über dieses Protokoll kann der Name des Benutzers, auch Name Identifier genannt, für die weitere Kommunikation geändert werden. Somit wird der Benutzer nicht über den ursprünglichen Namen angesprochen, sondern über einen Referenznamen. Des Weiteren bietet das Protokoll die Möglichkeit die Kommunikation über den Referenznamen zu beenden.
5) **Single Logout Protocol:** Mit dem Single Logout Mechanismus lassen sich offene Session eines Benutzers gleichzeitig schließen. Das Single Logout kann sowohl vom Benutzer, vom Service Provider oder Identity Provider initiiert werden. Vom Service Provider, wird das Single Log out angestoßen, wenn es zu einem Timeout kommt. Gründe für ein Single Log out lassen sich im Reason Attribute eines Single Logout Protocol festlegen.
6) **Name Identifier Mapping Protocol:** Möchte ein Service Provider mit einem anderen Service Provider kommunizieren und den Name Identifier behalten, mit dem der Benutzer identifiziert wird, dann muss das Name Identifier Mapping Protocol verwendet werden. Die Nutzung des Protokolls ist jedoch nur sinnvoll, wenn der Identity Provider jeweils einen Name Identifier für beide Service Provider kennt. Dadurch ist es dem Service Provider möglich mit dem anderen Service Provider über den gleichen Name Identifier zu kommunizieren, da die Name Identifier über dem Identity Provider gemappt werden.

(Michael Kain 2017)

4.4.7 Binding

Das Binding definiert wie das SAML Protokoll mit den Transportprotokollen wie SOAP oder HTTP interagiert. Somit wird geregelt, wie SAML Anfragen und Antworten mit den SOAP oder HTTP Protokollen ausgeführt werden können. Durch Vorhandensein von unterschiedlichen Anwendungsfälle und unterschiedlichen Transportprotokollen unterscheidet man zwischen einer Fülle von Bindings, welche unten angeführt sind.

1) **SAML SOAP Binding:** Mit dem SAML SOAP Binding wird festgelegt, wie SAML Nachrichten mit SOAP über HTTP verschickt werden.
2) **Reverse SOAP Binding:** Das Reserve SOAP Binding wird hauptsächlich für Kommunikation über WAP Gateways verwendet. Dabei kann ein HTTP Client, ein SOAP Nachrichtenübermittler sein und somit sind die Rollen Sender und Empfänger über das HTTP Protokoll nicht dieselben, wie über das SOAP Protokoll.
3) **HTTP Redirect Binding:** Bei Weiterleitungen legt dieses Binding fest, wie SAML Nachrichten über HTTP versendet werden.
4) **HTTP Post Binding:** Werden SAML Nachrichten von einem Inhalt aus einem Formular wegeschickt, dann wird über das HTTP Post Binding definiert, wie diese Nachrichten übermittelt werden.
5) **HTTP Artifact Binding:** Mit diesem Binding wird determiniert, wie ein Artifact von einem Nachrichtensender zu einem Nachrichtenempfänger über HTTP versendet wird. Das kann entweder über ein HTML Formular über einen Abfragestring in einer URL erfolgen.
6) **SAML URI Binding:** Das SAML URI Binding wird verwendet um SAML Assertionen aus einer URI aufzulösen.

(IBM 2017)

4.4.8 Profil

Profile definieren, wie SAML Assertionen, Protokolle und Bindings miteinander kombiniert werden. Die nachfolgenden Profile setzen sich aus den oben erklärten Assertionen, Protokollen und Bindings zusammen.

1) **Web Browser SSO Profile:** Das Profil beschreibt, wie der Web Browser Single Sign On unterstützt. Kombiniert werden Authentification Request Protokoll mit den Bindings HTTP Redirect, HTTP Post und HTTP Artifact.
2) **Enhanced Client und Proxy (ECP) Profile:** Dieses Profil wurde speziell für Mobil Telefone mit WAP Gateway Front End entwickelt. Das Authentification Request Protokoll wird mit Reverse SOAP Binding benutzt, um die Kommunikation zwischen Client und Server ermöglichen.
3) **Identity Provider Discovery Profile:** Ein Profil mit dem ein Identity Provider aufgespürt wird, um den Single Sign On Anmeldeprozess anzustoßen.
4) **Single Logout Profile:** Das Single Logout Profil definiert, wie das Single Logout Protokoll mit den Bindings SOAP, HTTP Redirect, HTTP Post und HTTP Artifact verwendet wird.

5) **Name Identifier Management Profile:** Das Name Identifier Management Profil erklärt wie das Name Identifier Management Protokoll mit dem SOAP und den HTTP Protokollen interagieren soll.
6) **Artifact Resolution Profile:** Das Artifact Resolution Profile synchronisiert das SOAP Binding mit dem Artifact Resolution Protokoll.
7) **Assertion Query/Request Profile:** Beschreibung, wie das SOAP Binding mit dem SAML Query Protokoll verwendet werden soll.
8) **Name Identifier Mapping Profile:** Die Benutzung zwischen SOAP Binding und Name Identifier Mapping Protokoll wird im Name Identifier Mapping Profil deklariert.

(Hal Lockahrt 2008)

4.4.9 Prozessworkflow in SAML

Die Kommunikation zwischen den Parteien Service Provider, Benutzer und Identity Provider im Zuge der Nutzung des Protokolls SAML läuft im Grunde ähnlich wie auch bei anderen SSO Technologien über mehrere Stufen ab. Die Prozessschritte zwischen den genannten Parteien sind in Abbildung 7 dargestellt. Es wird angenommen, dass Google als Service Provider und eine Drittpartei als Identity Provider fungiert.

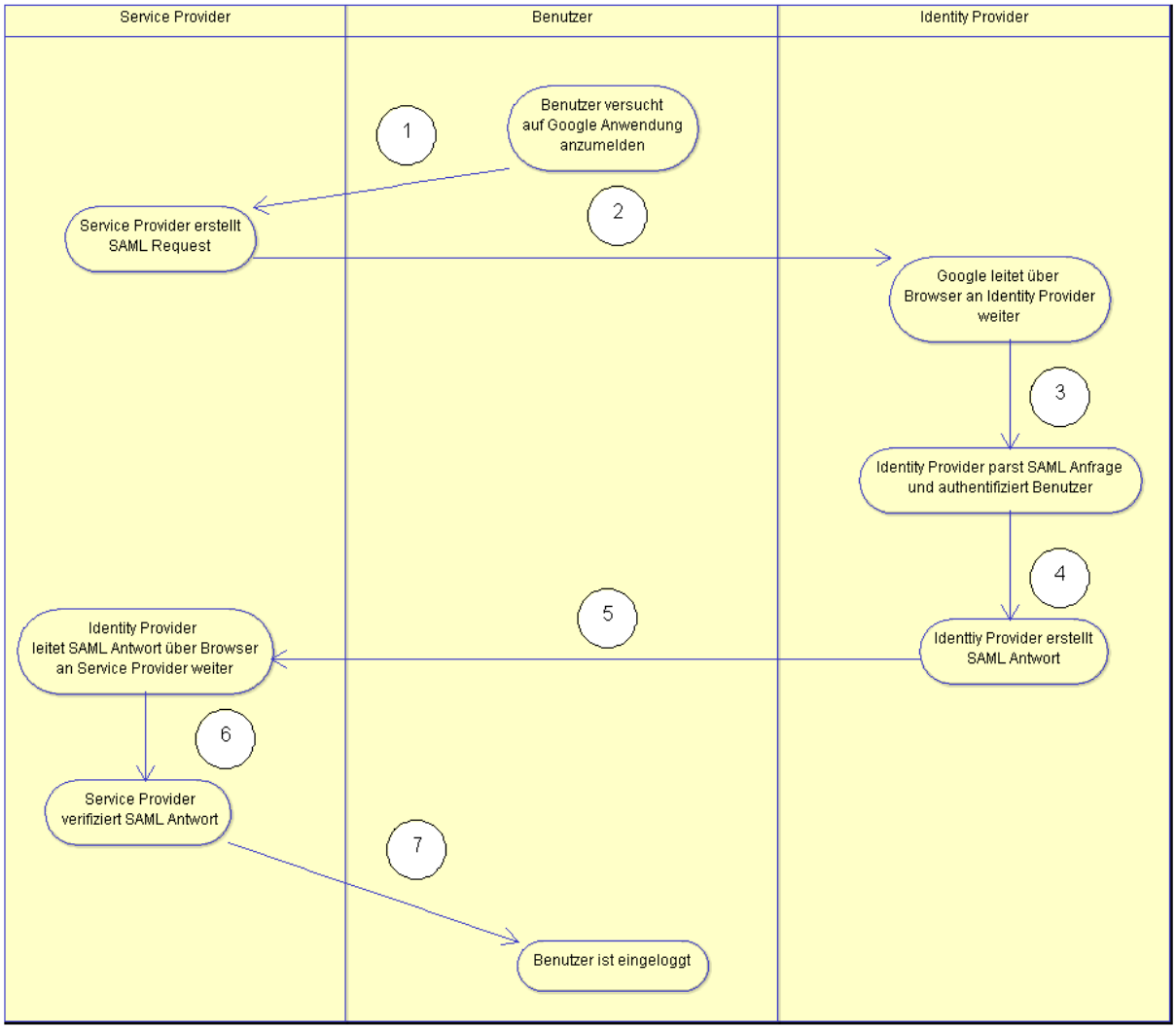

Abbildung 7: Prozessschritte in SAML (eigene Abbildung)

1) **Benutzer versucht sich auf einer Google Anwendung anzumelden:** Der Benutzer navigiert zur Google Anwendung und versucht sich dort mit seinen Credentials anzumelden.
2) **Service Provider erstellt SAML Anfrage:** Die verschlüsselte SAML Anfrage, welche vom Service Provider erstellt wird, enthält die URL des Service Providers, sowie Anmeldeinformationen des Nutzers, um diese den Identity Provider zur Authentifizierung vorlegen zu können.
3) **Google leitet SAML Anfrage über Browser an Identity Provider weiter:** Die SAML Anfrage wird über den Browser des Users an den Identity Provider weitergeleitet.
4) **Identity Provider parst SAML Anfrage und authentifiziert Benutzer:** Der Identity Provider entschlüsselt und extrahiert die Informationen über den Service Provider und den Benutzer.

5) **Identity Provider erstellt SAML Antwor**t: Wenn sowohl der Service Provider als vertrauenswürdig eingestuft wurde und der User eindeutig identifiziert wurde, wird vom Identity Provider eine SAML Antwort erstellt. Diese gibt Aufschluss darüber, ob der User authentifiziert wurde oder nicht. Die Antwort erfolgt aus Sicherheitsgründen asymmetrisch mit einem RSA Zertifikat.
6) **Identity Provider leitet SAML Antwort über Browser an Service Provider weiter:** Die SAML Antwort wird an den Client mittels Javascript zurückgeschickt.
7) **Service Provider verifiziert SAML Antwort:** Der Service Provider entschlüsselt die Nachricht mit dem öffentlichen Schlüssel des Identity Providers. Wenn die Antwort aus Sicht des Benutzers positiv ausfällt, dann leitet der Service Provider zur angefragten Ressource weiter.
8) **Benutzer ist eingeloggt:** Benutzer ist nun erfolgreich bei der Google Anwendung angemeldet.

(Sadiq 2016)

4.5 Open ID Connect

Open ID Connect ist ein offenes Authentifizierungsprotokoll aus dem Jahr 2014, welches die Einmalanmeldung über einen Identity Provider ermöglicht. Open ID Connect setzt dabei auf das Framework OAUTH 2.0 auf, dass die Autorisierung des Benutzers beim angemeldeten System gewährleistet. Open ID Connect erweitert das Framework OAUTH 2.0 um die Authentisierungsmöglichkeit bei einem Identity Provider. Dieser Standard wird bereits von verschiedenen namhaften Unternehmen wie Microsoft oder Google angeboten und betrieben, damit zukünftig Unternehmen ihr lokale Benutzerverwaltung in eine vertrauenswürdige Cloudumgebung verlagern. (Search Security 2017)

4.5.1 Prozessworkflow in Open ID Connect

In diesem Beispiel wird über den Blog „www.gafu-blog.at“ auf eine Google API zugegriffen. Dabei fungiert Google als Identity Provider und meldet gleichzeitig den Benutzer bei „www.gafu-blog.at“ an und gewährt über OAUTH 2.0 Zugriff auf eine Google API.

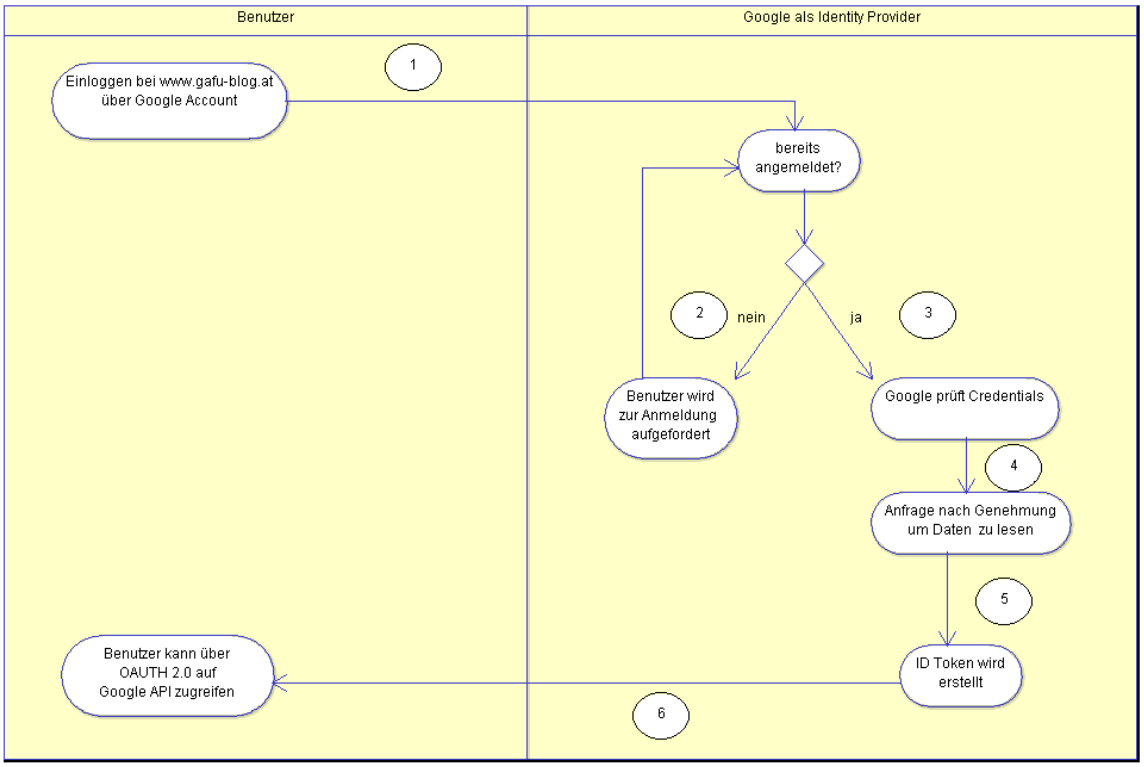

Abbildung 8: Prozessworkflow in Open ID Connect (Scott Brady 2017)

1) **Einloggen auf www.gafu-blog.at:** Der Benutzer versucht sich über ein Google Account im Blog anzumelden.
2) **Benutzer wird zur Anmeldung aufgefordert:** Ist der Benutzer noch nicht bei Google angemeldet, wird er zum Anmeldungsformular weitergeleitet.
3) **Google prüft Credentials:** Google prüft die Credentials und authentifiziert den Benutzer. Nach erfolgreicher Validierung wird ein ID Token erstellt.
4) **Anfrage nach Genehmigung um Daten zu lesen:** Der Benutzer muss bestätigen, dass er einverstanden ist, dass OAUTH 2.0 bei Zugriff auf die Google API bestimmte Daten liest.
5) **ID Token und Access Token wird erstellt:** Google als Identity Provider erstellt einen ID Token, der alle nötigen Userinformationen für die Authentifizierung des Benutzers enthält und einen Access Token, damit OAUTH 2.0 auf die Google API zugreifen kann.
6) **Benutzer kann über OAUTH 2.0 auf Google API zugreifen:** Nach erfolgreiche Dekodierung des ID Tokens ist der Benutzer beim Webblog www.gafu-blog.at eingeloggt. Gleichzeit kann über OAUTH 2.0 auf die Google API zugegriffen werden.

(Scott Brady 2017)

4.5.2 Abgrenzung zwischen Open ID Connect und OAUTH 2.0

Open ID Connect wurde als Standard entwickelt, um OAUTH 2.0 um einen Authentifizierungsdienst zu erweitern und um diverse Anwendungen die Möglichkeit zu geben Single Sign On zu nutzen. Zugleich wurde ein Standard geschaffen, der die vielen proprietären Authentifizierungsdienste ablöste, welche die gleichen Aufgaben vollrichteten. Da Open ID Connect auf OAUTH 2.0 aufbaut, hat dieses Protokoll mittlerweile weite Akzeptanz bei zahlreichen Entwicklern erlangt und wird in vielen webbasierenden Anwendungen eingesetzt.

Besonders bei mobilen Anwendungen, auch Apps genannt, werden Open ID Connect und OAUTH 2.0 verwendet. Das führt darauf zurück, da Apps häufig auf weitere externe Services zugreifen müssen. Auch Erweiterungen in Form von Plug-ins sind sicherheitstechnisch nur über die genannten Protokolle sinnvoll. (Torsten Lodderstedt 2014)

4.5.3 Rollen in Open ID Connect

Resource Server: Der Resource Server enthält benutzerbezogene Daten, auf welche der Benutzer zugreifen möchte. Diese Ressourcen sind durch OAUTH 2.0 geschützt.

Resource Owner: Der Resource Owner ist der Benutzer der Applikation, welcher Zugriff auf die Daten des Resource Servers gewähren kann.

Client: Der Client ist die Anwendung oder der Browser welcher Requests im Auftrag des Resource Owners verschickt, um Zugriff auf die gewünschten Ressourcen zu erhalten.

Authorization Server: Der Authorization Server erstellt unter Zustimmung des Ressource Owners für die Authentifizierung einen ID-Token und für die Autorisierung einen Access Token. (Boyd 2012)

4.5.4 Tokens

Tokens werden in OAUTH 2.0 verwendet, damit Benutzer autorisiert sind auf Daten zugreifen zu können. Tokens haben den Vorteil, dass sie leichtgewichtig sind und auf etwaige Verschlüsselungsmechanismen verzichtet werden können. OAUTH 2.0 kennt die unten angeführten Tokens:

1) **Access Token:** Dieser Token wird vom Client an den Authorization Server übergeben, um Zugriff auf bestimmte Daten zu erlangen.
2) **Refresh Token:** Der Refresh Token wird benötigt, damit der Access Token aktualisiert wird und somit der Zugriff über die Lebensdauer des Access Tokens gesichert ist. Refresh Tokens müssen vom Client geschützt gespeichert oder aufbewahrt werden, da ein Diebstahl dieses Tokens zu einem Datenverlust führen kann. Aus diesem Grund sollte ein Authorization Server dem Client nur einen Access Token ausstellen, wenn die Vertrauensbasis gegeben ist. (OAuth.com 2017)

4.5.5 Server Side Web Application Flow

OAUTH 2.0 kennt verschiedene Workflows, die für verschiedene Einsatzzwecke konzipiert wurden. Es wird zwischen

- Server-Side Web Application Flow,
- Client Sie Web Application Flow,
- Ressource Owner Flow und
- Client Credetials Flow

unterschieden. Da der Server Sie Web Application Flow der gängigste Workflow für Webapplikationen und mobile Applikationen ist, wird in diesem Unterkapitel die Prozessschritte dieses Workflows im Detail beschrieben. Auf die anderen Workflows wird im Unterkapitel 4.5.6 eingegangen.

Damit sich ein Benutzer über Single Sign On bei einer Applikation anmelden kann, müssen die einzelnen Parteien miteinander kommunizieren. Nachfolgend wird der Kommunikationsablauf zwischen den einzelnen Parteien im sogenannten ,,Server-Side Web Application Flow“ gezeigt

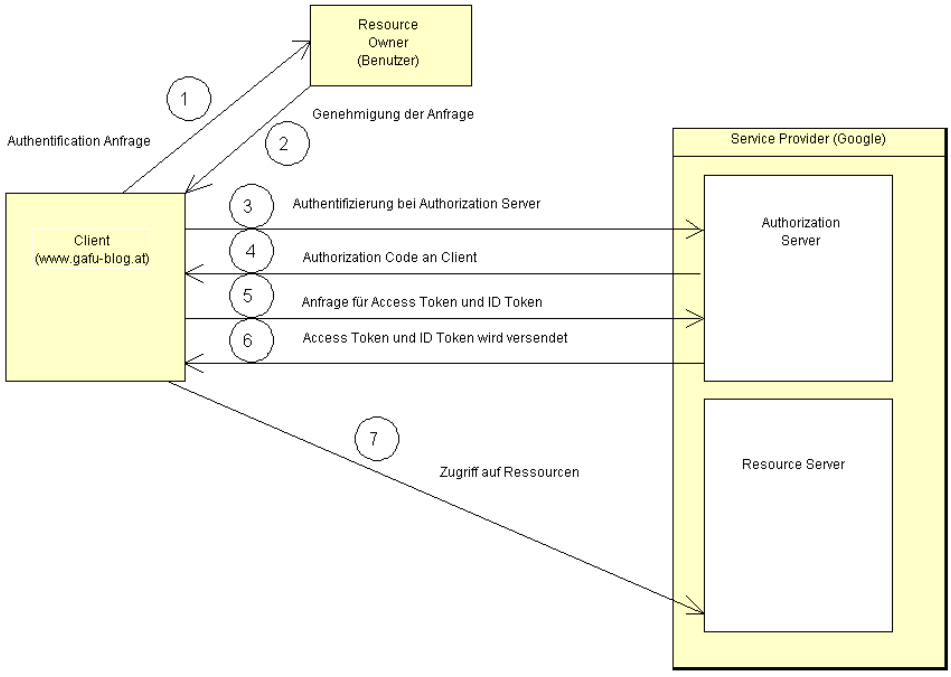

Abbildung 9: Server Side Web Application Flow (eigene Abbildung)

1) **Authentification Anfrage:** Der Client muss wissen, dass der Ressource Owner auf die Ressourcen zugreifen will, die sich am Resource Server befinden.

2) **Genehmigung der Anfrage:** Der Resource Owner initiert die Authentifizierung und wird über den Client zum Authorization Server weitergeleitet.
3) **Authentifizierung beim Authorization Server:** Der Client leitet den Benutzer zum Authorization Server weiter. Der Benutzer muss dem Authorization Server bestätigen, dass er Zugriff auf die Ressourcen des Resource Servers erhalten möchte. Folgende Parameter müssen vom Client mitgeschickt werden, damit der Authorization Server den Client eindeutig authentifizieren kann:

   client_id: Für die Nutzung einer Google API muss man sich registrieren und erhält eine Client-ID.

   redirect_uri: Die Redirect Uri enthält den Link auf welchen der Benutzer weitergeleitet wird, wenn er den Zugriff auf den Resource Sever bestätigt.

   scope: Der Scope gibt an, auf welche Ressourcen der Benutzer explizit zugreifen möchte. Möchte er auf die Google Tasks zugreifen, dann ist der Scope https://www.googleapis.com/auth/tasks. Des Weiteren muss der Scope ,,openid“ angegeben werden, damit dem Authorization Server signalisiert wird, dass sich der Benutzer über Single Sign On anmelden möchte.

   response type: Lautet der response type „code“, dann wird mit dieser Aussage gefordert, dass der Authoriaztion Server dem Client einen Authorization Code zurückschickt, wenn der Benutzer den Zugriff auf die Ressourcen erlaubt.

   approval_prompt: Bei Mitgabe des Parameters „force“, wird der Benutzer jedes Mal bei Besuch der Webseite http://www.gafu-blog.at aufgefordert, den Zugriff zu erlauben. Der Parameter „auto“ ermöglicht, dass der Benutzer nur beim ersten Mal den Zugriff erlauben muss.

   access type: Wird explizit der access type „offline“ mitgegeben, dann kann die Applikation auf die Ressourcen zugreifen, auch wenn der Benutzer nicht anwesend ist. Im Hintergrund werden laufend Refresh-Tokens erstellt, um den Zugriff aufrechtzuerhalten. Wird der Parameter „online“ mitgeschickt, werden keine Refresh Token erstellt.

   state: Das „state“ Attribut enthält einen eindeutigen Wert, damit CSRF unterbunden wird. Der Wert sollte serverseitig in einer Session gespeichert sein.
4) **Authorization Code an Client:** Der Authorization Server schickt, nach Bestätigung des Benutzers einen Authorization Code an den Client. Zusätzlich zum Authorization Code wird ein „state“ Parameter mitgeschickt, welche ident mit dem „state“ Parameter aus der Anfrage sein muss. Sind diese nicht ident, muss der Worklfow abgebrochen werden.
5) **Anfrage für Access Token und ID Token:** Damit die Applikation API Requests machen kann, muss der Benutzer einen ID Token und einen Access Token mitschicken, um auf

die Ressourcen zugreifen zu dürfen. Um den Access Token, sowie den ID Token zu erhalten, muss der Client einen HTTP Post Request an den Authorization Server schicken. Der Request enthält die nachfolgend beschriebenen Parameter.

Code: Der erhaltene Authorization Code muss als Bestätigung an den Authorization Server zurückgeschickt werden.

Redirect_uri: Der gleiche Link, der beim ersten Request mitgeschickt wurde, muss auch beim 2.Request angeführt werden.

Grant type: Der Grant type muss „authorization_code“ lauten, damit dem Authorization Server signalisiert wird, dass der Client den Authorization Code durch einen Access Token ersetzen möchte.

Client Id und Client Secret: Zusätzlich müssen noch die Client Id und Client Secret für die Authentisierung des Clients beim Authorization Server mitgeschickt werden.

6) **Access Token und ID Token wird versendet:** Der Authorization Server überprüft die Parameter und schickt nach erfolgreichen Überprüfungen eine Antwort in Form einer JSON Datei an den Client.

   Die Antwort enthält die unten angeführten Details, damit der Benutzer schlussendlich auf die gewünschten Ressourcen zugreifen kann.

   Access Token: Access Token ist notwendig um autorisierte Requests abzusenden.

   ID Token: ID Token wird verwendet, um den Benutzer eindeutig für die Applikation http://www.gafu-blog.at zu identifizieren.

   Expires in: Der Expire_in Parameter gibt die verbleibende Lebenszeit des Access Tokens in Sekunden an.

   Refresh_token: Dieser Refresh Token kann benutzt werden, um einen neuen Access Token zu erhalten, wenn dieser abläuft.

7) **Zugriff auf Ressourcen:** Der Benutzer hat nun Zugriff auf die Ressourcen des Resource Servers, entweder auf die Lebenszeit des Access Tokens oder unbegrenzt, wenn laufend Refresh Token erstellt wird. Refresh Token werden aus Sicherheitsgründen serverseitig in einer Datenbank gespeichert. Um auf die Daten des Resource Servers zugreifen zu können, wird der Access Token beim nächsten HTTP-Request im Authorization Header mitgeschickt.

(Yammer 2017)

4.5.6 Authoration Flows in OAUTH 2.0

Wie bereits erwähnt, ist der Server Side Application Workflow nicht der einige Workflow, welcher in der Praxis relevant ist. Um möglichst alle Anwendungsfälle abzudecken, welche die

Authentifizierung und Autorisierung bei einem Service Provider betreffen, bietet OAUTH 2.0, die unten angeführten Kommunikationsworkflows an.

Server-Side Web Application Flow: Dieser Workflow ist passend für serverseitige Applikationen. Wenn der Ressource Owner Zugriff auf die gewünschten Ressourcen beim Authorization Server angefordert hat, erhält er einen Authorization Code zurück. Dieser Authorization Code muss noch durch einen Access Token ausgetauscht werden, damit der Benutzer Zugriff auf die API erhält.

Client-Side Web Application Flow: Ist der Client ein Browser, dann wird vom Authorization Server der Access Token direkt über die URL an den Client geschickt. Der Nachteil dieses Workflows ist es, dass keine Refresh Token erstellt werden und der Access Token dem User dirkekt im Browser ersichtlich ist und deshalb unbedingt verschlüsselt werden muss.

Resource Owner Password Flow: Dieser Workflow erlaubt es, dass die Credentials gegen einen OAUTH Access Token ausgetauscht werden. Es wird nur bei hoch vertrauliche Clients verwendet, wie bei mobile Anwendungen, welche selbst vom IP Provider angeboten werden. Das Passwort des Benutzers muss nicht auf dem Gerät gespeichert werden. Nach der initialen Authentifizierung muss lediglich der Token gespeichert werden, der den Zugriff auf die gewünschten Daten ermöglicht.

Client Credential Flow: Der Initiator bei diesem Workflow ist die Applikation selbst. Damit wird es der Applikation ermöglicht ohne Zustimmung des Benutzers Zugriff auf die gewünschten Ressourcen zu erhalten. APIs, die ohne Einverständnis des Benutzers benutzt werden, können Datenbanken oder Speicherdienste sein.(Scott Brady 2017)

4.5.7 Zugriff auf User-Endpoint

Da Tokens nur Benutzerinformationen by Reference anbieten, muss ein spezieller Endpoint vom Client anvisiert werden, um diese Informationen auslesen zu können.
Der User Endpoint der über den Authorization Server erreichbar ist, stellt weitere Informationen über den Benutzer bereit. Diese Informationen, auch Claim genannt, werden über eine Open ID Schnittstelle angeboten und können vom Benutzer abgefragt werden.
Open ID kennt in ihrer Standardspezifikation 4 Parameter, welche vom Benutzer abgerufen werden können:

- **Profile:** Mit dem Attribut Profile können persönliche Daten, wie Name, Familienname, Geburtsdatum, Bild abgerufen werden.
- **Email:** Das Attribut E-Mail erlaubt es die E-Mail Adresse zu erhalten.
- **Address:** Bei Übergabe des Parameters Address erhält man, wenn vorhanden, die Straße, die Region, den Ort und die Postleitzahl.
- **Phone:** Zusätzlich zu den obengenannten Attributen, ist es noch möglich die Telefonnummer des Benutzers abzufragen.

Grundsätzlich muss bei Abfrage von Benutzerinformationen auch der gesamte Workflow, welcher im Unterkapitel 4.5.1 beschrieben wurde, durchlaufen werden. Als einzigen Unterschied muss beim initialen Request vom Client an den Authorization Server zusätzlich über das Attribut „scope“ einer der obengenannten Parameter übergeben werden, um die entsprechenden Benutzerinfos zu erhalten. Damit der Benutzer schlussendlich die Daten erhält, benötigt der Client wieder einen Access Token, damit er autorisiert ist auf diese zuzugreifen. (Connect2Id 2017)

5 SERVICE ORIENTIERTE ARCHITEKTUR UND WEBSERVICE

Da in webbasierende SSO Lösungen die Kommunikation der Parteien nicht nur auf der gleichen Domäne passiert, sondern domänenübergreifend über mehre Schnittstellen von Statten geht, beschäftigt sich dieses Kapitel mit Service orientierte Architektur und Webservices. Dieses Kapitel gibt einen Einblick über die Prinzipen von SOA und Webservices und grenzt diese Begriffe voneinander ab. Da Sicherheitsrisiken von Webservice auch das Risiko von SSO Lösungen beeinflussen, wird gesondert in Kapitel 5.2.1 darauf eingegangen.

5.1 Service orientierte Architektur

Service orientierte Architektur ist ein Designprinzip, um komplexe Systeme zu integrieren und zu implementieren. Der Fokus bei diesem Architekturprinzip liegt auf die Geschäftsprozesse im Unternehmen, aus denen sich Services herausbilden. Die Hauptprinzipien der SOA Architektur fassen den Nutzen und den Vorteil dieser Architektur gut zusammen. Einerseits durch die Vorteile, wie Granularität, Wiederverwendbarkeit, Interoperabilität und Modularität bezogen auf die Systemarchitektur und andererseits durch den Kostenvorteil der durch das An-/Entkoppeln von Services untereinander erreicht wird, ist SOA im unternehmerischen Umfeld sehr gefragt. Aufgrund dessen sind Service orientierte Architekturen in den verschiedensten technischen Ausführungen anzutreffen. (Douglas K Barry 2017)

5.1.1 Workflow in einer SOA Umgebung

Die Abbildung 10 zeigt eine einfach gehaltene SOA Umgebung, welche aus den Diensten Service Provider und Service Customer Application besteht. Des Weiteren gibt es ein zentrales Registery, welche alle Informationen über die verschiedensten registrierten Services enthält. Das ist natürlich bei einer Architektur, welche aus verteilten Systemen und unzähligen Schnittstellen besteht notwendig, damit der Service Consumer weiß auf welches Service zugegriffen werden muss um das gewünschte Resultat zu erreichen.

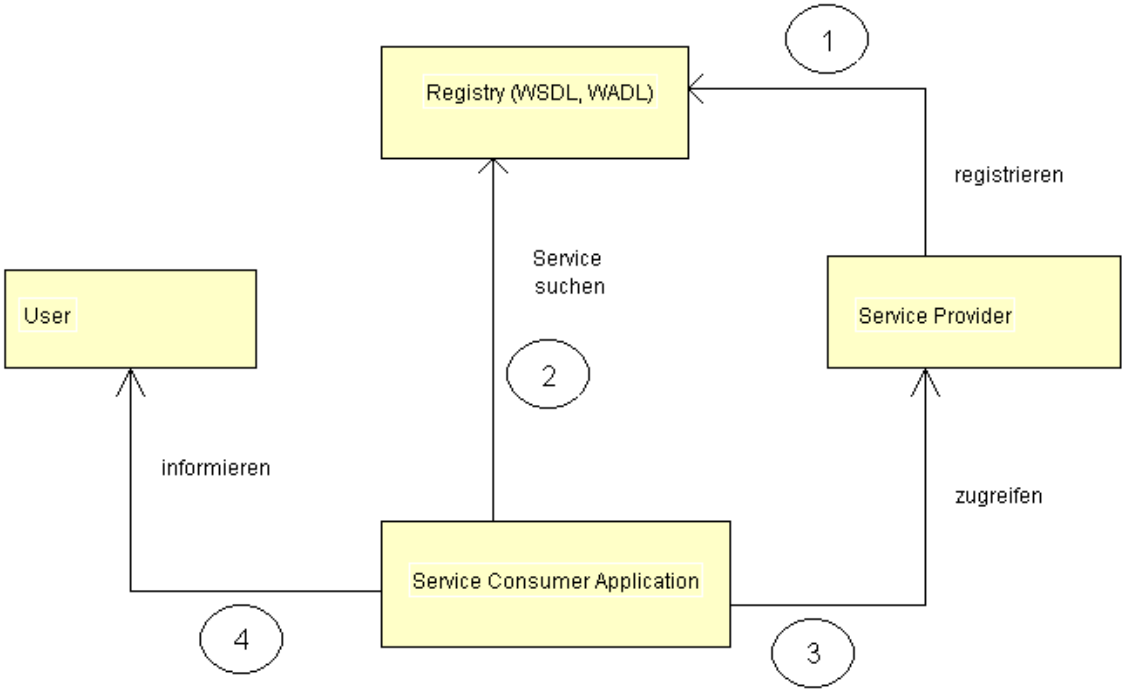

Abbildung 10: SOA Architektur (Sadiq 2016)

1) **Service Provider registriert sich bei Registry:** In einer SOA Architektur muss sich jeder Service Provider bei einer Registrierungsstelle anmelden, damit die Service Consumer diese erreichen können.
2) **Service Consumer stellt Anfrage an Registry:** Hat ein User eine URL aufgerufen und wurde eine Anfrage an den Service Consumer gestellt, dann stellt dieser eine Anfrage an den Registry, damit der passende Service aufgerufen wird.
3) **Service Consumer erhält Zugriff:** Nachdem der Registry ein passendes Service gefunden hat, antwortet dieser dem Service Consumer. Diese Antwort enthält alle notwendigen Daten, um auf den Service Provider zuzugreifen.
4) **User wird informiert:** Dem User ist nun ersichtlich, dass er auf die gewünschte Ressource zugreifen kann.

(Sadiq 2016)

5.2 Webservice

Die Begriffe Webservice und Service orientierte Architektur grenzen sich voneinander ab, auch wenn sie oft in der Praxis als Synonyme behandelt werden. Webservices sind Applikationen, die über eine Schnittstelle angesprochen werden. Im Gegensatz dazu versteht man unter SOA ein umfassendes Architekturprinzip, welches Webservices beinhaltet. (W3School 2017c)

Die Kommunikation mit einem Webservice erfolgt über das Protokoll HTTP und die Nachrichten werden in Form einer XML oder JSON Datei verschickt.

SOAP und REST haben sich als die 2 gebräuchlichsten und wichtigsten Webservice Standards etabliert.

1) **SOAP (Simple Object Access Protocol):** SOAP ist ein XML basiertes Nachrichtenprotokoll um Informationen zwischen Client und Webservice auszutauschen. Die Methoden des Webservices, auf die zugegriffen werden können, sind im XML basierten WSDL Dokument deklariert. (W3School 2017b)
2) **REST (Representational State Transfer):** REST ist eine neue Kommunikationsform, die für die Kommunikation mit einem Webservice verwendet wird. In REST hat jede Ressource eine URL und für die Kommunikation werden HTTP Header Operationen genutzt. (Todd Fredrich 2017)

5.2.1 Sicherheitsrisiken bei Webservices

Ein Grund, warum eine Webserviceschnittstelle für eine reibungslose und sichere Kommunikation zwischen Client und Applikation allein nicht ausreicht, liegt daran, dass REST und SOAP keine Spezifikation für Sicherheitsmechanismen besitzen. Auch das Protokoll HTTP welche die Nachrichten zwischen den Parteien übermittelt, enthält aufgrund der Aufrechterhaltung der Leichtgewichtigkeit, keine Sicherheitsmechanismen. (TechChannel 2017)

Um die Sicherheit von Webservices zu gewährleisten müssen 4 grundlegende Konzepte implementiert sein.

Authentifikation: Authentifikation identifiziert eindeutig den Benutzer der Applikation. Benutzer hat typerweise Benutzername und Passwort einzugeben, damit er Zugriff auf die Applikation erhält. Das implizit, dass jeder Benutzer eine einzigartige Benutzererkennung haben muss, damit dieser eindeutig identifiziert werden kann.

Autorisierung: Der Autorisierungsprozess legt fest, welche Berechtigungen der Benutzer am angemeldeten System erhalten soll. Autorisierung tritt gleichzeitig im Kontext der Authentifizierung auf und deshalb unterstützen Protokolle, wie OpenID und SAML 2.0 beides.

Kryptographie: Um die Privatsphäre und Vertraulichkeit von sensiblen Daten zu schützen und aufrecht zu erhalten, werden symmetrische oder asymmetrische Verfahren angewandt. Kryptographie verfolgt die Sicherheitsziele mit den Schlagwörtern Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit.

Zurechenbarkeit: Die Zurechenbarkeit misst die Ressourcen welche ein Benutzer während der Benutzung des Systems verbraucht. In Zahlen kann, dass durch die Benutzungsdauer oder durch die Anzahl der verbrauchten Ressourcen ausgedrückt werden. Die gewonnenen Informationen und Statistiken aus Benutzersessions dienen um die Autorisierung zu kontrollieren, Trends zu analysieren und um Rückschlüsse für die Kapazitätsplanung zu erhalten.(Margaret Rouse 2010)

Da Webservices auf den obersten Protokollebenen wie HTTP ansetzen, sind diese nicht von Angriffen befreit, wenn nicht die nötigen Sicherheitsvorkehrungen getroffen werden. Besonders REST Webservices sind anfällig, da ihre Architektur auf URI basiert. Nachfolgend sind einige Gefahren und Risiken angeführt, die man sich als Entwickler bewusst sein sollte.

Cross Site Request Forgery: Angreifer versuchen durch die Setzung von Links oder durch Erzwingung eines URL-Aufrufs des Benutzers, eine HTTP-Anfrage durchzuführen. Der Benutzer muss jedoch bei einer Applikation authentifiziert sein. Das Sicherheitsrisiko entsteht dadurch, dass durch Statuslosigkeit des HTTP-Protokolls, die Daten der jeweiligen Sitzung des Users an den Applikationsserver geschickt werden muss. Eine gängige Abwehrmaßnahme gegen CSRF Attacken ist es, dass bei jedem Request ein CSRF-Token mitgeschickt wird, welcher dem Angreifer nicht bekannt ist. (Daniel Bachfeld 2009)

XXS Cross Site Scripting: Durch XXS Cross Site Scripting werden von Angreifer Skripte wie Javascripts eingeschleust, um das System des Benutzers Schaden zuzufügen. Die Sicherheitslücke tut sich durch fehlende Validierung von Formulardaten auf. Ziele von XXS Cross Site Scripting sind es unter anderem zu Benutzerdaten gelangen, dynamische Webseiteninhalte zu manipulieren oder Pishing- und Malwareattacken zu starten. Um die Risiken durch das XXS Cross Site Scripting als Webseitenbetreiber zu minimieren, sollten die Dateneingabe sowie die Datenausgabe geschützt werden. Alle Eingaben sollten als potenzielle Sicherheitslücke betrachtet werden und nach verschiedensten Kriterien überprüft werden. Auch die Datenausgaben können durch Ersetzung von HTML Metadaten geschützt werden. Somit lassen sich Skripte nicht in den HTML Code einschleusen. (1&1 2016)

SQL Injection: SQL Injection tritt auf, wenn ein Angreifer ein SQL-Statement in ein Eingabefeld schreibt und dieses dazu genutzt wird, um ein SQL Statement im Hintergrund zu manipulieren. Dadurch besteht die Möglichkeit für den Angreifer auf sensible Daten zuzugreifen, sowie sensible Daten aus der Datenbank zu entfernen. Durch SQL Parameter, welche die Parameter während der Laufzeit validieren, können SQL Injection verhindert werden. (W3School 2017a)

XML Poisoning: Die XML Schema Information wird von einem Angreifer verändert oder zerstört, welche im Zuge einer Webservice Kommunikation zwischen Client und Server ausgetauscht wird. Durch gezielte Denial-of-Service Angriffe kann die Manipulation des XML Schemas bewirkt werden. Mögliche Manipulationen am XML-Schema können das Entfernen eines Attributes, die Änderung eines Datentypes oder die Änderung der Codierung sein. Um XML Poisoning zu umgehen, muss das XML Schema vor unautorisierten Zugriff geschützt werden. (Capec 2017b)

WSDL Scanning: Durch WSDL Scanning versuchen Angreifer an Webservice Beschreibungen zu gelangen, um sensible Informationen über Aufrufmuster, Technologieimplementierungen und Schwachstellen der Webservices zu erhalten. Die Webservice Beschreibung enthält detaillierte Informationen über Service Ports und Bindings. Dadurch kann der Angreifer unberechtigten Zugriff auf Datenbankeinträge erlangen oder einen Denial-of-Service Angriff auf das Webservice durchführen. Somit ist es notwendig das WSDL File vor unautorisierten Zugriff zu schützen. Des Weiteren sollten nur jene Funktionen veröffentlicht werden, welche für den Client essentiell sind und sichergestellt werden, dass diese nicht gegen Angriffe verwundbar sind.

(Capec 2017a)

Replay Attack: Bei Replay Attacken gibt sich der Angreifer als authentifizierter Benutzer aus. Konkret belauscht der Angreifer die Kommunikation zwischen Sender und Empfänger und sendet das gleiche Datenpaket nochmals im Namen des Senders ab. Verhindert werden können Replay Attacken durch Einsatz von nur einmal verwendete Buchstaben- und Ziffernkombinationen, auch Nonces genannt. Somit wäre bei einem erneuten Absenden durch den Angreifer das Datenpaket nicht mehr gültig. (ITWissen.info 2017)

5.2.2 Standards für Webservice Sicherheit

Jedoch hat die XML Webservice Community in den letzten Jahren über 40 Sicherheitsstandards in den verschiedensten Implementierungsstufen entwickelt, um die Risiken zu minieren. Die Organisationen, welche den größten Beitrag zur Entwicklung der Sicherheitsstandards geleistet haben, sind W3C und Oasis. Während die W3C, Standards konzipiert hat, die Webservices, das Protokoll SOAP und Sicherheitsmechanismen wie XML Digital Signature und XML Encryption vorschreiben, hat sich Oasis auf High Level Standards spezialisiert. Mit WS-Security wurde ein Standard geschaffen, der mithilfe von XML-DSIG und XML Encryption SOAP Nachrichten verschlüsselt. Zusätzlich lassen sich mit dem WS-Security Framework kryptographische Kennzeichnungen und Identitätsinformationen mit Hilfe von SAML 2.0 sicher verschicken. (Rich Salz 2005)

Im Folgekapitel 6 wird nun das in der Praxis bewährte Modell Technology Acceptance Model näher erörtert, um Faktoren herauszuarbeiten, welche für die Messung der Benutzerakzeptanz von Single Sign On Lösungen benötigt werden.

6 TECHNOLOGY ACCEPTANCE MODEL

Das Technology Acceptance Model ist einer der populärsten Modellen, welches benutzt wird, um den Nutzen von Informationssystemen zu erklären. Weiterführend soll das Modell, welches von Davis im Jahr 1989 entwickelt wurde, die Benutzerakzeptanz eines Informationssystems vorhersagen. Interessant an diesem Modell ist, dass es als Basis für weitere in der Vergangenheit entwickelten Modellen gilt und diese somit auf das Technology Acceptance Model aufbauen. (Uni Hildesheim 2017)

6.1 Bedeutung des Technology Acceptance Model

Da die fehlende Benutzerakzeptanz und fehlende Toleranz in Bezug auf neue Technologien einer der Hauptfaktoren für das Scheitern von neuen Implementierungen darstellt, kommt dem Technology Acceptance Model in der Praxis große Bedeutung zu. Ein weiterer Faktor für die Wichtigkeit von TAM resultiert daraus, dass die Komplexität der IT Systemen in den letzten Jahren zugenommen hat und die Benutzer dadurch vor größeren Anpassungsproblemen und Herausforderungen stehen. Beispiele aus der Praxis zeigen, dass eine fehlende oder zu geringe Benutzerakzeptanz zu einem Produktivitätsparadox führt. Unter einem Produktivitätsparadox versteht man die negative Auswirkung einer IT Investition auf die Unternehmensleistung. Hewlett-Packard musste Einbußen von über $160 Millionen Dollar im Jahr 2004 aufgrund dieses Effektes verkraften. Um diesen Effekt zu vermeiden oder dagegenzuwirken müssen Führungskräfte entsprechend eingreifen, um eine erhöhte Benutzerakzeptanz zu erreichen. Das Technology Acceptance Model, besonders das Technology Acceptance Model 3, welches noch im Folgekapitel beschrieben wird, dient als Werkzeug für Führungskräfte um ein Verständnis über die Einflussgrößen der Benutzerakzeptanz zu erhalten. Folgend können sie technische und organisatorische Maßnahmen ableiten, um die Benutzerakzeptanz zu verbessern und um die Nutzung der Software zu gewährleisten. (Daniel Baumann 2006)

6.2 Modellbeschreibung

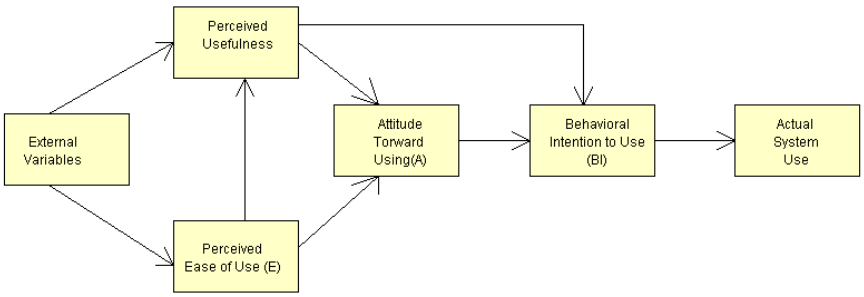

Abbildung 11:Technology Acceptance Model (Priyanke Surendran)

Das Modell in Abbildung 11 besteht aus den Hauptfaktoren Perceived Usefulness und Perceived Ease of Use, die das Nutzungsverhalten eines Benutzers auf das Informationssystem beschreiben. Externe Faktoren beeinflussen diese Hauptfaktoren und können dazu führen, dass sich die Sicht des Nutzers auf die Nützlichkeit der Anwendung und Benutzbarkeit verändert. Bevor die Applikation von einem potenziellen Benutzer verwendet wird, sind die Einstellung des Nutzers zur Anwendung und die Handlungsintentionen während der Nutzung essentiell. Nachfolgend werden die einzelnen Bestandteile des Modells beschrieben, um einen ersten Eindruck zu bekommen, welche Faktoren für die Benutzerakzeptanz von Single Sign On Lösungen in Betracht kommen.

1) **External Variables:** Die externen Faktoren beeinflussen den Nutzungskomfort, sowie die Effizienz der Nutzung einer Anwendung. Diese externen Faktoren können aus sozialen, politische und kulturellen Faktoren bestehen, welche die Nutzungsakzeptanz beträchtlich beeinflussen können.
2) **Perceived Usefulness:** Perceived Usefulness beschreibt laut Davis, die Wahrscheinlichkeit für den jeweiligen Benutzer, dass durch die Nutzung einer Anwendung, die Arbeitsleistung und -effizenz gesteigert wird.
3) **Perceived Ease of Use:** Durch diesen Faktor wird der benutzerbezogene Komfort eruiert, die durch die jeweilige Anwendung erreicht wird. In anderen Worten, der Faktor beschreibt die Erwartungen eines Benutzers, zu welchem Grad die Anwendung frei von Hemmnissen ist.
4) **Attitude Torward Using:** Grundsätzlich gibt dieser Faktor an, wie die Einstellung des Benutzers ist oder die Erwünschtheit, die Anwendung auch einzusetzen. Der Faktor Attitude Toward Using kann durch den wahrgenommenen Nutzungskomfort und durch die wahrgenommene Nützlichkeit der Anwendung beeinflusst werden.

5) **Behavioral Intention to Use:** Im Vorfeld kann ein Benutzer Absichten oder Vorhaben äußern eine Applikation zu verwenden. Die wahrgenommene Brauchbarkeit der Applikation kann das Handlungsvorhaben des Nutzers beeinflussen.

6) **Actual System Use:** Letztlich, wenn die Brauchbarkeit der Anwendung durch den Nutzer erkannt wird, die Anwendung als leicht bedienbar wahrgenommen wird, die Einstellung gegenüber der Applikation positiv ist und der Nutzer seine Vorhaben mit der Applikation umsetzen kann, dann wird die Applikation höchstwahrscheinlich genutzt. (Priyanke Surendran)

6.3 Ergebnisse der Fallstudie von Davis

Davis entwickelte im Zuge der Analyse seiner 2 Fallstudien zusätzlich zu den 2 Kernfaktoren wahrgenommene Brauchbarkeit und wahrgenommenen Nutzungskomfort weitere 6 Teilfaktoren. In der ersten Fallstudie bewerteten 120 Mitarbeiter von einem großen IT Unternehmen die Nutzbarkeit von 2 kommerziellen Softwareprodukten ein, die im beruflichen Alltag Verwendung fanden. Als Kontrast wurden in einer 2. Fallstudie 40 berufsbegleitende Studenten um eine Bewertung für eine Software gebeten mit der sie erst zu Beginn der Fallstudie das erste Mal in Berührung gekommen sind. Die Bewertung beruhte, wie erwähnt aus 6 Teilfaktoren, die nachfolgend angeführt sind.

Brauchbarkeit	**Bedienungsfreundlichkeit**
Verkürzung der Arbeitszeit	Leicht zu lernen
Arbeitsleistung	Kontrollierbar
Steigerung der Produktivität	Klar und verständlich
Effektivität	Flexibel
Erleichterung der Arbeit	Einfach um geübt zu werden
Nützlichkeit	Einfach zu benutzen

Tabelle 1: 6 Teilfaktoren der Kernfaktoren (Thomas Birken 2014)

Es wurde in beiden Fällen ein signifikantes Ergebnis zwischen beiden Hauptfaktoren zu der tatsächlichen Nutzung der Software festgestellt. Jedoch wurde in beiden Fällen belegt, dass die Brauchbarkeit einen weitaus größeren Effekt auf die Nutzungswahrscheinlichkeit hat als die Bedienungsfreundlichkeit. Einerseits wurde durch eine Korrelation zwischen Bedienungsfreundlichkeit und Brauchbarkeit resultiert, dass Bedienungsfreundlichkeit vorausgesetzt wird, damit die Brauchbarkeit einer Applikation gegeben ist. Andererseits wurde argumentiert, dass ein Benutzer gewillter ist eine eher nicht sehr bedienungsfreundliche Anwendung zu tolerieren, wenn ihm der Nutzen der jeweiligen Anwendung bewusst und bekannt ist. Wird die Bedienungsfreundlichkeit als hoch eingestuft, jedoch die Nützlichkeit und Brauchbarkeit der Anwendung für die Aufgaben des Benutzers nicht wahrgenommen, dann ist Akzeptanz beim Benutzer nicht gegeben. (Thomas Birken 2014)

6.4 Kritik an Technology Acceptance Modell

Als Schwachpunkt des Technology Acceptance Model wird gesehen, dass sich die Theorie aus Sicht der Sozialforschung nur auf die Nutzungsabsicht der Benutzer beschränkt und weitere essentielle Faktoren wie Verhaltenskontrolle, Selbstwirksamkeit, Persönlichkeit, demographische Merkmale nicht berücksichtigt werden. Aus diesem Grund wurden die Nachfolgemodelle TAM 2 und TAM 3 ins Leben gerufen, um weitere verhaltensbezogene Faktoren zu berücksichtigen damit das Modell die Benutzerakzeptanz besser erklärt.

Das Technology Acceptance Modell basiert aus theoretischen Konstrukten und wurde meist in wissenschaftlichen Schriften lediglich quantitativ erprobt. Das stellt einen großen Nachteil dar, da durch qualitativer Exploration Verhaltensmuster erkannt werden können, die noch nicht Bestandteil des TAM sind. Dennoch wird das Technology Acceptance Modell als Theorie für viele wissenschaftlichen Hochschulschriften verwendet, da es durch ein quantitatives Erhebungsinstrument wie einen Fragebogen einfach anzuwenden ist, plausible Ergebnisse geliefert werden können und das Modell in den letzten Jahren verbreitete Anerkennung gefunden hat.

Das Technology Acceptance Model in ihrer Grundform, liefert nur eine theoretische Faktorenanalyse, jedoch keinen Maßnahmenkatalog für Führungskräfte, um die Benutzerakzeptanz zu erhöhen. Somit gibt das Technology Acceptance Model an, dass eine Anwendung nützlich und einfach zu nutzen sein soll, jedoch nicht wie dieser Status erreicht wird.

Des Weiteren ist das Modell sehr stark generalisiert, dass es sich für die Akzeptanzanalyse jedes denkbaren Softwareproduktes anwenden lässt.

Durch die Evaluierungen verschiedenster Softwareprodukten anhand dieses Akzeptanzmodelles, wurde festgestellt, dass die Varianz zwischen der Intention etwas zu Nutzen und der tatsächlichen Nutzung kaum voneinander abweicht. Schlussfolgend kann garantiert werden, wenn ein Benutzer das Vorhaben hat, eine Anwendung zu nutzen, diese Anwendung auch tatsächlich nutzt. (Viswanath Venkatesh, Fred D. Davis, 2000)

Laut Schlussfolgerungen vom Institut für Organisation und Wirtschaftsinformatik in Osnabrück fokussieren sich die meisten Verfasser wissenschaftlicher Arbeiten auf die Erklärung von Benutzerakzeptanz und nicht darauf, wie Akzeptanz durch gezielte Maßnahmen verbessert werden könnte.

Der Zeitraum nach der Einführung der Software, ist für das Technology Acceptance Model relevant. Daraus resultiert, dass die Phasen während des Entwicklungsprozesses nicht bei der Akzeptanzanalyse miteinbezogen werden. Das ist schade, da sich die Akzeptanzfaktoren des Kunden oder Benutzers während der Zeit zwischen ersten Kundenkontakt und Abnahme des Softwareproduktes, sowie Benutzung der Anwendung verändern. (Kristin Vogelsang, Melanie Steinhueser, Uwe Hoppe ,2013)

6.5 Technology Acceptance Model 3

Aufgrund der oben genannten Kritikpunkte, wurde im Laufe der Jahre das Technology Acceptance Model erweitert. Zunächst wurden verschiedenste Akzeptanzmodelle für bestimmte Anwendungsbereiche, wie E-Commerce , elektronische Kommunikationssysteme oder CASE Tools entwickelt, um Faktoren erhalten, die für den jeweiligen Anwendungsbereich gelten. Dennoch gab es auch Anstrengungen um das generische Technology Acceptance Model zu optimieren. Das führte dazu, dass das Technology Acceptance Model 2 und das Technology Acceptance Model 3 folgten. Da das TAM 3 auf das TAM 2 aufbaut, wird das TAM 2 in den Folgekapiteln nicht näher betrachtet, sondern nur auf das Technology Acceptance Model 3 näher eingegangen. (Shu-Hsung Chang, Chien-Hsiang Chou, Jiann-Min Yang, 2009)

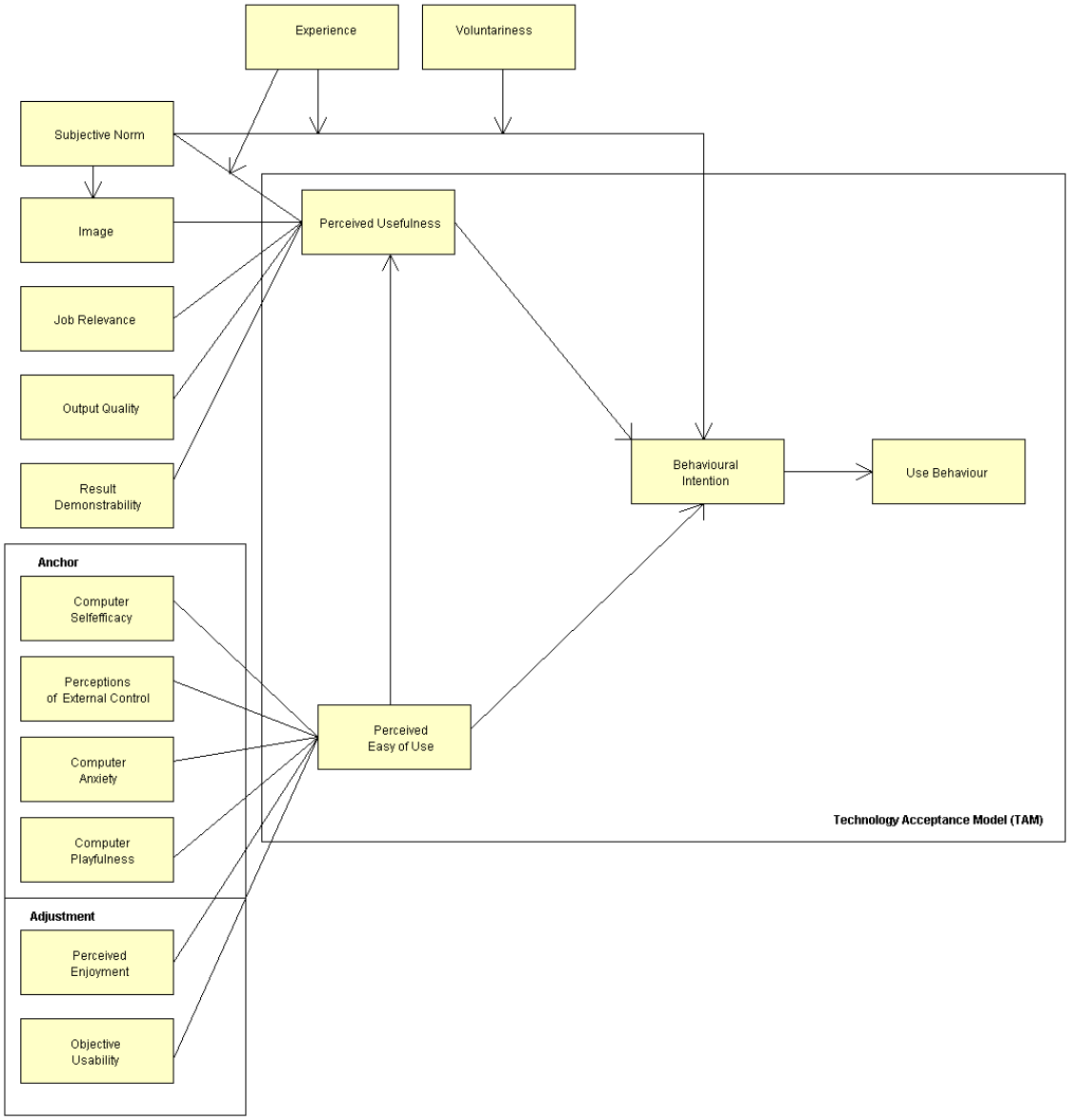

Abbildung 12: Technology Acceptance Model 3 (Viswanath Venkatesh, 2008)

Die Abbildung 12 zeigt, dass das Technology Acceptance Model in ihrer Grundform im Technology Acceptance Model 3 eingebettet ist. Da das Technology Acceptance Model in Kapitel 8.2 detailliert erklärt wurde, werden in diesem Unterkapitel nur die neu dazugekommenen Einflussgrößen auf die Faktoren Perceived Usefulness, Perceived Easy of Use und Behavioural Intention beschrieben. Dazu zählen die Moderatoren, die sozialen Einflussgrößen, die angepassten Merkmale, die Anker und die Systemmerkmale. (Viswanath Venkatesh, 2008)

6.5.1 Moderatoren

Die Moderatoren beeinflussen die anderen Faktoren wie die subjektive Norm und das Handlungsvorhaben.

Im Technology Acceptance Model 3 setzen sich die Moderatoren aus Erfahrung, die Applikation zu nutzen und aus der Freiwilligkeit die Applikation zu nutzen, zusammen.

Experience: Dieser Faktor beschreibt die Erfahrungen, die ein Benutzer sammelt, indem er eine Applikation nutzt.

Voluntariness: Applikationen werden nicht immer freiwillig genutzt, sondern es wird von Führungskräften oder Bezugspersonen verlangt die Applikation zu nutzen. (Viswanath Venkatesh, 2008)

6.5.2 Soziale Einflussfaktoren

Die sozialen Einflussfaktoren haben Auswirkungen auf die Nützlichkeit der Applikation, sowie auf das Handlungsvorhaben, die Applikation zu nutzen.

Subjective Norm: Die subjektive Norm gibt das Ausmaß der Wahrnehmung einer Person an, eine bestimmte Anwendung aufgrund von gewünschten Erwartungen naheliegenden Personen zu nutzen.

Image: Das Image ist die Wahrnehmung des Benutzers in wie fern, die Anwendung den eigenen Status in der Gesellschaft verbessert.

Um die sozialen Einflüsse und deren Prozesse zu verstehen, wurden bereits im Technology Acceptance Model 2 die unten angeführten sozialen Einflussmechanismen theoretisiert.

- **Compliance:** Benutzer üben ein bestimmtes Verhalten aus, um nicht bestraft zu werden oder eine Belohnung zu erhalten.
- **Verinnerlichung:** Die Verinnerlichung ist in der Sozialforschung die Eingliederung von Meinungen und Ansichten Nahestehender in das eigene Wertgefüge.
- **Identifikation:** Der Glaube des Benutzers, dass sich der eigene Status verbessern wird, da wichtige Bezugspersonen ein bestimmtes Verhalten für richtig halten.

Die 2 Faktoren Subjektive Norm und Image beeinflusst die Nützlichkeit einer Applikation über die sozialen Einflussmechanismen Verinnerlichung und Identifikation. (Viswanath Venkatesh, 2008)

6.5.3 System Merkmale

Zusätzlich zu den sozialen Einflussfaktoren wird die Nützlichkeit einer Applikation an den System Merkmalen gemessen. Dabei vergleicht der Benutzer, was die Applikation zu Stande ist zu leisten mit dem was getan werden muss, um die Aufgaben im eigenen Berufsumfeld zu erledigen.

Job Relevance: Die Job Relevanz gibt die Wahrnehmung an, ob eine Person glaubt, dass das IT System im eigenen beruflichen Umfeld anwendbar ist.

Output Quality: Die Output Qualität gibt die Wahrnehmung des Benutzers an, wie performant das System in der eigenen Arbeitsumgebung funktioniert.

Result Demonstrability: Die Ergebnisbeweiskraft gibt an, in welchem Grad die Ergebnisse, welche das System liefert, greifbar, feststellbar und kommunizierbar sind.

Venkentesh & Davis fanden heraus, dass die Ergebnisbeweiskraft einen direkten Einfluss auf die wahrgenommene Nützlichkeit der Applikation hat. Job Relevanz und Output Qualität wirken schwächer auf die wahrgenommene Nützlichkeit ein, da sich diese 2 Faktoren gegenseitig beeinflussen. Das heißt, je höher die Output Qualität ist, umso stärker ist der Effekt der Job Relevanz auf die wahrgenommene Nützlichkeit. (Viswanath Venkatesh, 2008)

6.5.4 Anker

Laut Venkatesh formen Benutzer frühe Wahrnehmungen über die Benutzerfreundlichkeit einer Applikation basierend auf sogenannte Anker, welche die grundsätzliche Einstellung der Benutzer gegenüber Computer ausdrückt.

Computer Self-Efficacy: Unter Selbstwirksamkeit versteht man die Selbsteinschätzung eines Benutzers, ob dieser die Fähigkeit besitzt eine spezifische Arbeit auf dem Computer erfolgreich zu erledigen.

Perception of External Control: Die Wahrnehmung über externe Unterstützung definiert, ob der Benutzer glaubt, dass organisatorische und technische Ressourcen im Unternehmen existieren um die Benutzung des Systems zu unterstützen.

Computer Anxiety: Computer Anxiety ist die Angst, welche ein Benutzer verspürt, wenn dieser mit einem Computer konfrontiert ist.

Computer Playfulness: Die Computer Playfulness ist die Spielfreude, die ein Benutzer verspürt, wenn dieser mit dem Computer interagiert. Das entsteht durch kognitive Prozesse, die dazu führen, dass der Benutzer neue Informationen verarbeiten muss, Probleme lösen muss und neue Fähigkeiten erlernt. (Viswanath Venkatesh, 2008)

6.5.5 Angepasste Merkmale

Des Weiteren argumentiert Vanketesh, dass sich Faktoren auf die Benutzerfreundlichkeit nach der Nutzung einer Anwendung verändern. Während die Selbstwirksamkeit und die Wahrnehmung über externe Unterstützung nach Benutzung der Anwendung weiterhin eine Rolle spielen, erlischt

die Bedeutung der Faktoren über die grundsätzliche Angst und Spielfreude an der Interaktion mit einem Computer. 2 Faktoren die zu den angepassten Merkmalen zählen, spielen jedoch eine große Rolle, nachdem der Benutzer bereits eine längere Zeit mit der neuen IT Anwendung interagiert hatte.

Perceived Enjoyment: Die eigene wahrgenommene Freude an der Applikation wird mit dem Faktor Perceived Enjoyment beschreiben.

Objective Usability: Der Faktor misst die Benutzerfreundlichkeit einer Anwendung im Vergleich zu anderen aktuellen Anwendungen. Sprich ein Benutzer wird die Applikation als benutzerfreundlich empfinden, wenn sich die Applikation in Bezug auf Usability am aktuellen Stand der Technik befindet. (Viswanath Venkatesh, 2008)

6.5.6 Erkenntnisse aus dem TAM 3

Vankentesh und Bala kamen bei der Entwicklung des Technology Acceptance Model 3 auf einige Erkenntnisse, wie die einzelnen Faktoren untereinander in Beziehung stehen und welchen Effekt diese Einflussgrößen auf die Benutzerakzeptanz haben.

Faktoren, welche die Benutzerfreundlichkeit beeinflussen, haben keinen Einfluss auf die Nützlichkeit der Anwendung: Da die Usability von der generellen Überzeugung des Benutzers über Computer und auch von weiteren individuellen Unterschiede jedes Einzelnen abhängig sind, sind laut Vankentesh und Bala die Kontrollierbarkeit, die Motivation und die von außenwirkenden Emotionen wichtige Einflussgrößen für die Benutzerfreundlichkeit. Die Nützlichkeit jedoch, fokussiert sich über die Wahrnehmungen über die Vorteile bei Nutzung einer bestimmten Anwendung. So wird argumentiert, dass die Kontrolle über ein System, nicht garantiert dass die Job Performance sich verbessert. Weiters heißt es, dass Spielfreude mit einer Anwendung nicht automatisch dazu führt, dass ein Benutzer effektiver arbeitet.

Zusammenhang zwischen wahrgenommener Benutzerfreundlichkeit und wahrgenommener Nützlichkeit wird beeinflusst durch Erfahrung: Durch Erhöhung der Hands-on Experience mit einem System, hat ein Benutzer mehr Informationen darüber, wie einfach und schwer eine Anwendung zu nutzen ist. Während die Benutzerfreundlichkeit für zukünftige Handlungsvorhaben noch nicht als wichtig erachtet wird, wird diese im Zeitablauf während der Nutzung für die Benutzer wichtiger. Aufgrund dessen bewerten Benutzer die Benutzerfreundlichkeit und formen Wahrnehmungen über die Nützlichkeit der Applikation. Somit wird angenommen, dass mit gewonnener Erfahrungen, der Einfluss von wahrgenommener Benutzerfreundlichkeit auf die wahrgenommenen Nützlichkeit der Anwendung steigt, da Benutzer die Benutzerfreundlichkeit in ihre Bewertung mitaufnehmen um die Nützlichkeit zu messen.

Zusammenhang zwischen Angst vor dem Computer und Benutzerfreundlichkeit wird beeinflusst durch die Erfahrung: Bei steigender Erfahrung erlischt der Effekt, Ängste vor einem Computer und dessen Anwendungen zu verspüren. Zusätzlich überwiegen während der Nutzung einer Applikation die systemspezifischen Vorstellungen gegenüber den generellen Vorstellungen über die Computernutzung. Damit sind die systemspezifischen Vorstellungen die dominierenden Faktoren, welche die Benutzerfreundlichkeit beeinflussen. Einerseits entwickeln Benutzer

genaue Wahrnehmungen über den Aufwand eine spezifische Aufgabe zu lösen, andererseits entdecken sie Facetten am System, welche zu Vergnügen führt. Forscher, wie Yadav und Mussweiler fanden heraus, dass der Einfluss von Anker, wie die Angst vor Computer verschwinden, wenn die angepassten Merkmale, wie wahrgenommene Freude zum Vorschein treten.

Zusammenhang zwischen Benutzerfreundlichkeit und Handlungsvorhaben beeinflusst durch die Erfahrung: Bei steigender Erfahrung wird der Effekt der Benutzerfreundlichkeit auf das Handlungsvorhaben, welches der Benutzer im Zuge der Zielerreichung hat, schwächer. Das heißt, erhält ein Benutzer mehr Erfahrung im Umgang mit der Anwendung, dann rückt die Benutzerfreundlichkeit in den Hintergrund und hat kaum Auswirkungen mehr auf das Handlungsvorhaben des Nutzers. Ein Grund dafür ist, dass Benutzer nicht mehr einen großen Wert auf die Benutzerfreundlichkeit schenken, um ihr Handlungsvorhaben zu formulieren. Jedoch der Zusammenhang zwischen wahrgenommener Nützlichkeit auf das Handlungsvorhaben bleibt im Zeitverlauf unverändert, da die ergebnisorientierten Faktoren während allen Phasen für den Benutzer als wichtig erachtet werden.

Effektänderung der subjektiven Norm auf Handlungsvorhaben beeinflusst bei Erfahrung und Freiwilligkeit: Der Effekt von subjektiver Norm auf Handlungsvorhaben wird bei zunehmender Erfahrung des Benutzers schwächer. Verstärkt wird dieser Effekt, wenn der Benutzer die Anwendung aus freien Willen benutzt. Ist die Anwendung im unternehmerischen Kontext für den Benutzer verpflichtet, dann hat schlussfolgend die subjektive Norm einen größeren Effekt auf das Handlungsvorhaben.

Signifikanz zwischen Handlungsvorhaben und tatsächliche Nutzung gegeben: In allen Phasen einer Benutzerakzeptanzanalyse, von der Kundenanforderung bis Nutzung eines Systems, sind die Faktoren Handlungsvorhaben und tatsächliche Nutzung signifikant zu einander. Das heißt, wenn ein Benutzer vorhat, eine Applikation zu nutzen, dann kann davon ausgegangen werden, dass er diese auch nutzen wird. (Viswanath Venkatesh, 2008)

6.5.7 Maßnahmen für Verbesserung von Nützlichkeit und Benutzerfreundlichkeit

Venkatesh und Bala haben in ihrer Studie ,,Research Agenda on Interventions“, einige Maßnahmen definiert, welche zur Verbesserung der Benutzerakzeptanz führen. Sie greifen somit einer der größten Schwachstellen des Technologie Acceptance Model auf und geben somit Unternehmer, Führungskräfte und Manager nützliche Tipps um eine desruptive Technologien trotz Widerwillen der Belegschaft im Unternehmen zu etablieren. Venkentash und Bala unterscheiden dabei jene Merkmale, welche vor Implementierung oder nach Implementierung eines Systems, durchgeführt werden können. (Viswanath Venkatesh, 2008)

6.5.8 Preimplementierungseingriffe

Die Preimplementierungseingriffe sind aufgrund folgender 2 Gründen wichtig, um die Benutzerakzeptanz zu verbessern:

1. Minimierung der Abwehrhaltung von Benutzer zu einem neuen System
2. Bildung von Wahrnehmungen über System Funktionen und Nützlichkeit der Applikation im Arbeitsalltag

Nachfolgend sind die Maßnahmen beschrieben, die von Führungskräften vor oder während der Implementierungsphase durchgeführt werden können, um einen positiven Effekt auf die Benutzerakzeptanz auszuüben. (Viswanath Venkatesh, 2008)

Entwurfsmerkmale optimieren: Entwurfsmerkmale können die Userakzeptanz im positiven Sinne beeinflussen. Die Entwurfsmerkmale lassen sich noch in System- und Information bezogenen Merkmale unterscheiden. Während die Information bezogenen Merkmale die wahrgenommene Nützlichkeit beeinflussen, beeinflussen die System bezogenen Merkmale die Benutzerfreundlichkeit. Studien aus den letzten Jahren haben ergeben, dass Informationsbezogene Merkmale dabei helfen die Produktivität und die Performance zu verbessern. Wenn Daten gut aufbereitet werden, verständlich, genau sowie zeitnah zugänglich sind, dann hilft es die Benutzer die richtigen Entscheidungen zu treffen und diese erkennen dadurch, die hohe Ergebnisqualität und Job Relevanz. Im Gegensatz dazu, umschließen die System bezogenen Merkmalen Faktoren, wie die Vertrauenswürdigkeit, die Flexibilität und die Einfachheit. Diese Merkmale beeinflussen die Benutzerfreundlichkeit einer Anwendung.

Dieser Bereich ist noch nicht sehr weit erforscht, da eine Feldtest sehr hohen Ressourcen- und Kostenaufwand verursachen würde. (Viswanath Venkatesh, 2008)

Nutzer Beteiligung anstreben: Die Nutzer Beteiligung beginnt, wenn ein Benutzer während des Implementierungsprozesses mit Aufgaben betraut wird. Daraus resultiert, dass der Nutzer Aktivitäten übernimmt und aktiv am Implementierungsprozess mitarbeitet. Aufgrund von einigen Studien wurde festgestellt, dass dieser Eingriff, besonders bei komplexen Systemen, zu einer besseren Systemakzeptanz und Benutzereinbindung führt. Bei komplexen Systemen deshalb, da angenommen wird, das komplexe Systeme und ihre Eingliederung in die System- und Unternehmenslandschaft zu einer Umgestaltung der Geschäftsprozesse führt. In der Literatur besteht die Nutzerbeteiligung aus:

1. Verantwortung
2. Benutzer-Informationssystem Beziehung
3. Hands-on Aktivität

Sind diese 3 Dimensionen aus Benutzersicht geregelt und wahrnehmbar, dann wird sich die Einstellung des Benutzers gegenüber des Systems positiv entwickeln. Die Beteiligung des Benutzers kann vielfältig sein und kann im Zuge von Prototyp Tests, Geschäftsprozessveränderungsinitiativen oder System Evaluierung und Anpassung erfolgen.

Durch die Initiative einer Nutzerbeteiligung werden die Faktoren der Nützlichkeit, wie Job Relevanz, Ergebnisqualität und Ergebnisdemonstration verbessert. Ist das Management während des Implementierungsprozesses an Aufgaben beteiligt, führt das zu einem größeren Systemverständnis, was sich wiederum auf die subjektive Norm als Faktor im Technology Acceptance Model 3 auswirkt. Aus Benutzersicht hat die Beteiligung während des Implementierungsprozesses positive Auswirkungen auf folgende Faktoren:

1) Ängste zu einem System
2) Wahrnehmung durch externe Kontrolle
3) Wahrgenommenes Vergnügen
4) Objektive Benutzerfreundlichkeit

Für Führungskräfte hat die Nutzerbeteiligung im Veränderungsprozess eine große Bedeutung. Wenn ihnen bewusst ist, welchen positiven Auswirkungen eine Beteiligung der Akteure hat, dann lassen sich effektive Change Management Strategien entwerfen. (Viswanath Venkatesh, 2008)

Als Führungskraft unterstützen: Die Management Unterstützung drückt die Wahrnehmung des Benutzers über die eingeschätzte Bereitschaft des Führungspersonals aus, eine erfolgreiche Implementierung und erfolgreichen Einsatz eines Systems zu erreichen. Das Management hat die Möglichkeit direkt oder indirekt während einer Systemumstellung oder Systemeinführung einzugreifen. Ein indirekter Eingriff kann in Form von zur Verfügung gestellten Ressourcen oder erstellten Richtlinien erfolgen. Direkte Eingriffe haben generell Auswirkungen auf eine Systemeinführung und können Anweisungen über benutzte Systemeigenschaften, über Änderungen und Erweiterungen von IT-Systemen, sowie über Aufgaben der Mitarbeiter und Prozesse während der Systemveränderung enthalten. Da durch Eingriffe des Führungspersonals oft Veränderungen in organisatorischen Strukturen, Belohnungssystemen, Kontrollmechanismen betroffen sind, wird die Management Unterstützung als wichtigen Basisfaktor für die Moral der Benutzer während des Implementierungsprozesses und für den schlussendlichen Erfolg der Implementierung selbst, angesehen. Die Management Unterstützung können folgende Faktoren des Technology Acceptance Model 3 positiv beeinflussen:

1) Image
2) Subjektive Norm
3) Job Relevanz
4) Ergebnisqualität
5) Ergebnispräsentation
6) Ängste gegenüber die Applikation
7) Wahrnehmung der externen Kontrolle

Besonders Punkt 3 bis 7 können durch direkten Eingriff im Implementierungsprozesses positiv verändert werden. (Viswanath Venkatesh, 2008)

Belohnungssystem: Es wurde in mehreren Studien herausgefunden, dass ein Belohnungssystem dazu führen kann, dass die Benutzerakzeptanz gegenüber eines Systems erhöht werden kann. Es mag sein, dass Benutzer eine positive Einstellung gegenüber einer Anwendung entwickeln, jedoch kann das in Einzelfällen nicht zu einem positiven Ergebnis führen, da keine Incentives gewährt wurden. Ein Belohnungssystem kann je nach Ausprägung, die selben Faktoren positiv beeinflussen, die auch durch Management Unterstützung positiv beeinflusst werden. (Viswanath Venkatesh, 2008)

6.5.9 Postimplementierungseingriffe

Postimplementierungseingriffe werden von Führungskräften nach Einführung einer Anwendung durchgeführt, um die Benutzerakzeptanz gegenüber dieser Anwendung zu verbessern. Ist ein System bereits angeführt, dann erleben höchstwahrscheinlich Benutzer Veränderungen, welche ihre Arbeitsprozesse, Routinen und Gewohnheiten betreffen. Während einige Nutzer den Veränderungen gut gesinnt sind, sehen andere Nutzer die Veränderungen als große Gefahr an. Durch Postimplementierungsmaßnahmen soll erreicht werden, dass Nutzer die neue Applikation als Möglichkeit sehen, in ihrem Beruf besser zu performen und dies möglichst ohne großen Aufwand. Nachfolgend sind die Maßnahmen aufgeführt, welche nach Implementierung einer Applikation zu besserer Benutzerakzeptanz führen kann.

Anbieten von Trainings: Trainingseinheiten sind in der Postimplementierungsphase sehr wichtig, da in dieser Phase die Applikation bereits ohne Einschränkungen nutzbar ist. Es wurde in mehreren Studien eruiert, dass unterschiedliche Formen von Trainings unterschiedliche Effekte auf die Akzeptanz eines neuen Systems hat. Venkentesh und Speier fanden in ihrer Studie heraus, dass spielbasierende Trainings eine größere Auswirkung auf die Wahrnehmung der Nutzer auf die wahrgenommene Nützlichkeit und Benutzerfreundlichkeit haben als traditionelle Trainings. Je komplizierter und komplexer ein System ist, umso wichtiger werden Trainings um die Ängste bei den Nutzern zu nehmen und negative Reaktionen in positive Reaktionen umzuwandeln.

Anbieten von organisatorischer Unterstützung: Organisatorische Unterstützung kann in verschiedenen Formen erfolgen, wie

- Anbieten von essentieller Infrastruktur
- Unterstützung durch Geschäftsprozessexperten
- Senden von Mitarbeiter zu Schulungen
- Einrichtung von Help Desks
- Unterstützung durch Experten

In der Postimplementationsphase ist das Vorhandensein von mehreren organisatorischen Unterstützungsaktivitäten, besonders bei komplexen Systemen sinnvoll, da dieses nicht einfach sind zu verstehen und zu benutzen.

Die Wahrnehmung der Nutzer über die externe Kontrolle wird positiv beeinflusst und führt dadurch zu einer größeren Benutzerakzeptanz. Besonders das zur Verfügung stellen von Experten kann zu einer positiven Beeinflussung der Wahrnehmung über die Nützlichkeit der Applikation und über die Bedienungsfreundlichkeit führen. Experten können Nutzer dabei helfen, alle Aspekte einer Applikation zu verstehen und bestimmte Aspekte zu verändern, um die Wahrnehmung über Job Relevanz, Ergebnis Qualität und Ergebnisrepräsentation zu verbessern.

Beeinflussung durch Berufskollegen: Durch die Unterstützung von Kollegen aus der eigenen Organisation oder von Kollegen aus anderen Organisationen, welche in der gleichen Branche arbeiten, lassen sich die Effektivität und die Akzeptanz zu einem System zum positiven verändern. Laut einer Studie von Jasperson im Jahr 2005 gibt es 3 Schlüsselaktivitäten die Berufskollegen setzen können:

1) Formales und informelles Training
2) Direkte Veränderung und Erweiterung von System- und Arbeitsprozessen
3) Erweiterung von System-und Arbeitsprozessen mit Unterstützung durch Nutzer

Das formale und informelle Training hilft Nutzer dabei, das System zu verstehen und Einsichten über Job Relevanz, Ergebnisqualität und Ergebnispräsentation zu erhalten. Die direkte Veränderung und Erweiterung von System- und Arbeitsprozessen bewirkt, dass die Ergebnisqualität des Systems sich verbessert und die Ängste der Nutzer genommen wird, die Applikation zu nutzen. Des Weiteren beeinflusst die Unterstützung durch Berufskollegen die subjektive Norm und das Image, welche wichtige Faktoren für die Nutzung von Applikationen darstellen. Vankentesh & Davis nehmen an, dass wenn Berufskollegen einem System gut gesinnt sind, diese Einstellung sich auch auf die Mitarbeiter übertragen lässt. (Viswanath Venkatesh, 2008)

6.6 Technology Acceptance Model 3 im Kontext von Single Sign On

Ob die Benutzerfreundlichkeit und die Nützlichkeit als 2 Hauptfaktoren der Benutzerakzeptanz einen Effekt auf Single Sign On Lösungen haben, ist nach reichlicher Recherche unerforscht. Da nicht alle Einflussgrößen vom Technology Acceptance Model 3 bei allen Anwendungen einen Einfluss ausüben, wird in diesem Unterkapitel betrachtet, welche Faktoren für die Akzeptanz von Single Sign On Lösungen in Betracht kommen. Nachfolgend ist eine Liste der Faktoren angeführt, welche Einfluss auf die Nützlichkeit und Benutzerfreundlichkeit von Applikationen laut Technology Acceptance Model 3 haben. Es wird kritisch betrachtet, welchen Einfluss diese Faktoren auf Single Sign On Lösungen ausüben. Diese Analyse soll als Basis für die empirische Untersuchung dienen und für eine zielgerichtete Fragebogenerstellung sorgen. Im Grunde sollten unrelevante Einflussfaktoren aus dem Technology Acceptance Model 3 im Vorhinein für die empirische Untersuchung eliminiert werden und relevante Einflussgrößen klassifiziert werden, welche für die Beantwortung der Forschungsfrage dienen.

Einflusskategorie	Einflussgrößen	Kritische Betrachtung	Relevanz
Moderatoren	Experience	In Single Sign On Lösungen übt die Erfahrung nicht unmittelbar Einfluss auf die Benutzerakzeptanz aus, wie bei komplexeren Systemen. Da Single Sign On Lösungen meist intuitiv benutzbar sind und nicht einen sehr großen Lernaufwand für die Nutzung der Single Sign On Lösungen aufgewendet werden muss, wird die Erfahrung im weiteren Verlauf kaum Einfluss auf andere Einflussgrößen haben.	nein
Moderatoren	Volaturiness	Für Mitarbeiter spielt es in Unternehmen eine große Rolle, ob die Freiwilligkeit für Nutzung gegeben ist. Ist sie nicht gegeben, dann hat das einen großen Einfluss auf die Akzeptanz einer Applikation. Deshalb ist es auch im Falle einer Single Sign On Lösung die Freiwilligkeit ein wichtiger Einflussfaktor.	ja
Soziale Einflussgröße	Subjective Norm	Im privaten Bereich ist es durchaus möglich, dass Bekannte oder der engere Freundschaftskreis, dem Nutzer anraten, eine Single Sign Lösung über Facebook, Twitter oder LinkedIn zu nutzen.	ja
Soziale Einflussgrößen	Image	Das Image hat im Kontext von Single Sign On Lösungen kaum einen Einfluss auf die wahrgenommene Nützlichkeit. Produkte von Trendsetter wie Apple, gelten als innovative Produkte, die für einen Konsumentenkreis ein Statussymbol verkörpert. Bei Single Sign On Lösung ist die Identifizierung mit dem Produkt nicht gegeben. Jedoch ist es möglich, dass man durch die Nutzung einer Single Sign Lösung für sich selbst in so einem Maße verinnerlicht, dass man nicht mehr darauf verzichten mag.	teilweise

Einflusskategorie	Einflussgrößen	Kritische Betrachtung	Relevanz
Systemmerkmale	Job Relevance	Auch für Single Sign On Lösungen ist die Job Relevanz essentiell für die Messung der Benutzerakzeptanz. Je relevanter die Lösung für den eigenen beruflichen Alltag ist, umso höher ist vermutlich die Akzeptanz in diesem Bereich.	ja
Systemmerkmale	Output Quality	Die Ergebnisqualität sollte einer der Hauptgründe sein, um eine Single Sign Lösung zu nutzen. Da eine Single Sign performanter ist als eine gewöhnliche Anmeldung und auch einfach benutzbar ist, sollte die Ergebnisqualität sehr hoch sein.	ja
Systemmerkmale	Result Demonstrability	Die Ergebnisse und Vorteile, die durch eine Single Sign On Lösungen erreicht werden, können gut festgestellt, präsentiert und kommuniziert werden.	Ja
Anker	Computer Self-Effeciancy	Die Selbstwirksamkeit sollte bei Single Sign Lösungen sehr hoch sein, da die Nutzung von Single Sign On Lösungen sehr intuitiv sein sollte.	Ja
Anker	Perception of External Control	Die organisatorische Unterstützung vom Unternehmen muss gegeben werden, dass eine Single Sign On Lösung im Unternehmen akzeptiert wird. Der Help Desk sollte Mitarbeiter bei Probleme unterstützen, falls es Probleme im Zuge der Nutzung von Single Sign On Lösungen auftreten.	Ja
Anker	Computer Axienty	Die grundsätzliche Einstellung eines Benutzers gegenüber eines Computers hat einen Einfluss auf die Benutzerakzeptanz von Anwendungen. Dieser Faktor ist nicht auf bestimmte Anwendung eingegrenzt und ist somit auch für Single Sign On Lösungen gültig.	Ja

Einflusskategorie	Einflussgrößen	Kritische Betrachtung	Relevanz
Anker	Computer Playfulness	Auch die Freude, die man grundsätzlich verspürt, mit dem Computer zu arbeiten kann, einen Effekt auf die Akzeptanz von Single Sign On Lösungen ausüben.	Ja
Angepasste Merkmale	Perceived Enjoyment	Die wahrgenommene Freude an der Applikation, spielt im Kontext von Single Sign On eine untergeordnete Rolle. Da die Nutzung von Single Sign On als Portal zu einer Anwendung verwendet wird und die Verweildauer deshalb sehr gering ist, wird das Erlebnis durch die Nutzung einer Single Sign On Lösung keine nachhaltige Freunde entwickeln.	Nein
Angepasste Merkmale	Objektive Usability	Zum Vergleich zu einer gewöhnlichen Anmeldung mit Benutzernamen und Passwort sollte die Anmeldung über Single Sign On benutzerfreundlicher sein. Aus dem Aspekt der Benutzerfreundlichkeit sollte sich der Nutzer für eine Single Sign On Lösung entscheiden.	Ja

Tabelle 2: Beurteilung Einflussfaktoren aus TAM 3 im Kontext von Single Sign On (eigene Abbildung)

In der empirischen Untersuchung sollten folgende 2 Faktoren aus dem Technology Acceptance Model 3 nicht berücksichtigt werden:

- wahrgenommene Freude
- Erfahrung

Alle anderen Faktoren sollten in der Fragebogenerstellung berücksichtigt werden, um relevante Faktoren der Benutzerakzeptanz im Kontext von Single Sign On herausarbeiten zu können.

7 INFORMATIONSSICHERHEIT

Da die Informationen in Unternehmen durch die täglichen operativen Tätigkeiten zunehmen, werden die 3 Ziele der Informationssicherheit Verfügbarkeit, Vertraulichkeit und Integrität stetig wichtiger. Durch Informationssicherheit wird erreicht, dass unberechtigte Dritte keinen Zugriff auf die benutzten Systeme in Unternehmen erhalten und Informationen über die gesamte eigene Wertschöpfungskette konform zu den 3 Zielen der Informationssicherheit verarbeitet werden. Da Single Sign On als Authentifizierungsdienst zur Informationssicherheit beiträgt, wird in diesem Unterkapitel auf die Relevanz von Informationssicherheit, auf das Informationssicherheitsmanagementsystem und auf den Informationssicherheitsstandard ISO 27001:2013 eingegangen. (Oliver Wege 2014)

7.1 Relevanz von Informationssicherheit

Das Bewusstsein für eine notwendige Informationssicherheit muss im gesamten Unternehmen verankert sein und von der Geschäftsführung und den Führungskräften vorgelebt werden. Die Geschäftsführung und die Führungskräfte haben Sorge zu tragen, dass jeder Mitarbeiter sicherheitsbewusst handelt und das jeder Mitarbeiter selbständig Maßnahmen treffen kann, um die Informationssicherheit im Unternehmen aufrecht zu erhalten.

Es gibt vielfältige Gründe, warum ein hoher Informationssicherheitsstandard nötig ist und gefordert wird. Nachfolgendend finden Sie einige Gründe, die für Informationssicherheit und weiterführend für ein Informationssicherheitsmanagementsystem sprechen.

Anforderung von Geschäftspartner: Informationssicherheit sollte nicht nur vom eigenen Unternehmen gelebt und verlangt werden, sondern auch von Kunden und Lieferanten. Aus diesem Grund werden von vielen Lieferanten, aber auch von Kunden ein ordnungsgemäßes Informationssicherheitsmanagement des Kooperationspartners verlangt. Als Bestätigung für das Betreiben eines ordnungsgemäßen Informationssicherheitsmanagements muss ein Zertifikat wie das ISO/IEC 27001:2013 vorgelegt werden.

Aufbau von Vertrauen: Dadurch, dass ein Unternehmen Informationssicherheit fördert und lebt, wird das Vertrauen nicht nur bei den Geschäftspartnern gestärkt, sondern auch bei den Mitarbeitern. Ein Mitarbeiter, der weiß, wie mit sensiblen Daten im Unternehmen umgegangen wird und wie er seinen Arbeitsalltag gestalten muss, um Informationssicherheit zu gewährleisten, wird gewillter sein, Sicherheitsrichtlinien zu befolgen.

Einhaltung von IT-Compliance: Unternehmen haben Sorge zu tragen, dass gesetzliche Vorgaben eingehalten werden. Unteranderem muss ein Risikomanagement betrieben werden und Investitionen für die IT-Informationssicherheit und IT-Sicherheit getätigt werden. Zusätzlich ist eine sorgfältige Dokumentationspflicht von Prozessen notwendig. Die Sorgfaltspflicht beinhaltet die Vollständigkeit, Korrektheit, Nachvollziehbarkeit, Termingerechtigkeit der Dokumentationen. Gesetze und Richtlinien, die Unternehmen zum Thema Informationssicherheit berücksichtigen müssen, sind nachfolgend aufgelistet.

- Datenschutzgrundverordnung (DSGVO)
- Produkthaftungsgesetz (ProdHaftG)
- Telekommunikationsgesetz (TKG)
- Urheberrechtsgesetz (UrhG)
- Strafgesetzbuch (StGB)

Schutz der Unternehmenswerte: Unternehmenswerte umfassen Informationen, Prozesse, Systeme welche besondere Relevanz genießen und deshalb mit höchster Priorität schutzbedürftig sind. (Hannes Federrath 2015)

7.2 Ziele der Informationssicherheit

Die Ziele der Informationssicherheit umfassen die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen.

Verfügbarkeit: Die adressierten Informationen eines Benutzers müssen jederzeit erreichbar sein. Das bedeutet, dass die Informationen nicht nur physisch abgelegt sind, sondern auch die Möglichkeit für den Nutzer besteht, diese auch zu konsumieren.

Integrität: Die Informationen sollten sich im korrekten und konsistenten Zustand befinden. Um Integrität zu prüfen werden Fehlererkennungs- und Fehlerkorrekturverfahren eingesetzt.

Vertraulichkeit: Unbefugte Dritte dürfen nicht Zugriff auf die jeweiligen Systeme zu erhalten. Durch ein eingerichtetes Berechtigungskonzept, welche den Zugriff auf die Systeme regelt und verwaltet, soll die notwendige Vertraulichkeit erreicht werden.

Nicht alle 3 Ziele sind für das jeweilige Einsatzgebiet gleichermaßen von Bedeutung. Bei öffentlich zugänglichen Informationen wird die Vertraulichkeit eine geringe Rolle spielen, jedoch die Integrität und Verfügbarkeit dennoch essentiell sein, um die Informationssicherheit zu gewährleisten. Zwischen den Zielen Integrität und Verfügbarkeit herrscht eine Wechselwirkung. Ist die Integrität der Informationen nicht gegeben, dann sind die Informationen nicht in der Form verfügbar, wie man sich es wünschen würde.

Im engeren Kontext wird durch Informationssicherheit gewährleistet das Bedrohungen abgewendet werden und Verwundbarkeiten der Systeme reduziert werden. Bestenfalls sollte präventiv Verwundbarkeiten von Systemen vermieden werden und Bedrohungen nicht zugelassen werden. Sollte es dennoch zu einem Angriff kommen, sollten reaktiv Maßnahmen erfolgen.

Bedrohungen können in Form durch eingeschleusten Würmen, Viren, Hacker- oder Spionage Angriffe entstehen. Die gefährlichste Form der Bedrohungen, sind jedoch nicht die erwähnten technischen Bedrohungen, sondern werden vom Mensch selbst verursacht. Sogenannte Social Engineers nutzen menschliche Schwächen aus, um Leute zu manipulieren und diese zu präferierten Aktionen zu bewegen. Social Engineers täuschen falsche Identitäten vor, um an Informationen zu gelangen für die sie nicht autorisiert sind. Erhält ein Opfer eine Anweisung von

einem Social Engineer und handelt das Opfer aufgrund falscher Annahmen, ist die Informationssicherheit im Unternehmen hochgradig gefährdet.

Weitere angreifbare Schwachstellen sind Pufferüberläufe und Konfigurationsfehler und stellen somit eine Gefahr für die Informationssicherheit dar. Beim Pufferüberlauf lenkt ein Angreifer die Rücksprungadresse auf eine Schadenssoftware, wenn mehr Speicher gebraucht wird als reserviert wurde und das Programm somit zum Absturz gekommen ist. Konfigurationsfehler können in verschiedensten Formen auftreten, von Parser Fehler bis zu schlecht eingerichteten Diensten und können Angreifer ermöglichen einen vergleichsweisen reibungslosen Einstiegspunkt in das System zu erhalten. (Wotan Monitoring 2017)

7.3 Informationssicherheitsmanagement

Da Informationen in Firmen in den verschiedensten Systemen gehalten werden und auch über interne und externe Schnittstellen ausgetauscht werden, stellen Informationen einen essentiellen Faktor für den Unternehmenserfolg dar. Es müssen jedoch Spielregeln festgelegt werden, wie die Informationssicherheit in Unternehmen geregelt wird. Dazu werden Sicherheitsprozesse etabliert, Risiken bewertet, Personen mit Verantwortungen ausgestattet und Maßnahmen determiniert, die gewährleisten, dass ein festgelegtes Sicherheitsniveau erreicht und gehalten werden kann. Die genannten Aufgaben werden von einem Informationssicherheitsmanagementsystem erfüllt. (DGO 2017)

7.3.1 Maßnahmen im Rahmen des Informationssicherheitsmanagements

Im Rahmen des Informationssicherheitsmanagements gibt es Prozesse, welche gewährleisten, dass sich die Informationssicherheit im Unternehmen etabliert. Weiterführend bilden die Prozesse einen Leitfaden ab, welche Aktivitäten im Informationssicherheitsmanagement getätigt werden sollten und welche Faktoren im Zuge des Betreibens eines Informationssicherheitsmanagements berücksichtigt werden sollten. Nachfolgend sind die Prozesse angeführt, die für einen hohen Informationssicherheitsstandard sorgen sollen.

Entwicklung einer Sicherheitspolitik: Bevor eine Sicherheitspolitik im Unternehmen verankert werden kann, muss ein Team formiert werden, welches sich rund um das Thema Informationssicherheitsmanagement beschäftigt. Wurde ein Team auserkoren, müssen Ziele in Bezug auf Informationssicherheit formuliert und festgelegt werden. Die Ziele werden unter Berücksichtigung folgenden bereits vorhandenen Konstrukten erstellt:

- Unternehmenspolitik- und Kultur
- Corporate Governance
- Compliance
- Rechtliche Rahmenbedingungen
- Charakteristiken des Unternehmens

Erstellung eines Sicherheitskonzeptes: Vor der Erstellung eines Sicherheitskonzeptes müssen alle Risiken im Unternehmen erkannt und bewertet werden. Danach können die schutzbedürftigen Objekte definiert werden und für diese schutzbedürftigen Objekte werden Sicherheitsanforderungen aufgestellt. Wurden alle schutzbedürftigen Objekte identifiziert, werden diese in die Sicherheitsarchitektur aufgenommen. Wurden alle Risiken identifiziert, priorisiert und eine Sicherheitsarchitektur erstellt, wird ein Konzept zur Realisierung der Sicherheitsarchitektur erstellt.

Realisierungsplan für IT-Sicherheitsmaßnahmen: Anfangs sollte nochmals überprüft werden, ob die festgelegten Maßnahmen zur Risikovermeidung oder -minimierung geeignet sind. In dieser Phase können noch Maßnahmenanpassungen vorgenommen werden. Daraufhin erfolgt eine Bewertung der Kosten und Aufwände und es werden Überlegungen angestellt, ob es wirtschaftlich sinnvoll ist, eine geplante Maßnahme durchzuführen. Die aus wirtschaftlicher Sicht sinnvollen Maßnahmen werden unter Berücksichtigung von Abhängigkeiten priorisiert. Die Verantwortungen bezüglich Umsetzung der Maßnahmen sollte auch in dieser Phase geklärt werden. Es ist wichtig zu wissen, welche Mitarbeiter die geplanten Maßnahmen umsetzten sollen und welche diese im Zuge der Qualitätssicherung kontrollieren sollen. Nicht zu vergessen ist bei der Realisierung der IT-Sicherheitsmaßnahmen auf begleitende Maßnahmen wie Schulungen und Bewusstseinsstärkung bei den Mitarbeitern. Schlussendlich fließen, die Erkenntnisse in Realisierungsplan, welcher ausfolgenden Bestandteilen besteht:

- Zielobjekt, Maßnahmen
- Priorisierung
- Verantwortlichkeiten
- Ressourcenaufzeichnung
- Termin- und Meilensteinplanung

Umsetzung der IT-Sicherheitsmaßnahmen: Natürlich muss der Realisierungsplan noch umgesetzt werden. Dazu müssen organisatorische und technische Prozesse geschaffen werden und diese in die Unternehmensprozesslandkarte aufgenommen werden. Im Zuge der Umsetzung müssen noch die Jobbeschreibungen um die Sicherheitsaspekte ergänzt werden und Informationen, Anleitungen und Hilfsmaterialien für die Mitarbeiter bereitgestellt werden

Erhaltung der IT-Sicherheit im laufenden Betrieb: Damit ein hoher IT-Sicherheitsstandard aufrechterhalten werden kann, müssen sich die Abteilungen im Unternehmen in regelmäßigen Abständen Prüfungen unterziehen. Dabei sollte der Arbeitsablauf und die vorhandenen Dokumentationen kontrolliert werden. Es muss darauf geachtet werden, dass die Arbeitsabläufe nach den Erfordernissen laufend angepasst werden sollten und dass die Dokumentationen aktuell gehalten werden. Bestenfalls sollten die Ergebnisse einer Prüfung im einem Managementreport dargestellt werden und in Meetings präsentiert werden. (Bundeskanzleramt Österreich 2017)

7.4 ISO 27001:2013

Die ISO 27001:2013 ist die neueste Revision der ISO 27001 Norm. Die ISO 27001:2013 wurde 2013 von der internationalen Standardisierungsorganisation, kurz ISO, novelliert. Durch diese Norm wird determiniert, wie Informationssicherheit in Unternehmen verankert und gelebt wird. Die ISO 27001:2013 hat weltweit Anerkennung gefunden und deshalb lassen sich viele Unternehmen zertifizieren, um die gelebte Informationssicherheit laut ISO 27001:2013 im Unternehmen bestätigen zu lassen.

Das Ziel der ISO 27001:2013 ist es die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen zu gewährleisten. Aus diesen Zielen leiten sich Bausteine ab, die wesentlich zum Erfolg eines hohen Informationssicherheitsstandards im Unternehmen beitragen. Nachfolgend sind die Bausteine der ISO 27001:2013 angeführt, welche in der Praxis von Bedeutung sind.

Kontext in der Organisation: Der Geltungsbereich von einem Informationsmanagementsystem muss klar abgesteckt sein. Dazu muss eine Umfeldanalyse gemacht werden und das Informationsmanagementsystem in das Gesamtumfeld des Unternehmens eingebettet werden. Die internen und externen Anforderungen an das Informationsmanagementsystem werden aufgenommen und die Interessengruppen festgelegt. Bei Implementierung eines Informationsmanagementsystems ist eine Kontextanalyse der erste Schritt, welcher durchzuführen ist.

Geschäftsführung und deren Unterstützung: Die Geschäftsführung kommt die Ehre zu teil, die Verantwortung für das Informationssicherheitsmanagement zu tragen. Die Wichtigkeit, dass die Geschäftsführung die alleinige Verantwortung zu teil halt, resultiert dadurch, dass Informationssicherheit beträchtliche Auswirkungen auf die Geschäftsprozesse hat. Die Verantwortung bringt mit sich, dass der Geschäftsführung die Aufgabe obliegt, für die Einhaltung der Informationssicherheit zu sorgen.

Informationssicherheitsziele: Die Ziele der Informationssicherheit müssen von den Unternehmenszielen abgeleitet werden. Das ist entscheidend, da das Nichterreichen von Informationssicherheitsziele zur Folge haben, dass auch die Unternehmensziele nicht zufriedenstellen erreicht wurden.

IS-Policy: Die IS-Policy wird meist vor Einführung eines Informationssicherheitsmanagements von dem Management erstellt. Sie stellt einen Leitfaden bereit, was die Beweggründe zu einem Informationssicherheitsmanagement waren und animiert die Mitarbeiter, an sie gestellte Verpflichtungen zu erfüllen, sowie die Verbesserungen des Informationssicherheitssystems voranzutreiben. Die Mitarbeiter müssen den Zweck und die Ziele des einzuführenden Informationssystems nachvollziehen können.

Rollen, Verantwortungen und Kompetenzen: Für die Instandhaltung und kontinuierliche Optimierung des Informationssicherheitsmanagements müssen Rollen definiert werden und den Rollen Verantwortungen zugeteilt werden. Es sollte auch drauf geachtet, dass jenen Personen Aufgabenbereiche des Informationssicherheitsmanagements zugeteilt werden für die er auch die Kompetenz besitzt.

Risikomanagement: Das Ziel des Risikomanagements ist es die vorhandenen Risiken zu identifizieren und in Folge den Schadenausmaß der durch das Risiko entsteht, zu vermeiden, zu lindern und bei Bedarf zu beheben. Im Zuge des Risikomanagements werden Risiken bewertet, detailliert dokumentiert und umfassend behandelt.

Leistungsüberwachung und KPIs: Um das Informationssicherheitsmanagement laufend zu verbessern, werden Leistungsindikatoren festgelegt, welche die Sollsituation abbilden. Im laufenden Betrieb wird die Ist-Situation mit der Soll-Situation verglichen und Maßnahmen für die Optimierung des Informationssicherheitsmanagements abgeleitet. Themenbereiche für welche Indikatoren im Informationssicherheitsmanagement erstellt werden sollten sind:

- Incident Management
- Softwarearchitektur und IT Operation
- Informationssicherheitsprojekte

Dokumentation: Die Dokumentationen sollten relevant, inhaltlich umfassend und leicht zugänglich sein. Zusätzlich sollte die Dokumentation nach einem festgelegten Arbeitsablauf erstellt, bearbeitet und veröffentlicht werden. Folgende Bestandteile sollte eine Dokumentation beinhalten, um dich Nachvollziehbarkeit und Auffindbarkeit zu erleichtern:

- Titel
- Datum
- Autor
- Archivierungsort
- Version

Vertrauliche und nichtvertrauliche Dokumente sollten gesondert aufbewahrt werden und sollten gesondert gekennzeichnet werden.

Kommunikation: Es sollte geregelt sein, wie innerhalb des Unternehmens kommuniziert wird und wie zwischen einem Unternehmen und deren Stakeholdern wie Lieferanten, Kunden und anderen Interessensgruppen die Kommunikation gehandhabt wird. Die Kommunikationswege müssen analysiert werden und folgende Rückschlüsse auf folgende Fragen liefern:

- Welche Informationen fließen im Anwendungsbereich des Informationssicherheitsmanagements?
- Welcher Informationskanal wird verwendet?
- An wen werden Informationen gesendet und wer erhält diese Informationen?

Erkenntnisse aus diesen Fragestellungen sollten in einem Kommunikationsplan münden.

Kompetenzen und Bewusstsein: Das größte Sicherheitsrisiko stellen nicht die vorhandenen Systeme selbst dar, sondern die Bediener, welche die Systeme benutzen. Deshalb sollten die Kompetenzen der Mitarbeiter und das Sicherheitsbewusstsein der Mitarbeiter durch gezielte

Schulungen gestärkt werden. Das Sicherheitsbewusstsein muss im Unternehmen gefordert und betrieben werden, um das Informationssicherheitsniveau hoch zu halten.

Lieferantenbeziehungen: Unternehmen arbeiten immer enger mit Lieferanten und Dienstleister zusammen. Das birgt auch Risiken, da sich das Sicherheitsverhalten externe Partner auf die Sicherheit des eigenen Unternehmens auswirkt. Deshalb definiert die ISO 27001:2013 einige Maßnahmen, um eine übergreifende Sicherheit zwischen Dienstleister und Unternehmen zu erreichen:

- Verpflichtung zu vertraglichen Vereinbarung
- Risikoanalyse beim externen Partner
- Kontrolle veranlassen
- Change Management reglementieren

Interne Audits: Interne Audits verfolgen das Ziel, die Maßnahmen und deren Wirksamkeit im Zuge des Betreibens eines Informationsmanagements zu messen und überprüfen die Einhaltung des Standards ISO 27001:2013. Es muss ein konkreter Auditplan erstellt werden, welcher einen Zeitplan und zusätzlich Informationen über Zuständigkeiten, Verantwortlichkeiten und die notwendigen Dokumentationen für das Auditverfahren enthält.

Incident Management: Störungen die auftreten und entscheidend den Betrieb eines Informationssicherheitssystems beeinflussen, müssen mit besonderer Sorgfalt behandelt werden. Incidents im Zuge des Informationsmanagements sind jene Vorfälle, welche einen schlechten Einfluss auf das Informationssicherheitsmanagementsystem selbst haben und die Verbesserung eines solchen Systems verhindern.

Kontinuierliche Verbesserung: In einem Unternehmen sollte ein kontinuierlicher Verbesserungsprozess betrieben werden, um auf die laufenden Veränderungen im Unternehmensumfeld und auf neue Gefahren in der IT Landschaft flexibel reagieren zu können. Als Vorgehensweise für die kontinuierliche Verbesserung kann der PDCA-Zykus verwendet werden. (Gerhard Funk 2016)

7.5 Informationssicherheit im Kontext von Single Sign On

Die Informationssicherheit muss im beruflichen und im privaten Umfeld gewahrt werden. In diesen Bereichen gibt es unterschiedliche Herausforderungen die an Privatpersonen, sowie an Unternehmen gestellt werden. In Unternehmen werden Authentisierungsdienste, wie Kerberos oder Shibboleth verwendet, welche vom Personal im Unternehmen selbst administriert werden. Im privaten Nutzungsumfeld, hat man keinen Einfluss auf den Authentisierungsdienst und ist auf Anbieter wie Facebook, Twitter oder LinkedIn angewiesen, ob die Daten vertraulich behandelt werden und geschützt vor Angriffen sind.

7.5.1 Informationssicherheit im privaten Umfeld

Wie schon erwähnt, wenn das Login über einen Identity Provider, wie Facebook erfolgt, dann ist der Benutzer angewiesen, dass der Identity Provider die Sicherheit über Identität, Vertraulichkeit und Integrität gewährleistet. In diesem Kontext gibt es einige Sicherheitsrisken, welche sich der Benutzer bewusst sein sollte.

Datenaustausch zwischen Applikationsbetreiber und Identity Provider: Bei Anmeldung eines Nutzers über eine Single Sign On Lösung wie Facebook Connect, werden im Zuge der Anmeldung öffentliche Profildaten vom Benutzer an den Applikationsbetreiber geschickt. Die Daten, die verschickt werden, sind nicht nur die Credentials, sondern können auch personenbezogen Daten, wie Beziehungsstatus, Name, Alter und Wohnort betreffen. Welche Informationen vom Identity Provider an den Service Provider übermittelt werden, ist von Identity Provider zu Identity Provider verschieden. Im Gegenzug erhält der Identity Provider vom Applikationsbetreiber Informationen zu Aktionen, die nach der Anmeldung vom Benutzer durchgeführt wurden.

Diese Daten werden den Profildaten angehängt. Der Applikationsbetreiber hat jedoch Sorge zu tragen, dass der Benutzer über die Datenübertragung von personenbezogenen Daten in Form einer Datenschutzerklärung informiert wird. Jedoch befinden sich Applikationsbetreiber und Identity Provider mit dem Handel von personenbezogenen Daten in einer Grauzone, da laut Telekommunikationsgesetz, nur Bestandsdaten ausgetauscht werden dürfen. Auch die Datenschutzerklärungen sind leider nicht immer eindeutig und offenbaren nicht, welche Daten zwischen Service Provider und Identity Provider ausgetauscht werden.

Der Nutzeffekt für Identity Provider wie Facebook ist es, dass durch die erhaltenen Daten gezielte personalisierte Werbungen geschalten werden können.

Abhängigkeit zu einem Identity Provider: Löscht der Nutzer ein Konto bei einem Identity Provider, dann werden auch alle anderen Logins bei den Applikationsbetreibern gelöscht. Dadurch kann es im schlimmsten Fall zu Datenverluste kommen, wenn der Benutzer nur über Single Sign On bei einem Applikationsbetreiber angemeldet war.

Bei erfolgreichem Angriff sind alle Zugänge betroffen: Würde ein Angreifer, das Facebook Profil eines Benutzers erfolgreich hacken, dann wäre es für ihn möglich, auf alle Applikationen zuzugreifen über dieses Facebook Konto.

Nutzer sind sich den Gefahren jedoch oft nicht bewusst, dessen sie sich ausgesetzt sind. In der empirischen Untersuchung wird deshalb überprüft, wie ausgeprägt das Sicherheitsbewusstsein der Benutzer ist und wie sich das auf die Akzeptanz von Single Sign On Lösungen auswirkt. (Cornelia Brinks 2015)

7.5.2 Informationssicherheit im beruflichen Umfeld

Wie in den vorigen Kapiteln beschrieben, stellt die Informationssicherheit einen essentiellen Faktor dar, um nachhaltig erfolgreich zu sein. Die ISO 27001:2013 als Standard stellt für ein

Unternehmen eine gute Basis bereit, um ein Informationsmanagementsystem aufzubauen und sich ständig nach neuen Gegebenheiten im Unternehmen weiterzuentwickeln. Jedoch um ein Informationsmanagementsystem erfolgreich zu betreiben, braucht es die Unterstützung aller Mitarbeiter, die sich konform bestehender IT-Compliance verhalten und somit zur Zielerreichung der definierten Ziele im Informationssicherheitsmanagementsystem beitragen. Um jedoch einen Mitarbeiter zu bewegen, dass dieser sich an die Richtlinien hält und auch zur Zielerreichung seinen Beitrag dazu leistet, können von Führungskräften einige Maßnahmen getroffen werden:

- Schulungen über Informationssicherheit im Unternehmen
- Vorstellung der Policy und der IT-Compliance im Unternehmen
- Demonstration der Auswirkungen bei Nichteinhaltung von IT-Compliance
- Unterweisung bei Einstellung neuer Mitarbeiter
- Kontrolle, ob die Spielregeln von den Mitarbeitern eingehalten werden
- Die Informationssicherheit wird vom Management vorgelebt

Im Kontext von Single Sign On können in Unternehmen bei Nichteinhaltung von den IT-Compliance durch Mitarbeiter verschiedenste Gefahren entstehen. Wird das Risiko im Zuge einer Risikoanalyse als sehr hoch eingestuft, können die vorhin genenannten Maßnahmen zur Risikominimierung beitragen und sollten eingesetzt werden, um die Informationssicherheit zu gewährleisten. Im Zuge der empirischen Untersuchung soll im Kontext von Single Sign On festgestellt werden, wie Benutzer die Informationssicherheit im eigenen Unternehmen wahrnehmen und ob auch Maßnahmen von Unternehmen getroffen werden, um den Informationssicherheitsstandard hoch zu halten. (Gerhard Funk 2016)

8 EVALUIERUNG

Das erste Kapitel dieser Arbeit gab einen Einblick über die Relevanz von Single Sign On Lösungen im privaten und im unternehmerischen Umfeld. Zum Abschluss des Kapitels wurde ein kurzer Ausblick auf die Folgekapitel geboten. Im Anschluss wurde eine Forschungsfrage gestellt, welche im Zuge der Arbeit beantwortet wird.

Aufgrund welcher Einflussgrößen der Userakzeptanz werden webbasierende SSO Lösungen der direkten Anmeldung über die jeweilige Webanmeldung vorgezogen?

Diese Forschungsfrage stellt die zentrale Problemstellung dieser Arbeit dar. Es werden die Einflussgrößen auf die Benutzerakzeptanz von Single Sign On Lösungen ermittelt und diese sollen Auskunft darüber geben, aus welchen Gründen Single Sign On gegenüber der gewöhnlichen Anmeldung vorgezogen wird. Aufgrund der festgelegten Hypothese werden das Sicherheitsbewusstsein, die Einstellung und IT-Affinität, sowie die Vertrauenswürdigkeit des Identity Provider als zentrale Faktoren gesehen, welche Einfluss auf die Akzeptanz der Single Sign On Lösung haben.

Die Hypothesen, die im Zuge der empirischen Untersuchung über den Einzelfall hinausgehen sollten, lauten wie folgt:

1. Je höher das Sicherheitsbewusstsein des Nutzers, umso geringer ist die Benutzerakzeptanz gegenüber Single Sign On Lösungen.
2. Je höher die Vertrauenswürdigkeit des Identity Providers, umso geringer ist das Sicherheitsbewusstsein der User.
3. Je höher die IT-Affinität der Nutzer ist, umso höher ist die Akzeptanz gegenüber Single Sign On Lösungen.
4. Je positiver der Nutzer gegenüber Single Sign On Lösungen eingestellt ist, umso höher ist die Akzeptanz gegenüber deren.

Die Beantwortung der Forschungsfrage und die Überprüfung der aufgestellten Hypothesen erfolgt detailliert in diesem Kapitel.

Rückblickend dient Kapitel 3 als Einführungskapitel in das Thema Single Sign On. Neben der Begriffserklärung von Single Sign On, wurden die Nachteile von Single Sign genannt und auch ein Kommunikationsworkflow zwischen den einzelnen beteiligten Parteien im Single Sign On Workflow illustriert. In den Folgekapiteln wurden einzelne SSO Technologien vorgestellt und im speziellen auf webbasierende SSO Lösungen wie SAML 2.0 und Open ID eingegangen.

Als Unterstützung für die Beantwortung der Forschungsfrage dienten die Kapitel 6 und 7. Kapitel 6 enthält im ersten Unterkapitel das Technology Acceptance Model. Da jedoch das Technology Acceptance Model einige Schwächen aufweist und keine Aufschlüsse auf die Einflussgrößen von Benutzerfreundlichkeit und Nützlichkeit einer Applikation gibt, wurde in weiterer Folge das Technology Acceptance Model 3 im Detail beschrieben, welche auch Einflussfaktoren von Nützlichkeit und Benutzerfreundlichkeit bestimmt. Im Verlauf des Kapitels wurden Faktoren für

die Akzeptanz von Single Sign On auf der Basis von TAM 3 herausgearbeitet, welche für die empirische Untersuchung verwendet werden.

Da die Ergebnisse auch von unternehmerischer Relevanz sein sollten, wurden in Kapitel 9 das Informationssicherheitsmanagement und die ISO 2013 vorgestellt, die dafür sorgen, dass Spielregen im Unternehmen definiert werden, wie Informationssicherheit im Unternehmen gemanagt wird. Im Schlussteil des Kapitels, wurden auf die Risiken eingegangen die Nutzer im privaten Bereich und Mitarbeiter im Arbeitsalltag ausgesetzt sind. Diese Risiken werden berücksichtigt, um gezielt Benutzer zu befragen, ob sie sich dessen bewusst sind. Des Weiteren enthält das Kapitel Maßnahmen, die von Führungspersonen im Unternehmen gesetzt werden können, um das Sicherheitsbewusstsein der Mitarbeiter zu stärken, die Informationssicherheit zu erhöhen und Risiken im IT Umfeld richtig einzuschätzen und zu behandeln.

Nun soll mit Hilfe einer quantitativen Forschungsmethode festgestellt werden, in welchem Ausmaß die Faktoren aus TAM 3 Einfluss auf die Benutzerakzeptanz von Single Sign On Lösungen ausüben. Unterstützend für die Beantwortung der Forschungsfrage und zur Überprüfung der Hypothesen soll eine Fallstudie dienen, um Aussagen und Erkenntnisse aus der quantitativen Befragung zu überprüfen und festigen. Die Fallstudie soll zusätzlich ermitteln, ob die Vertrauenswürdigkeit des Identity Provider und die Applikationsart Einfluss auf die Nutzung von Single Sign On haben.

8.1 Quantitative Befragung

Um eine große Anzahl von Personen zu erreichen und einen Einblick zu erhalten, welche Faktoren die Benutzerakzeptanz von Single Sign On Lösungen beeinflussen, wurde eine quantitative Befragung als Forschungsinstrument gewählt. Der Fragebogen wurde mit Hilfe von my.survio.com erstellt und auch für die Analyse wurde auf der generierten Datenbasis von my.survio.com zugegriffen.

8.1.1 Struktur des Fragebogens

Der Fragebogen beinhaltet 33 Fragen, welche sich aus:

- Demographische Fragen
- Fragen über Sicherheitsbewusstsein im Kontext von Single Sign On Lösungen
- Fragen über generelles Sicherheitsbewusstsein von Benutzer
- Fragen über die Einstellung gegenüber Single Sign On
- Fragen über IT-Sicherheit
- Fragen über die generelle Nutzung eines Computers
- Fragen über Nutzungsverhalten im Kontext von Single Sign On

zusammensetzen. Um den Fragebogen quantitativ auswerten zu können, wurden die Fragen geschlossen in Form von Matrizen-Bewertungen, Sternebewertungen und Skala-Bewertungen gestellt. Die Likert-Skala wurde dabei zwischen 1 und 5 gewählt, da für alle Fragen eine mittlere Ausprägung mit 3 als sinnvoll erachtet wurde.

Auf bestimmten Fragen konnte verschiedene Antwortmöglichkeiten ausgewählt werden, da für die Analyse die Mehrfachausprägungen sinnvoll waren. So ist für die Frage über die bereits genutzten Single Sign On Lösungen interessant zu wissen gewesen, über welche Anbieter sich die Nutzer bereits angemeldet haben.

Ergänzend wurde bei den meisten Antworten, dem Antwortenden die Möglichkeit geboten eine optionale Antwort anzugeben, welche nicht in der Liste angeführt wurde. Damit wurde erreicht, dass nicht berücksichtige Antwortmöglichkeiten, nicht unberücksichtigt blieben.

Der Fragebogen hat auch eine klare Einleitung, die dem Teilnehmer den Zweck der Befragung offenlegt und einen Einblick über den Inhalt der Befragung gibt.

8.1.2 Durchführung der Befragung

Die Befragung war vom 20.10.2017 bis 10.11.2017 über 3 Internetkanälen für die Öffentlichkeit zugänglich. Insgesamt haben den Fragebogen 129 Personen vollständig beantwortet. 112 Fragebögen wurden im Zuge der empirischen Untersuchung ausgewertet, da 17 Personen, den Fragebogen in der Pre-Test Phase vom 20.10.2017 bis 25.10.2017 beantwortet haben. Diese 17 Personen wurden befragt, ob die Fragen folgende Merkmale aufwiesen:

- Die Fragen sind verständlich formuliert
- Der Inhalt der Fragen ist verständlich
- Der Fragebogen ist gut strukturiert
- Die Reihenfolge der Fragen ist nachvollziehbar
- Der Fragebogen ist benutzerfreundlich
- Alle notwendigen Antwortmöglichkeiten sind vorhanden
- Die Bearbeitungsdauer des Fragebogens ist gut gewählt
- Der Fragebogen lässt keine Verzerrungen durch soziale Erwünschtheit zu

Dadurch sollte gewährleistet werden, dass es durch missverstandene Fragen und durch fehlende Antwortmöglichkeiten keine Methodenverzerrungen entstehen. Der Fragebogen musste noch an paar Stellen adaptiert werden, da es sowohl inhaltlich und strukturell von den Versuchspersonen Verbesserungsvorschläge gab. Die Bearbeitungsdauer von ca. 8-10 Minuten wurde als gut befunden und der Fragebogen war laut Teilnehmer auch abwechslungsreich und nicht ermüdend.

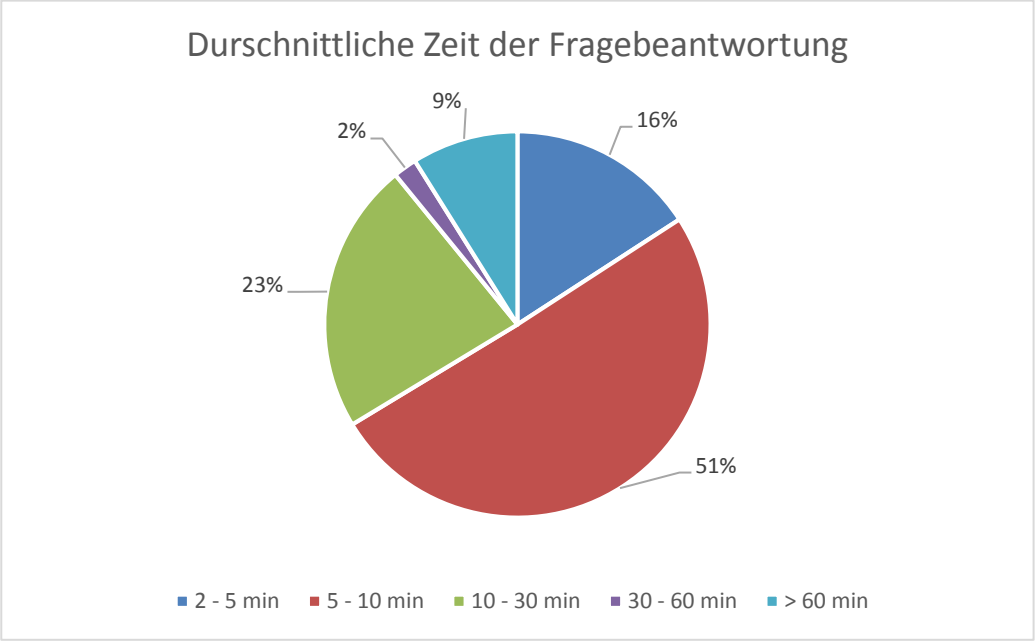

Abbildung 13: Durchschnittliche Zeit der Fragebogenbeantwortung (eigene Abbildung)

Das Ergebnis in Abbildung 13 zeigt auch, dass 51% den Fragebogen in 5-10 Minuten erledigen konnten. 16% haben für diesen Fragebogen nur 2-5 Minuten benötigt. Ein Drittel der Personen hat länger als die erwarteten 8 bis 10 Minuten gebraucht.

8.1.3 Stichprobe

An der Umfrage konnten berufstätige Personen mit Internetzugang teilnehmen. Dabei wurde geachtet, dass möglichst jede berufstätige Person, die gleiche Chance hat in die Stichprobe aufgenommen zu werden. Leider ließ sich aus finanziellen und zeitlichen Gründen keine probabilistische Stichprobe ziehen.

Dennoch wurde darauf geachtet, dass der Fragebogen auf verschiedensten Internetkanälen öffentlich gemacht wurde. Berufstätige Mitarbeiter konnten auf den Fragebogen über folgende Kanäle Zugriff erlangen:

- FH Campus 02 Sharepoint
- Facebook
- Survey Circle

Da nicht alle Personen die Chance hatten, potenziell an der Umfrage teilzunehmen, handelt es sich, wie schon erwähnt, um eine nichtprobabilistische Befragung. Leider konnten Personen, die keinen Internetzugang hatten und nicht bei diesen Internetkanälen registriert waren, an der Befragung nicht teilnehmen.

Auch eine 100%ige Repräsentativität der Stichprobe ist durch die Befragung nicht gesichert, da die befragten Personen nicht der Grundgesamtheit entsprechen. Jedoch wurde darauf Wert gelegt, dass Personen unterschiedlichen Alters, unterschiedlichen Geschlechts und unterschiedlichen Berufsfelder an der Befragung teilnahmen.

8.1.4 Codierung des Fragebogens

Zahlenmäßig erfasste Werte, wie das Alter wurden im Zuge der Analyse nicht codiert. Kategorische Werte, wie die Berufszugehörigkeit, wurden numerisch codiert. Die Einzelantworten im Form von Rating Skalen wurden aufsteigend nach Zustimmung und Intensität codiert. Somit wurde geringe Intensität oder Zustimmung mit 1 codiert und hohe Intensität oder Zustimmung mit 5 codiert. Mehrfachantworten wurden wie mehrere Einzelantworten behandelt und jede Antwortmöglichkeit wurde separat codiert.

8.1.5 Vorgehensweise bei der Fragebogenauswertung

Für die Auswertung des Fragebogens wurde das Statistikprogramm R verwendet. Bevor die Daten in R verarbeitet werden konnten, mussten sie entsprechend codiert werden. Danach wurden die einzelnen Fragen Kategorien zugeordnet, welche die Akzeptanz selbst und die Einflussfaktoren auf die Benutzerakzeptanz von Single Sign On Lösungen enthalten. Als abhängige Variable wurde die Benutzerakzeptanz selbst definiert, da wir die Einflüsse auf die Benutzerakzeptanz messen möchten. Aufgrund von der theoretischen Aufbereitung in Form des Technology Acceptance Model 3 und der Informationssicherheit, wurden folgende unabhängigen Variablen in Tabelle 2 definiert, welche Einfluss auf die Benutzerakzeptanz nehmen:

Gruppe	**Faktor**
A	IT Affinität & Einstellung zu Computer
C	Single Sign On Erfahrung
D	Einstellung zu Single Sign On
E	Probleme mit Anmeldungen
F	Sicherheit im Unternehmen
G	Sicherheitsbewusstsein im Allgemeinen
H	Sicherheitsbewusstsein im Kontext von Single Sign On

Tabelle 3: Faktorengruppen des Fragebogens (eigene Tabelle)

Die Tabelle 10 im Anhang A zeigt eine Liste, wo die einzelnen Fragen bereits den untersuchenden Faktoren zugeordnet wurden. Um diese finale Liste zu erhalten, wurde in R der Scree Test und eine explorative Faktorenanalyse mit „minchi“ und Cronbachs Alpha durchgeführt. Durch die Faktorenanalyse sollte erreicht werden, dass nur jene Fragen für die Ergebnisgenerierung miteinbezogen werden, die eine ausreichend erklärende Varianz und einen hohen Eigenwert aufwiesen. Nachfolgend sind die Methoden erklärt, welche im Zuge der Faktorenanalyse durchgeführt wurden.

Scree-Test: Der Scree-Test vergleicht die Korrelation einzelner möglicher Faktoren mit der Korrelation von Zufallszahlen. Jene Faktoren sind interessant welche eine höhere Korrelation

aufweisen als die Zufallszahlen. Als Ergebnis liefert der Scree-Test eine Anzahl von Faktoren, die sich aus den einzelnen Fragen statistisch berechnet haben. (Ledesma et al. 2015)

Explorative Faktorenanalyse mit „minchi“: Bei der explorativen Faktorenanalyse nach „minchi“, welche auf dem Scree-Test basiert, wird durch Angabe der Faktorenanzahl, die Konsistenz der einzelnen Faktoren gemessen. Dabei werden die Cronbach Alpha Werte zu den einzelnen Faktoren geladen und es ist auf den ersten Blick ersichtlich, ob die definierten Faktoren, den Faktoren der explorativen Faktorenanalyse entspricht. (R Documentation 2017)

Cronbachs Alpha: Durch Cronbachs Alpha wird die interne Konsistenz der Fragen untereinander geschätzt. Sie errechnet sich durch die durchschnittliche Korrelation und gibt einen Richtwert an, ob eine Frage als Bestandteil eines Faktors relevant ist. Eine Frage sollte verwendet werden, wenn der Alpha-Wert zwischen 0.65 und 0.95 liegt. (Chelsea Goforth 2015)

Da nicht alle Fragen positiv gestellt wurden, mussten die Ergebnisse einzelner Fragen umgedreht werden, damit die Antworten korrekt ausgewertet wurden.

8.1.6 Ergebnisse der Faktorenanalyse

Wie bereits in 10.1.5 erwähnt wurde induktiv aus den Ableitungen der Literatur 7 Faktoren definiert, welche Einfluss auf die Benutzerakzeptanz von Single Sign On Lösungen nehmen. Nachfolgend sind in der Tabelle 3, die angewandten Methoden der Faktorenanalyse angeführt, sowie deren Ergebnisse.

Methode	Ergebnis	Interpretation
Scree Test	Der Scree-Test ergab, dass die 32 Fragen des Fragebogens 7 Kategorien zugeordnet werden sollten.	Die 7 Faktoren, die aufgestellt wurden, sind ok, da der Scree Test nicht abweicht. Meine erste Überlegung war es die Faktoren Sicherheitsbewusstsein im Kontext Single Sign On und Sicherheitsbewusstsein im Allgemeinen noch zusammenzuführen. Da sich die Ergebnisse beider Faktoren stark unterscheiden, wurde entschieden, diese 2 Faktoren trotzdem separat auszuwerten.
Explorative Faktorenanalyse mit „minchi“	Abbildung 28 im Anhang A zeigt die Zuordnung der Fragen zu den 8 Faktoren. Im	Fragen E5 bis E10 wurden aus der Kategorie Probleme mit Anmeldungen

Methode	Ergebnis	Interpretation
	Allgemeinen wurden die bereits kategorisierten Fragen korrekt den einzelnen Faktoren zugeordnet.	rausgenommen, da diese nicht konsistent mit den anderen Fragen in dieser Kategorie waren. D12 trägt für die Messung der Einstellung über Single Sign On Lösungen wenig bei und wurde deshalb aus der Auswertung entfernt. Die Fragen in der Faktorengruppe D können laut der explorativen Faktorenanalyse mit „minchi“ in 3 unterschiedlichen Faktoren unterteilt werden. Jedoch fiel die Entscheidung gegen die Splittung, da unterschiedliche Aspekte abgefragt wurden und alle diese notwendig sind, um die Einstellung des Nutzers gegenüber von Single Sign On zu messen. Auch die Fragen zum Sicherheitsbewusstsein im Allgemeinen könnten nach der explorativen Faktoren-analyse in 2 separate Faktoren aufgesplittet werden. Nach näher Betrachtung betrifft eine mögliche Kategorie, die Fragen über Sicherheits-bewusstsein der Mitarbeiter in Bezug auf Social Engineering. Da durch das Trennen der 2 Faktoren, eine Autokorrelation der beiden Faktoren entstehen würde,

Methode	Ergebnis	Interpretation
		fiel die Entscheidung gegen eine Splittung.
Cronbachs Alpha	Die Folgende Liste zeigt die Konsistenz der einzelnen Faktoren: A: 0.67 C: 0.70 D: 0.81 E: 0.68 F: 0.67 G: 0.74 H: 0.76:	Aufgrund dieses Ergebnisses, sind die Faktoren intern konsistent und ausreichend stabil, um diese in der empirischen Untersuchung zu belassen.

Tabelle 4: Faktorenanalyse (eigene Tabelle)

8.2 Bayessche Statistik

Die Auswertung des Fragebogens wird mit Unterstützung der bayesschen Statistik durchgeführt. Im Gegensatz zur linearen Regression, gibt der Satz von Bayes Auskunft über die Wahrscheinlichkeit des Modells, in Anbetracht der vorliegenden Daten. Der Vorteil wird durch den Prior (Vorwissen) erkauft, welcher bei der Modellbeschreibung mitberücksichtigt wird. Im Gegensatz dazu wird bei der linearen Regression die bedingte Wahrscheinlichkeit vorausgesagt. Sprich, wie wahrscheinlich werden die Daten gesehen, wenn angenommen wird, dass die Hypothese stimmt.

Schlussfolgernd wird der Posterior in der bayesschen Statistik mit folgendem mathematischen Ausdruck beschrieben:

$p(\theta|Daten)$

Die lineare Regression, welche die bedingte Wahrscheinlichkeit als Ergebnis liefert, lässt sich mit folgenden Ausdruck beschreiben:

$p(Daten|\theta)$

Der große Nachteil, welche die lineare Regression jedoch liefert ist, dass die Hypothese bzw. die Nullhypothese nicht auf Allgemeingültigkeit bestimmt werden kann, sondern die Hypothese nur für ein bestimmtes Experiment falsifiziert werden kann. Aus diesem Grund wurde bei der Auswertung der Daten die bayessche Statistik als Verfahren gewählt. (Nicola Döring 2017)

8.2.1 Grundlagen des Satz von Bayes

Der Satz von Bayes, welcher von Thomas Bayes stammt, setzt sich aus den unten angeführten Bestandteilen zusammen.

Bestandteil	Formel	Interpretation
Prior	$p(\theta)$	Der Prior gibt das Vorwissen an, dass zu einem bestimmten Modell gegeben ist und wie wahrscheinlich die Modellparameter sind bzw. die Verteilung der Modell-parameter ist. In der Praxis und auch bei der Analyse der Masterarbeit wird ein schwacher Prior angenommen, welcher wenig Einfluss auf den Posterior ausübt.
Likelihood	$p(Y\|\theta)$	Die Likelihood gibt an, wie wahrscheinlich die Daten aus dem Fragebogen gesehen werden.
Evidenz	$p(Y)$	Die Evidenz wird benötigt, damit die Fläche (Integral) vom Posterior 1 ist.
Posterior	$p(\theta\|Y) = \frac{p(Y\|\theta) * p(\theta)}{p(Y)}$	Der Posterior gibt die Wahrscheinlichkeit des Modells an, unter der Voraussetzung, dass bestimmte Daten gesehen werden. Wird errechnet durch Multi-plikation von Prior * Likelihood dividiert durch Evidenz.

Tabelle 5: Bayesanische Statistik

(Christian Reinboth 2017)

8.2.2 Sampling

Grund für das Sampling ist, dass nicht jeder Punkt des Priors und jeder Punkt der Likelihood miteinander multipliziert werden kann, da die Berechnung zu einem zu hohen Rechenaufwand führen würde. Besonders wenn mehrere Parameter im Modell berücksichtigt werden müssen, wird der Rechenaufwand enorm sein. Aus diesem Grund werden Sampling Verfahren genutzt, welche aus einer Wahrscheinlichkeitsverteilung Stichproben ziehen, welche repräsentativ für die gesamte Datenbasis ist. Im Zuge der Evaluierung wurde als Sampling Verfahren, das Markov-Chain-Monte-Carlo-Verfahren genutzt, welche auf Basis einer Markov Kette die Ziehung der Stichprobe durchführt. Um die Zuverlässigkeit und die Genauigkeit des Samplings beurteilen zu können, werden mehrere Markov Ketten gesampelt, welche sich im Verlauf nicht weit voneinander abweichen sollten. (Tom Loredo 2014)

8.2.3 Einbettung der linearen Regression in Bayessche Statistik

Die lineare Regression wird in der Statistik genutzt, um eine Zielvariable durch unabhängige Variablen erklären zu lassen. Durch die unten angeführte mathematische Gleichung wird die lineare Regression beschrieben.

$$y \sim \alpha + \beta_1 x_1 + \beta_2 x_2 + \varepsilon$$

Koeffizienten	Bedeutung
Y	y ist die Zielgröße oder auch abhängige Variable genannt, auf die aufgrund der unabhängigen Variablen geschlossen wird.
β	Die Beta Werte sind die Steigungen der x Werte.
X	Dieser Variablen kennzeichnen die Messwerte der unabhängigen Variablen, welche in Regressionsanalyse miteinfließen.
ε	ε kennzeichnet die Residuen des Modells, welche jenen Anteil ausmacht, die vom Modell selbst nicht erklärt werden kann.

Tabelle 6: Regressionskoeffizienten (Volker Tresp 2011)

Im Zuge der Einbettung der linearen Regression in die Bayessche Statistik müssen für die Messwerte, für die Zielgröße und für die Residuen jeweils Priors festgelegt werden. Damit wird erreicht, dass Vorwissen in die Berechnungen einfließen und eine Aussage getroffen werden kann, wie hoch die Wahrscheinlichkeit ist, dass zwischen abhängiger und unabhängiger Variable eine signifikante Korrelation besteht.

Die Messdaten werden aus den codierten Fragebogenergebnissen gezogen und mit einem schwachen Prior gesampelt, um auf die Zielgröße zu schließen.

Im Zuge der Evaluierung in dieser Arbeit wird die Bayessche Statistik in Kombination mit der linearen Regression angewandt, um Korrelationen und Effekte zwischen den einzelnen Größen zu messen. (Volker Tresp 2011)

8.2.4 HDI – Highest Density Interval

Der HDI in der bayessche Statistik gibt ein Wahrscheinlichkeitsmaß an und bestimmt ein Intervall, welches jene Werte enthält, welche die größte Wahrscheinlichkeitsdichte haben. Sprich, Werte mit geringer Wahrscheinlichkeit finden sich nicht im HDI wieder, da sie im Intervall nicht mitberücksichtigt werden. Im Zuge der empirischen Untersuchung wird die Signifikanz zwischen einzelnen Faktoren über den HDI beurteilt. Es werden nur jene Zusammenhänge als signifikant angesehen, wenn das Intervall entweder gänzlich positiv oder gänzlich negativ ist. Im Anhang A können die HDI Diagramme aus der empirischen Untersuchung entnommen werden. Die Argumentationen in der empirischen Untersuchung leiten sich aus den vorhin genannten HDI Diagrammen ab. (Mike Meredith 2016)

8.3 Ergebnisse der empirischen Untersuchung

Die Untersuchung erfolgte deduktiv durch Auswertung des Fragebogens. Als statistische Verfahren wurden die lineare Regression in Kombination mit dem bayesschen Verfahren eingesetzt, um Zusammenhänge zwischen einzelnen Faktoren zu erkennen und auch gezielt auf Gruppenunterschiede einzugehen. Zusätzlich werden noch einige Fragen rein deskriptiv ausgewertet, welche als Faktoren nicht in Betracht gezogen wurden oder im Zuge der Faktorenanalyse eliminiert wurden.

8.3.1 Probleme bei Systemanmeldungen

Um die Relevanz von Single Sign On Lösungen in der Praxis zu verstehen, ist es zunächst wichtig zu wissen, aus welchen Gründen Systemanmeldungen scheitern. Es wurden alle 112 Personen danach befragt, mit welchen Probleme sie im Zuge einer gewöhnlichen Anmeldung bereits konfrontiert waren. In Abbildung 14 ist ersichtlich, dass der Hauptgrund für das Scheitern einer Anmeldung, an den Credentials selbst liegt. 79 Personen gaben an, dass sie ihr Passwort vergessen haben und deshalb der Login gescheitert ist. Auch das abgelaufene Passwort hat bei 69 Personen zu Problemen geführt. Weiters ist im Balkendiagramm in Abbildung 14 gut ersichtlich, dass die Applikation selbst oder der betriebene Server, weit weniger oft Probleme verursacht hat als das vergessene oder abgelaufene Passwort. Eine interessante Information ist noch dass eine nicht abgeschlossene Registrierung nur bei 15 Personen jemals zu Problemen geführt hat. Unter dem Punkt Sonstige wurden von den Teilnehmern noch folgende weitere Probleme im Zuge der Anmeldung angegeben:

- Benutzername vergessen
- Passwort mehrmals falsch eingegeben
- Verbindungsprobleme zwischen Computer und Server

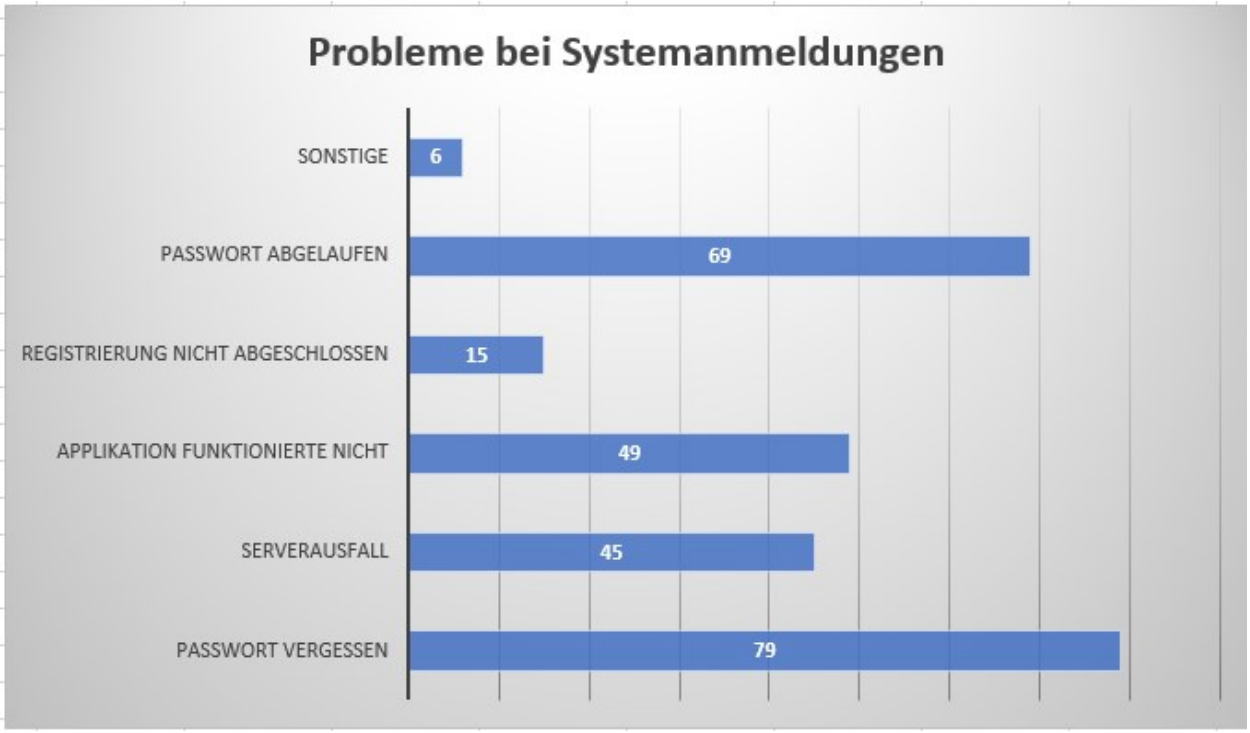

Abbildung 14: Probleme mit Systemanmeldungen (eigene Abbildung)

8.3.2 Präferenzen – Anmeldevarianten

Den Befragten wurden 3 Bilder gezeigt, welche unterschiedliche Anmeldeverfahren zeigten. Ersteres konnten sie sich für eine gewöhnliche Anmeldung entscheiden, welche die Authentifizierung über Benutzername und Passwort ermöglicht. Weiters konnten sie sich für ein Anmeldeverfahren entscheiden, welche sowohl Single Sign On und die gewöhnliche Anmeldung über Benutzername und Passwort unterstützte. Letzteres wurde ein Bild von einem Anmeldeverfahren gezeigt, welche nur Single Sign On unterstützte.

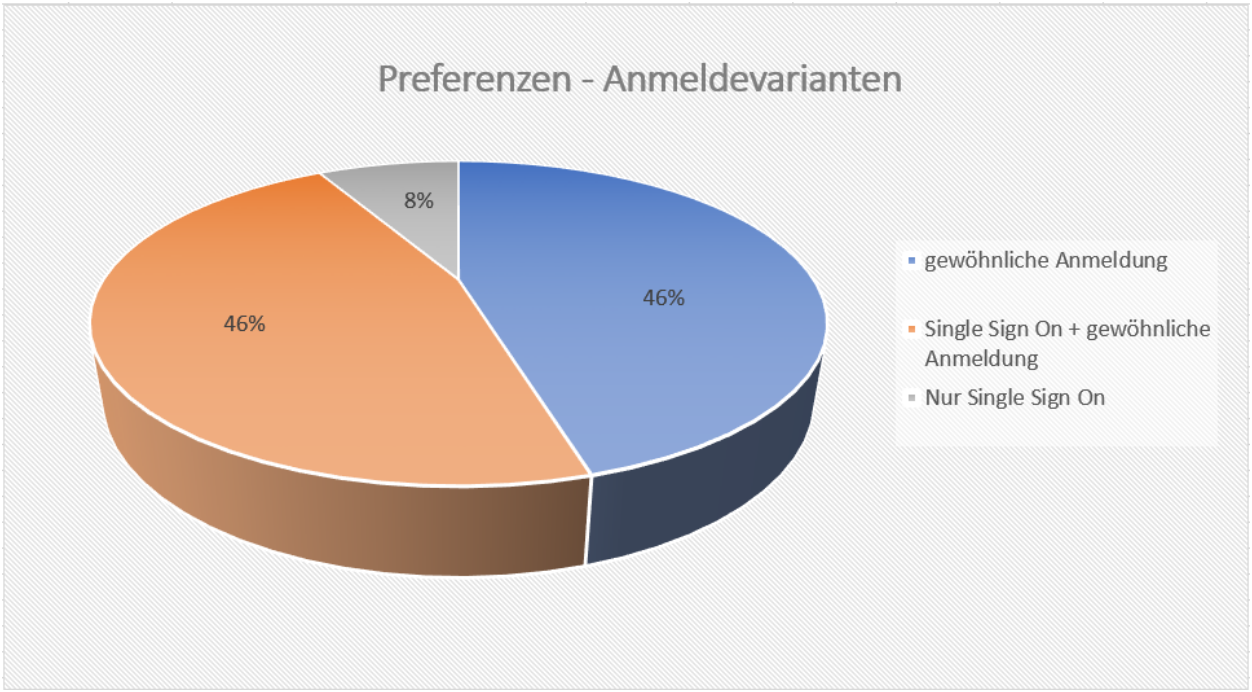

Abbildung 15: Präferenzen bei Anmeldevarianten (eigene Abbildung)

Wie in Abbildung 15 ersichtlich, haben sich 46% der Teilnehmer für die gewöhnliche Anmeldung entschieden. Ebenfalls 46% haben sich für das Anmeldevariante entschieden, welche beide Anmeldeverfahren unterstützt. Lediglich 8% der Befragten würden ein Anmeldeverfahren nur über Single Sign On präferieren. Das Ergebnis zeigt somit gut, dass die Benutzerakzeptanz von Single Sign On durchaus gegeben ist, jedoch das herkömmliche Anmeldeverfahren der Einmalanmeldung vorgezogen wird.

8.3.3 Single Sign On im Unternehmen

Die Teilnehmer wurden befragt, ob sie sich im Unternehmen mittels Single Sign On Technologie anmelden. Während bei 39% der Befragten laut eigenen Aussagen eine Single Sign On Lösung im Unternehmen eingesetzt wird, wird bei 61% der Befragten ein anderes Authentifizierungsverfahren verwendet. Somit sind die gewöhnlichen Anmeldemöglichkeiten mittels Benutzername und Passwort laut der entnommenen Stichprobe in Unternehmen weiterverbreitet als Single Sign On Lösungen. Abbildung 16 stellt das Ergebnis über die Nutzung von Single Sign On Lösungen im Unternehmen grafisch dar.

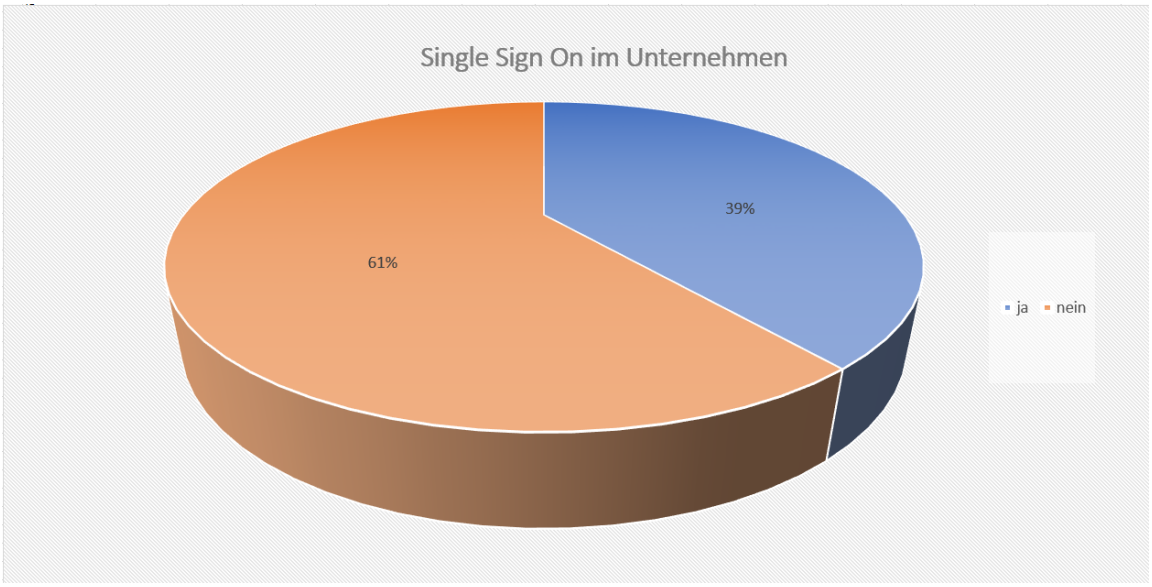

Abbildung 16: Single Sign On im Unternehmen (eigene Abbildung)

8.3.4 Kein signifikanter Unterschied zwischen Altersgruppen

Die Teilnehmer des Fragebogens wurden in 5 Altersgruppen eingeteilt, welche in Tabelle 6 ersichtlich sind.

Altersgruppen
< 20
< 30
< 40
< 50
< 60

Tabelle 7: Altersgruppen (eigene Tabelle)

Zwischen den einzelnen Altersgruppen konnte kein signifikanter Unterschied festgestellt werden, da der HDI der Altersgruppen den 0 Wert miteinschließt. Es konnten somit keine Rückschlüsse gezogen werden, ob das Alter Einfluss auf die Benutzerakzeptanz von Single Sign On Lösungen hat. Zusätzlich ist die Standardabweichung bzw. die Varianz der einzelnen Altersgruppen sehr hoch.

8.3.5 Kein signifikanter Unterschied zwischen Geschlechter

Zwischen Frauen und Männer konnte auch kein signifikanter Unterschied erkannt werden. Das Geschlecht übt auch keinen signifikanten Einfluss auf die Benutzerakzeptanz aus. Tendenziell kann angenommen werden, dass Frauen Single Sign On Lösungen in größeren Maße akzeptieren als Männer. Da jedoch der HDI bei Frauen und Männern den 0 Wert einschließt, ist dieser Effekt statistisch nicht aussagekräftig.

8.3.6 Kein Effekt der subjektiven Norm auf die Benutzerakzeptanz

Die subjektive Norm hat keine Auswirkungen auf die Benutzerakzeptanz von Single Sign On Lösungen. Somit hat die Beeinflussung durch Freunden und Bekannten, keinen nennenswerten Effekt, ob eine Single Sign On Lösung benutzt wird oder nicht.

8.3.7 Signifikanz zwischen positiver Einstellung und Akzeptanz von Single Sign On

Der HDI, welcher das Intervall für den Faktor Einstellung darstellt, ist positiv. Schlussfolgend hat eine positive Einstellung die Folge, dass Nutzer vermehrt Single Sign On Lösungen nutzen. Folgende Teilfaktoren wurden im Zuge der Umfrage abgefragt, um auf die Einstellung des jeweiligen Teilnehmers gegenüber Single Sign On zu schließen:

- Einstellung zu den Vorteilen von Single Sign On
- Nützlichkeit von Single Sign On
- Präferenzen zu Single Sign On gegenüber der herkömmlichen Anmeldung

8.3.8 Signifikanz zwischen IT-Affinität und Akzeptanz von Single Sign On

Auch die IT-Affinität hat einen signifikanten Effekt auf die Akzeptanz von Single Sign On Lösungen. Je IT-affiner ein Nutzer ist, umso höher ist die Wahrscheinlichkeit, dass dieser eine Single Sign On Lösung nutzt. Die IT-Affinität wurde gemessen, indem der Benutzer angeben musste, wie oft er einen Computer täglich benutzt, wie gerne er mit dem Computer interagiert und welche Einstellung der Nutzer generell gegenüber Computer hat.

8.3.9 Kein Zusammenhang zwischen Probleme mit Anmeldungen und Akzeptanz von Single Sign On

Es könnte angenommen werden, dass Nutzer, welche mehrfach Probleme mit Anmeldungen hatten, Single Sign On Lösungen präferieren würden. Jedoch konnte keine Signifikanz zwischen Probleme mit Anmeldungen und Akzeptanz von Single Sign On Lösungen festgestellt werden.

Folgende Problembereiche bei der gewöhnlichen Anmeldung mit Benutzername und Passwort wurden identifiziert und die Nutzer wurden über diese Bereiche passende Fragen gestellt:

- Probleme mit Systemanmeldungen im Unternehmen
- Anzahl der zu merkenden Passwörter im Unternehmen
- Anfragen an Helpdesk

Schlussfolgend, kann somit keine Aussage getroffen werden, ob entstandene Probleme bei Anmeldungen in der Vergangenheit zu einer größeren oder niedrigeren Benutzerakzeptanz gegenüber Single Sign On führen.

8.3.10 Signifikanz zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und Akzeptanz von Single Sign On

Zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und Akzeptanz von Single Sign On konnte eine signifikante Korrelation festgestellt werden. Je höher das Sicherheitsbewusstsein der Nutzer in Bezug auf Single Sign On Lösungen ist, umso höher ist die Akzeptanz von Single Sign On Lösungen.

Um das Sicherheitsbewusstsein im Kontext von Single Sign On zu determinieren, wurden den Teilnehmern um eine Einschätzung über die Sicherheit von Single Sign On Lösungen von Drittanbieter wie Facebook, Twitter, gebeten. Konkret wurde um eine Einschätzung über folgende Themenbereiche gebeten:

- Datenübermittlung zwischen Identity Provider und Service Provider
- Potenzielle Angriffsgefahr
- Nachvollziehbarkeit und Rückverfolgung der Aktionen von Nutzer

Das Ergebnis ist insofern überraschend, da jene Nutzer Single Sign On Lösungen bevorzugen, welche sich über die Risiken von Single Sign On Lösungen bewusst sind. Somit kann angenommen werden, dass Nutzer die Risiken aufgrund des Nutzungskomforts in Kauf nehmen.

8.3.11 Keine Signifikanz zwischen Sicherheitsbewusstsein im Allgemeinen und Akzeptanz von Single Sign On

Es wurden auch Fragen gestellt, die auf das generelle Sicherheitsbewusstsein der Teilnehmer abzielten.

Unter anderem wurde das Sicherheitsbewusstsein in den unten angeführten Bereichen abgefragt.

- Sicherheitsbewusstsein bei Nutzung des E-Banking
- Sicherheitsbewusstsein bei Onlinenutzung
- Sicherheitsbewusstsein am Arbeitsplatz
- Sicherheitsbewusstsein über potenzielle Angriffe

Auch hier ist die Tendenz gegeben, dass je höher das Sicherheitsbewusstsein der Nutzer ist, umso höher die Benutzerakzeptanz. Da jedoch der HDI Wert die 0 einschließt, ist kein signifikantes Ergebnis gegeben und es kann keine eindeutige Aussage getroffen werden, dass durch erhöhtes allgemeines Sicherheitsbewusstsein die Akzeptanz von Single Sign On Lösungen steigt.

8.4 Empirische Detailanalyse bezogen auf Alter, Geschlecht, Ausbildung und Berufsfeld

Es wurden Detailanalysen bezogen auf verschiedenste Kategorien durchgeführt. Die unten angeführten Detailanalysen sind auch grafisch in den einzelnen ,,Star Wars“ - Diagrammen in Anhang A ersichtlich.

- Einfluss des Geschlechtes auf unabhängige Variablen der Benutzerakzeptanz,
- Einfluss des Alters auf die unabhängigen Variablen der Benutzerakzeptanz und
- Einfluss der Ausbildung auf die unabhängigen Variablen der Benutzerakzeptanz
- Einfluss des Berufsfeld auf die unabhängigen Variablen der Benutzerakzeptanz

Es wurde dabei nur mehr auf die signifikanten Faktoren:

- Sicherheitsbewusstsein im Kontext von Single Sign On
- IT-Affinität
- Einstellung zu Single Sign On

in der Analyse eingegangen. Alle anderen Faktoren lieferten auch in der Detailanalyse für die verschiedenen Geschlechter und Altersgruppen keine signifikanten Ergebnisse. Aus diesem Grund wurden nur die 3 oben genannten relevanten unabhängigen Variablen grafisch dargestellt.

8.4.1 Signifikanz bei Männer in Bezug auf positiver Einstellung und Akzeptanz von Single Sign On

In Abbildung „Einfluss Geschlecht auf unabhängigen Variablen der Benutzerakzeptanz“ in Anhang A ist gut ersichtlich, dass ein signifikantes Ergebnis zwischen Einstellung gegenüber Single SIgn On und Akzeptanz von Single Sign On, nur bei den Männern gegeben ist. Bei Frauen lässt sich nicht rückschließen, ob eine positive Einstellung gegenüber Single Sign On dazu führt, dass eine Single Sign On Lösung tatsächlich genutzt wird.

8.4.2 Signifikanz bei Frauen in Bezug auf IT-Affinität und Akzeptanz von Single Sign On

Frauen, welche IT-affiner sind, nutzen Single Sign On Lösungen vermehrt. Hingegen bei Männer hat die IT-Affinität keinen Einfluss auf die Akzeptanz von Single Sign On Lösungen. Es ist ein interessanter Aspekt, dass bei den Männern die Affinität zum Computer keine prämiere Rolle für die Akzeptanz von Single Sign On Lösungen spielt.

8.4.3 Simpson Paradox bei Sicherheitsbewusstsein im Kontext von Single Sign On

Obwohl das Sicherheitsbewusstsein im Kontext von Single Sign On ein signifikantes Ergebnis zeigt, sind die Teilergebnisse für Frauen und Männer nicht signifikant. Dieses Phänomen wird in der Statistik auch Simpson Paradox genannt. Das Simpson Paradox besagt, dass die Ergebnisse einer Analyse unterschiedlich ausfallen kann, wenn man Ergebnisse von verschiedenen Gruppen einzeln betrachtet oder das Gesamtergebnis selbst betrachtet. (Ivan Koswara 2017)

Der mögliche Einflussfaktor, warum dieses Phänomen in dieser empirischen Untersuchung auftaucht, ist die ungleich verteilte Frauen/Männerquote. Durch die unterschiedliche Gewichtung ist es möglich, dass sich die Teilergebnisse der Männer und Frauen einen anderen Effekt zeigen als das Gesamtergebnis, welche Frauen und Männer enthält.

8.4.4 Signifikante Ergebnisse bei jungen Teilnehmer in Bezug auf Einstellung zu Akzeptanz von Single Sign On

Bei der Gruppe der unter 20-jährigen hat eine negative Einstellung zu Single Sign On zur Folge, dass vermehrt Single Sign On Lösungen von Jugendlichen genutzt werden. Das bedeutet, obwohl sie mit dem Nutzen und mit den Vorteilen von Single Sign On nicht zufrieden sind, benutzen sie die Lösung, um sich bequem für diverse Anwendungen anzumelden. Es ist möglich, dass sich die Nutzer der Generation Z deshalb kritisch zu Single Sign On Lösungen geäußert haben, da sie noch Verbesserungspotenzial für die Zukunft sehen, um sich noch bequemer, auch über andere Technologien, anmelden zu können.

Sowohl bei 20 bis 30-jährigen und 30 bis 40-jährigen Personen zeigt sich der gegenteilige Effekt. Je positiver die Einstellung zu Single Sign On ist, umso höher ist die Akzeptanz. Diese Altersgruppe, hat bereits positive Erfahrungswerte mit Single Sign On gesammelt, und nutzt aus diesem Grund auch diese Technologie.

Bei den älteren Generationen konnte jedoch keine Signifikanz zwischen Einstellung und Akzeptanz festgestellt werden. Somit kann keine Aussage getroffen werden, ob die Einstellung einen beträchtlichen Einfluss auf die Akzeptanz und Nutzung hat.

8.4.5 Signifikanz zwischen IT-Affinität und Akzeptanz von Single Sign On bei den 30- bis 40 Jährigen

Einzig bei den 30- bis 40- Jährigen lässt sich eine Signifikanz zwischen IT-Affinität und Akzeptanz von Single Sign On Lösungen feststellen. Bei dieser Altersgruppe übt die IT-Affinität einen Einfluss auf die Benutzerakzeptanz von Single Sign On Lösungen aus. Je IT-affiner ein Nutzer ist, umso öfters wird die Single Sign On Lösung genutzt. Bei allen anderen Altersgruppen konnte keine signifikante Korrelation zwischen den 2 Faktoren eruiert werden.

8.4.6 Simpson Paradox zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und Benutzerakzeptanz gruppiert nach Altersgruppen

Wie schon bei der Analyse nach dem Geschlecht, tritt auch bei der Gruppierung nach den Altersgruppen das Phänomen des Simpson Paradox auf. Es konnte bezogen auf die einzelnen Altersgruppen keine signifikante Korrelation zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und Benutzerakzeptanz festgestellt werden.

8.4.7 Simpson Paradox zwischen Einstellung und Benutzerakzeptanz gruppiert nach Ausbildung

Zwischen Einstellung des Nutzers gegenüber Single Sign On und Benutzerakzeptanz gruppiert nach der Ausbildung gibt es keine signifikanten Ergebnisse. Sowohl bei Maturanten, Akademiker, Lehrlinge und Pflichtschulabgänger können keine Rückschlüsse gezogen werden, ob die Einstellung einen positiven oder negativen Effekt auf die Benutzerakzeptanz ausübt.

8.4.8 Signifikanz zwischen IT-Affinität und Benutzerakzeptanz bei Akademiker

Bei Akademiker übt die IT-Affinität einen signifikanten Effekt auf die Benutzerakzeptanz aus. Bei erhöhter IT-Affinität von Akademiker steigt die Benutzerakzeptanz und die Nutzung gegenüber Single Sign On Lösungen. Bei den anderen Ausbildungsgruppen konnte kein Effekt festgestellt werden.

8.4.9 Simpson Paradox zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und Benutzerakzeptanz gruppiert nach Ausbildung

Wie schon bei der Detailanalyse nach Alter und Geschlecht, lässt sich zwischen dem Sicherheitsbewusstsein und der Benutzerakzeptanz gruppiert nach Ausbildung kein relevanter Effekt feststellen.

8.4.10 Signifikantes Ergebnis zwischen IT-Affinität und Benutzerakzeptanz bei Informationstechnologen

Informationstechnologen müssen schon aufgrund ihrer Tätigkeit im beruflichen Alltag IT affine sein. Als IT affiner Nutzer ist man auch gewillter neue Technologien zu nutzen. Aus diesem Grund ist es nicht sehr überraschend, dass IT-Affinität und Benutzerakzeptanz bei den Informationstechnologen signifikant korrelieren.

8.4.11 Signifikanz zwischen Einstellung zu Single Sign On und Benutzerakzeptanz bei Informationstechnologen

Je besser die Einstellung der Informationstechnologen auf Single Sign On Lösungen ist, umso häufiger werden vorhin genannte auch genutzt. Auch hier ist das Ergebnis nicht sehr überraschend, da fast alle befragten Informationstechnologen eine positive Einstellung zu Single Sign On haben und auch fast alle aufgrund ihrem IT Interesse und beruflichen Tätigkeit Single Sign On Lösungen nutzen. Bei allen anderen Berufsgruppen konnte interessanterweise kein signifikanter Effekt festgestellt werden.

8.4.12 Signifikantes Ergebnis zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und Benutzerakzeptanz bei Büroangestellten

Bei Teilnehmer, welche im Berufsfeld Büro, Wirtschaft, Finanzwesen und Recht arbeiten, lässt sich ein signifikanter Effekt zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und Benutzerakzeptanz feststellen. Je höher das Sicherheitsbewusstsein der Mitarbeiter im Kontext von Single Sign On ist, umso häufiger werden Single Sign On Lösungen genutzt. Das bedeutet, dass Mitarbeiter in diesem Berufsfeld über die Gefahr des Missbrauchs von personenbezogenen Daten bewusst sind und dennoch Single Sign On Lösungen nutzen. Überraschend ist somit, dass sie vermehrt Single Sign On Lösungen nutzen, je ausgeprägter ihr Sicherheitsbewusstsein ist.

8.5 Fallstudie

Die Fallstudie bestehend aus 2 Gruppen wurde im Zeitraum vom 01.01.2018 und 25.02.2018 mit 14 Personen durchgeführt. Das Ziel der Fallstudie war es in einer realen Umgebung zu testen, für welches Anmeldeverfahren sich Personen entscheiden. Es wurden gängige Webapplikationen und Apps ausgewählt, welche sowohl die gewöhnliche Anmeldung über Benutzername und Passwort unterstützten, sowie Single Sign On Lösungen.

Die Probanden mussten sich bei insgesamt 4 Anwendungen anmelden. 2 Anwendungen waren Webapplikationen, welche über Laptop/PC aufzurufen waren und die anderen 2 Anwendungen waren Apps, welche über ein mobiles Endgerät installiert werden sollten.

Um mehrere Anwendungen in die Fallstudie einbeziehen zu können, wurden 2 Gruppen gebildet, welchen jeweils andere Anwendungen für die Registrierung vorgelegt wurden. Somit wurden insgesamt 4 Webapplikationen und 4 Apps in die empirische Untersuchung mitaufgenommen.

Tabelle 8 enthält eine Übersicht der benutzten Anwendungen der Probanden während der Fallstudie. Des Weiteren ist der Nutzen der Anwendung angeführt und über welchen Identity Provider es möglich war, die Anmeldung bei der jeweiligen Anwendung durchzuführen.

Art	Anwendung	Funktion der Anwendung	Identity Provider
Webapplikation	Shpock	Shpock ist eine Flohmarkt-App mit denen verschiedenste Gegenstände gekauft oder verkauft werden können. (shpock.com 2018)	Facebook Google Plus
Webapplikation	Wo gibt's was	Bei Wo gibt's was hat man alle regionalen Angebote im Überblick. (wogibtswas.at 2018)	Facebook Google Plus
Webapplikation	Codeacademy.com	Codeacademy.com bietet interaktiven Programmierunterricht in verschiedenen Sprachen an. (Team Twago 2014)	Facebook Google Plus
Webapplikation	Pinterest	Über Pinterest können jegliche Probleme und Ideen aus dem Alltagsleben geteilt werden. (Google Play Store 2018a)	Facebook Google Plus
App	Airbnb	Mit Airbnb lassen sich Apartments auf der ganzen Welt buchen. (Airbnb 2018)	Facebook
App	Quizduell	Über Quizduell können Freunde, Bekannte oder andere Internetbenutzer zu Wissensduellen herausgefordert werden. (Google Play Store 2018b)	Facebook Google Plus
App	Tinder	Bei Tinder handelt es sich um eine Dating-App, die das Ziel hat Leute zusammenzubringen. (Google Play Store 2018c)	Facebook
App	Runtastic	Mit der Fitnessapp Runtastic können Aufzeichnungen über Laufaktivitäten gemacht werden und diese Aufzeichnungen mit Freunden geteilt werden. (Runtastic 2018)	Facebook Google Plus

Tabelle 8: Übersicht der Anwendungen in der Fallstudie (eigene Tabelle)

8.5.1 Ziel der Fallstudie

Das Ziel der Fallstudie war es vorrangig, die Akzeptanz von Single Sign On Lösungen im Feld zu testen. Zusätzlich sollte anhand dieser Fallstudie ermittelt werden, ob die Auswahl des Identity Provider einen entscheiden Einfluss auf die Benutzerakzeptanz von Single Sign On Lösungen ausübt. Ein interessanter Aspekt welcher noch berücksichtigt werden sollte, ob auch die Art der Anwendung einen entscheidenden Einfluss auf Benutzerakzeptanz ausübt. Um die Informationen zu erhalten, mussten die Probanden als Abschluss der Fallstudie einen Fragebogen ausfüllen. Dieser Fragebogen ist in Anhang D ersichtlich und enthält Fragen über folgende Merkmale:

1. Erstregistrierung oder wiederholte Anmeldung
2. Entscheidung über das Anmeldeverfahren
3. Begründung für die Entscheidung
4. Einschätzung über die Schwierigkeit der Entscheidung

8.5.2 Gewähltes Anmeldeverfahren der Probanden

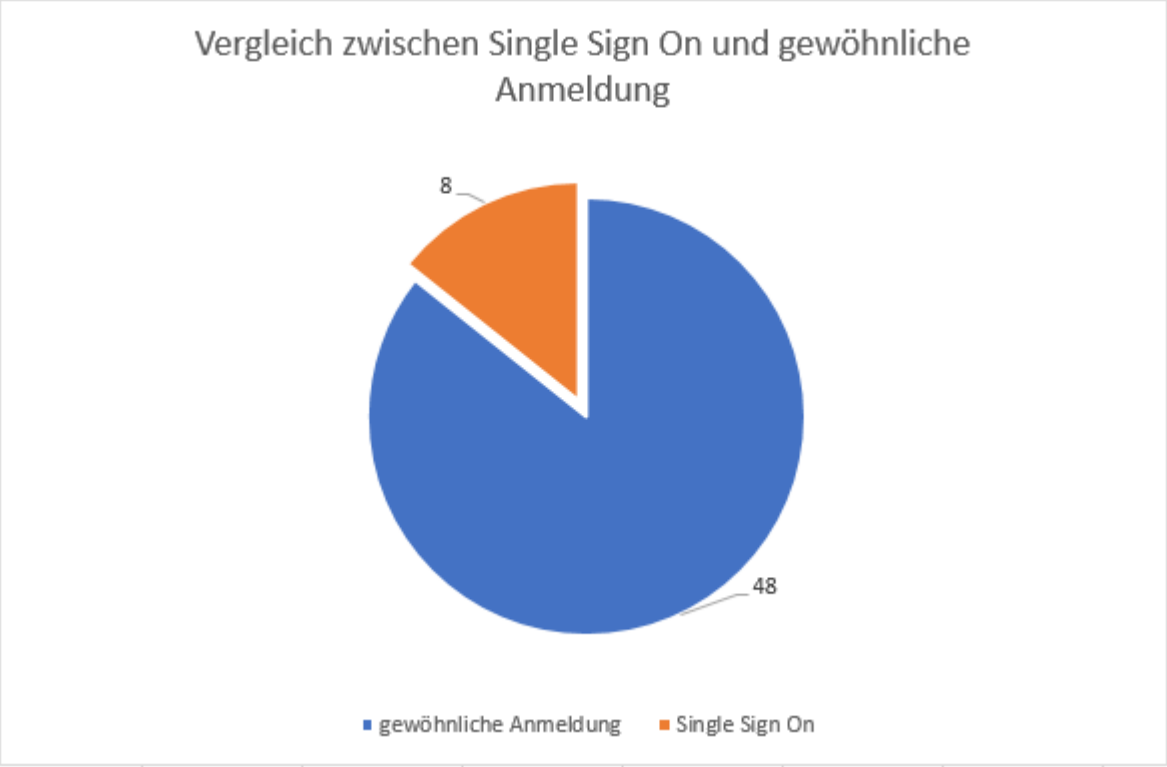

Abbildung 17: Vergleich zwischen Single Sign ON und gewöhnliche Anmeldung (eigene Abbildung)

Wie in Abbildung 17 illustriert, haben sich die 14 Teilnehmer bei 56 Applikationen angemeldet. Lediglich 8 Mal wurde als Anmeldeverfahren Single Sign On verwendet. Im Gegensatz dazu haben sich die jeweiligen Probanden 48 Mal mit Benutzername und Passwort angemeldet. In

Prozent ausgedrückt, haben sich die Probanden zu 14,29% für Single Sign On entschieden und zu 85,71% für das herkömmliche Anmeldeverfahren.

8.5.3 Unterschiede bei den Anmeldeverfahren zwischen Apps und Webapplikationen

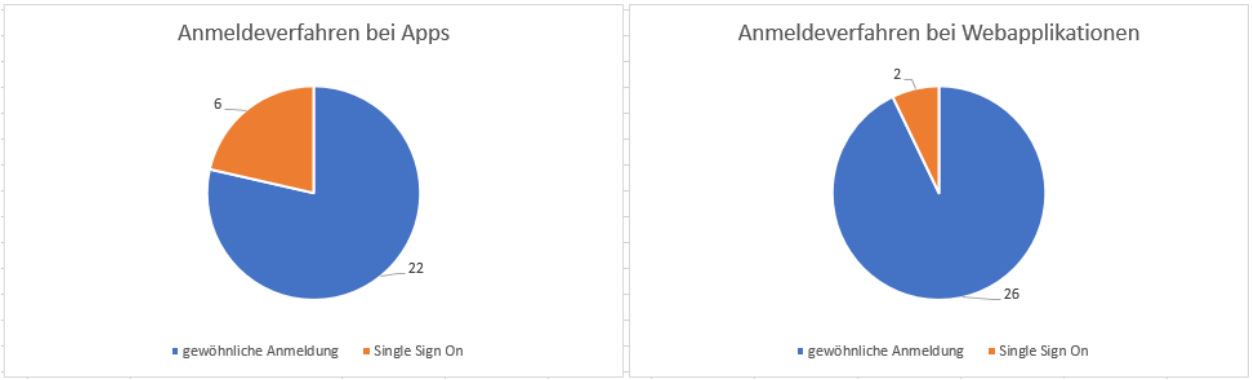

Abbildung 18: Unterschiede bei den Anmeldeverfahren zwischen Apps und Webapplikationen (eigene Abbildung)

In Abbildung 18 ist gut ersichtlich, dass sich die Teilnehmer im Zuge der Anmeldung bei Apps öfters für Single Sign On entscheiden haben, als bei Anmeldungen über diverse Webapplikationen. Während sich Teilnehmer im Zuge der Anmeldung auf einer Webplattform nur 2 Mal für Single Sign On entscheiden haben, haben sich die Teilnehmer bei Anmeldung über diverse Apps 6 Mal für Single Sign On entschieden.

8.5.4 Gründe für Auswahl der herkömmlichen Anmeldung

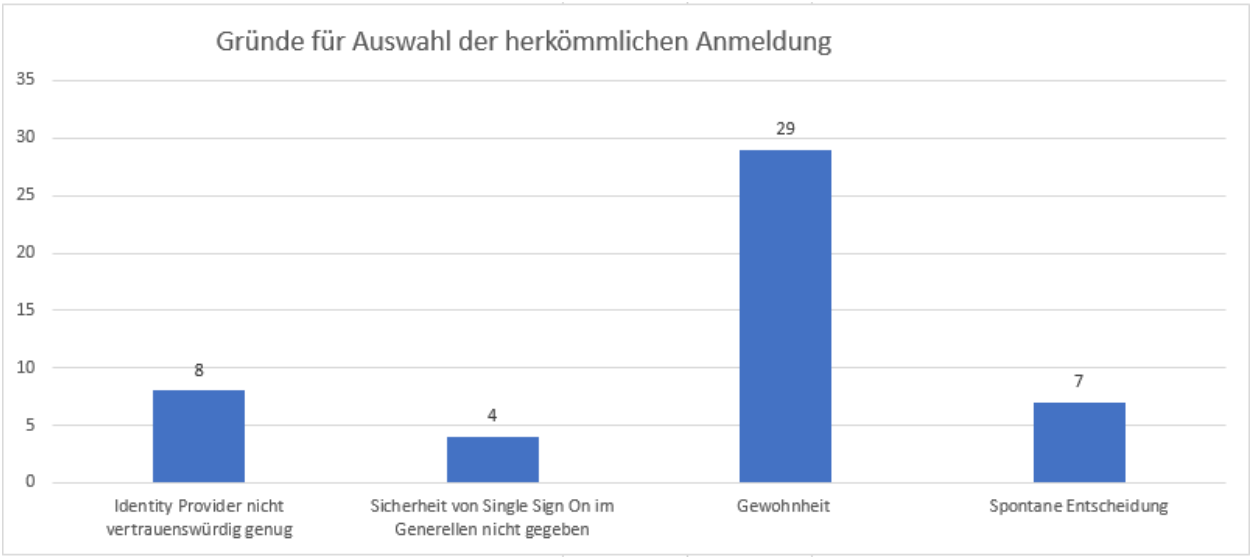

Abbildung 19: Gründe für Auswahl des traditionellen Anmeldeverfahrens (eigene Abbildung)

Der Hauptgrund, weshalb sich die Teilnehmer für die herkömmliche Anmeldevariante mittels Benutzername und Passwort entschieden haben, ist die Gewohnheit sich bislang über das

Anmeldeverfahren angemeldet zu haben. Prozentuell ergab sich folgende Verteilung für die Gründe, warum sich Teilnehmer für das herkömmliche Anmeldeverfahren entschieden haben:

Gründe	**Prozentuelle Verteilung**
Gewohnheit	60,42%
Identity Provider nicht vertrauenswürdig genug	16,67%
Spontane Entscheidung	14,58%
Sicherheit von Single Sign On im Generellen nicht gegeben	8,33%

Tabelle 9: Prozentuelle Verteilung - Gründe für traditionelle Anmeldung (eigene Tabelle)

Interessant ist das Faktum, dass nur für ein Viertel der Teilnehmer der Grund für die Wahl der herkömmlichen Variante, die unzureichende Sicherheit von Single Sign On ausschlaggebend war.

8.5.5 Gründe für Auswahl von Single Sign On

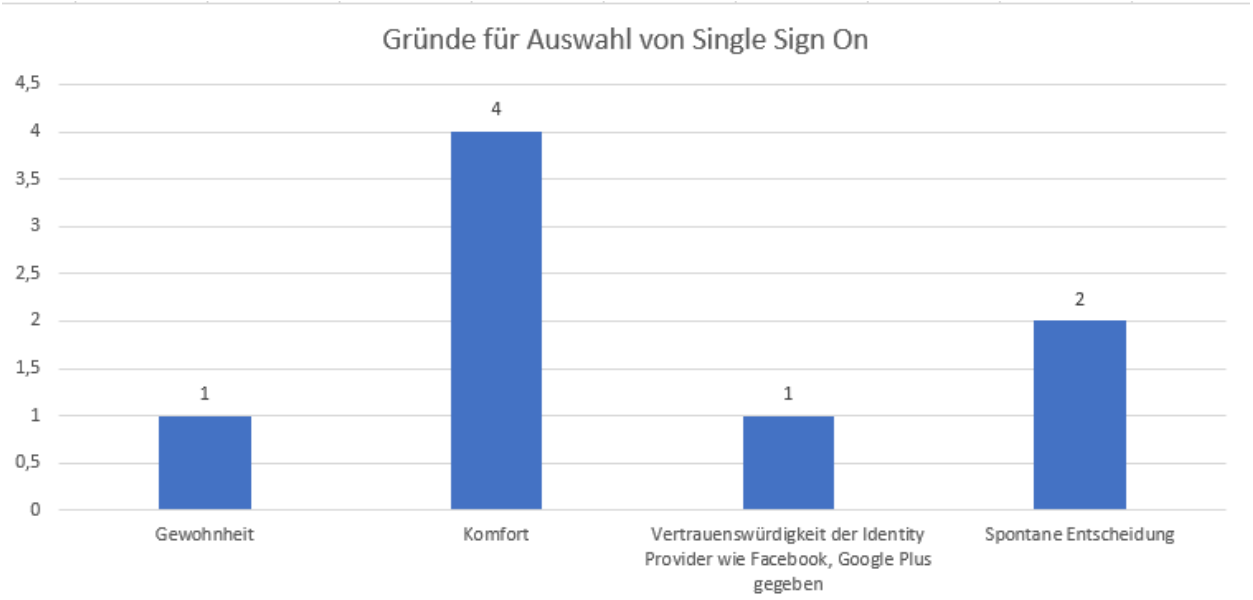

Abbildung 20: Gründe für Auswahl von Single Sign On (eigene Abbildung)

Wie in Abbildung 20 illustriert, wurde 8 Mal Single Sign On als Anmeldeverfahren von den Teilnehmern gewählt. Von den Teilnehmern wurde angegeben, dass der Hauptgrund für die Entscheidung der Komfort ist, welche eine Single Sign On Lösung im Vergleich zu der herkömmlichen Anmeldevariante mit sich bringt.

Nachfolgend die prozentuelle Verteilung, warum sich die Teilnehmer für eine Anmeldung über Single Sign On entschieden haben:

Gründe	Prozentuelle Verteilung
Komfort	50,00%
Spontane Entscheidung	25,00%
Gewohnheit	12,50%
Vertrauenswürdigkeit der Identity Provider wie Facebook, Google Plus gegeben	12,50%

Tabelle 10:Prozentuelle Verteilung - Gründe für die Anmeldung über Single Sign On (eigene Tabelle)

In Tabelle 10 ist gut erkennbar, dass die Vertrauenswürdigkeit des Identity Providers, sowie die Gewohnheit bei der Nutzung des Anmeldeverfahrens eine untergeordnete Rolle spielen. Noch eher hat das Bauchgefühl zu einer Entscheidung für eine Single Sign On bewogen.

8.5.6 Auswahl des Identity Providers

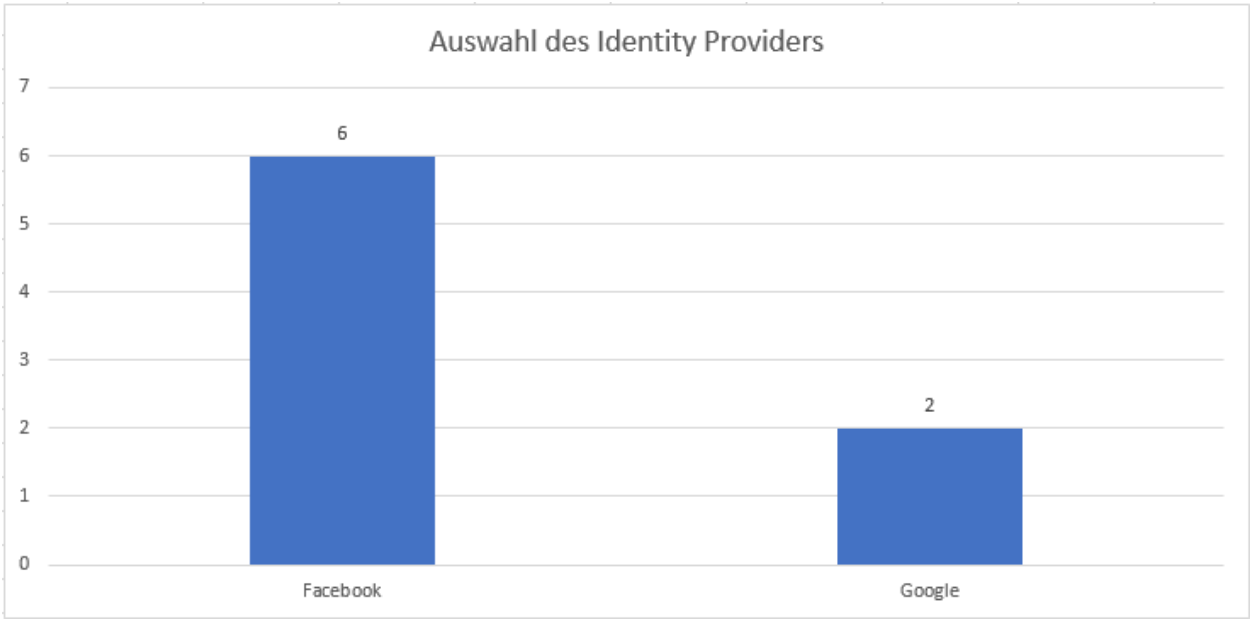

Abbildung 21: Auswahl des Identity Providers (eigene Abbildung)

In 6 von 8 Fällen haben sich die Teilnehmer über Facebook bei der Applikation angemeldet und nur bei 2 von 8 Fällen über Google. Des Weiteren sieht man in Abbildung 20, dass sich die Teilnehmer im Zuge der Studie für keinen anderen Identity Provider als Facebook oder Google entschieden haben.

8.5.7 Schwierigkeitsgrad der Entscheidungsfindung

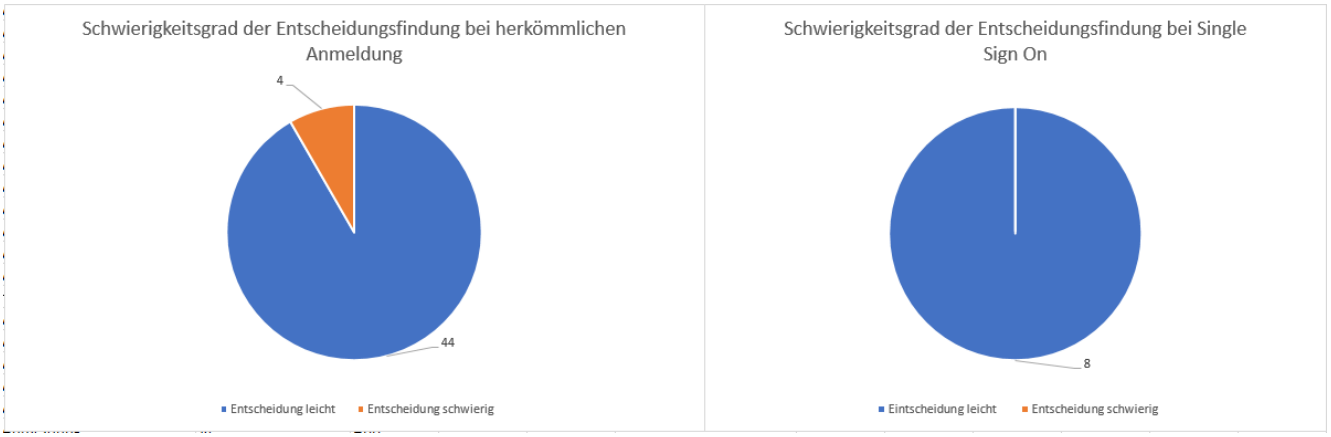

Abbildung 22: Schwierigkeitsgrad der Entscheidungsfindung (eigene Abbildung)

Im Grunde haben sich die Teilnehmer leichtgetan, sich zwischen einer Single Sign On Lösung oder einer herkömmlichen Anmeldevariante zu entscheiden. Lediglich bei 4 von insgesamt 56 Anmeldungen ist ihnen die Entscheidung schwergefallen. Wie in Abbildung 22 dargestellt, ist ihnen bei den 4 Anmeldungen die Entscheidung schwergefallen, wo sie sich für eine herkömmliche Anmeldung mittels Benutzername und Passwort entschieden haben.

8.5.8 Tendenz für das Anmeldeverfahren bei bereits registrierten Applikationen und nicht registrierten Applikationen

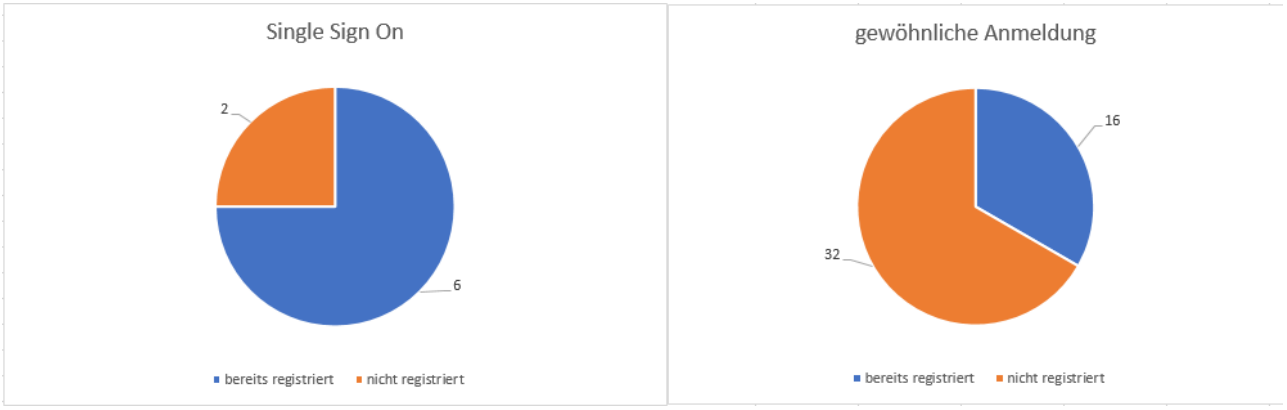

Abbildung 23: Tendenz bei bereits registrierten und nicht registrierten Applikationen (eigene Abbildung)

Die Teilnehmer haben am Beginn des Fragebogens angeben müssen, ob sie bereits bei der jeweiligen Applikation angemeldet waren. In Abbildung 23 ist deutlich zu erkennen, dass jene Teilnehmer, die sich für Single Sign On entschieden hatten, bereits über Single Sign On bei der jeweiligen Anwendung registriert waren. Es hat im der Zuge der Fallstudie nur 2 Neuanmeldungen über Single Sign On gegeben. Ein gegensätzlicher Trend lässt sich bei den Registrierungen über das gewöhnliche Anmeldeverfahren erkennen. 2/3 der Anmeldungen über das gewöhnliche Anmeldeverfahren waren Neuanmeldungen, während 1/3 der Anmeldungen bereits im Vorfeld getätigt wurden.

9 RESUMEE

Im letzten Kapitel werden nochmals die Ergebnisse aus Kapitel 8 zusammengefasst, diese kritisch hinterfragt, die Hypothesen belegt oder widerlegt und es wird ein Ausblick gegeben, für welche weiteren wissenschaftlichen Arbeiten diese Arbeit als Basis dienen soll.

9.1 Diskussion

In diesem Unterkapitel werden zunächst die Erkenntnisse aus Kapitel 8 nochmals zusammengefasst und abschließen kritisch auf Schwachstellen der empirischen Untersuchung mittels Fragebogen eingegangen.

9.1.1 Zusammenfassende Erkenntnisse aus der Faktorenanalyse basierend auf der erstellten Umfrage

Die Evaluierung aus den Fragebogen, welche ausführlich in Kapitel 8 beschrieben wurde, hat zusammenfassend grundsätzlich folgende Erkenntnisse erbracht:

- Das Vergessen von Passwörter ist der Hauptgrund für Probleme bei Systemanmeldungen
- Die Anmeldung mittels Passwort und Benutzername wird der Anmeldung über Single Sign On vorgezogen
- Je besser die Einstellung der Nutzer gegenüber Single Sign On ist, umso öfter wird Single Sign On genutzt
- Je IT affiner Nutzer sind, umso öfter werden Single Sign On Lösungen verwendet
- Je höher das Sicherheitsbewusstsein im Kontext von Single Sign On ist, umso öfter wird Single Sign On verwendet

In einer empirischen Detailanalyse wurden signifikante Zusammenhänge von Faktoren einzelner Gruppen herausgearbeitet. Folgende Ergebnisse waren dabei von Relevanz:

- Je positiver die Einstellung von Männern gegenüber Single Sign On ist, umso öfters wird Single Sign On genutzt
- Je IT affiner Frauen sind, umso öfters nutzen sie Single Sign On
- Je höher die IT-Affinität bei 30 bis 40-jährigen ist, umso öfters nutzen sie Single Sign On
- Bei Akademiker hat eine höhere IT Affinität zur Folge, dass Single Sign On öfters genutzt wird
- Je IT affiner Informationstechnologen sind, umso öfters nutzen sie Single SIgn On
- Je höher das Sicherheitsbewusstsein von Büroangestellten im Kontext von Single Sign On ist, umso häufiger nutzen sie Single Sign On Lösungen

9.1.2 Erkenntnisse aus der durchgeführten Fallstudie

Wie schon in Kapitel 8 beschrieben, haben sich die Teilnehmer der Studie 48 Mal für die gewöhnliche Anmeldung entschieden und lediglich 8 Mal für eine Single Sign On Lösung. Des Weiteren zeigte die Fallstudie folgende Tendenzen:

- Single Sign On wurde als Anmeldeverfahren über Apps öfters gewählt als auf Webapplikationen
- Aus Gewohnheit haben sich Teilnehmer für die gewöhnliche Anmeldeverfahren entschieden
- Der Hauptgrund, dass sich Teilnehmer für Single Sign On entschieden habe, war die einfache Handhabung der Single Sign On Lösung
- Facebook wurde am öftesten als Identity Provider von den Teilnehmern ausgewählt
- Die Entscheidung sich zwischen einer der beiden Anmeldemöglichkeiten zu entscheiden, ist den Teilnehmern einfach gefallen
- Bei Neuregistrierungen wurde die herkömmliche Anmeldevariante mit Passwort und Benutzername, der Single Sign On Lösung vorgezogen

9.1.3 Kritik an die Repräsentativität der Stichprobenerhebung

Die Repräsentativität, um von der Stichprobe auf die Grundgesamtheit zu schließen, war bei der Stichprobenerhebung des Fragebogens nicht gänzlich gegeben.

Wie in Abbildung 24 ersichtlich, wurden 41 Frauen und 76 Männer befragt. Ein Männer- und Frauenanteil von 50% wurde nicht erreicht, da sich zu wenig Frauen bereit erklärt haben, bei der Umfrage mitzumachen. Dennoch wurden trotz ungleichmäßiger Verteilung alle Fragen der Teilnehmer ausgewertet, da ein Informationsverlust in der empirischen Untersuchung vermieden werden sollte.

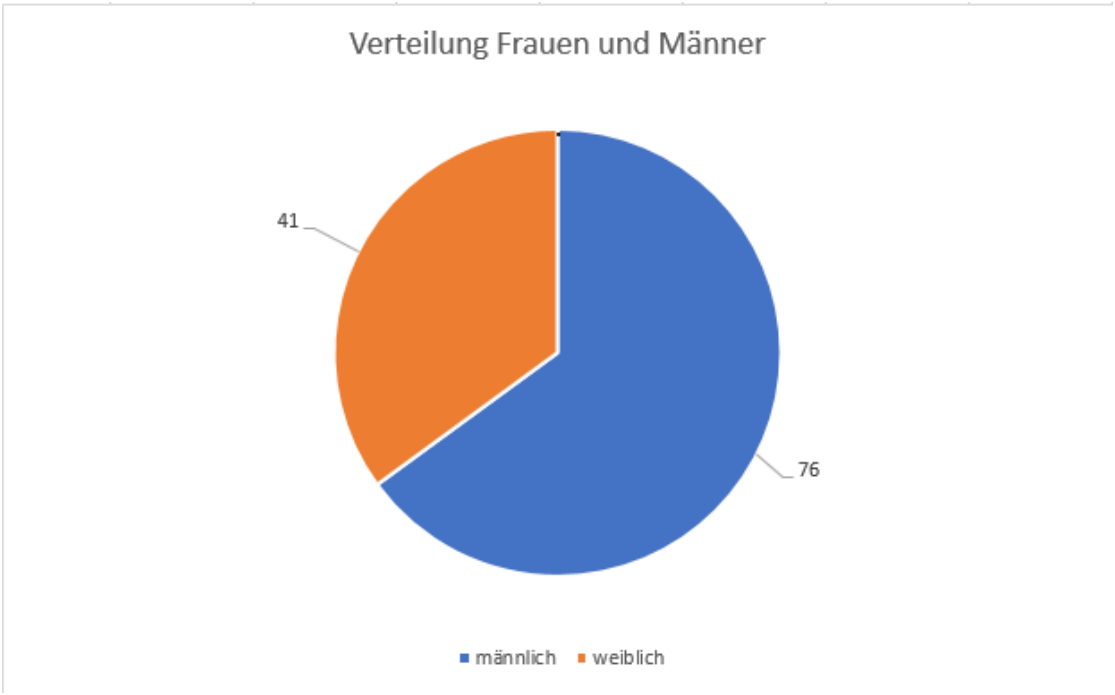

Abbildung 24:Verteilung Frauen und Männer (eigene Abbildung)

Auch die Altersverteilung der Teilnehmer ist nicht repräsentativ. Es sind zwar alle möglichen Altersgruppen von 20 – 60 Jahren vertreten, jedoch wurden hauptsächlich Personen befragt, welche zwischen 20 und 29 Jahren alt waren. Leider konnte keine bessere Verteilung durch die Aussendung des Fragebogens über die verschiedensten Internetkanäle erreicht werden. Besonders kritisch sind die signifikanten Ergebnisse, der 0-19 Jährigen zu betrachten. Da lediglich 5 Personen in dieser Altersgruppe an der Befragung teilgenommen haben, sind Ergebnisse aus dieser Alterskategorie nicht aussagekräftig genug. In Abbildung 25 ist die Altersverteilung illustriert.

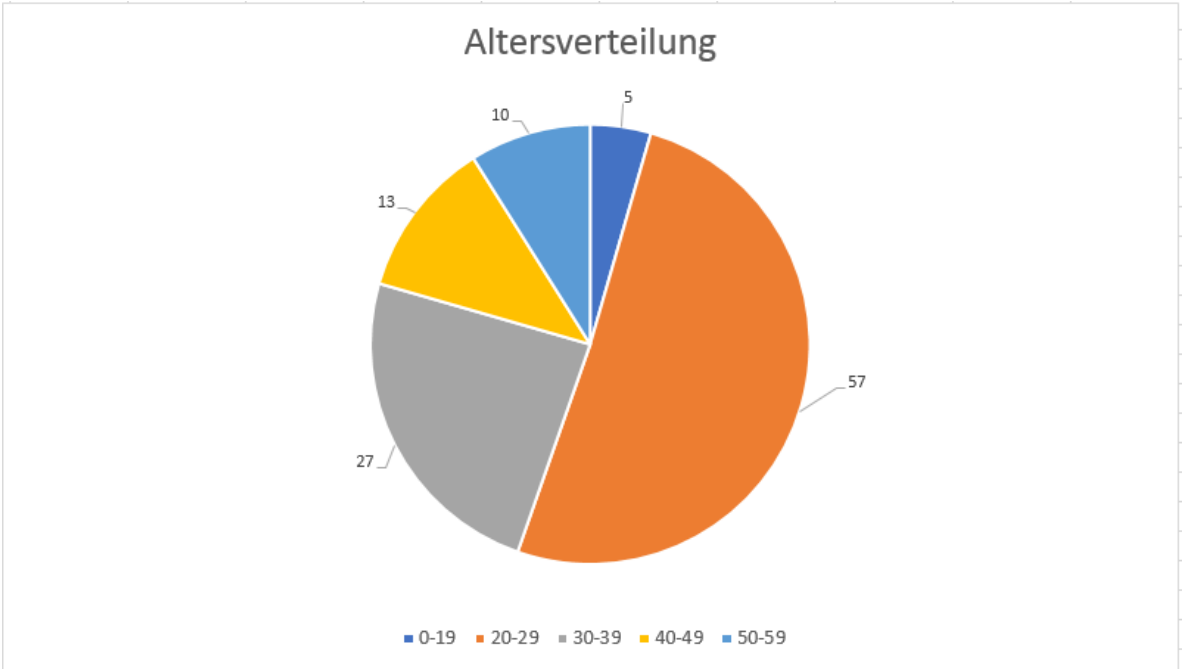

Abbildung 25:Altersverteilung (eigene Abbildung)

Auch die Verteilung der Berufsgruppen ist ungleichmäßig verteilt. Den größten Anteil der Teilnehmer sind in den Bereichen Informationstechnologie und Büro, Wirtschaft, Finanzweisen und Recht tätig. Nur für diese 2 Berufsfelder sind relevante Zusammenhänge interpretierbar und relevant, da für die anderen Berufsgruppen zu wenig Teilnehmer gefunden wurden. In Abbildung 25 ist gut erkenntlich, dass Teilnehmer verschiedensten Berufsfeldern gefunden wurden, jedoch nur die erwähnten Berufsfelder verdichtete Informationen lieferte.

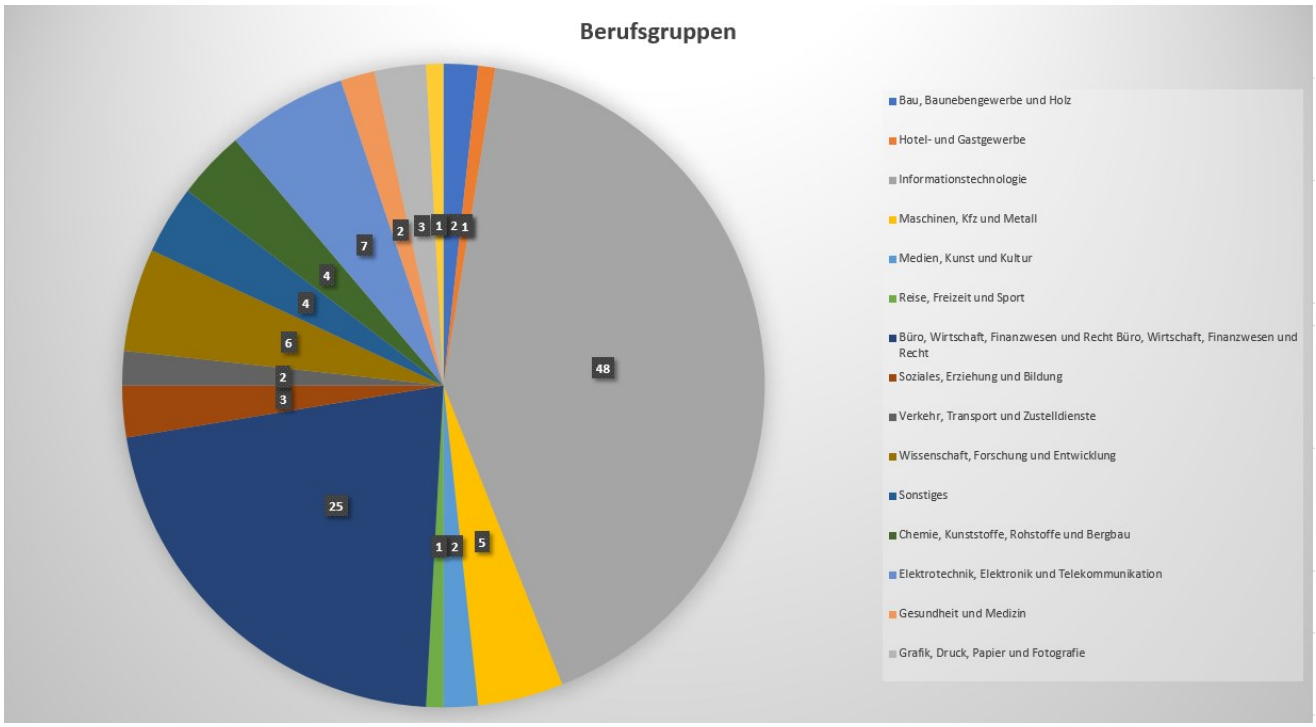

Abbildung 26:Berufsgruppen (eigene Abbildung)

Der Fragebogen hat weiters hauptsächlich Akademiker und Maturanten erreicht. Deshalb sind signifikante Zusammenhänge nur mit diesen 2 Ausbildungsgruppen relevant, da für die beiden genannten Ausbildungsgruppen eine ausreichend große Stichprobe gezogen werden konnte. Wie in Abbildung 27 ersichtlich, konnten wenige Personen erreicht werden, welche einen Lehrabschluss haben, eine Fachschule besucht haben oder die Pflichtschulausbildung als höchsten Ausbildungsgrad hatten.

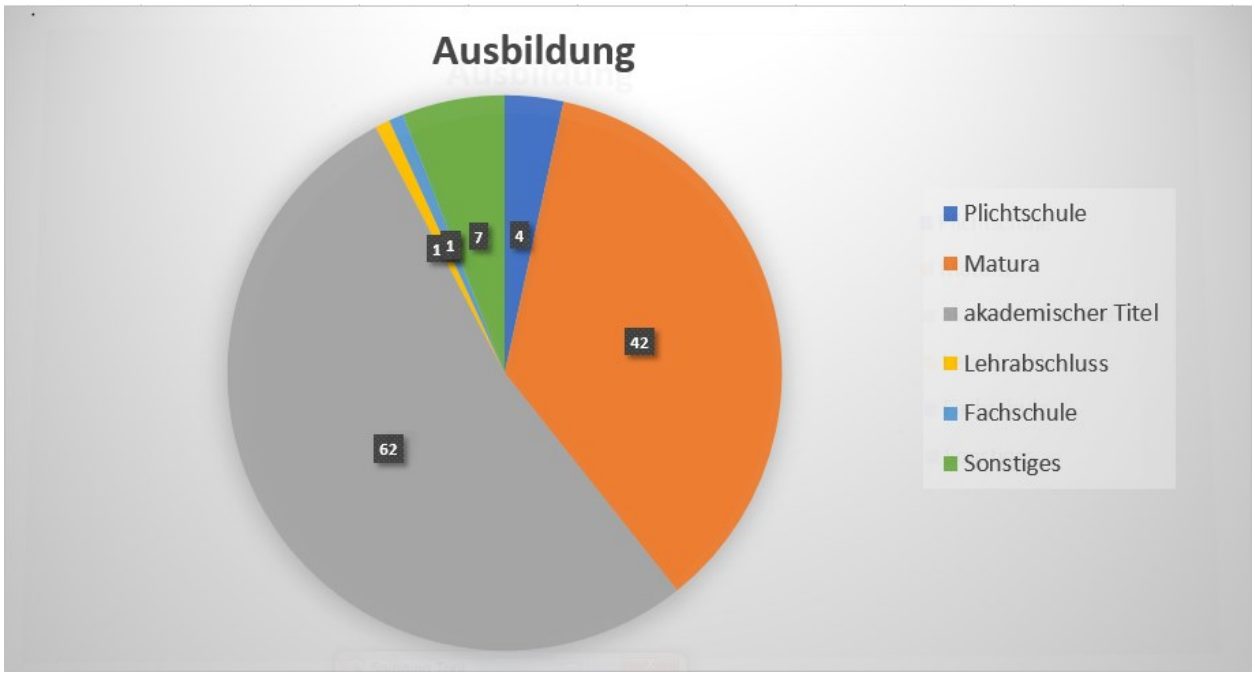

Abbildung 27: Ausbildung (eigene Abbildung)

9.2 Beantwortung der Forschungsfrage

In Kapitel 2 wurde das Ziel der Arbeit anhand folgender Forschungsfrage konkretisiert:

Aufgrund welcher Einflussgrößen der Userakzeptanz werden webbasierende SSO Lösungen der direkten Anmeldung über die jeweilige Webanmeldung vorgezogen?

Im Unterkapitel 9.1.1 wurden bereits die Erkenntnisse aus der Umfrage und der Fallstudie detailliert analysiert, welche als Basis zur Beantwortung der Forschungsfrage dienen.

Zusammenfassend aus Punkt 9.1.1 lässt sich sagen, dass die IT-Affinität und die Einstellung gegenüber einer Single Sign On Lösung die 2 Haupteinflussfaktoren auf die Benutzerakzeptanz von Single Sign On Lösungen sind.

Somit lässt sich sagen, wenn die Einstellung der Nutzer gegenüber Single Sign On sehr positiv ist und sie auch eine starke Vorliebe für Informationstechnologien besitzen, dann wird die Anmeldung über Single Sign On bevorzugt.

9.3 Überprüfung der Hypothesen

Nachfolgend werden die 4 gestellten Alternativhypothesen aus Kapitel 2.2 beantwortet. Die Beantwortung erfolgt auf Basis der Faktorenanalyse der Umfrage und der getätigten Analyse der Fallstudie.

9.3.1 Hypothese 1: Nullhypothese zutreffend bei Zusammenhang zwischen Sicherheitsbewusstsein und Benutzerakzeptanz

Die Evaluierung hat ergeben, dass folgende Nullhypothese zutreffend ist:

Das Sicherheitsbewusstsein wirkt sich nicht auf die Benutzerakzeptanz von Single Sign On Lösungen aus.

Zwischen dem allgemeinen Sicherheitsbewusstsein der Nutzer und der Benutzerakzeptanz konnte kein signifikanter Zusammenhang festgestellt werden. Tendenziell konnte jedoch der überraschende Effekt festgestellt werden, dass Personen, welche sicherheitsbewusster sind auch öfters Single Sign On Lösungen verwenden. Es wurden im Zuge der Umfrage Fragen zum allgemeinen Sicherheitsbewusstsein gestellt, sowie Fragen welche sich auf das Sicherheitsbewusstsein im Umgang mit Single Sign On Lösungen konzentrierten. Dabei stellte sich ein signifikanter Zusammenhang zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und der Benutzerakzeptanz heraus. Überraschenderweise brachte der signifikante Zusammenhang zwischen Sicherheitsbewusstsein im Kontext von Single Sign On und Benutzerakzeptanz, ein ähnliches Ergebnis wie der Zusammenhang zwischen Sicherheitsbewusstsein im Allgemeinen und Benutzerakzeptanz. Das Ergebnis, dass ein erhöhtes Sicherheitsbewusstsein einen positiven Einfluss auf die Benutzerakzeptanz hat, ist im Kontext von Single Sign On stärker ausgeprägt. Da jedoch, wie erwähnt, zwischen Sicherheitsbewusstsein im Allgemeinen und Benutzerakzeptanz kein signifikanter Effekt festgestellt worden konnte, ist die Nullhypothese zutreffend, dass zwischen Sicherheitsbewusstsein und Benutzerakzeptanz kein Zusammenhang besteht.

9.3.2 Hypothese 2: Nullhypothese zutreffend bei Zusammenhang zwischen Vertrauenswürdigkeit des Identity Provider und Benutzerakzeptanz

Lediglich bei einer Anmeldung von 8 Single Sign Anmeldungen wurde als Hauptgrund angegeben, dass die ausreichende Vertrauenswürdigkeit des Identity Providers ausschlaggebend war für die Entscheidung. Noch dazu haben Teilnehmer nur bei 8 von 48 Anmeldungen über Benutzername und Passwort angegeben, dass die unzureichende Vertrauenswürdigkeit des Identity Provider der Hauptgrund für die Entscheidung für die gewöhnliche Anmeldung war. Durch die Analyse der Fallstudie ergab sich, dass die Gewohnheit ein Anmeldeverfahren zu nutzen und sogar die Spontanität einen größeren Einfluss auf die Benutzerakzeptanz hatten. Anhand der empirischen Untersuchung in Form der Fallstudie konnte schlussendlich jedoch kein signifikanter Zusammenhang zwischen Wahl des Identity Provider und der Benutzerakzeptanz festgestellt werden.

9.3.3 Hypothese 3: Alternativhypothese zutreffend bei Zusammenhang zwischen IT-Affinität und Benutzerakzeptanz

Je höher die IT-Affinität der Nutzer ist, umso höher ist die Benutzerakzeptanz gegenüber Single Sign On Lösungen. Der statistisch signifikante Zusammenhang wurde durch die Faktorenanalyse mithilfe der bayesschen Statistik festgestellt. Weiterführend hat sich in den Gruppenanalysen ergeben, dass ein solch signifikanter Zusammenhang bei

- Frauen
- 30-40 Jährigen
- Akademiker
- Informationstechnologen

auftritt. Dieser Zusammenhang ist auch begründbar, da jene Personen, die von Single Sign On bereits gehört haben und den Umgang mit einer Single Sign On Lösung gewohnt sind, auch gewillter sind diese Lösung zu nutzen.

9.3.4 Hypothese 4: Alternativhypothese zutreffend bei Zusammenhang zwischen Einstellung und Benutzerakzeptanz

Je positiver ein Nutzer gegenüber Single Sign On eingestellt, umso höher ist die Akzeptanz und die Chance, dass der Nutzer selbiges Anmeldeverfahren verwendet. In den Gruppenanalysen wurde festgestellt, dass besonders für Männer eine positive Einstellung gegenüber einer Single Sign On Lösung essentiell ist, damit sie dieses Anmeldeverfahren nutzen und bedienen. Im Technology Acceptance Model in ihrer Grundform ist die Einstellung ein wichtiger Faktor, ob ein Nutzer eine Anwendung akzeptiert. Im Zuge dieser empirischen Untersuchung wurde die Annahme des theoretischen Konstrukts bestätigt.

9.4 Maßnahmenvorschläge für Unternehmen um die Benutzerakzeptanz von Single Sign On Lösungen zu steigern

Nachfolgend sind einige Vorschläge für Unternehmen angeführt, um die Benutzerakzeptanz von Single Sign On Lösungen bei den Nutzern zu steigern.

9.4.1 Schulungen über Single Sign On und deren verbundenen Sicherheitsrisiken

Den Mitarbeiter müssen die Sicherheitsrisiken von Single Sign On im privaten Bereich, sowie im beruflichen Bereich aufgezeigt werden. Da im beruflichen Bereich auf vertrauenswürdige Identity Provider wie Shibboleth oder Kerberos zurückgegriffen werden, muss dennoch argumentiert werden, wie die Technologie durch den Angriff vor Dritten gesichert wird und wie mit

personenbezogenen Daten bei der Übermittlung umgegangen wird. Aufgrund dieser expliziten Schulung sollte eine gute Vertrauensbasis zwischen der verwendeten Lösung im Unternehmen und dessen Nutzer geschaffen werden. Das solche Schulungen notwendig sind, hat auch die Umfrage ergeben. 72 von 117 Befragten gaben an, dass sie noch nie oder selten Schulungen über IT-Sicherheit erhalten haben. Das Ergebnis ist schockierend, da 61,5% der Befragten von Unternehmen nicht über die Sicherheitsrisiken informiert werden und auch nicht wissen, welche Pflichten sie selbst für die Risikovermeidung treffen müssen. Des Weiteren wurde von 31 der 117 Befragten bestätigt, dass das IT Sicherheitsbewusstsein der Kollegen niedrig sei. Um das Sicherheitsbewusstsein der Kollegen zu steigern, müssen Awareness Schulungen explizit durchgeführt werden.

9.4.2 Schulungen und Guidelines über die Verwendung der implementierten Single Sign On Lösung

Die IT-Affinität der Nutzer spielt eine große Rolle bei der Akzeptanz von Single Sign On Lösungen. Aus diesem Grund ist es wichtig, dass Unternehmen die Nutzer auf die benutzte Single Sign On Lösung einschulen und zusätzlich eine Dokumentation im Intranet bereitstellen, auf welche die Nutzer jederzeit zugreifen können. Auch wie simple eine Anwendung, wie im Falle einer Single Sign On Lösung sein mag, ist es trotzdem wichtig, den nicht so IT affinen Nutzern einen Einblick zu geben, wie diese Anwendung funktioniert. Ohne Schulung oder vorhandenen Guidelines würden nicht sehr IT affine Nutzer nie auf die Idee kommen, eine Single Sign On Lösung als Anmeldeverfahren zu nutzen, wenn alternativ ein gewöhnliches Authentifizierungsverfahren mittels Benutzername und Passwort zur Verfügung steht.

9.4.3 Schulungen über den Nutzen von Single Sign On

In der Umfrage ist hervorgegangen, dass die Befragten besonders folgende Vorteile an der Nutzung von Single Sign On sehen:

- Einfache Handhabung
- Zeitersparnis
- Wegfall von unzähligen Passwörter
- Geringer administrativer Aufwand

Diese Vorteile müssen auch den Nutzern veranschaulicht werden, um Bewusstsein zu schaffen, welche Vorteile eine Single Sign On Lösung gegenüber einer gewöhnlichen Anmeldung mittels Passwort und Benutzername hat. 25 von 117 Personen geben sogar an, noch nie vom Begriff Single Sign On gehört zu haben. Aus diesem Grund ist eine Schulung über Single Sign On selbst und den Nutzen von Single Sign On unerlässlich.

9.4.4 Verwendung von Single Sign On als einziges Authentifizierungsverfahren

Es wäre sehr ratsam unternehmensintern für alle Applikationen nur ein Authentifizierungsverfahren zu verwenden, damit die Akzeptanz des Authentifizierungsverfahrens gefördert wird. Der große Vorteil ist, wenn Single Sign On als Anmeldeverfahren verwendet wird, dass nur auf eine Benutzerdatenbank zugegriffen wird und Redundanzen vermieden werden. Natürlich wird man bei der Ablösung von einem gewöhnlichen Anmeldeverfahren mittels Benutzername und Passwort zu einer Single Sign On Lösung Schritt für Schritt vorgehen. Jedoch sollte schlussendlich das Ziel sein, dass die gesamte Anmeldelandschaft aus einer Single Sign On Lösung besteht. Das Vorhaben ist nicht immer einfach umzusetzen, da man teilweise auch auf externe Applikationsbetreiber angewiesen ist und aus diesem Grund sollten diese Partner auch in der Umstellungsphase miteingebunden werden.

9.4.5 Verwendung von Standards zur Gewährleistung von Informationssicherheit

Standards, wie die ISO 27001:2013 sind empfehlenswert, damit die Informationssicherheit im Unternehmen gewährleistet ist. Da die Vertraulichkeit zu einer der 3 Hauptziele von Informationssicherheit gehört und bei Verwendung von Single Sign On Lösungen im Unternehmen, die Vertraulichkeit gegeben werden sein muss, ist es ratsam, Maßnahmen aus dem ISO 27001:2013 Katalog im eigenen Unternehmen einzuführen. Die Benutzerakzeptanz der Nutzer wird dadurch gesteigert, da durch das Leben eines Informationssicherheitsmanagements im Unternehmen, auch das Sicherheitsbewusstsein der Mitarbeiter gesteigert wird und der konforme Umgang mit einer Single Sign On Lösung durch das Wissen von notwendigen Risiken im Kontext der Informationssicherheit gewährleistet wird. Aufgrund von neuen rechtlichen Auflagen und potenziellen neuen Risiken, ist es wichtig, dass Maßnahmen getroffen werden, mit denen sich auch die Mitarbeiter miteinander auseinandersetzen.

9.4.6 KPIs als Unterstützung um Benutzerakzeptanz der Nutzer gegenüber Single Sign On zu erhöhen

Folgende KPIs kann für die Geschäftsführung als Argumentationsbasis dienen, um die Akzeptanz von Single Sign On Lösungen unternehmensweit zu erhöhen:

- Monatliche Anzahl der Supportanfragen bezüglich Anmeldeprobleme
- Monatlicher Zeitaufwand für Bewältigung der Anfragen
- Anzahl der Probleme bei Systemanmeldungen pro Mitarbeiter
- Anzahl der zu merkenden Passwörter pro Mitarbeiter
- Anzahl der verwendeten Anwendungen
- Häufigkeit der Informationssicherheitsverletzungen durch Mitarbeiter

Laut Umfrage hatten nur 14 von 117 Personen oft Probleme bei Systemanmeldungen. Dahingegen hatten 75 Personen nie oder selten Probleme mit Systemanmeldungen. Dennoch muss individuell im Unternehmen eruiert werden, welchen Anteil von Systemproblemen auf die Authentifizierung anfallen. Ist der Anteil sehr hoch, würde das als gute Basis dienen, warum Single Sign On im Unternehmen eingeführt werden sollte.

In der Umfrage mussten die Teilnehmer auch angegeben, wie viele Passwörter sie sich im beruflichen Umfeld merken müssen. Lediglich 34 von 117 Personen gaben an, dass sie sich mehr als 5 Passwörter in der Arbeit merken müssen. Obwohl sich nur 29% der Teilnehmer mehr als 5 Passwörter in der Arbeit merken müssen, ist das ein Hauptgrund warum Single Sign On im Unternehmen in Einsatz kommen kann. Aus Erfahrungen heraus, kann eine einzelne Person durch unsorgfältige Aufbewahrung von Passwörter ein hohes Unternehmensrisiko darstellen. Aus diesem Grund, ist eine Risikoanalyse und Risikobewertung essentiell, um dieses Risiko passend im eigenen Unternehmen einschätzen zu gehen und Gegenmaßnahmen planen zu können. Ist die Gefahr groß, dass im eigenen Unternehmen Verletzungen gegenüber der Informationssicherheit entstehen, wäre das ein weiterer Punkt weshalb eine Single Sign On Lösung im Unternehmen eingeführt werden sollte.

9.4.7 Nutzung von Server-Cluster Technologie, um Single Point of Failure zu vermeiden

Bei den Anmeldungen der User muss eine Verbindung zum Server aufgebaut werden, welche den Authentifizierungsdienst betreibt. Würde der Server ausfallen, dann könnte sich der Nutzer bei keiner Applikation mehr anmelden. Aus diesem Grund sollte durch eine Server-Cluster Technologie gewährleistet werden, dass die Applikation am Server immer betrieben werden kann. Durch die Server-Cluster Technologie wird sichergestellt, dass bei Ausfall eines Servers, ein anderer Server aktiv wird und eine duplizierte Applikation ausgeführt wird, damit sich der Nutzer weiterhin anmelden kann.

9.5 Maßnahmenvorschläge, wie die Benutzerakzeptanz von Single Sign On Lösungen im privaten Umfeld erhöht werden kann

Wie aus der Fallstudie herausgeht, wird Single Sign On nicht sehr oft für private Zwecke genutzt. Lediglich 8 Mal wurde Single Sign On als Anmeldeverfahren genutzt, wobei 6 Anmeldungen über Single Sign On bereits vor der Durchführung der Fallstudie getätigt wurden. Identity Provider, wie Facebook und Google müssen daher ein paar Maßnahmen treffen, damit Single Sign On bei den Nutzern besser akzeptiert wird und somit öfters genutzt wird.

9.5.1 Identity Provider übermitteln nur für die Authentifizierung notwendigen benutzerbezogenen Daten

Leider übermitteln Identity Provider, wie Facebook oder Google nicht nur Authentifizierungsdaten der Nutzer an den Service Provider, sondern auch personenbezogene Daten, wie Name, Geburtsdatum und Wohnort. Das führt bei den potenziellen Nutzern zu Unmut, da mehr Daten für den Anmeldeprozess verarbeitet werden, als für den Authentifizierungsvorgang benötigt werden. Noch dazu birgt das bei einer Privatperson ein erhöhtes Schadensausmaß, wenn die Daten in die Finger von Dritten gelangen. Die genannten Identity Provider befinden sich aufgrund der personenbezogenen Datenübermittlung in einer rechtlichen Grauzone. Damit personenbezogene Daten, nicht über ihren eigentlichen Zweck und Nutzen verwendet werden, müssen trotz Einwilligungserklärung des Nutzers rechtliche Konsequenzen etabliert werden. Zurzeit sieht das Datenschutzgesetz und das Telemediengesetz keine Sanktionen, da der Nutzer von Facebook und Google um die Einwilligung von personenbezogenen Daten vor der Übermittlung gebeten wird. Dennoch ist in der beigefügten Datenschutzerklärung oft nicht sichtbar, welche personenbezogenen Daten konkret übermittelt werden. Als erster Schritt sollte die Datenschutzerklärung über alle übermittelten Daten im Zuge der Authentifizierung informieren und von Identity Provider nur jene Daten übermittelt werden, die für die Authentifizierung benötigt werden. Damit ist gewährleistet, dass eine bessere Vertrauensbasis zwischen Nutzer, Applikationsbetreiber und Identity Provider geschaffen wird.

9.5.2 Applikationsbetreiber übermitteln keine Daten an Identity Provider

Applikationsbetreiber können Aktionsdaten von Nutzern an Identity Provider, wie Facebook und Google übermitteln. Somit hat der Identity Provider die Möglichkeit, mehr Informationen über den Nutzer zu erfahren und diese Daten an Dritte weiterzuverkaufen. Das ist ein weiterer Punkt, welche die Vertrauensbasis zwischen Nutzer und Applikationsbetreiber mit Single Sign On Lösungen hemmt. Applikationsbetreiber sind daher angehalten, keine Nutzungsdaten an Identity Provider weiterzugeben, damit das Vertrauen zwischen Nutzer und Applikationsbetreiber gestärkt wird.

9.5.3 Einführung von Zertifikaten für vertrauenswürdige Single Sign On Anbieter

Für vertrauenswürdige Single Sign On Anbieter könnte von einer unabhängigen Zertifizierungsstelle ein Zertifikat ausgestellt werden, damit Applikationsbetreiber keine Bedenken haben müssen, Single Sign On in ihren Anwendungen zu implementieren. Die Zertifizierungsstelle könnte folgende Kriterien für ihre Bewertung heranziehen:

- Übermittlung von personenbezogenen Daten
- Potenzielle Gefahr durch Angriff von Dritten
- Datenschutzerklärung des Identity Provider

- Implementierungsdokumentation
- Verwendung von Authentifizierungsstandards wie SAML oder Open ID

Somit sollten möglichst alle Risiken abgedeckt werden, welche potenzielle bei Verwendung einer Single Sign On Lösung auftreten können.

9.5.4 Mehrere Applikationsbetreiber müssen Single Sign On Lösungen anbieten

Viele mobile Applikationen bieten bereits den Nutzern die Möglichkeit an, sich über Single Sign On anzumelden. Dennoch gibt es auch einige Apps, welche die komfortable Anmeldemöglichkeit noch nicht anbieten. Um die Akzeptanz bei den Nutzern zu steigern, muss die Implementierung des Authentifizierungsverfahren vorangetrieben werden. In reinen Webapplikationen findet man dieses Anmeldeverfahren noch selten an. Dort überwiegen die Authentifizierungsverfahren mittels Benutzername und Passwort. Auch hier müssen Applikationsbetreiber die Implementierung vorantreiben, damit das Anmeldeverfahren jedem Nutzer geläufig wird und damit sie sich auch für das Anmeldeverfahren entscheiden können.

9.6 Ausblick

Die Umfrage und auch die Fallstudie hat ergeben, dass das 100% Vertrauen der Nutzer eine Single Sign On Lösungen noch nicht gegeben ist. Einige wissen über Single Sign On und dessen Nutzen kaum Bescheid, andere sehen Sicherheitsbedenken diese Technologie zu verwenden. Weiter Nutzer verwenden aus Gewohnheit die herkömmliche Anmeldevariante mittels Benutzername und Passwort. Um die Unwissenheit, die Bedenken und den Gewohnheitstrotz entgegenzuwirken wurden in den Kapiteln 9.4 und 9.5 Maßnahmen vorgeschlagen, welche Unternehmen nutzen können, um die Benutzerakzeptanz von Nutzern gegenüber Single Sign On zu verbessern.

Diese Arbeit sollte Unternehmen einen Einblick geben, welche Single Sign On Lösungen zurzeit populär und weitverbreitet sind. Es wurde das Technology Acceptance Model 3 angewandt, um Faktoren zu ermitteln, die für die Analyse der Benutzerakzeptanz in Betracht kommen. Da die Sicherheit bei einem Anmeldeverfahren sehr hoch sein muss, wurde im Kapitel 7 auf die Informationssicherheit und im speziellen auf das Informationssicherheitsmanagement in Unternehmen eingegangen. Schlussendlich sollte durch die empirische Untersuchung die Probleme bezüglich Benutzerakzeptanz aufgezeigt werden, welche Unternehmen konfrontiert sind, wenn eine Single Sign On Lösung im Unternehmen eingeführt wird.

Diese Arbeit kann für weitere wissenschaftlichen Arbeiten als Basis dienen, um meine aufgestellten Hypothesen zu prüfen. Da meine gezogene Stichprobe bei Durchführung der Umfrage nicht 100% repräsentativ zur Grundgesamtheit war, könnte eine weitere Umfrage erstellt werden, wo die Repräsentativität zu 100% gegeben ist. Weiterführend können noch

Experteninterviews eingeholt werden, um die validen Aussagen aus der empirischen Untersuchung zu stärken.

Weiterführend kann diese Arbeit als Referenzwerk für folgende Themenbereiche dienen:

- Authentifizierungsdienste
- Benutzerakzeptanzanalysen von diversen Technologien
- Informationssicherheit
- Sicherheitsbewusstseinsanalysen bei Nutzer

Es ist zu erwarten, dass es in Zukunft noch weitere wissenschaftliche Arbeiten über Single Sign On geben wird, da durch das vermehrte Nutzen von sozialen Netzwerken, Cloud und Servicelösungen in Unternehmen, auch ein einfach zu nutzendes Authentifizierungsverfahren für die Nutzer zur Verfügung stehen muss. Abrundend endet somit diese Masterabeit mit den Worten des Botanikers Herman Boerhaave:

Das Siegel der Wahrheit ist die Einfachheit

(Herman Boerhaave 1668-1738)

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

LITERATURVERZEICHNIS

1&1 (2016): XSS/Cross-Site-Scripting unterbinden und Sicherheitslücken schließen. Hg. v. 1&1. Online verfügbar unter https://www.1und1.at/digitalguide/websites/web-entwicklung/was-ist-xss-bzw-cross-site-scripting/.

Academic (2017): Single Sign On. Online verfügbar unter http://partners.academic.ru/dic.nsf/dewiki/1292227.

AGNIESZKA CZERNIK (2016): Single Sign-on: Tipps beim Einsatz der Login-Technologie. Hg. v. Datenschutzbeauftragter Info. Online verfügbar unter https://www.datenschutzbeauftragter-info.de/single-sign-on-tipps-beim-einsatz-der-login-technologie/.

Airbnb (2018): Buche individuelle Unterkünfte und Entdeckungen überall auf der Welt. Hg. v. airbnb.at. Online verfügbar unter https://www.airbnb.at/.

Andreas Neumann (2017): Register easily and securely via Facebook, Twitter, & Other Sites. Online verfügbar unter http://www.ic-consult.com/en-US/social-media-login.html.

Andrew Hindle (2014): ACCESS CONTROL. Online verfügbar unter https://www.axiomatics.com/blog/authentication-vs-authorization-part-1-federated-authentication-2/.

Bepeach.com (2018): Auf Bepach online nach verfügbarem Personal suchen. Hg. v. Bepeach.com. Online verfügbar unter https://bepach.com/arbeitskraftsuche.

Bitium (2017): Media Solutions (Formerly ValueClickMedia) Single Sign-On (SSO) Powered by Bitium. Hg. v. Bitium. Online verfügbar unter https://www.bitium.com/valueclickmedia-single-sign-on-sso-provider.

Borges, G.; Schwenk, J.; Stuckenberg, C. F.; Wegener, C. (2011): Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte: Springer Berlin Heidelberg. Online verfügbar unter https://books.google.at/books?id=suMfBAAAQBAJ.

Boyd, Ryan (2012): Getting Started with OAuth 2.0. [programming clients for secure web API authrorization and authentication]. Sebastopol, Calif.: O'Reilly (Safari Tech Books Online). Online verfügbar unter http://proquest.safaribooksonline.com/9781449317843.

Bundeskanzleramt Österreich (2017): Österreichisches Informationssicherheitshandbuch. Online verfügbar unter https://www.sicherheitshandbuch.gv.at/siha.php.

Canor Cahill (2008): Liberty Alliance Web Services Framework. A Technical Overview Version 1.0. Unter Mitarbeit von Carolina Canles, Hubert A. Le Van Gong, Paul Madsen, Eve Maler,

Greg Whitehead. Hg. v. Intel. Washington. Online verfügbar unter http://xml.coverpages.org/LibertyWebServices-TechOverview2008.pdf.

Capec (2017a): WSDL Scanning. Online verfügbar unter https://capec.mitre.org/data/definitions/95.html.

Capec (2017b): XML Schema Poisoning. Hg. v. Capec. Online verfügbar unter https://capec.mitre.org/data/definitions/146.html.

Carol Geyer (2007): Assertions. Online verfügbar unter http://saml.xml.org/assertions.

Chelsea Goforth (2015): Using and Interpreting Cronbach's Alpha. Hg. v. University of Virginia Library. Online verfügbar unter http://data.library.virginia.edu/using-and-interpreting-cronbachs-alpha/.

Christian Reinboth (2017): Grundlagen der Statistik: Der Satz von Bayes. Online verfügbar unter http://wissenschafts-thurm.de/grundlagen-der-statistik-der-satz-von-bayes/.

Christopher Perry (2016): 3 Things I Wish Everyone Knew about Web Single Sign On. Online verfügbar unter https://www.portalguard.com/blog/2016/12/02/3-things-web-single-sign-on/.

Connect2Id (2017): OpenID Connect UserInfo endpoint. Online verfügbar unter https://connect2id.com/products/server/docs/api/userinfo.

Cornelia Brinks (2015): „Facebook Login" – Was sagt der Datenschutz zum Single Sign On? Online verfügbar unter https://www.datenschutz-notizen.de/facebook-login-was-sagt-der-datenschutz-zum-single-sign-on-2710695/.

Cryptas (2017): Single Sign On System- SSO. Online verfügbar unter https://www.cryptas.com/cryptas/wissen-unterstuetzung/authentisierung/single-sign-on.html.

Daniel Bachfeld (2009): Schutz vor Attaken durch Cross-Site-Request-Forgery ausgehebelt. Online verfügbar unter https://www.heise.de/security/meldung/Schutz-vor-Attacken-durch-Cross-Site-Request-Forgery-ausgehebelt-6769.html.

Daniel Baumann (2006): Was bewirkt IT im Unternehmen? Methoden und Empirischer Nachweis zur Bestimmung des IT-Nutzens (WKOE:06WI) WS des Jahres 2006. Online verfügbar unter http://www.wi-frankfurt.de/veranstaltungen/referatliste.php?vernr=480.

DGO (2017): Datenschutz und Informationssicherheitsmanagement. Online verfügbar unter https://shop.dgq.de/themen/weiterbildung-datenschutz-und-informationssicherheitsmanagement.

Douglas K Barry (2017): Service-Oriented Architecture. Hg. v. Service Architecture. Online verfügbar unter http://www.service-architecture.com/articles/web-services/service-oriented_architecture_soa_definition.html.

Gerhard Funk (2016): Implementierungsleitfaden ISO/IEC 27001:2013. Hg. v. ISACA Germany Chapter e.V. Online verfügbar unter https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/isaca_leitfaden_i_gesamt_web.pdf.

Google Play Store (2018a): Pinterest. Online verfügbar unter https://play.google.com/store/apps/details?id=com.pinterest&hl=de.

Google Play Store (2018b): Quizduell. Online verfügbar unter https://play.google.com/store/apps/details?id=se.feomedia.quizkampen.de.lite&hl=de.

Google Play Store (2018c): Tinder. Online verfügbar unter https://play.google.com/store/apps/details?id=com.tinder&hl=de.

Hal Lockahrt (2008): Security Assertion Markup Language (SAML) V2.0 Technical Overview. Unter Mitarbeit von Brian Campbell, Nick Ragouzis, John Hughes, Rob Philpott, Eve Maier, Paul Madsen, Tom Savco. Online verfügbar unter http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

Hannes Federrath (2015): SMT Informationssicherheitsmanagement. Online verfügbar unter https://svs.informatik.uni-hamburg.de/teaching/smt-30secmgmt.pdf.

Herman Boerhaave (1668-1738): Herman Boerhaave. Leiden.

IBM (2017): SAML 2.0 bindings. Online verfügbar unter https://www.ibm.com/support/knowledgecenter/en/SSPREK_9.0.0/com.ibm.isam.doc/config/concept/fed_SAML20_bindings.html.

Insights For Professionals (Hg.) (2017): Das Phänomen ,,Passwörter auf Post-its" stoppen. Online verfügbar unter https://www.insightsforprofessionals.com/blog/das-phanomen-passworter-auf-post-its-stoppen.

ITWissen.info (2017): Replay-Angriff. Hg. v. ITWissen.info. Online verfügbar unter http://www.itwissen.info/Replay-Angriff-replay-attack.html.

Ivan Koswara (2017): Simpson's Paradox. Online verfügbar unter https://brilliant.org/wiki/simpsons-paradox/.

Jed Breinholt (2017): Google Authentification as SAML Ipd. Canvas. Online verfügbar unter Jed Breinholt.

John Carl Villanueva (2014): 5 Big Business Benefits of Using SSO (Single Sign-On). Hg. v. JSCAPE. Central Visayas. Online verfügbar unter http://www.jscape.com/blog/bid/104856/5-Big-Business-Benefits-of-Using-SSO-Single-Sign-On, zuletzt aktualisiert am 01.02.2014.

Konfuzius: Konfuzius. 551 v. Chr.

Kristin Vogelsang, Melanie Steinhueser, Uwe Hoppe (2013): Theorieentwicklung in der Akzeptanzforschung: Entwicklung eines Modells auf Basis einer qualitativen Studie. Uni Osnabrück, Osnabrück. Institut für Organisation und Wirtschaftsinformatik. Online verfügbar unter http://www.wi2013.de/proceedings/WI2013%20-%20Track%2010%20-%20Vogelsang.pdf.

La Parisien (2017): Single Sign On. Hg. v. La Parisien. Online verfügbar unter http://dictionnaire.sensagent.leparisien.fr/Single%20Sign-on/de-de/#Medienl.C3.B6sung.

Langer, S. (2016): Sicherheit von passwortbasierten Authentifizierungssystemen: Diplom.de. Online verfügbar unter https://books.google.at/books?id=yq3PDAAAQBAJ.

Ledesma, Rubén Daniel; Valero-Mora, Pedro; Macbeth, Guillermo (2015): The Scree Test and the Number of Factors. A Dynamic Graphics Approach. In: *The Spanish journal of psychology* 18, E11. DOI: 10.1017/sjp.2015.13.

Margaret Rouse (2010): authentification, authorization, and accounting. Hg. v. Tech Target. Online verfügbar unter http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting.

Matthew Davis (2013): The Pros And Cons Of Single Sign-On For Web Services. Hg. v. Future Hosting. Online verfügbar unter https://www.futurehosting.com/blog/the-pros-and-cons-of-single-sign-on-for-web-services/.

Michael Kain (2017): SAML 2.0, ein Tutorium - Teil1: Theorie. Unter Mitarbeit von Guido Keller. Online verfügbar unter https://www.acando.de/fileadmin/redaktion/news/2016/publikationen/kain_keller_js_05_07.pdf.

Michael Strecker (2010): Potenzial von Single Sign-on bei Webapplikationen. Fachhochschule Kufstein, Kufstein.

Michel Smidt (2016): Kurz erklärt: Einmalige Anmeldung per Single Sign-on. Hg. v. Univention. Online verfügbar unter https://www.univention.de/2016/12/einmalige-anmeldung-per-single-sign-on/.

Mike Decrescenzo (2014): Is Single Sign On (SSO) secure? Online verfügbar unter https://www.tools4ever.com/blog/2014/is-single-sign-on-sso-secure/.

Mike Meredith, John Kruschke (2016): Package ‘HDInterval’. Hg. v. WCS Org. Online verfügbar unter https://cran.r-project.org/web/packages/HDInterval/HDInterval.pdf.

Misra, S.; Misra, S. C.; Woungang, I. (2010): Selected Topics in Communication Networks and Distributed Systems: World Scientific. Online verfügbar unter https://books.google.at/books?id=BbtpDQAAQBAJ.

Nate Klingenstein (2017): FlowsAndConfig. Unter Mitarbeit von Scott Cantor. Hg. v. Snibboleth Wiki. Online verfügbar unter https://wiki.shibboleth.net/confluence/display/CONCEPT/FlowsAndConfig.

Nicola Döring (2017): Bayes-Statistik. Hg. v. Markus Antonius Wirtz. Online verfügbar unter https://m.portal.hogrefe.com/dorsch/bayes-statistik/.

OASIS (2017): SAML 2.1. Hg. v. OASIS. Online verfügbar unter https://wiki.oasis-open.org/security/SAML21.

OAuth.com (2017): Refreshing Access Tokens. Hg. v. Okta. Online verfügbar unter https://www.oauth.com/oauth2-servers/access-tokens/refreshing-access-tokens/.

Oliver Wege (2014): Informationssicherheit. Online verfügbar unter http://www.secupedia.info/wiki/Informationssicherheit.

OpenGroup (2010): Single Sign-On. Hg. v. Open Group. Online verfügbar unter http://www.opengroup.org/security/sso/.

Oracle (2017): Liberty Alliance Project. Online verfügbar unter https://docs.oracle.com/cd/E19462-01/819-4674/admaq/index.html.

Pearson (2017): The Open Group Professional Certifications. Online verfügbar unter http://www.pearsonvue.com/theopengroup/.

Priyanke Surendran: Technology Acceptance Model: A Survey of Literature, S. 175–178.

Pröhl, Mark (2011): Kerberos. Single Sign-on in gemischten Linux/Windows-Umgebungen. 1. Aufl. Heidelberg: dpunkt.verlag. Online verfügbar unter http://ebooks.ciando.com/book/index.cfm/bok_id/328124.

Prowse, D. L. (2014): CompTIA Security+ SY0-401 Cert Guide, Academic Edition: Pearson Education. Online verfügbar unter https://books.google.at/books?id=cd9vBAAAQBAJ.

R Documentation (2017): Exploratory Factor analysis using MinRes (minimum residual) as well as EFA by Principal Axis, Weighted Least Squares or Maximum Likelihood. Online verfügbar unter https://personality-project.org/r/html/fa.html.

Rich Salz (2005): Sorting out Web services security standards. Hg. v. Computerworld. Online verfügbar unter http://www.computerworld.com/article/2568185/security0/sorting-out-web-services-security-standards.html.

Romain Péchayre (2015): The single sign out problem. Online verfügbar unter http://romain.pechayre.me/blog/2015/06/26/single-sign-out-problem/.

Runtastic (2018): Runtastic.com - Deine Health- und Fitness Community. Online verfügbar unter https://www.runtastic.com/de/.

Sadiq, Shazia (2016): SAML Security Model for RESTful Web Services. 1. Auflage, neue Ausgabe. Saarbrücken: LAP LAMBERT Academic Publishing.

Sandro Wefel (2012): User Acceptance of Token based Authentificatzion by Single Sign-On. Unter Mitarbeit von Paul Molitor. Hg. v. Research Gate. Online verfügbar unter https://www.researchgate.net/publication/232760840_User_Acceptance_of_Token_based_Authentication_by_Single_Sign-On.

Scott Brady (2017): OpenID Connect Flows. Hg. v. Scott Brady. Online verfügbar unter https://www.scottbrady91.com/OpenID-Connect/OpenID-Connect-Flows.

Scott Cantor (2012): NativeSPCookieUsage. Unter Mitarbeit von Scott Cantor. Hg. v. Shibboleth Wiki. Online verfügbar unter https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPCookieUsage.

Search Security (2017): OpenID (OpenID Connect). Online verfügbar unter http://www.searchsecurity.de/definition/OpenID-OpenID-Connect.

Shibboleth (2017): Shibboleth Consortium. Online verfügbar unter https://www.shibboleth.net/.

Shivakumar, S. K. (2016): A Complete Guide to Portals and User Experience Platforms: CRC Press. Online verfügbar unter https://books.google.at/books?id=Y6CmCwAAQBAJ.

shpock.com (2018): FAQ bei Shpock – die Flohmarkt App für schöne Dinge. Online verfügbar unter https://www.shpock.com/faq/.

Shu-Hsung Chang, Chien-Hsiang Chou, Jiann-Min Yang: The literature review of Technology Acceptance Model: A Study of the bibliometric distributions, S. 1634–1640. Online verfügbar unter http://www.pacis-net.org/file/2010/P01-13.pdf.

Socialcast (2017): Single Sign On (SSO). Online verfügbar unter http://developers.socialcast.com/community-administrator-documentation/admin/single-sign-on/.

Stefan Egeler (2014): Awareness-Fragebogen für Unternehmen. Unter Mitarbeit von Maxim Vinokurov Daniel Pandzic. Hg. v. eicar.org. Online verfügbar unter http://www.eicar.org/files/awareness-fragebogen_unternehmen.pdf.

survio.com (2018): Sportverhalten, Selbstmitgefühl und Risikoneigung. Online verfügbar unter survio.com.

Team Twago (2014): Die Top 12 Webseiten um Programmieren zu lernen. twago. Online verfügbar unter https://www.motocms.com/blog/de/webdesigner-werden-kostenlose-webdesigner-ausbildung/.

TechChannel (2017): Sicherheit bei Web Services. Online verfügbar unter https://www.tecchannel.de/a/sicherheit-bei-web-services,479383.

Thomas Birken (2014): IT-basierte Innovation als Implementationsproblem. Hg. v. ISF München. München. Online verfügbar unter http://www.isf-muenchen.de/pdf/Birken_2014_IT-basierte_Innovation_als_Implementationsproblem.pdf.

Todd Fredrich (2017): What Is REST? Online verfügbar unter http://www.restapitutorial.com/lessons/whatisrest.html.

Tom Loredo (2014): Bayesian Computation: Posterior Sampling & MCMC. Hg. v. Cosmic Populations (http://astrostatistics.psu.edu/su14/lectures/CosPop14-2-2-BayesComp-2.pdf).

Torsten Lodderstedt (2014): Open ID Connect: Login mit OAuth, Teil1. Online verfügbar unter https://www.heise.de/developer/artikel/OpenID-Connect-Login-mit-OAuth-Teil-1-Grundlagen-2218446.html?seite=all.

Uni Hildesheim (2017): Technologie Acceptance Model. Hg. v. Uni Hildesheim. Online verfügbar unter http://cookiis.iis.uni-hildesheim.de/node/16.

Viswanath Venkatesh, Hillol Bala: Technology Acceptance Model 3 and a Research Agenda on Interventions, S. 279–304. Online verfügbar unter https://ai2-s2-pdfs.s3.amazonaws.com/d112/d71f9dcd74cf1a44df50dee44bc48c6a9217.pdf.

Viswanath Venkatesh, Fred D. Davis: A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies, S. 187–204. Online verfügbar unter https://s3.amazonaws.com/academia.edu.documents/42921312/20002_MS_Venkatesh_Davis_ext_TAM_NO.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1513622106&Signature=S1i9SHG3HPF6jzvffWQZlwLhoX0%3D&response-content-disposition=inline%3B%20filename%3DA_Theoretical_Extension_of_the_Technolog.pdf.

Volker Tresp (2011): Frequentistische Statistik und Bayessche Statistik. Online verfügbar unter http://www.dbs.ifi.lmu.de/Lehre/MaschLernen/SS2011/folien/FrequentistenBayesianer2011.pdf.

W3School (2017a): SQL Injection. Online verfügbar unter https://www.w3schools.com/sql/sql_injection.asp.

W3School (2017b): WSDL Documents. Online verfügbar unter https://www.w3schools.com/xml/xml_wsdl.asp.

W3School (2017c): XML Web Services. Online verfügbar unter https://www.w3schools.com/xml/xml_services.asp.

wogibtswas.at (2018): wogibtswas.at. Online verfügbar unter https://www.wogibtswas.at/.

Wotan Monitoring (2017): DIE SCHUTZZIELE DER INFORMATIONSSICHERHEIT UND IT: „VERFÜGBARKEIT, INTEGRITÄT UND VERTRAULICHKEIT“. Online verfügbar unter

https://wotan-monitoring.com/de/news/news-detail/die-schutzziele-der-informationssicherheit-verfuegbarkeit-integritaet-und-vertraulichkeit.html.

Yammer (2017): OAuth 2: Server & Client-Side Flow. Hg. v. Yammer. Online verfügbar unter https://developer.yammer.com/docs/oauth-2.

ANHANG A - 1. ANHANG

Gruppe	Faktor	Frage
A	IT-Affinität & Einstellung zu Computer	Wie viel Stunden am Tag verwenden Sie einen Computer?
A	IT-Affinität & Einstellung zu Computer	Lieben Sie es mit dem Computer zu arbeiten, da Sie mit Unterstützung des Computers Probleme lösen können, neue Informationen verarbeiten dürfen und sich neue Dinge aneignen können? (1 = trifft nicht zu, 5 = trifft völlig zu)
C	Single Sign On Erfahrung	Wie oft haben Sie bislang vom Begriff Single Sign On gehört?
C	Single Sign On Erfahrung	Wie oft melden Sie sich über Single Sign On an?
C	Single Sign On Erfahrung	Mit welchen Anbietern haben Sie sich schon mal über Single Sign On angemeldet? (Mehrfachauswahl möglich)
C	Single Sign On Erfahrung	Ist Single Sign On in ihrem Unternehmen im Einsatz? Sprich, melden Sie sich bei allen Applikationen gleichzeitig an?
D	Einstellung zu Single Sign On	Würden Sie sich wünschen, dass bei mehreren Applikationen die Anmeldung über Single Sign On erfolgt?
D	Einstellung zu Single Sign On	Ist aus Nutzersicht die Anmeldung über einer Single Sign On Lösung wie Facebook Connect einfach durchzuführen?
D	Einstellung zu Single Sign On	Hatten Sie schon das Problem, dass die Anmeldung bei einer Applikation nur über Single Sign On erfolgt werden konnte? (1 = nie, 5 = sehr oft)
D	Einstellung zu Single Sign On	Wenn der Zugriff auf eine gewünschte Applikation nur über eine Single Sign On Lösung erfolgen kann und Sie sich bei dem unbekannten Identity Provider noch nicht registriert haben, würden Sie daraufhin die Registrierung durchführen?
D	Einstellung zu Single Sign On	Bitte bewerten Sie die Vorteile von Single Sign On Lösungen! (1 = sehr kleiner Nutzen, 5 = sehr großer Nutzen)
E	Probleme mit Anmeldungen	Wie viele Passwörter müssen Sie sich in der Arbeit merken?
E	Probleme mit Anmeldungen	Wie oft hatten Sie schon Probleme mit Systemanmeldungen in Ihrer Firma?
E	Probleme mit Anmeldungen	Wie oft stellen Sie in der Firma an den Help Desk oder an den IT Support Anfragen bezüglich Anmeldeprobleme? (1=nie, 5= sehr oft)
E	Probleme mit Anmeldungen	Werden Sie von den Help-Desk Mitarbeitern bezüglich Ihre Anmeldeprobleme zufriedenstellend unterstützt?
F	Sicherheit im Unternehmen	Wie oft hatten Sie schon Schulungen über IT-Sicherheit in Ihrem Unternehmen? (1=nie, 5=sehr oft)
F	Sicherheit im Unternehmen	Wie würden Sie das Sicherheitsbewusstsein der Mitarbeiter in Ihrem Unternehmen einschätzen?
F	Sicherheit im Unternehmen	Wie schätzen Sie die IT-Sicherheit in Ihrem Unternehmen im Allgemeinen ein? (1=niedrig, 5 = sehr hoch)
G	Sicherheitsbewusstsein im Allgemeinen	*Ich überprüfe beim Online Banking vor der Eingabe von Kontonummer und PIN immer das Adressfeld des Browsers*
G	Sicherheitsbewusstsein im Allgemeinen	*Ich antworte nicht auf per EMail zugeschickte Forderungen meiner Bank zur Herausgabe persönlicher Transaktionsdaten und benutze ebenfalls keine Software, die mir meine Bank per EMail zugeschickt hat*

Gruppe	Faktor	Frage
G	Sicherheitsbewusstsein im Allgemeinen	*Ich habe die automatische Update-Funktion meines Betriebssystems aktiviert bzw. überprüfe selbst regelmäßig, ob neue Sicherheitspatches für von mir benutzte Computerprogramme vorliegen*
G	Sicherheitsbewusstsein im Allgemeinen	*Ich verlasse meinen Arbeitsplatz auch bei kurzer Abwesenheit immer so, dass keinesensiblen Daten abrufbar sind (passwortgeschützter Screensaver, Schränke abgesperrt,Büro abgesperrt).*
G	Sicherheitsbewusstsein im Allgemeinen	*Ich weiß, wie in meinem Unternehmen sensible Daten und Texte behandelt werden, und kann zu dieser Frage einiges sagen.*
G	Sicherheitsbewusstsein im Allgemeinen	*Ich kenne alle anderen Mitarbeiter in meinem Unternehmen und alle Zulieferer und kann deshalb Eindringlinge von hier arbeitenden Menschen unterscheiden.*
G	Sicherheitsbewusstsein im Allgemeinen	*Ich weiß, wie ein Angreifer selbst einfache Organigramme benutzen kann, um so zu tun,als wäre er ein Mitarbeiter einer anderen Abteilung.*
G	Sicherheitsbewusstsein im Allgemeinen	*Ich erlebe oft Situationen, in denen die Arbeit der Systemspezialisten nur durch die Mitarbeit der IT-Nutzer erfolgreich werden kann.*
G	Sicherheitsbewusstsein im Allgemeinen	*Wenn ich an wichtigen oder sensiblen Daten arbeite, bin ich über die Konsequenzen, die drohen, falls sie in falsche Hände geraten, angemessen informiert.*
G	Sicherheitsbewusstsein im Allgemeinen	*Ich kenne sowohl den Unterschied, als auch den Zusammenhang zwischen Hacking und Social Engineering.*
G	Sicherheitsbewusstsein im Allgemeinen	*Ich kenne und erkenne einige Social Engineering Angriffsarten.* (Stefan Egeler 2014)
H	Sicherheitsbewusstsein im Kontext von Single Sign On	Wie schätzen Sie die Sicherheit von Single Sign On Lösungen von Anbieter (Identity Provider) wie Facebook, Twitter, Google Plus und Amazon ein?
H	Sicherheitsbewusstsein im Kontext von Single Sign On	Unternehmen können sich über das Unternehmensserviceportal bei mehreren E-Governance Anwendungen wie FinanzOnline, Mein Postkorb, E-Rechnung etc. über Single Sign On anmelden. Wie sicher würden Sie solch eine Single Sign On Lösung einschätzen?
H	Sicherheitsbewusstsein im Kontext von Single Sign On	Wie wahrscheinlich schätzen Sie ein, dass durch einen Identity Provider wie Facebook, Daten an Applikationsbetreiber weitergegeben werden? (5 sehr hoch)
H	Sicherheitsbewusstsein im Kontext von Single Sign On	Wie würden Sie die Wahrscheinlichkeit einstufen, dass ein Identity Provider wie Facebook angegriffen wird und somit Ihre Anmeldedaten an Dritte gelangen? (5 sehr hoch)
H	Sicherheitsbewusstsein im Kontext von Single Sign On	Wie wahrscheinlich schätzen Sie ein, dass ein Identity Provider wie Facebook ihre Aktionen mitverfolgt, die nach der Anmeldung von Ihnen getätigt werden? (5 sehr hoch)

Tabelle 11: Zuordnung der Fragen zu Faktoren (eigene Tabelle)

	MC2	MC1	MC4	MC8	MC3	MC5	MC7	MC6
No								
D12	0.544							
N1				0.569				
A1	0.455							
A2								
C1								
D1				0.612				
D2								
D3				0.494				
D4		0.883						
D5		0.979						
D6		0.722						
D7								0.672
D8		0.758						
D9								0.701
D10								0.457
D11				0.696				
E1			0.415					
E2			0.530					
E3			0.840					
E4			0.814					
E5.inverse			0.448					
E6								
E7								
E8								
E9								
E10								
F1						0.674		
F2						0.482		
F3						0.694		
G1					0.556			
G2					0.542	-0.414		
G3					0.584			
G4					0.608			
G5					0.710			
H1							0.410	
H2							0.486	
H3							0.462	
H4								
H5							0.497	
H6							0.477	
H7	0.468							
H8								
H9							0.440	
H10	1.028							
H11	1.005							

Abbildung 28: Faktorenanalyse (eigene Abbildung)

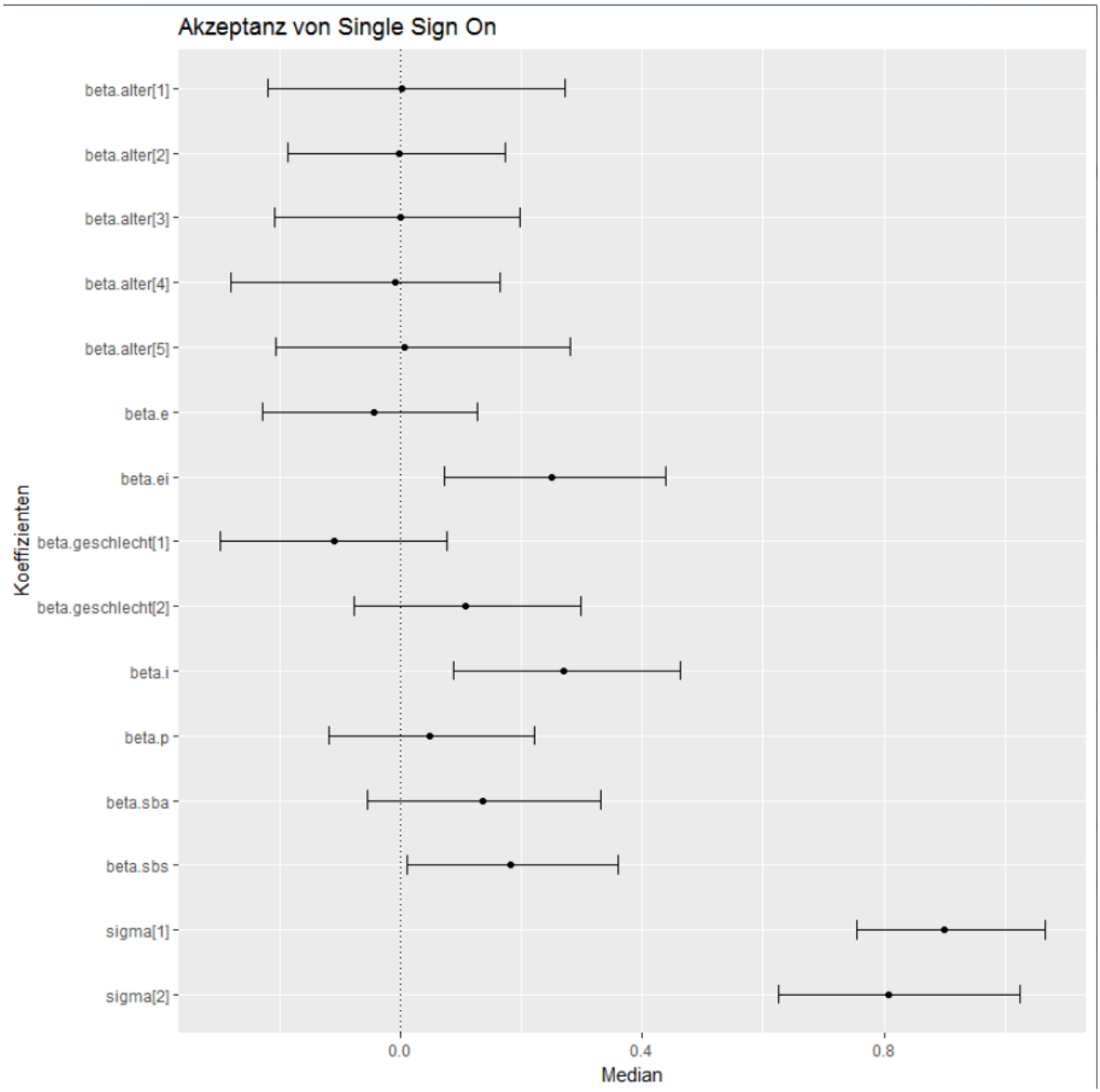

Abbildung 29: Star Wars Diagramm - Einfluss auf Akzeptanz von Single Sign On (eigene Abbildung)

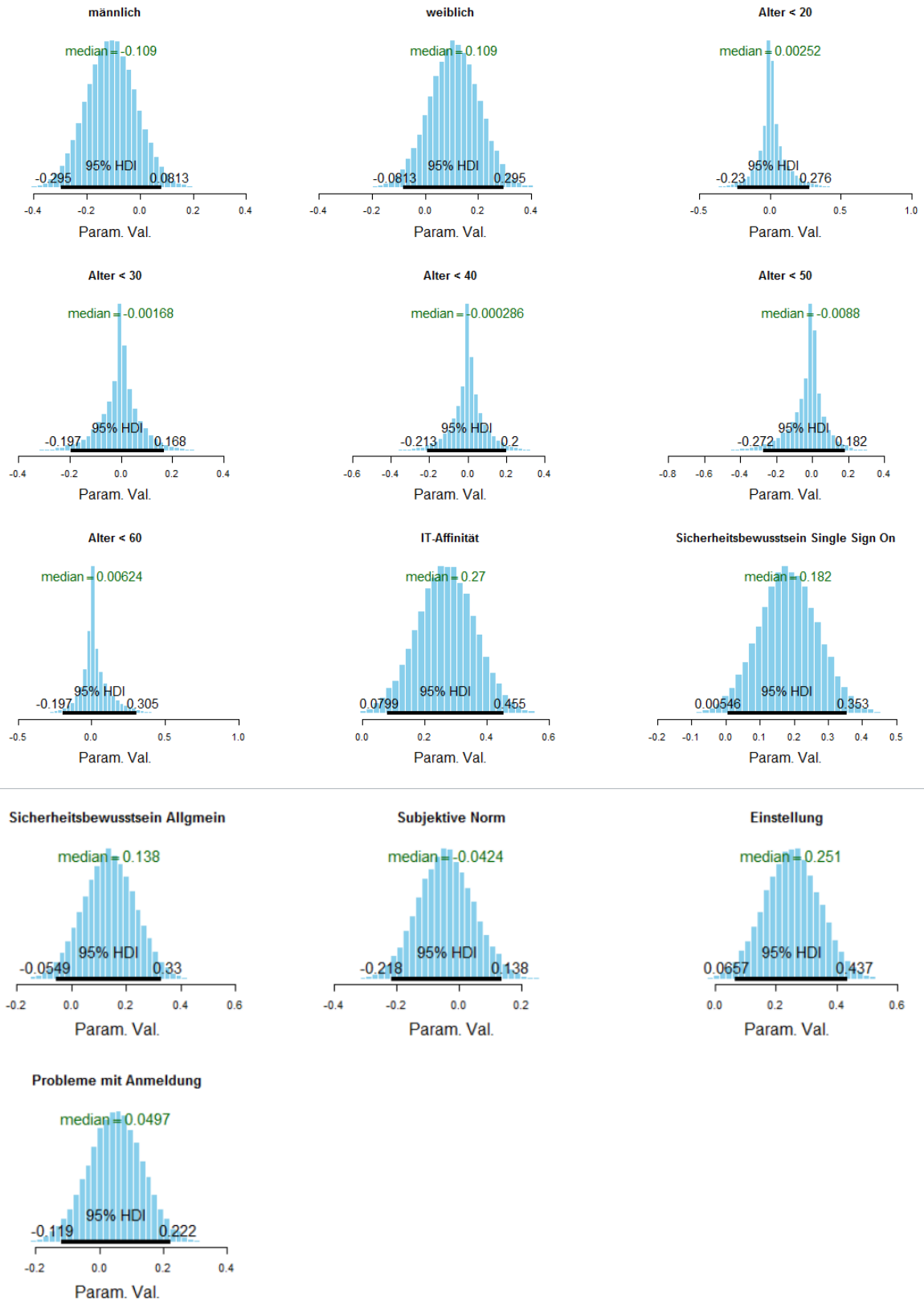

Abbildung 30: HDI Analyse – Einfluss auf Akzeptanz von Single Sign On (eigene Abbildung)

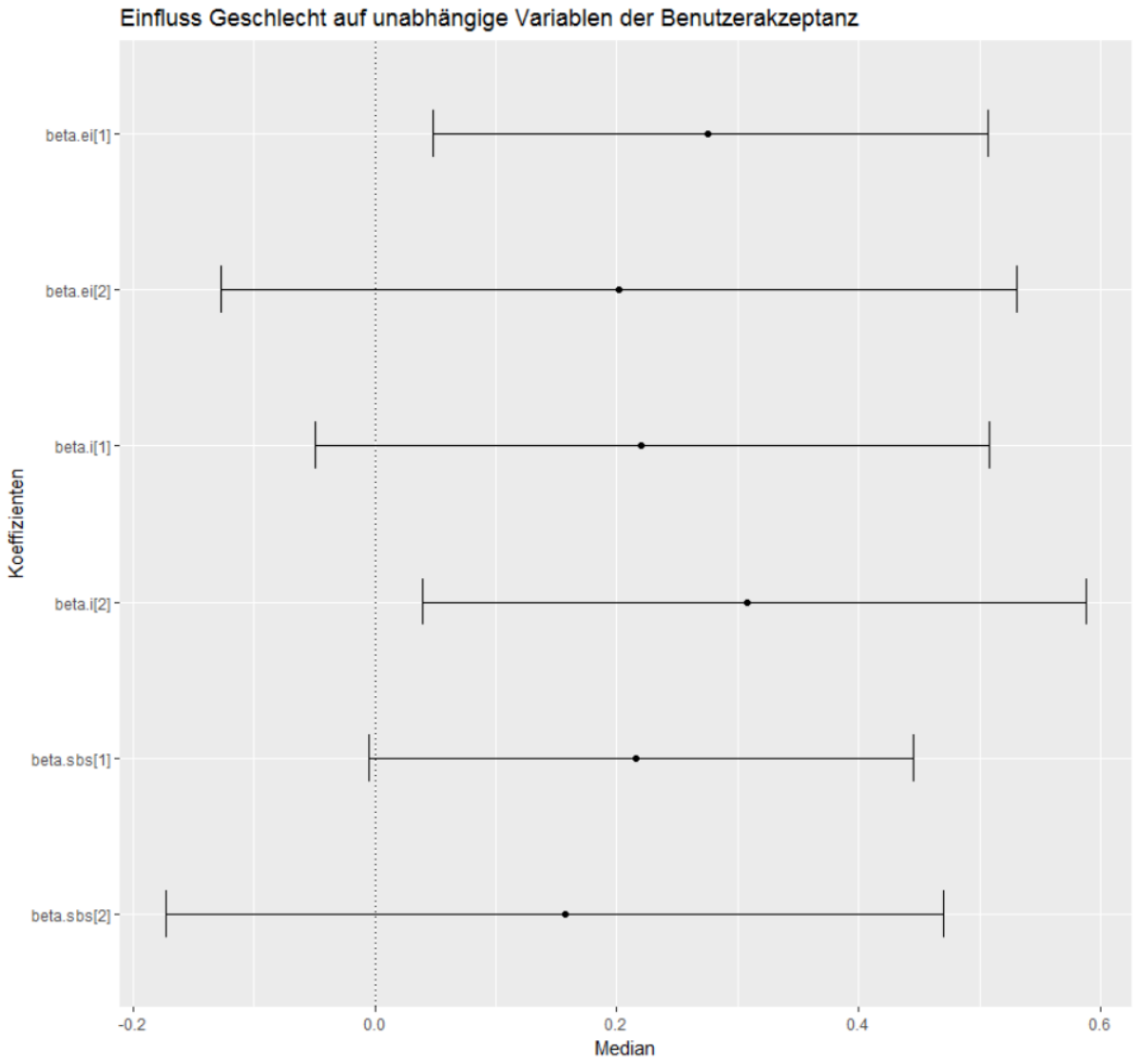

Abbildung 31: Star Wars Diagramm – Einfluss des Geschlechts auf unabhängigen Variablen der Benutzerakzeptanz (eigene Abbildung)

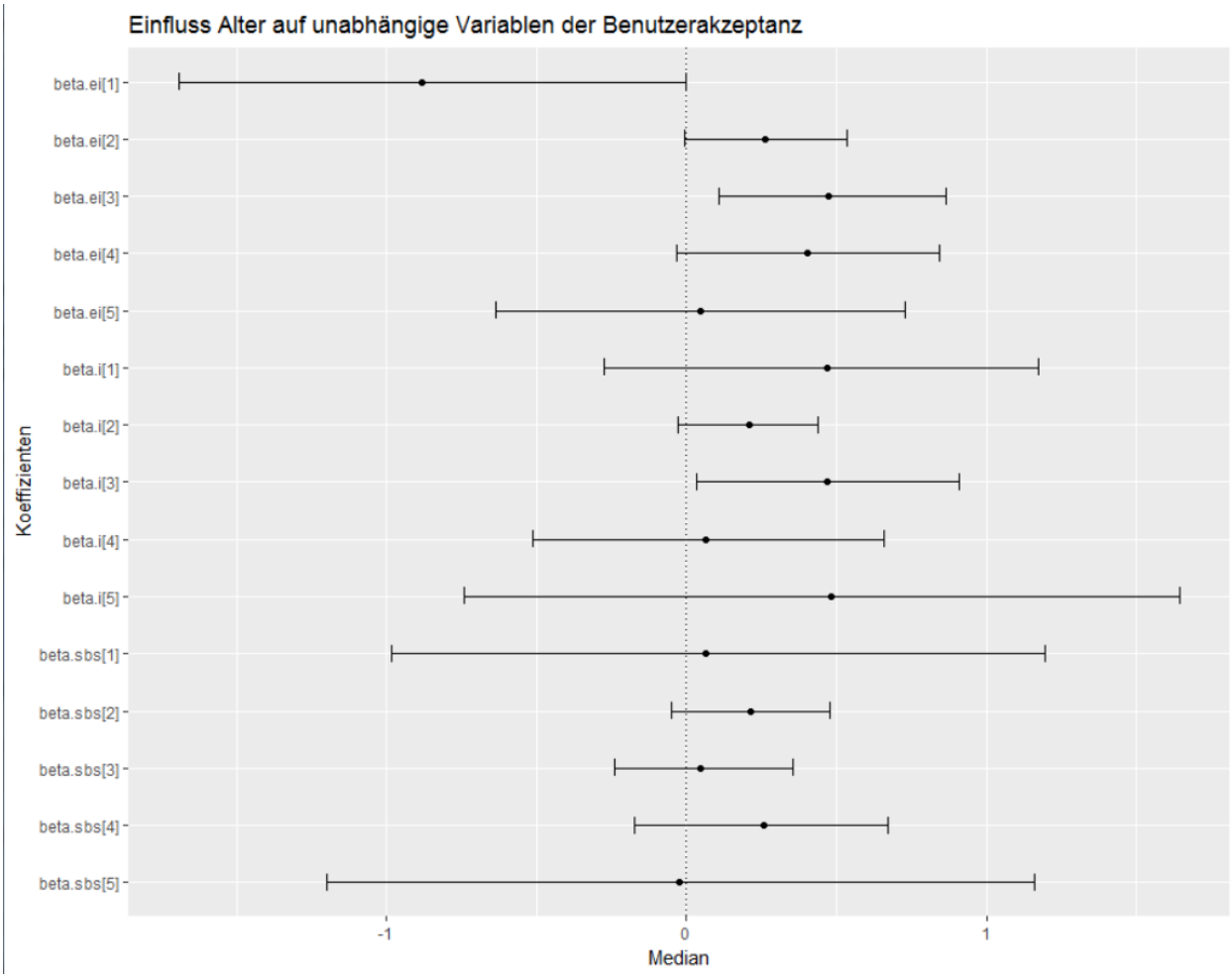

Abbildung 32: Star Wars Diagramm – Einfluss des Alters auf unabhängige Variablen der Benutzerakzeptanz (eigene Abbildung)

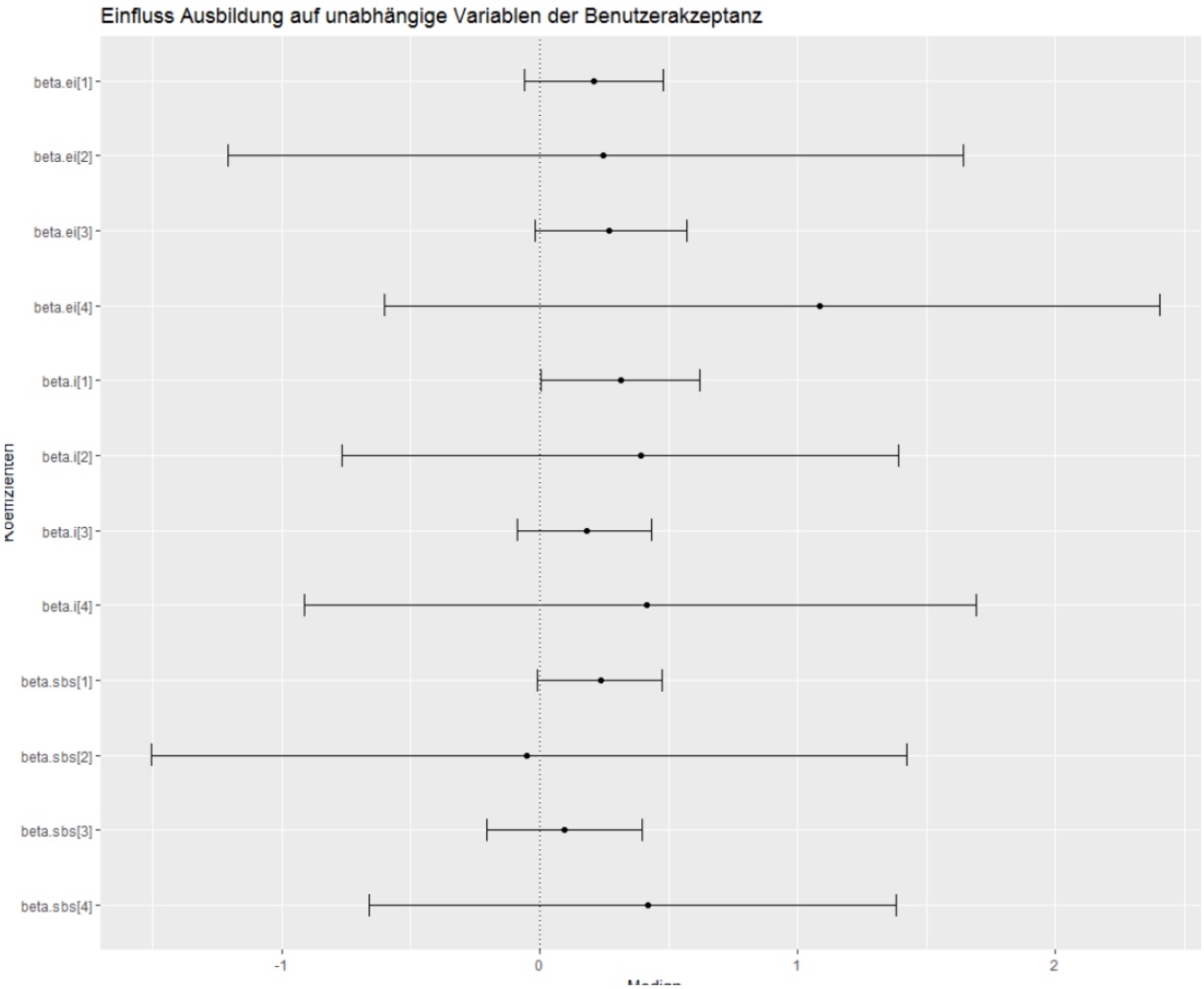

Abbildung 33: Star Wars Diagramm – Einfluss der Ausbildung auf unabhängige Variablen der Benutzerakzeptanz (eigene Abbildung)

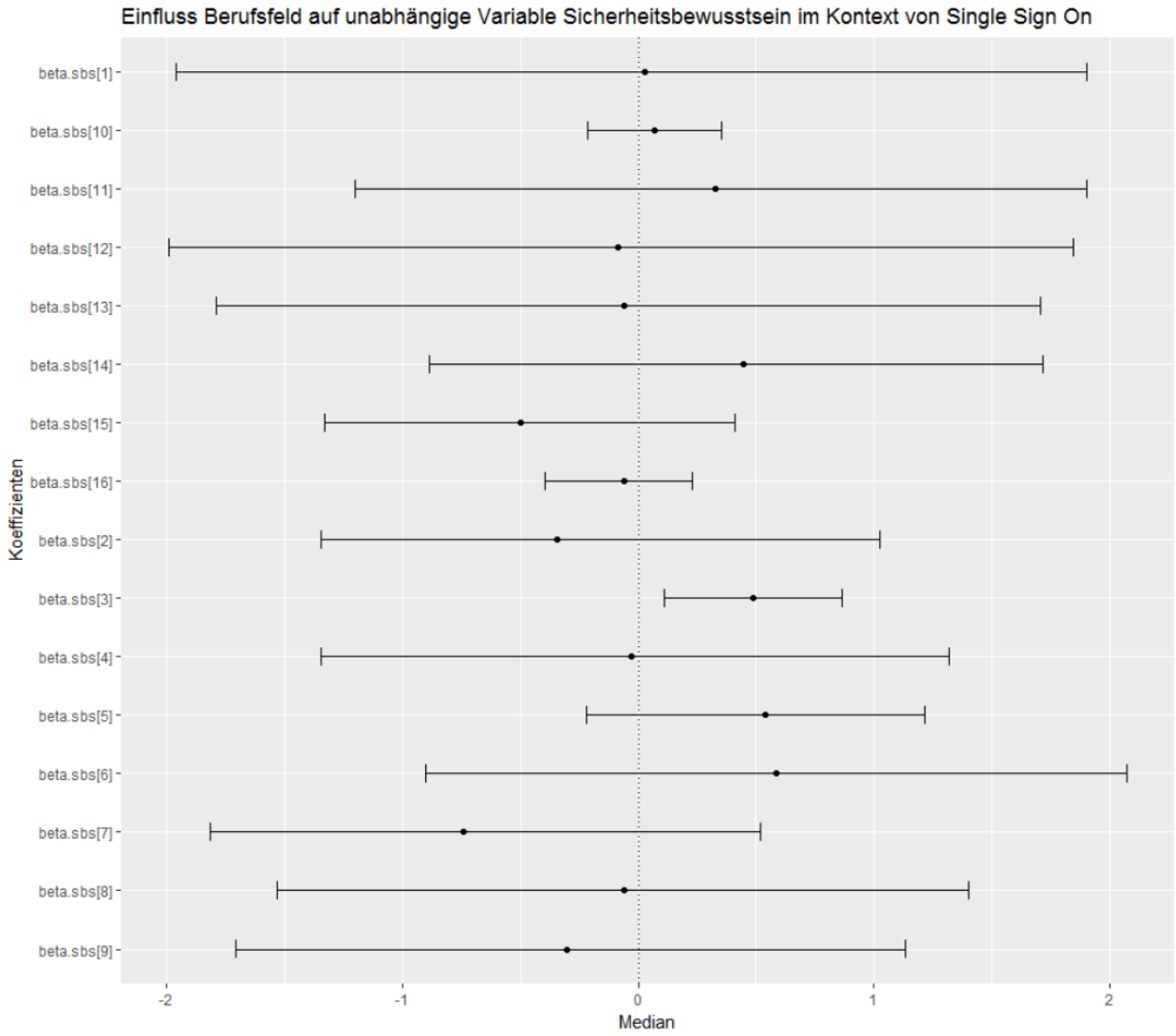

Abbildung 34: Star Wars Diagramm – Einfluss Berufsfeld auf unabhängige Variable Sicherheitsbewusstsein im Kontext von Single Sign On (eigene Abbildung)

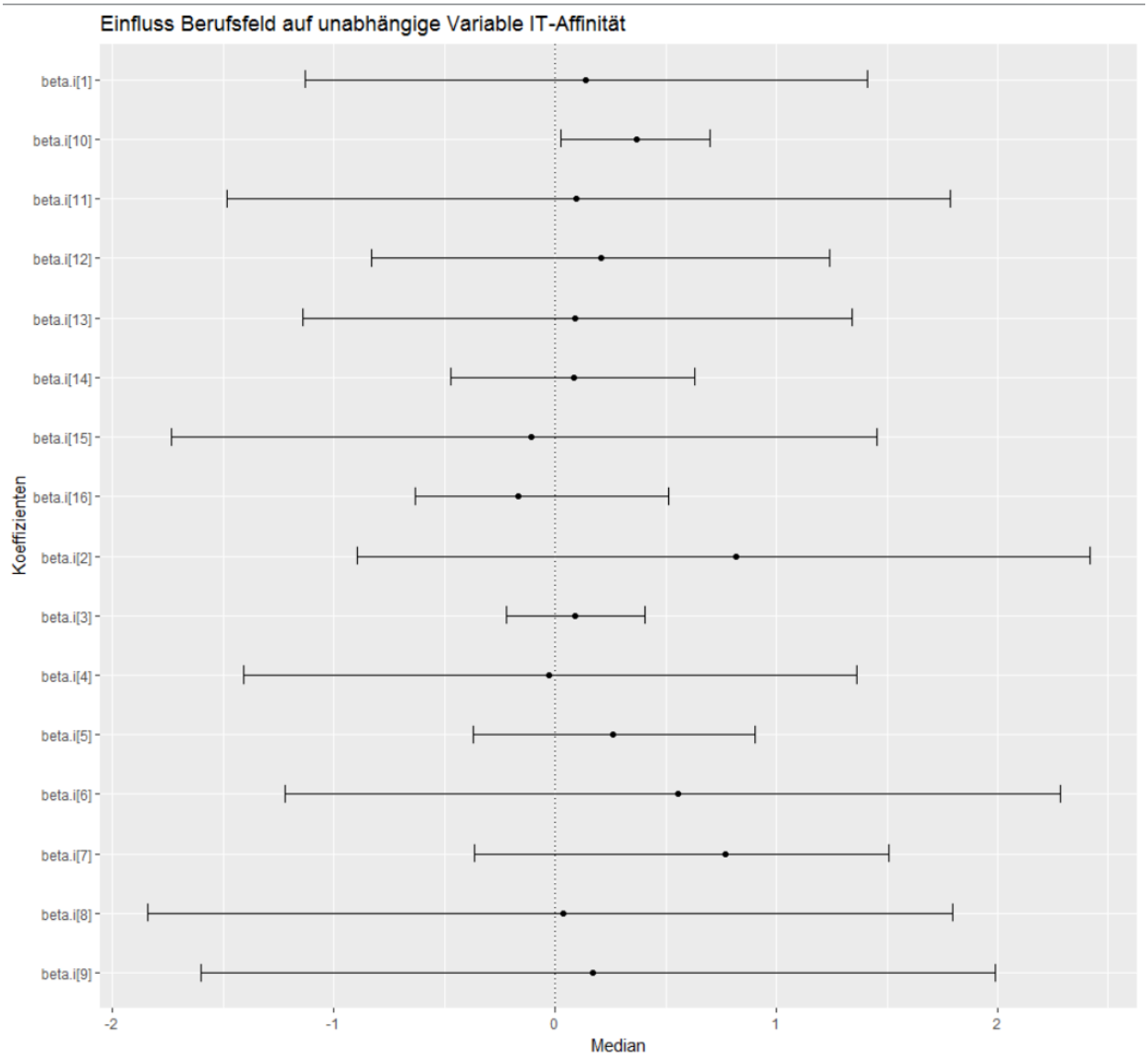

Abbildung 35: Star Wars Diagramm – Einfluss des Berufsfeldes auf unabhängige Variable IT-Affinität (eigene Abbildung)

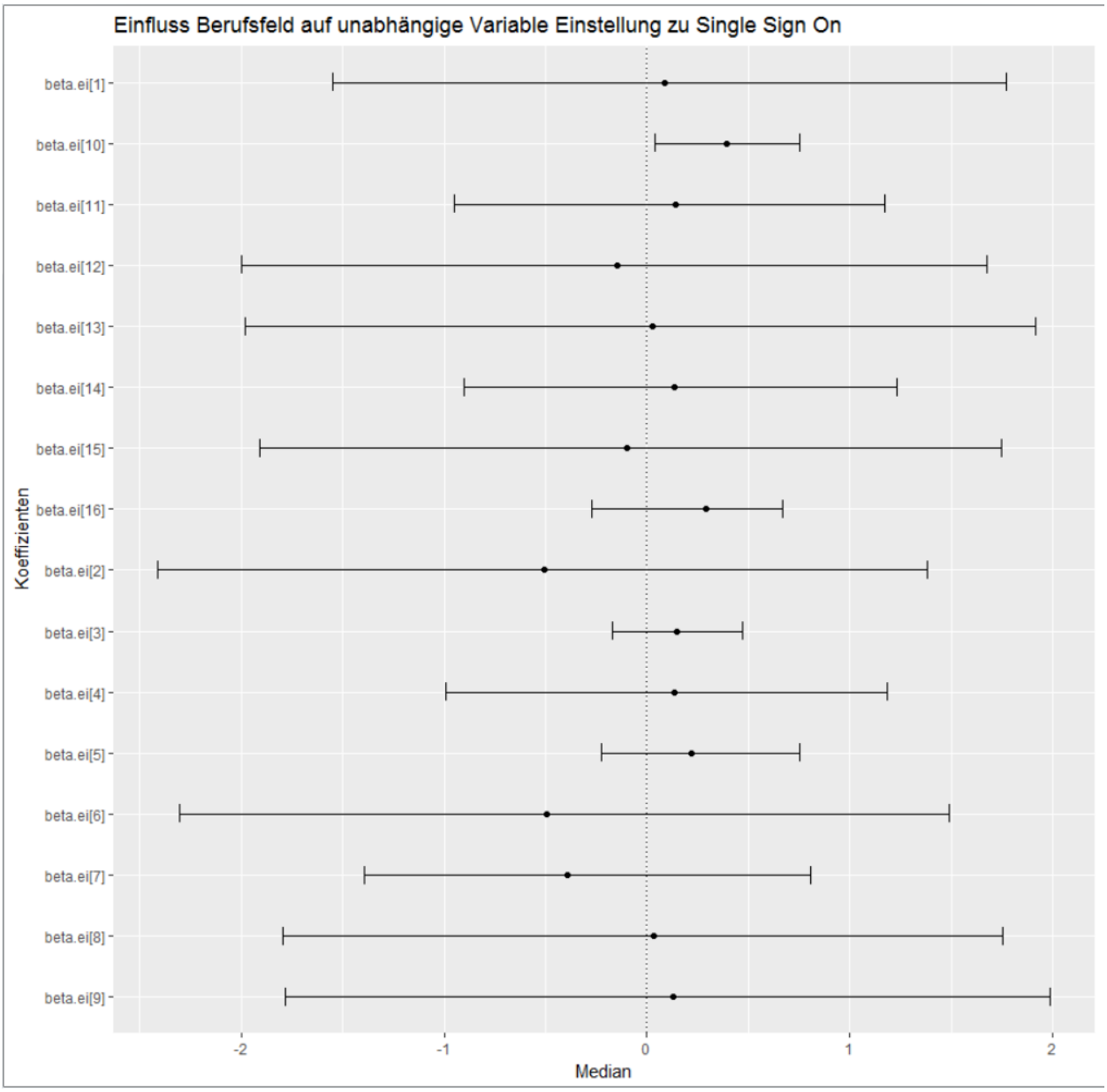

Abbildung 36: Einfluss des Berufsfeldes auf unabhängige Variable Einstellung zu Single Sign On (eigene Abbildung)

ANHANG B - 2. ANHANG

Fragebogen zur Akzeptanz von Single Sign On Lösungen

Im Rahmen meiner Masterarbeit an der FH Campus 02 führe ich eine empirische Untersuchung über ,,ANALYSE DER USERAKZEPTANZ IN WEBBASIERENDEN SINGLE SIGN ON LÖSUNGEN" durch.

Bitte nehmen Sie sich ca. zehn Minuten Zeit, um die Fragen zu beantworten. Beim Beantworten der Fragen gibt es kein „Richtig oder Falsch." Wichtig ist ebenfalls, dass Sie die Fragen nach Ihren persönlichen Meinungen und Empfindungen anzukreuzen. Sollten Sie sich bei Fragen unsicher sein, welche Antwort auf Sie zutrifft,kreuzen Sie bitte die am ehesten zutreffende Antwort an.

Ihre Daten werden anonym ausgewertet und nicht an Dritte weiter gegeben.

Vielen Dank für Ihre Mithilfe an diesem Forschungsprojekt.

(survio.com 2018)

LG

Gabriel-Antonio Furthmaier

Frage 1: Wie viel Stunden am Tag verwenden Sie einen Computer?

☐ weniger als 1 Stunde
☐ 1-2 Stunden
☐ 2-3 Stunden
☐ 3-4 Stunden
☐ mehr als 4 Stunden

Frage 2: Lieben Sie es mit dem Computer zu arbeiten, da Sie mit Unterstützung des Computers Probleme lösen können, neue Informationen verarbeiten dürfen und sich neue Dinge aneignen können? (1 = trifft nicht zu, 5 = trifft völlig zu)

Frage 3: Welche der 3 Anmeldevarianten bevorzugen Sie?

Frage 4: Wie oft haben Sie bislang vom Begriff Single Sign On gehört?

☐ nie
☐ selten
☐ gelegentlich
☐ oft
☐ sehr oft

Frage 5: Wie oft melden Sie sich über Single Sign On an?

☐ täglich
☐ mehrmals wöchentlich
☐ wöchentlich
☐ monatlich
☐ nie

Frage 6: Mit welchen Anbietern haben Sie sich schon mal über Single Sign On angemeldet? (mehrfachauswahl möglich)

☐ Facebook
☐ Google Plus
☐ Amazon
☐ Twitter
☐ LinkedIn
☐ Salesforce

☐ mit keinem Anbieter

Frage 7: Wurde Ihnen schon mal von Freunden nahegelegt sich über Single Sign On anzumelden?

☐ nie
☐ selten
☐ gelegentlich
☐ oft
☐ sehr oft

Frage 8: Würden Sie sich wünschen, dass bei mehreren Applikationen die Anmeldung über Single Sign On erfolgt?

☐ trifft zu
☐ trifft eher zu
☐ teils-teils
☐ trifft eher nicht zu
☐ trifft nicht zu

Frage 9: Ist aus Nutzersicht die Anmeldung über einer Single Sign On Lösung wie Facebook Connect einfach durchzuführen?

☐ trifft zu
☐ trifft eher zu
☐ teils-teils
☐ trifft eher nicht zu
☐ trifft nicht zu

Frage 10: Hatten Sie schon das Problem, dass die Anmeldung bei einer Applikation nur über Single Sign On erfolgt werden konnte? (1 = nie, 5 = sehr oft)

 **0 / 5**

Frage 11: Wenn der Zugriff auf eine gewünschte Applikation nur über eine Single Sign On Lösung erfolgen kann und Sie sich bei dem unbekannten Identity Provider noch nicht registriert haben, würden Sie daraufhin die Registrierung durchführen?

☐ trifft nicht zu

☐ trifft eher nicht zu

☐ teils-teils

☐ trifft eher zu

☐ trifft zu

Frage 12: Bitte bewerten Sie die Vorteile von Single Sign On Lösungen! (1 = sehr kleiner Nutzen, 5 = sehr großer Nutzen)

	1	2	3	4	5
einfache Handhabung	☐	☐	☐	☐	☐
Zeitersparnis	☐	☐	☐	☐	☐
Wegfall von unzähligen Passwörter	☐	☐	☐	☐	☐
Vermeidung von unsicheren Passwörter	☐	☐	☐	☐	☐
Geringer administrativer Aufwand	☐	☐	☐	☐	☐
Reduzierung von Angriffen durch Dritte	☐	☐	☐	☐	☐
Entlastung des Help-Desks	☐	☐	☐	☐	☐

Frage 13: Ist Single Sign On in ihrem Unternehmen im Einsatz? Sprich, melden Sie sich bei allen Applikationen gleichzeitig an?

☐ ja

☐ nein

Frage 14: Wie viele Passwörter müssen Sie sich in der Arbeit merken?

☐ < 2

☐ < 5

☐ < 10

☐ < 20

☐ größer

Frage 15: Wie oft hatten Sie schon Probleme mit Systemanmeldungen in Ihrer Firma?

☐ nie

☐ selten

☐ gelegentlich

☐ oft

☐ immer

Frage 16: Wie oft stellen Sie in der Firma an den Help Desk oder an den IT Support Anfragen bezüglich Anmeldeprobleme? (1=nie, 5= sehr oft)

 **0 / 5**

Frage 17: Werden Sie von den Help-Desk Mitarbeitern bezüglich Ihre Anmeldeprobleme zufriedenstellend unterstützt?

☐ trifft zu
☐ trifft eher zu
☐ teils-teils
☐ trifft eher nicht zu
☐ trifft nicht zu
☐ Ich habe noch keinen Help-Desk Mitarbeiter für Anmeldeprobleme benötigt

Frage 18: Wie oft hatten Sie schon Schulungen über IT-Sicherheit in Ihrem Unternehmen? (1=nie, 5=sehr oft)

 **0 / 5**

Frage 19: Wie würden Sie das Sicherheitsbewusstsein der Mitarbeiter in Ihrem Unternehmen einschätzen?

☐ sehr hoch
☐ ziemlich hoch
☐ mittelmäßig
☐ eher niedrig
☐ sehr niedrig

Frage 20: Wie schätzen Sie die IT-Sicherheit in Ihrem Unternehmen im Allgemeinen ein? (1=niedrig, 5 = sehr hoch)

 **0 / 5**

Frage 21: Welche Probleme hatten Sie bezüglich Systemanmeldungen bislang in der Praxis? (Mehrfachantwort möglich)

☐ Passwort vergessen

☐ Serverausfall

☐ Applikation funktionierte nicht

☐ Registrierung nicht abgeschlossen

☐ Passwort abgelaufen

Frage 22: Wie schätzen Sie die Sicherheit von Single Sign On Lösungen von Anbieter (Identity Provider) wie Facebook, Twitter, Google Plus und Amazon ein?

☐ gar nicht sicher

☐ kaum sicher

☐ mittelmäßig sicher

☐ ziemlich sicher

☐ außerordentlich sicher

Frage 23: Unternehmen können sich über das Unternehmensserviceportal bei mehreren E-Governance Anwendungen wie FinanzOnline, Mein Postkorb, E-Rechnung etc. über Single Sign On anmelden. Wie sicher würden Sie solch eine Single Sign On Lösung einschätzen?

☐ gar nicht sicher

☐ kaum sicher

☐ mittelmäßig sicher

☐ ziemlich sicher

☐ außerordentlich sicher

Frage 24: Wie wahrscheinlich schätzen Sie ein, dass durch einen Identity Provider wie Facebook, Daten an Applikationsbetreiber weitergegeben werden? (5 sehr hoch)

 **0 / 5**

Frage 25: Wie würden Sie die Wahrscheinlichkeit einstufen, dass ein Identity Provider wie Facebook angegriffen wird und somit Ihre Anmeldedaten an Dritte gelangen? (5 sehr hoch)

 **0 / 5**

Frage 26: Wie wahrscheinlich schätzen Sie ein, dass ein Identity Provider wie Facebook ihre Aktionen mitverfolgt, die nach der Anmeldung von Ihnen getätigt werden? (5 sehr hoch)

Frage 27: Bitte bewerten Sie die Aussagen von 1 = trifft nicht zu, 5 = trifft zu

	trifft nicht zu	trifft eher nicht zu	teils-teils	trifft eher zu	trifft zu
Ich überprüfe beim Online Banking vor der Eingabe von Kontonummer und PIN immer das Adressfeld des Browsers	☐	☐	☐	☐	☐
Ich antworte nicht auf per EMail zugeschickte Forderungen meiner Bank zur Herausgabe persönlicher Transaktionsdaten und benutze ebenfalls keine Software, die mir meine Bank per EMail zugeschickt hat	☐	☐	☐	☐	☐
Ich habe die automatische Update-Funktion meines Betriebssystems aktiviert bzw. überprüfe selbst regelmäßig, ob neue Sicherheitspatches für von mir benutzte Computerprogramme vorliegen	☐	☐	☐	☐	☐

(Stefan Egeler 2014)

Frage 28: Bitte bewerten Sie die Aussagen von 1 = trifft nicht zu, 5 = trifft zu

	trifft nicht zu	trifft eher nicht zu	teils-teils	trifft eher zu	trifft zu
Ich verlasse meinen Arbeitsplatz auch bei kurzer Abwesenheit immer so, dass keinesensiblen Daten abrufbar sind (passwortgeschützter Screensaver, Schränke abgesperrt,Büro abgesperrt).	☐	☐	☐	☐	☐
Ich weiß, wie in meinem Unternehmen sensible Daten und Texte behandelt werden, und kann zu dieser Frage einiges sagen.	☐	☐	☐	☐	☐
Ich kenne alle anderen Mitarbeiter in meinem Unternehmen und alle Zulieferer und kann deshalb Eindringlinge von hier arbeitenden Menschen unterscheiden.	☐	☐	☐	☐	☐
Ich weiß, wie ein Angreifer selbst einfache Organigramme benutzen kann, um so zu tun,als wäre er ein Mitarbeiter einer anderen Abteilung.	☐	☐	☐	☐	☐

(Stefan Egeler 2014)

Frage 29: Bitte bewerten Sie die Aussagen von 1 = trifft nicht zu, 5 = trifft zu

	trifft nicht zu	trifft eher nicht zu	teils-teils	trifft eher zu	trifft zu
Ich erlebe oft Situationen, in denen die Arbeit der Systemspezialisten nur durch die Mitarbeit der IT-Nutzer erfolgreich werden kann.	☐	☐	☐	☐	☐
Wenn ich an wichtigen oder sensiblen Daten arbeite, bin ich über die Konsequenzen, die drohen, falls sie in falsche Hände geraten, angemessen informiert.	☐	☐	☐	☐	☐
Ich kenne sowohl den Unterschied, als auch den Zusammenhang zwischen Hacking und Social Engineering.	☐	☐	☐	☐	☐
Ich kenne und erkenne einige Social Engineering Angriffsarten.	☐	☐	☐	☐	☐

(Stefan Egeler 2014)

Frage 30: Wie alt sind Sie?

_____

Frage 31: Sie sind…

☐ männlich

☐ weiblich

Frage 32: Ihr höchster Abschluss ist…

☐ Plichtschule

☐ Matura

☐ akademischer Titel

☐ Lehrabschluss

☐ Fachschule

☐ Sonstiges

Frage 33: In welchen Bereich arbeiten Sie?

☐ *Bau, Baunebengewerbe und Holz*
☐ *Büro, Wirtschaft, Finanzwesen und Recht Büro, Wirtschaft, Finanzwesen und Recht*
☐ *Chemie, Kunststoffe, Rohstoffe und Bergbau☐ Fachschule*
☐ *Elektrotechnik, Elektronik und Telekommunikation*
☐ *Gesundheit und Medizin*
☐ *Glas, Keramik und Stein*
☐ *Grafik, Druck, Papier und Fotografie*
☐ *Handel und Verkauf*
☐ *Hilfsberufe und Aushilfskräfte*
☐ *Hotel- und Gastgewerbe*
☐ *Informationstechnologie*
☐ *Körper- und Schönheitspflege*
☐ *Landwirtschaft, Gartenbau und Forstwirtschaft*
☐ *Lebensmittel*
☐ *Maschinen, Kfz und Metall*
☐ *Medien, Kunst und Kultur*
☐ *Reinigung und Hausbetreuung*
☐ *Reise, Freizeit und Sport*
☐ *Sicherheitsdienste*
☐ *Soziales, Erziehung und Bildung*
☐ *Textil, Mode und Leder*
☐ *Umwelt*
☐ *Verkehr, Transport und Zustelldienste*
☐ *Wissenschaft, Forschung und Entwicklung*
☐ *Sonstiges*

(Bepeach.com 2018)

ANHANG C - 3.ANHANG

Fallstudie 1: Verhalten von Nutzer bei webbasierenden Anmeldungen

Sehr geehrter Teilnehmer,

danke für Teilnahme bei der Studie über das ,,Verhalten von Nutzer bei webbasierenden Anmeldungen". Diese Studie wird von Gabriel-Antonio Furthmaier im Zuge der Masterarbeit ,,Analyse der Userakzeptanz in webbasierenden Single Sign On Lösungen" durchgeführt. Die Teilnahme ist unverbindlich und kann jederzeit abgebrochen werden. Des Weiteren werden Ihre Daten aus dem Fragebogen anonym ausgewertet und nicht an Dritte weitergegeben.

Die Dauer für die Teilnahme an dieser Studie beträgt zwischen 10 und 15 Minuten.

Bei der Auswahl der Anwendungen wurde darauf geachtet, dass es sich um kostenfreie Applikationen handelt, die jederzeit deinstalliert werden können. Sie gehen bei der Registrierung bzw. Installation der Anwendung keine Verpflichtungen ein. (survio.com 2018)

Anforderungen für erfolgreiche Studienteilnahme

Eine erfolgreiche Studienteilnahme ist an folgenden 2 Faktoren abhängig. Einerseits muss man sich erfolgreich bei verschiedenen Webapplikationen bzw. Apps anmelden und andererseits müssen die unten angeführten Fragen vollständig ausgefüllt werden.

Nachfolgend finden Sie eine Liste von Apps und Webapplikationen, bei denen Sie sich während der Teilnahme an der Studie registrieren müssen.

Anmeldungen bei Apps über Mobiltelefon oder Tablet

- Airbnb
- Quizduell

Anmeldungen bei Applikationen über Laptop/PC

- Shpock
- Wo gibt's was

Airbnb

Zur App: Mit der kostenlosen App Airbnb finden und buchen Sie von überall Apartments auf der ganzen Welt. (Airbnb 2018)

To Do's

Bitte gehen Sie in den App Store und suchen Sie nach Airbnb. Laden Sie Airbnb runter und registrieren Sie sich bei Airbnb via Facebook oder über traditionellen Login. Sie dürfen frei über die Auswahl entscheiden.

Bitte beantworten Sie nach Registrierung bei Airbnb die nachfolgenden Fragen.

Frage 1: Waren Sie schon auf Airbnb angemeldet?

☐ ja

☐ nein

Frage 2: Für welches Anmeldeverfahren haben Sie sich entschieden?

☐ gewöhnliche Anmeldung

☐ Single Sign On

Frage 3: Aus welchen Grund haben sie sich für Single Sign On entschieden? (Entscheidung für das Zutreffendste)

☐ Komfort

☐ Vertrauenswürdigkeit von Facebook als Identity Provider gegeben

☐ Spontane Entscheidung

☐ Gewohnheit

☐ Andere_____

Frage 4: Aus welchen Grund haben Sie sich für das traditionelle Anmeldeverfahren entschieden? (Entscheiden Sie sich für das Zutreffendste)

☐ Gewohnheit

☐ Sicherheit von Single Sign On im Generellen nicht gegeben

☐ Facebook nicht vertrauenswürdig genug

☐ Spontane Entscheidung

☐ Andere_____

Frage 5: Ist Ihnen die Entscheidung zwischen Single Sign On oder gewöhnlichen Anmeldung leicht gefallen?

☐ ja

☐ nein

Quizduell

Zur App: *Quizduell ist ein intelligentes, farbenfrohes und unterhaltsames soziales Quiz, in dem du deine Freunde und andre Spieler zu einem Wissensduell herausforderst und dabei neue & spannende Fakten lernst!* (Google Play Store 2018b)

To Do's

Bitte gehen Sie in den App Store und suchen Sie nach der Gratisversion von Quizduell. Laden Sie die kostenfreie Quizduellversion runter und registrieren Sie sich bei Quizduell via Facebook oder über traditionellen Login. Sie dürfen frei über die Auswahl entscheiden.

Bitte beantworten Sie nach Registrierung bei Quizduell die nachfolgenden Fragen:

Frage 6: Waren Sie schon bei Quizduell angemeldet?

☐ ja

☐ nein

Frage 7: Für welches Anmeldeverfahren haben Sie sich entschieden?

☐ gewöhnliche Anmeldung

☐ Single Sign On

Frage 8: Aus welchen Grund haben sie sich für Single Sign On entschieden? (Entscheidung für das Zutreffendste)

☐ Komfort

☐ Vertrauenswürdigkeit von Facebook als Identity Provider gegeben

☐ Spontane Entscheidung

☐ Gewohnheit

☐ Andere_____

Frage 9: Aus welchen Grund haben Sie sich für das traditionelle Anmeldeverfahren entschieden? (Entscheiden Sie sich für das Zutreffendste)

☐ Gewohnheit

☐ Sicherheit von Single Sign On im Generellen nicht gegeben

☐ Facebook nicht vertrauenswürdig genug

☐ Spontane Entscheidung

☐ Andere_____

Frage 10: Ist Ihnen die Entscheidung zwischen Single Sign On oder gewöhnlichen Anmeldung leicht gefallen?

☐ ja

☐ nein

Wo gibt's was

Zur Webapplikation: Bei Wo gibt's was hat man alle Angebote im Überblick Wo gibt's was IN AKTION? Wo gibt's Bier in Aktion? Welche Angebote gibt's diese Woche bei Hofer? Was gibt's im aktuellen Lidl Flugblatt? Wann gibt's wieder Waschmittel im Angebot? (wogibtswas.at 2018)

To Do's

Bitte gehen Sie auf die Webseite https://www.wogibtswas.at/ -> Anmelden. Registrieren Sie sich bei https://www.wogibtswas.at via Facebook, Google oder über traditionellen Login. Sie dürfen frei über die Auswahl entscheiden.
Bitte beantworten Sie nach Registrierung bei https://www.wogibtswas.at die nachfolgenden Fragen.

Frage 11: Waren Sie schon auf Wo gibt's was angemeldet?

☐ ja

☐ nein

Frage 12: Für welches Anmeldeverfahren haben Sie sich entschieden?

☒ gewöhnliche Anmeldung

☐ Single Sign On

Frage 13: Aus welchen Grund haben sie sich für Single Sign On entschieden? (Entscheidung für das Zutreffendste)

☐ Komfort

☐ Vertrauenswürdigkeit des Identity Providers wie Facebook, Google Plus

☐ Spontane Entscheidung

☐ Gewohnheit

☐ Andere_____

Frage 14: Für welchen Identity Provider haben Sie sich entschieden?

☐ Google

☐ Facebook

Frage 15: Warum ist ihre Entscheidung explizit auf Facebook oder Google gefallen?

_____

Frage 16: Aus welchen Grund haben Sie sich für das traditionelle Anmeldeverfahren entschieden? (Entscheidung für das Zutreffendste)

☐ Gewohnheit

☐ Sicherheit von Single Sign On im Generellen nicht gegeben

☐ Facebook und Google nicht vertrauenswürdig genug

☐ Spontane Entscheidung

☐ Andere_____

Frage 17: Ist Ihnen die Entscheidung zwischen Single Sign On oder gewöhnlichen Anmeldung leicht gefallen?

☐ ja

☐ nein

Shpock

Zur Webapplikation: Shpock ist eine der am häufigsten heruntergeladenen Flohmarkt-Apps und monatlich kaufen und verkaufen mehr als 10 Millionen User mit Shpock. (shpock.com 2018)

To Do's

Bitte gehen Sie auf die Webseite https://www.shpock.com/my/login/. Registrieren Sie sich bei https://www.shpock.com/my/login/ via Facebook, Google oder über traditionellen Login. Sie dürfen frei über die Auswahl entscheiden.
Bitte beantworten Sie nach Registrierung bei shpock.com die nachfolgenden Fragen.

Frage 18: Waren Sie schon auf shpock.com angemeldet?

☐ ja

☐ nein

Frage 19: Für welches Anmeldeverfahren haben Sie sich entschieden?

☐ gewöhnliche Anmeldung

☐ Single Sign On

Frage 20: Aus welchen Grund haben sie sich für Single Sign On entschieden? (Entscheidung für das Zutreffendste)

☐ Komfort

☐ Vertrauenswürdigkeit des Identity Providers wie Facebook, Google Plus

☐ Spontane Entscheidung

☐ Gewohnheit

☐ Andere_____

Frage 21: Für welchen Identity Provider haben sie sich entschieden?

☐ Google

☐ Facebook

Frage 22: Warum ist ihre Entscheidung explizit auf Facebook oder Google gefallen?

_____

Frage 23: Aus welchen Grund haben Sie sich für das traditionelle Anmeldeverfahren entschieden? (Entscheidung für das Zutreffendste)

☐ Gewohnheit

☐ Sicherheit von Single Sign On im Generellen nicht gegeben

☐ Facebook und Google nicht vertrauenswürdig genug

☐ Spontane Entscheidung

☐ Andere_____

Frage 24: Ist Ihnen die Entscheidung zwischen Single Sign On oder gewöhnlichen Anmeldung leicht gefallen?

☐ ja

☐ nein

Frage 25: Wie alt sind Sie?

☐ unter 20 Jahre

☐ zwischen 20 und 30 Jahre

☐ zwischen 30 und 40 Jahre

☐ zwischen 40 und 50 Jahre

☐ zwischen 50 und 60 Jahre

Frage 26: Sie sind....

☐ weiblich

☐ männlich

Frage 27: In welchen Bereich arbeiten Sie?

☐ Bau, Baunebengewerbe und Holz

☐ Büro, Wirtschaft, Finanzwesen und Recht Büro, Wirtschaft, Finanzwesen und Recht

☐ Chemie, Kunststoffe, Rohstoffe und Bergbau☐ Fachschule

☐ Elektrotechnik, Elektronik und Telekommunikation

☐ Gesundheit und Medizin

☐ Glas, Keramik und Stein

☐ Grafik, Druck, Papier und Fotografie

☐ Handel und Verkauf

☐ Hilfsberufe und Aushilfskräfte

☐ Hotel- und Gastgewerbe

☐ Informationstechnologie

☐ Körper- und Schönheitspflege

☐ Landwirtschaft, Gartenbau und Forstwirtschaft

☐ Lebensmittel

☐ Maschinen, Kfz und Metall

☐ Medien, Kunst und Kultur

☐ Reinigung und Hausbetreuung

☐ Reise, Freizeit und Sport

☐ Sicherheitsdienste

☐ Soziales, Erziehung und Bildung

☐ Textil, Mode und Leder

☐ Umwelt

☐ Verkehr, Transport und Zustelldienste

☐ Wissenschaft, Forschung und Entwicklung

☐ Sonstiges

Frage 28: Ihr höchster Abschluss ist….

☐ Plichtschule

☐ Matura

☐ akademischer Titel

☐ Lehrabschluss

☐ Fachschule

☐ Sonstiges

Fallstudie 2: Verhalten von Nutzer bei webbasierenden Anmeldungen

Sehr geehrter Teilnehmer,

danke für Teilnahme bei der Studie über das ,,Verhalten von Nutzer bei webbasierenden Anmeldungen". Diese Studie wird von Gabriel-Antonio Furthmaier im Zuge der Masterarbeit ,,Analyse der Userakzeptanz in webbasierenden Single Sign On Lösungen" durchgeführt. Die Teilnahme ist unverbindlich und kann jederzeit abgebrochen werden. Des Weiteren werden Ihre Daten aus dem Fragebogen anonym ausgewertet und nicht an Dritte weitergegeben.

Die Dauer für die Teilnahme an dieser Studie beträgt zwischen 10 und 15 Minuten.

Bei der Auswahl der Anwendungen wurde darauf geachtet, dass es sich um kostenfreie Applikationen handelt, die jederzeit deinstalliert werden können. Sie gehen bei der Registrierung bzw. Installation der Anwendung keine Verpflichtungen ein. (survio.com 2018)

Anforderungen für erfolgreiche Studienteilnahme

Eine erfolgreiche Studienteilnahme ist an folgenden 2 Faktoren abhängig. Einerseits muss man sich erfolgreich bei verschiedenen Webapplikationen bzw. Apps anmelden und andererseits muss der angefügte Fragebogen vollständig ausgefüllt werden.

Nachfolgend finden Sie eine Liste von Apps und Webapplikationen, bei denen Sie sich während der Teilnahme an der Studie registrieren müssen.

Anmeldungen bei Apps über Mobiltelefon oder Tablet

- Tinder
- Runtastic

Anmeldungen bei Applikationen über Laptop/PC

- Codeacademy.com
- Pinterest

Tinder

Zur App: *Die Grundfunktionalitäten von Tinder sind gratis. Bei Tinder handelt es sich um eine Dating-App, die das Ziel hat um neue Leute kennen zu lernen.* (Google Play Store 2018c)

To Do's

Bitte gehen Sie in den App Store und suchen Sie nach Tinder. Laden Sie Tinder runter und registrieren Sie sich bei Tinder via Facebook oder über traditionellen Login. Sie dürfen frei über die Auswahl entscheiden.

Bitte beantworten Sie nach Registrierung bei Tinder die nachfolgenden Fragen.

Frage 1: Waren Sie schon auf Tinder angemeldet?

☐ ja

☐ nein

Frage 2: Für welches Anmeldeverfahren haben Sie sich entschieden?

☐ gewöhnliche Anmeldung

☐ Single Sign On

Frage 3: Aus welchen Grund haben sie sich für Single Sign On entschieden? (Entscheidung für das Zutreffendste)

☐ Komfort

☐ Vertrauenswürdigkeit von Facebook als Identity Provider gegeben

☐ Spontane Entscheidung

☐ Gewohnheit

☐ Andere_____

Frage 4: Aus welchen Grund haben Sie sich für das traditionelle Anmeldeverfahren entschieden? (Entscheidung für das Zutreffendste)

☐ Gewohnheit

☐ Sicherheit von Single Sign On im Generellen nicht gegeben

☐ Facebook nicht vertrauenswürdig genug

☐ Spontane Entscheidung

☐ Andere_____

Frage 5: Ist Ihnen die Entscheidung zwischen Single Sign On oder gewöhnlichen Anmeldung leicht gefallen?

☐ ja

☐ nein

Runtastic

Zur App: *Die Grundfunktionalitäten von Runtastic sind gratis. Mit den mobilen Apps von Runtastic kannst du all deine Fitnessaktivitäten per GPS oder manuell aufzeichnen und mit deinen Freunden teilen.* (Runtastic 2018)

To Do's

Bitte gehen Sie in den App Store und suchen Sie nach Runtastic. Laden Sie Runtastic runter und registrieren Sie sich bei Runtastic via Facebook oder über traditionellen Login. Sie dürfen frei über die Auswahl entscheiden.

Bitte beantworten Sie nach Registrierung bei Runtastic die nachfolgenden Fragen:

Frage 6: Waren Sie schon bei Runtastic angemeldet?

☐ ja

☐ nein

Frage 7: Für welches Anmeldeverfahren haben Sie sich entschieden?

☐ gewöhnliche Anmeldung

☐ Single Sign On

Frage 8: Aus welchen Grund haben sie sich für Single Sign On entschieden? (Entscheidung für das Zutreffendste)

☐ Komfort

☐ Vertrauenswürdigkeit von Facebook, Google Plus als Identity Provider gegeben

☐ Spontane Entscheidung

☐ Gewohnheit

☐ Andere_____

Frage 9: Für welchen Identity Provider haben Sie sich entschieden?

☐ Google

☐ Facebook

Frage 10: Warum ist die Entscheidung für den gewählten Identity Provider gefallen? (z.B warum für Facebook und nicht für Google)

_____

Frage 11: Aus welchen Grund haben Sie sich für das traditionelle Anmeldeverfahren entschieden? (Entscheidung für das Zutreffendste)

☐ Gewohnheit

☐ Sicherheit von Single Sign On im Generellen nicht gegeben

☐ Facebook und Google nicht vertrauenswürdig genug

☐ Spontane Entscheidung

☐ Andere_____

Frage 12: Ist Ihnen die Entscheidung zwischen Single Sign On oder gewöhnliche Anmeldung leicht gefallen?

☐ ja

☐ nein

Codeacademy.com

Zur Webapplikation: Codeacademy ist eine interaktive Internet-Plattform, die kostenlosen Programmierunterricht in vier Sprachen für viele Programmiersprachen anbietet (darunter Python, PHP, jQuery, JavaScript, AngularJS und Ruby, wie auch HTML und CSS). (Team Twago 2014)

To Do's

Bitte gehen Sie auf die Webseite https://www.codecademy.com/. Regestrieren Sie sich bei Codeacademy.com via Facebook, Google oder über traditionellen Login. Sie dürfen frei über die Auswahl entscheiden.
Bitte beantworten Sie nach Registrierung bei Codeacademy.com die nachfolgenden Fragen.

Frage 13: Waren Sie schon auf Codeacademy.com angemeldet?

☐ ja

☐ nein

Frage 14: Für welches Anmeldeverfahren haben Sie sich entschieden?

☐ gewöhnliche Anmeldung

☐ Single Sign On

Frage 15: Aus welchen Grund haben sie sich für Single Sign On entschieden? (Entscheidung für das Zutreffendste)

☐ Komfort

☐ Vertrauenswürdigkeit von Facebook, Google Plus als Identity Provider gegeben

☐ Spontane Entscheidung

☐ Gewohnheit

☐ Andere_____

Frage 16: Für welchen Identity Provider haben sie sich entschieden?

☐ Google

☐ Facebook

Frage 17: Warum ist ihre Entscheidung explizit auf Facebook oder Google gefallen?

_____

Frage 18: Aus welchen Grund haben Sie sich für das traditionelle Anmeldeverfahren entschieden? (Entscheidung für das Zutreffendste)

☐ Gewohnheit

☐ Sicherheit von Single Sign On im Generellen nicht gegeben

☐ Facebook und Google nicht vertrauenswürdig genug

☐ Spontane Entscheidung

☐ Andere_____

Frage 19: Ist Ihnen die Entscheidung zwischen Single Sign On oder gewöhnlichen Anmeldung leicht gefallen?

☐ ja

☐ nein

Pinterest

Zur Webapplikation: Pinterest ist eine Ideenplattform, die dir dabei hilft, kleine und große Projekte in deinem Alltag umzusetzen. Hier kannst du die besten Ideen aus dem gesamten Web entdecken, von deutschen aber auch von internationalen Seiten. (Google Play Store 2018a)

To Do's

Bitte gehen Sie auf die Webseite https://www.pinterest.at/. Registrieren Sie sich bei https://www.pinterest.at/ via Facebook, Google oder über traditionellen Login. Sie dürfen frei über die Auswahl entscheiden.
Bitte beantworten Sie nach Registrierung bei pinterest.at die nachfolgenden Fragen.

Frage 20:Waren Sie schon in Pinterest angemeldet?

☐ ja

☐ nein

Frage 21: Für welches Anmeldeverfahren haben Sie sich entschieden?

☐ gewöhnliche Anmeldung

☐ Single Sign On

Frage 22: Aus welchen Grund haben sie sich für Single Sign On entschieden? (Entscheidung für das Zutreffendste)

☐ Komfort

☐ Vertrauenswürdigkeit von Facebook, Google Plus als Identity Provider gegeben

☐ Spontane Entscheidung

☐ Gewohnheit

☐ Andere_____

Frage 23: Für welchen Identity Provider haben sie sich entschieden?

☐ Google

☐ Facebook

Frage 24: Warum ist ihre Entscheidung explizit auf Facebook oder Google gefallen?

_____

Frage 25: Aus welchen Grund haben Sie sich für das traditionelle Anmeldeverfahren entschieden? (Entscheidung für das Zutreffendste)

☐ Gewohnheit

☐ Sicherheit von Single Sign On im Generellen nicht gegeben

☐ Facebook und Google nicht vertrauenswürdig genug

☐ Spontane Entscheidung

☐ Andere_____

Frage 26: Ist Ihnen die Entscheidung zwischen Single Sign On oder gewöhnlichen Anmeldung leicht gefallen?

☐ ja

☐ nein

Frage 27: Wie alt sind Sie?

☐ unter 20 Jahre

☐ zwischen 20 und 30 Jahre

☐ zwischen 30 und 40 Jahre

☐ zwischen 40 und 50 Jahre

☐ zwischen 50 und 60 Jahre

Frage 28: Sie sind....

☐ weiblich

☐ männlich

Frage 29: In welchen Bereich arbeiten Sie?

☐ Bau, Baunebengewerbe und Holz

☐ Büro, Wirtschaft, Finanzwesen und Recht Büro, Wirtschaft, Finanzwesen und Recht

☐ Chemie, Kunststoffe, Rohstoffe und Bergbau☐ Fachschule

☐ Elektrotechnik, Elektronik und Telekommunikation

☐ Gesundheit und Medizin

☐ Glas, Keramik und Stein

☐ Grafik, Druck, Papier und Fotografie

☐ Handel und Verkauf

☐ Hilfsberufe und Aushilfskräfte

☐ Hotel- und Gastgewerbe

☐ Informationstechnologie

☐ Körper- und Schönheitspflege

☐ Landwirtschaft, Gartenbau und Forstwirtschaft

☐ Lebensmittel

☐ Maschinen, Kfz und Metall

☐ Medien, Kunst und Kultur

☐ Reinigung und Hausbetreuung

☐ Reise, Freizeit und Sport

☐ Sicherheitsdienste

☐ Soziales, Erziehung und Bildung

☐ Textil, Mode und Leder

☐ Umwelt

☐ Verkehr, Transport und Zustelldienste

☐ Wissenschaft, Forschung und Entwicklung

☐ Sonstiges

Frage 30: Ihr höchster Abschluss ist….

☐ Plichtschule

☐ Matura

☐ akademischer Titel

☐ Lehrabschluss

☐ Fachschule

☐ Sonstiges

LISTING – BAYESSCHE STATISTIK IN R

```
library(ggplot2)
library(arm)
library(car)
library(coin)
library(corrplot)
library(dplyr)
library(effects)
library(lme4)
library(lmtest)
library(psych)
library(pwr)
library(ROCR)
library(runjags)
library(coda)
library(VIM)
rjags::load.module("glm")
getwd()

setwd("C:/Users/gafu/Desktop/CAMPUS02_FH")
singlesign <- read.csv("singlesign_on_surveydata.csv", sep = ";")

summary(singlesign)

par(mfrow=c(3,3))

for (i in 1:length(colnames(singlesign))) {
  if(is.numeric(singlesign[,i]))
  {
    hist(singlesign[,i],
         main=colnames(singlesign)[i],
         col="lightblue" ,xlab=colnames(singlesign)[i])
  }
}

summary(singlesign$E5.inverse)

reverseLikertScale = function(df, cols) {
  df[,cols] = lapply(df[,cols],
                     function(col) car::recode(col,
"1=5;2=4;3=3;4=2;5=1"))
  return(df)
}



singlesign = reverseLikertScale(singlesign,
c("E5.inverse","G3","G4","G5"))

for (i in 1:length(colnames(singlesign))) {
  if(is.numeric(singlesign[,i]))
  {
    hist(singlesign[,i],
         main=colnames(singlesign)[i],
         col="lightblue" ,xlab=colnames(singlesign)[i])
  }
```

```
}

items.all = names(singlesign)
items.all
items.vars = singlesign[!items.all %in%
c("Alter","Geschlecht","Ausbildung","Berufsfeld")]
items.demo = singlesign[items.all %in%
c("Alter","Geschlecht","Ausbildung","Berufsfeld")]

par(mfrow=c(1,1))

nrow(singlesign)
sum(complete.cases(singlesign))


cor.single <- cor(items.vars)

corrplot(cor.single)

fa.parallel(items.vars)

alpha(items.vars[c("A1","A2")],na.rm =TRUE)
alpha(items.vars[c("C1")],na.rm =TRUE)
alpha(items.vars[c("D1","D2","D3","D4","D5","D6","D7","D8","D9","D10","D11
")],na.rm =TRUE)
alpha(items.vars[c("E1","E2","E3","E4","E5.inverse")],na.rm =TRUE)
alpha(items.vars[c("F1","F2","F3")],na.rm =TRUE)
alpha(items.vars[c("G1","G2","G3","G4","G5")],na.rm =TRUE)
alpha(items.vars[c("H1","H2","H3","H4","H5","H6","H8","H7","H9","H10","H11
")],na.rm =TRUE)


fa.res = fa(r=items.vars, nfactors=8, fm="minchi", rotate = "promax")
print(loadings(fa.res), cutoff=.4)

paramSingleSign = data.frame(
  Geschlecht = items.demo$Geschlecht,
  Alter = items.demo$Alter,
  Geschlecht.int = as.integer(items.demo$Geschlecht),
  Ausbildung = items.demo$Ausbildung,
  Berufsfeld = items.demo$Berufsfeld,
  UseSingleSignOn = apply(items.vars[c("N1")], 1, mean),
  ITAffinitaet = apply(items.vars[c("A1","A2")],1,mean),
  ExpierenceSingleSignOn = apply(items.vars[c("C1")],1,mean),
  EinstellungSingleSignOn =
apply(items.vars[c("D1","D2","D3","D4","D5","D6","D7","D8","D9","D10","D11
")],1,mean),
  ProblememitAnmeldung =
apply(items.vars[c("E1","E2","E3","E4","E5.inverse")],1,mean),
  SicherheitimUnternehmen = apply(items.vars[c("F1","F2","F3")],1,mean),
  SicherheitsbewusstseinSingle =
apply(items.vars[c("G1","G2","G3","G4","G5")],1,mean),
  SicherheitsbewusstseinAllg =
apply(items.vars[c("H1","H2","H3","H4","H5","H6","H7","H8","H9","H10","H11
")],1,mean)
)

for (row in 1:nrow(paramSingleSign)) {
```

```
  if(paramSingleSign[row, "Alter"] <= 20)
  {
    paramSingleSign[row,"Alter.kat"] = 1
  }
  else if(paramSingleSign[row, "Alter"] > 20 & paramSingleSign[row,
"Alter"] <= 30)
  {
    paramSingleSign[row,"Alter.kat"] = 2
  }
else if(paramSingleSign[row, "Alter"] > 30 & paramSingleSign[row, "Alter"]
<= 40)
{
  paramSingleSign[row,"Alter.kat"] = 3
}
  else if(paramSingleSign[row, "Alter"] > 40 & paramSingleSign[row,
"Alter"] <= 50)
  {
    paramSingleSign[row,"Alter.kat"] = 4
  }
  else if(paramSingleSign[row, "Alter"] > 50 & paramSingleSign[row,
"Alter"] <= 60)
  {
    paramSingleSign[row,"Alter.kat"] = 5
  }
}

head(paramSingleSign,10)



model = lm(UseSingleSignOn ~ ITAffinitaet + ExpierenceSingleSignOn +
EinstellungSingleSignOn + ProblememitAnmeldung + SicherheitimUnternehmen +
SicherheitsbewusstseinSingle + SicherheitsbewusstseinAllg, data=df.fac)
summary(model)

SingleSignOnModell = "
data{
N <- length(UseSingleSignOn[])
NGeschlecht <- max(Geschlecht[])
NAlter <- max(Alter[])
}

model{


for(i in 1:N)
{
  UseSingleSignOn[i] ~
  dnorm(mu[i],1/sigma[Geschlecht[i]]^2)


  mu[i] <- beta.a[Alter[i]] + beta.g[Geschlecht[i]] + beta.i *
ITAffinitaet[i] + beta.e * ExpierenceSingleSignOn[i] + beta.ei *
EinstellungSingleSignOn[i] + beta.p * ProblememitAnmeldung[i] + beta.s *
SicherheitimUnternehmen[i] + beta.sbs * SicherheitsbewusstseinSingle[i] +
beta.sba * SicherheitsbewusstseinAllg[i]
}

#4 Gruppen, kein Shrinkage
```

```
for(g in 1:NGeschlecht)
{
  beta.g[g] ~ dnorm(0,1/1^2)
}


for(g in 1:NGeschlecht)
{
  sigma[g] ~ dexp(1)
}

shrink.factor.mu ~ dnorm(0,1/1^2)
shrink.factor.sigma ~ dexp(1)
for(a in 1:NAlter)
{
  beta.a[a] ~ dnorm(shrink.factor.mu,1/shrink.factor.sigma^2)
}

# Eigentliche Beta-Koeffizienten ausrechnen
for (g in 1:NGeschlecht) {
for (a in 1:NAlter) {
mtx[g,a] <- beta.g[g] + beta.a[a]
}
}


intercept <-mean(mtx[1:NGeschlecht,1:NAlter])
for (g in 1:NGeschlecht) {
beta.geschlecht[g] <- mean(mtx[g,1:NAlter]) - intercept
}

for (a in 1:NAlter) {
beta.alter[a] <- mean(mtx[1:NGeschlecht,a]) - intercept
}


beta.i ~ dnorm(0,1/1^2)
beta.sbs ~ dnorm(0,1/1^2)
beta.sba ~ dnorm(0,1/1^2)
beta.e ~ dnorm(0,1/1^2)
beta.ei ~ dnorm(0,1/1^2)
beta.p ~ dnorm(0,1/1^2)
beta.s ~ dnorm(0,1/1^2)

}

"

modell = run.jags(
  model = SingleSignOnModell,
  data = list(
    Geschlecht = paramSingleSign$Geschlecht.int,
    Alter = paramSingleSign$Alter.kat,
    UseSingleSignOn = my.scale(paramSingleSign$UseSingleSignOn),
    ITAffinitaet = my.scale(paramSingleSign$ITAffinitaet),
    ExpierenceSingleSignOn =
my.scale(paramSingleSign$ExpierenceSingleSignOn),
    EinstellungSingleSignOn =
my.scale(paramSingleSign$EinstellungSingleSignOn),
```

```
    ProblememitAnmeldung = my.scale(paramSingleSign$ProblememitAnmeldung),
    SicherheitimUnternehmen =
my.scale(paramSingleSign$SicherheitimUnternehmen),
    SicherheitsbewusstseinSingle =
my.scale(paramSingleSign$SicherheitsbewusstseinSingle),
    SicherheitsbewusstseinAllg =
my.scale(paramSingleSign$SicherheitsbewusstseinAllg)
  ),
  #3 Ketten
  n.chains=3,
  #wenn Sample erhöht wird, konvegiert das Modell meistens besser, jeoch
Verlangsamung
  sample=10000,
  #auch Thin kann verwendet werden, damit das Modell verbessert wird
  #20000 Durchläufe werden gemacht und nur jedes 2.Ergebnis wird behalten,
jedoch Verlangsamung
  thin=2,

monitor=c("beta.geschlecht","beta.alter","beta.i","beta.sbs","beta.sba","b
eta.e","beta.ei","beta.p","sigma")
)

summary(paramSingleSign$Geschlecht.int)
summary(modell)


plot.Coef.Summary(modell,c("beta.geschlecht","beta.alter","beta.i","beta.s
bs","beta.sba","beta.e","beta.ei","beta.p","sigma"), "Gruppenvergleich")


resultMatrix = as.matrix(modell$mcmc)

beta.geschlecht1 = resultMatrix[,"beta.geschlecht[1]"]
beta.geschlecht2 = resultMatrix[,"beta.geschlecht[2]"]
beta.alter1 = resultMatrix[,"beta.alter[1]"]
beta.alter2 = resultMatrix[,"beta.alter[2]"]
beta.alter3 = resultMatrix[,"beta.alter[3]"]
beta.alter4 = resultMatrix[,"beta.alter[4]"]
beta.alter5 = resultMatrix[,"beta.alter[5]"]
beta.i = resultMatrix[,"beta.i"]
beta.sbs = resultMatrix[,"beta.sbs"]
beta.sba = resultMatrix[,"beta.sba"]
beta.e = resultMatrix[,"beta.e"]
beta.ei = resultMatrix[,"beta.ei"]
beta.p = resultMatrix[,"beta.p"]


summary = plotPost(beta.geschlecht1, cenTend =
"median",main="Geschlecht1")
summary = plotPost(beta.geschlecht2, cenTend =
"median",main="Geschlecht2")
summary = plotPost(beta.alter1, cenTend = "median",main="Alter < 20")
summary = plotPost(beta.alter2, cenTend = "median",main="Alter < 30")
summary = plotPost(beta.alter3, cenTend = "median",main="Alter < 40")
summary = plotPost(beta.alter4, cenTend = "median",main="Alter < 50")
summary = plotPost(beta.alter5, cenTend = "median",main="Alter < 60")
summary = plotPost(beta.i, cenTend = "median", main="IT-Affinität")
summary = plotPost(beta.sbs, cenTend = "median",
main="Sicherheitsbewusstsein Single Sign On")
```

```
summary = plotPost(beta.sba, cenTend = "median",
mein="Sicherheitsbewusstsein Allgmein")
summary


#Geschlecht, Sicherheitsbewusstsein Single Sign On, Einstellung Single
Sign On, IT Affinität Single Sign On


SingleSignOnModellAlter = "
data{
N <- length(UseSingleSignOn[])
NGeschlecht <- max(Geschlecht[])
NAlter <- max(Alter[])
}

model{


for(i in 1:N)
{
  UseSingleSignOn[i] ~
  dnorm(mu[i],1/sigma[Geschlecht[i]]^2)

  #Intercept ist bereits in Liga und Positionen enthalten
  mu[i] <- beta.a[Alter[i]] + beta.g[Geschlecht[i]] +
beta.i[Geschlecht[i]] * ITAffinitaet[i] + beta.e *
ExpierenceSingleSignOn[i] + beta.ei[Geschlecht[i]] *
EinstellungSingleSignOn[i] + beta.p * ProblememitAnmeldung[i] + beta.s *
SicherheitimUnternehmen[i] + beta.sbs[Geschlecht[i]] *
SicherheitsbewusstseinSingle[i] + beta.sba * SicherheitsbewusstseinAllg[i]
}

for(g in 1:NGeschlecht)
{
  beta.g[g] ~ dnorm(0,1/1^2)
}

 for(g in 1:NGeschlecht)
{
  sigma[g] ~ dexp(1)
}

shrink.factor.mu ~ dnorm(0,1/1^2)
shrink.factor.sigma ~ dexp(1)
for(a in 1:NAlter)
{
  beta.a[a] ~ dnorm(shrink.factor.mu,1/shrink.factor.sigma^2)
}

# Eigentliche Beta-Koeffizienten ausrechnen
for (g in 1:NGeschlecht) {
for (a in 1:NAlter) {
mtx[g,a] <- beta.g[g] + beta.a[a]
}
}


intercept <-mean(mtx[1:NGeschlecht,1:NAlter])
```

```
for (g in 1:NGeschlecht) {
beta.geschlecht[g] <- mean(mtx[g,1:NAlter]) - intercept
}

for (a in 1:NAlter) {
beta.alter[a] <- mean(mtx[1:NGeschlecht,a]) - intercept
}



for(g in 1:NGeschlecht) {
beta.i[g] ~ dnorm(0,1/1^2)
}

beta.sba ~ dnorm(0,1/1^2)

for(g in 1:NGeschlecht){
beta.sbs[g] ~ dnorm(0,1/1^2)
}

beta.e ~ dnorm(0,1/1^2)

for (g in 1:NGeschlecht) {
beta.ei[g] ~ dnorm(0,1/1^2)
}

beta.p ~ dnorm(0,1/1^2)
beta.s ~ dnorm(0,1/1^2)

}

"

modell = run.jags(
  model = SingleSignOnModellGeschlecht,
  data = list(
    Geschlecht = paramSingleSign$Geschlecht.int,
    Alter = paramSingleSign$Alter.kat,
    UseSingleSignOn = my.scale(paramSingleSign$UseSingleSignOn),
    ITAffinitaet = my.scale(paramSingleSign$ITAffinitaet),
    ExpierenceSingleSignOn =
my.scale(paramSingleSign$ExpierenceSingleSignOn),
    EinstellungSingleSignOn =
my.scale(paramSingleSign$EinstellungSingleSignOn),
    ProblememitAnmeldung = my.scale(paramSingleSign$ProblememitAnmeldung),
    SicherheitimUnternehmen =
my.scale(paramSingleSign$SicherheitimUnternehmen),
    SicherheitsbewusstseinSingle =
my.scale(paramSingleSign$SicherheitsbewusstseinSingle),
    SicherheitsbewusstseinAllg =
my.scale(paramSingleSign$SicherheitsbewusstseinAllg)
  ),
  #3 Ketten
  n.chains=3,
  #wenn Sample erhöht wird, konvegiert das Modell meistens besser, jeoch
Verlangsamung
  sample=10000,
  #auch Thin kann verwendet werden, damit das Modell verbessert wird
```

```
  #20000 Durchläufe werden gemacht und nur jedes 2.Ergebnis wird behalten,
jedoch Verlangsamung
  thin=2,

monitor=c("beta.geschlecht","beta.alter","beta.i","beta.sbs","beta.sba","b
eta.e","beta.ei","beta.p","sigma")
)

summary(paramSingleSign$Geschlecht.int)
summary(modell)

plot.Coef.Summary(modell,c("beta.sbs","beta.i","beta.ei"),
"Gruppenvergleich")



#Alter, Sicherheitsbewusstsein Single Sign On, Einstellung Single Sign On,
IT Affinität Single Sign On


SingleSignOnModellGeschlecht = "
data{
N <- length(UseSingleSignOn[])
NGeschlecht <- max(Geschlecht[])
NAlter <- max(Alter[])
}

model{


for(i in 1:N)
{
  UseSingleSignOn[i] ~
  dnorm(mu[i],1/sigma[Geschlecht[i]]^2)

  #Intercept ist bereits in Liga und Positionen enthalten
  mu[i] <- beta.a[Alter[i]] + beta.g[Geschlecht[i]] + beta.i[Alter[i]] *
ITAffinitaet[i] + beta.e * ExpierenceSingleSignOn[i] + beta.ei[Alter[i]] *
EinstellungSingleSignOn[i] + beta.p * ProblememitAnmeldung[i] + beta.s *
SicherheitimUnternehmen[i] + beta.sbs[Alter[i]] *
SicherheitsbewusstseinSingle[i] + beta.sba * SicherheitsbewusstseinAllg[i]
}

for(g in 1:NGeschlecht)
{
  beta.g[g] ~ dnorm(0,1/1^2)
}

for(g in 1:NGeschlecht)
{
  sigma[g] ~ dexp(1)
}

shrink.factor.mu ~ dnorm(0,1/1^2)
shrink.factor.sigma ~ dexp(1)
for(a in 1:NAlter)
{
  beta.a[a] ~ dnorm(shrink.factor.mu,1/shrink.factor.sigma^2)
}
```

```
# Eigentliche Beta-Koeffizienten ausrechnen
for (g in 1:NGeschlecht) {
for (a in 1:NAlter) {
mtx[g,a] <- beta.g[g] + beta.a[a]
}
}


intercept <-mean(mtx[1:NGeschlecht,1:NAlter])
for (g in 1:NGeschlecht) {
beta.geschlecht[g] <- mean(mtx[g,1:NAlter]) - intercept
}

for (a in 1:NAlter) {
beta.alter[a] <- mean(mtx[1:NGeschlecht,a]) - intercept
}


for(g in 1:NAlter) {
beta.i[g] ~ dnorm(0,1/1^2)
}

beta.sba ~ dnorm(0,1/1^2)

for(g in 1:NAlter){
beta.sbs[g] ~ dnorm(0,1/1^2)
}

beta.e ~ dnorm(0,1/1^2)

for (g in 1:NAlter) {
beta.ei[g] ~ dnorm(0,1/1^2)
}

beta.p ~ dnorm(0,1/1^2)
beta.s ~ dnorm(0,1/1^2)

}

"

modell = run.jags(
  model = SingleSignOnModellGeschlecht,
  data = list(
    Geschlecht = paramSingleSign$Geschlecht.int,
    Alter = paramSingleSign$Alter.kat,
    UseSingleSignOn = my.scale(paramSingleSign$UseSingleSignOn),
    ITAffinitaet = my.scale(paramSingleSign$ITAffinitaet),
    ExpierenceSingleSignOn =
my.scale(paramSingleSign$ExpierenceSingleSignOn),
    EinstellungSingleSignOn =
my.scale(paramSingleSign$EinstellungSingleSignOn),
    ProblememitAnmeldung = my.scale(paramSingleSign$ProblememitAnmeldung),
    SicherheitimUnternehmen =
my.scale(paramSingleSign$SicherheitimUnternehmen),
    SicherheitsbewusstseinSingle =
my.scale(paramSingleSign$SicherheitsbewusstseinSingle),
```

```
    SicherheitsbewusstseinAllg =
my.scale(paramSingleSign$SicherheitsbewusstseinAllg)
  ),
  #3 Ketten
  n.chains=3,
  #wenn Sample erhöht wird, konvegiert das Modell meistens besser, jeoch
Verlangsamung
  sample=10000,
  #auch Thin kann verwendet werden, damit das Modell verbessert wird
  #20000 Durchläufe werden gemacht und nur jedes 2.Ergebnis wird behalten,
jedoch Verlangsamung
  thin=2,

monitor=c("beta.geschlecht","beta.alter","beta.i","beta.sbs","beta.sba","b
eta.e","beta.ei","beta.p","sigma")
)

summary(paramSingleSign$Geschlecht.int)
summary(modell)

plot.Coef.Summary(modell,c("beta.sbs","beta.i","beta.ei"),
"Gruppenvergleich")
```