



Fakultät für Ingenieurwissenschaften

## **Master-Thesis**

Analyse von Fallback Methoden im Identity and Access  
Management

Abschlussarbeit zur Erlangung des Grades eines

## **Master of Engineering**

der Hochschule Wismar

eingereicht von:

Stefan Alfeis

Studiengang IT-Sicherheit und Forensik

Erstgutachter:

Prof. Dr. Nils Gruschka

Zweitgutachter:

Prof. Dr. Antje Raab-Düsterhöft

Hannover, den 05. September 2024

---

## **Vorwort und Danksagung**

Ich möchte mich bei all denjenigen bedanken, die mich während der Anfertigung dieser Master Thesis unterstützt, begleitet und motiviert haben. Mein erster Dank gilt Herrn Prof. Dr. Nils Gruschka für die Betreuung dieser Master Thesis und seine Unterstützung bei Fragen und Diskussionen. Weiterhin bedanke ich mich bei Frau Prof. Dr. Antje Raab-Düsterhöft für die freundliche Übernahme des Korreferats. Mein weiterer Dank gilt meinen Kommilitonen für die schöne Studienzeit, insbesondere Thorben Höppner, Nikolay Isakov und Maik Ringleb für unsere gemeinsamen Fahrten zu den Präsenzterminen. Ebenso bedanke ich mich bei Jascha Schütte für sein offenes Ohr bei Fragen und seine Denkanstöße, die mir häufig weiter halfen. Abschließend möchte ich mich bei meiner Frau und meinem Sohn bedanken, die mich während des Studiums immer mit aller Kraft unterstützt und motiviert haben, wenn es mal hakte.

Stefan Alfeis

---

## Aufgabenstellung

Viele Unternehmen und Internetdienste bieten ihren Nutzern die Möglichkeit mittels Identity and Access Management Zugang zu Onlinediensten und Anwendungen zu erhalten. Diese Verfahren zur Authentifizierung bestehen meistens aus mehreren Faktoren, wie zum Beispiel Nutzername, Passwort und einem zweiten Faktor (z.B. Nutzung eines One Time Password OTP). Vergisst der Nutzer diese Faktoren teilweise oder in Gänze, hat er die Möglichkeit, sich über einen Fallback Zugang zum Dienst oder der Anwendung zu verschaffen. Fallback Methoden oder Wiederherstellungsmethoden können unterschiedlich implementiert werden, als Beispiel seien hier durch den Nutzer ausgewählte Fragen oder zusätzliche Codes genannt. Durch die Verringerung der Anzahl notwendiger Faktoren, sind diese Daten für Cyberkriminelle von hohem Interesse.

Ziel dieser Masterthesis ist es, verschiedene Umsetzungen von Wiederherstellungsmethoden zu betrachten und ihre Unterschiede zu vergleichen. In die Betrachtung werden auch aktuelle bekannte Angriffe auf Wiederherstellungsmethoden einbezogen sowie deren Wirksamkeit und Erfolg.

Anschließend soll eine Bewertung der Wiederherstellungsmethoden erfolgen. Zur Bewertung sollen vorhandene Methoden aufgegriffen und durch ergänzende Faktoren erweitert werden. Ziel hierbei ist es, die Spanne zwischen Informationssicherheit und Verwendbarkeit / Erreichbarkeit der Wiederherstellungsmethode zu verringern und somit einen potentiellen Missbrauch zu vermeiden. Aufbauend auf der erfolgten Bewertung soll die Möglichkeit zur Entwicklung einer sicheren Wiederherstellungsmethode ergründet werden.

---

## Abstrakt

Wiederherstellungsmethoden sind für Zugänge zu Onlinediensten und Anwendungen enorm wichtig für den Fall, dass ein Benutzer die primären Authentifikationsfaktoren nicht mehr zur Verfügung hat. Ähnlich wie für die primären Authentifikationsfaktoren gilt auch für die Wiederherstellungsmethoden, dass der Zugriff für Unbefugte möglichst verhindert wird. Es gibt verschiedene Varianten für Wiederherstellungsmethoden, angefangen bei E-Mails mit einem Link oder Passwort bis hin zu Code-Listen und auch die Verwendung von Token.

Anbieter von Onlinediensten setzen Wiederherstellungsmethoden unterschiedlich um. Hierfür wurden in dieser Masterthesis für einige ausgewählte Anbieter die Wiederherstellungen durchgeführt und mittels eines Graphen-Tools bewertet. Weiterhin wurde eine Benutzer-Umfrage zum Thema Wiederherstellungsmethoden durchgeführt. Diese Umfrage sollte Erkenntnisse zu den Erfahrungen und Anforderungen der Benutzer zu diesen Methoden bringen. In der abschließenden Diskussion wurden die Wiederherstellungsmethoden bewertet. Es wurde festgestellt, dass die Kombination von einigen Methoden für eine höhere Sicherheit sorgen kann, im Vergleich zur parallelen Umsetzung mehrerer Methoden.

---

## **Abstract**

Fallback methods are extremely important for access to online services and applications in the event that a user no longer has the primary authentication factors available. As with the primary authentication factors, the fallback methods also aim to prevent unauthorized access as far as possible. There are various variants of fallback methods, ranging from emails with a link or password to code lists and the use of tokens.

Providers of online services implement fallback methods in different ways. In this master's thesis, recoveries were carried out for a few selected providers and evaluated using a graph tool. A user survey was also carried out on the topic of fallback methods. This survey was intended to provide insights into the users' experiences and requirements for these methods. In the final discussion, the fallback methods were evaluated. It was found that the combination of some methods can provide greater security compared to the parallel implementation of several methods.

# Inhaltsverzeichnis

<b>1. Einleitung</b>	<b>1</b>
1.1. Motivation . . . . .	1
1.2. Zielsetzung und Problemstellung . . . . .	2
1.3. Vorgehen und Ablauf . . . . .	3
<b>2. Grundlagen</b>	<b>4</b>
2.1. Identity and Access Management . . . . .	4
2.1.1. Autorisierung und Authentifizierung . . . . .	5
2.1.2. Passwörter . . . . .	7
2.1.3. Multifaktor Authentifizierung . . . . .	9
2.1.4. Risikobasierte Authentifizierung . . . . .	9
2.1.5. Single-Sign-On . . . . .	10
2.1.6. Zero Trust-Ansatz . . . . .	12
2.1.7. Fast Identity Online . . . . .	12
2.2. Wiederherstellungsmethoden . . . . .	13
2.2.1. Wiederherstellungsmethode Code oder Codeliste . . . . .	14
2.2.2. Wiederherstellungsmethode soziale Authentifikation . . . . .	14
2.2.3. Wiederherstellungsmethode persönliche Fragen / Sicherheitsfragen . . . . .	15
2.2.4. Wiederherstellungsmethode E-Mail oder SMS basiert . . . . .	16
2.2.5. Wiederherstellungsmethode Token basiert . . . . .	17
2.3. Cyberangriffe auf Wiederherstellungsmethoden . . . . .	18
2.3.1. Social Engineering . . . . .	18
2.3.2. Trusted Friend Attacke . . . . .	19
2.3.3. Account Takeover Attacken . . . . .	20
2.3.4. Aktuelle Cyberangriffe auf Wiederherstellungsmethoden . . . . .	22
2.4. Analyse Tool . . . . .	24
2.4.1. Sicherheit . . . . .	24
2.4.2. Zugänglichkeit . . . . .	25
<b>3. Bestandsaufnahme und Methode</b>	<b>27</b>
3.1. Einschränkung und Auswahl der zu bewertenden Accounts . . . . .	27

---

3.2.	Erstellung von Accounts . . . . .	28
3.2.1.	Account Amazon . . . . .	28
3.2.2.	Account Apple . . . . .	29
3.2.3.	Account Google . . . . .	31
3.2.4.	Account Microsoft . . . . .	32
3.2.5.	Account Meta . . . . .	33
3.2.6.	Account Web.de . . . . .	33
3.2.7.	Account Ubiquiti Unifi . . . . .	34
3.2.8.	Account Steam . . . . .	35
3.2.9.	Account Facebook . . . . .	35
3.3.	Umsetzung von Wiederherstellungsmethoden . . . . .	36
3.3.1.	Wiederherstellung Amazon . . . . .	36
3.3.2.	Wiederherstellung Apple . . . . .	38
3.3.3.	Wiederherstellung Google . . . . .	41
3.3.4.	Wiederherstellung Microsoft . . . . .	44
3.3.5.	Wiederherstellung Meta . . . . .	44
3.3.6.	Wiederherstellung Web.de . . . . .	45
3.3.7.	Wiederherstellung Ubiquiti Unifi . . . . .	49
3.3.8.	Wiederherstellung Steam . . . . .	51
3.4.	Methode . . . . .	54
3.4.1.	Benutzer-Umfrage . . . . .	54
<b>4.</b>	<b>Analyse</b>	<b>59</b>
4.1.	Analyse der Sicherheitswerte . . . . .	59
4.1.1.	Sicherheitsbewertung Amazon . . . . .	59
4.1.2.	Sicherheitsbewertung Apple . . . . .	60
4.1.3.	Sicherheitsbewertung Google . . . . .	61
4.1.4.	Sicherheitsbewertung Microsoft . . . . .	62
4.1.5.	Sicherheitsbewertung Meta . . . . .	62
4.1.6.	Sicherheitsbewertung Web.de . . . . .	63
4.1.7.	Sicherheitsbewertung Ubiquiti Unifi . . . . .	64
4.1.8.	Sicherheitsbewertung Steam . . . . .	65
4.2.	Analyse der Zugänglichkeit . . . . .	66
4.2.1.	Zugänglichkeitsbewertung Amazon . . . . .	66
4.2.2.	Zugänglichkeitsbewertung Apple . . . . .	67
4.2.3.	Zugänglichkeitsbewertung Google . . . . .	68
4.2.4.	Zugänglichkeitsbewertung Microsoft . . . . .	69
4.2.5.	Zugänglichkeitsbewertung Meta . . . . .	70
4.2.6.	Zugänglichkeitsbewertung Web.de . . . . .	71

4.2.7.	Zugänglichkeitsbewertung Ubiquiti Unifi . . . . .	72
4.2.8.	Zugänglichkeitsbewertung Steam . . . . .	73
<b>5.</b>	<b>Umfrage</b>	<b>74</b>
5.1.	Auswertung der Umfrage . . . . .	74
5.1.1.	Frage 1 „Wie alt sind Sie?“ . . . . .	74
5.1.2.	Frage 2 „Welche Erfahrung haben Sie mit Informationstechnologien?“ . . . . .	75
5.1.3.	Frage 3 „Welche der folgenden Wiederherstellungsmethoden kennen Sie?“ . . . . .	75
5.1.4.	Frage 4 „Haben Sie bei einem der folgenden Anbieter einen Benutzeraccount?“ . . . . .	76
5.1.5.	Frage 5 „Welche Wiederherstellungsmethode haben Sie für den / die Anbieter gewählt?“ . . . . .	77
5.1.6.	Frage 6 „Wenn in der vorherigen Frage „Andere“ ausgewählt wurde, welche Methode wird verwendet? (Bitte Anbieter nennen)“ . . . . .	78
5.1.7.	Frage 7 „Haben Sie schon einmal für einen Onlinezugang eine Wiederherstellung durchgeführt oder durchführen müssen?“ . . . . .	79
5.1.8.	Frage 8 „Wenn Frage 7 mit Ja beantwortet wurde, welche Methode wurde für die Wiederherstellung angewendet? (Bitte Anbieter und Methode nennen)“ . . . . .	79
5.1.9.	Frage 9 „Wenn Frage 8 beantwortet wurde, wie zufrieden waren Sie mit der gewählten / geforderten Methode? (1 Daumen = unzufrieden, 5 Daumen = sehr zufrieden)“ . . . . .	80
5.1.10.	Frage 10 „Was ist Ihnen wichtiger, wenn Sie an Wiederherstellungsmethoden denken, Sicherheit oder Bedienbarkeit?“ . . . . .	80
5.1.11.	Frage 11 „Wären Sie bereit für eine höhere Sicherheit bei Wiederherstellungsmethoden zusätzliche technische Maßnahmen in Kauf zu nehmen? (z.B. eine Handy-App, USB-Token oder ähnliches)“ . . . . .	81
5.2.	Fazit der Umfrage . . . . .	81
<b>6.</b>	<b>Bewertbarkeit von Wiederherstellungsmethoden</b>	<b>83</b>
<b>7.</b>	<b>Diskussion und Empfehlung</b>	<b>89</b>
<b>8.</b>	<b>Fazit und Ausblick</b>	<b>95</b>
8.1.	Fazit . . . . .	95
8.2.	Ausblick . . . . .	96



---

<b>Literatur</b>	<b>97</b>
<b>Abbildungsverzeichnis</b>	<b>107</b>
<b>Tabellenverzeichnis</b>	<b>108</b>
<b>Abkürzungsverzeichnis</b>	<b>109</b>
<b>A. Anhang</b>	<b>110</b>
A.1. Weitere Darstellungen des AAG . . . . .	110
A.2. Bilder aus Benutzerumfrage . . . . .	111
A.3. Rohdaten zur Benutzerumfrage . . . . .	113

# 1. Einleitung

„Wie lautet der Mädchenname Ihrer Mutter?“ Diese Frage werden viele Benutzer von Onlinediensten bereits gestellt bekommen haben[1]. Solche Abfragen werden häufig im Rahmen einer Registrierung bei einem Onlinedienst gestellt und sollen als Recovery Option (Rückhol-Option) oder Fallback-Methode (Wiederherstellungsmethode) für den jeweiligen Onlinezugang (Account) dienen. Verliert der Benutzer seine primären Anmeldedaten, so wird über diese Wiederherstellungsmethode die Möglichkeit gegeben, Zugang zum jeweiligen Account zu erhalten. Viele Anbieter von Online-Diensten (z.B. Google, Apple, Meta) bieten ihren Kunden die Möglichkeit verschiedene Dienste und Plattformen mittels Identity und Access Management zu nutzen. Hierdurch können die Kunden für diese Anwendungen und Plattformen die gleichen Authentifizierungsmethoden nutzen.

## 1.1. Motivation

Wiederherstellungsmethoden können auf unterschiedliche Arten umgesetzt sein, unter anderem Einmal-Passwörter oder Sicherheitsfragen, wie im einleitenden Satz bereits genannt. Auch die Nutzung der sozialen Interaktion des Benutzers (social-graph) oder von Token sind verbreitete Maßnahmen[2].

Anwender und Administratoren nutzen heutzutage eine Vielzahl von verschiedenen Accounts. Diese Accounts dienen dem Zugriff auf Systeme, Webseiten oder Anwendungen. Unternehmen nutzen für die Authentifizierung und Autorisierung der Anwender ein Identity and Access Management (IAM). Für viele Authentifikationsmethoden gibt es neben der Möglichkeit zur Nutzung eines zweiten Faktors zur Authentifizierung (2FA) auch Wiederherstellungsmethoden[2]. Diese Wiederherstellungsmethoden bieten die Möglichkeit bei Verlust der primären Authentifizierungsdaten den Zugriff auf Systeme oder Anwendungen zu erhalten.

Die Nutzung von multiplen Authentifizierungsfaktoren erhöht die Sicherheit von Accounts signifikant gegenüber der reinen Authentifizierung durch die Nutzung eines Passwortes[3]. Durch die Nutzung eines zweiten Faktor reicht es für einen potentiellen

---

Angreifer nicht mehr aus, das zum Account gehörige Passwort zu erlangen. Daher ist es für Cyberkriminelle äußerst lukrativ an die Daten der Wiederherstellungsmethode zu gelangen, um somit Zugang zu Systemen oder Anwendungen zu erhalten.

Die Anwender von IAM stehen bei der Wahl der Absicherung ihrer Accounts häufig vor der Wahl einer Methode mit hoher Informationssicherheit (information security) oder einer einfacheren Verwendbarkeit (usability) / Erreichbarkeit (accessability). Dieser Umstand führt schnell dazu, dass eine leichtere Erreichbarkeit präferiert wird und somit die Informationssicherheit gemindert wird. Als Beispiel sei hier die Nutzung von Passwort Managern genannt. Diese bieten meist eine hohe Sicherheit bei der Erzeugung und Ablage von Passwörtern, es gibt jedoch diverse Bedenken zumeist älterer Anwender (z.B. Hoheit über die eigenen Daten bei Ablage der Daten in einer Cloud oder der Passwort Manager als Single Point of Failure) gegenüber diesen Tools[4].

Cyberkriminelle haben vermehrt den Fokus auf Wiederherstellungsmethoden gelegt, da es bei Erlangung der zugehörigen Informationen schnell möglich ist, einen Account zu übernehmen. Dies ist hier einfacher, da für Wiederherstellungsmethoden meist weniger Faktoren verwendet werden, als für die primäre Authentifizierung[5].

## **1.2. Zielsetzung und Problemstellung**

Ziel dieser Master-Thesis ist es, die Umsetzungen vorhandener Wiederherstellungsmethoden zu analysieren und aktuelle Angriffe auf Wiederherstellungsmethoden aufzuzeigen. Im Jahr 2023 gab es einen massiven Anstieg im Bereich der Account takeover attacks (ATO)[5]. Diese Tendenz zeigt, dass eine möglichst hohe Sicherheit für Wiederherstellungsmethoden durch die jeweiligen Anbieter anzustreben ist.

Im Detail ist mit der Analyse der vorhandenen Methoden zum einen die Darstellung der Umsetzung von Anbietern gemeint. Da es häufig zu einem Konflikt zwischen der Informationssicherheit und der Verwendbarkeit / Erreichbarkeit kommt, sollen Möglichkeiten zur Entschärfung dieses Konflikts analysiert werden. Zum anderen soll untersucht werden, wie ein Missbrauch von Wiederherstellungsmethoden erschwert oder unterbunden werden kann.

Abschließend werden die Möglichkeiten zur Entwicklung sicherer Wiederherstellungsmethoden betrachtet.

---

## 1.3. Vorgehen und Ablauf

Das erste Kapitel dient zur Einleitung in die Thematik und der Darstellung der Motivation für diese Master-Thesis.

In Kapitel 2 erläutert die Grundlagen, die für das Verständnis dieser Master-Thesis notwendig sind. Hierbei werden zunächst die Begriffe des Identity and Access Managements erklärt. Aufbauend hierauf folgen die Grundlagen zu den Wiederherstellungsmethoden. Es werden die Methoden einzeln erläutert und mögliche Cyberangriffe auf Wiederherstellungsmethoden betrachtet.

Kapitel 3 befasst sich mit der genauen Darstellung der Umsetzung ausgewählter Wiederherstellungsmethoden. Eine umfassende Betrachtung aller Methoden ist im Rahmen dieser Master-Thesis nicht durchführbar, daher wird die Auswahl der Varianten und Anbieter eingeschränkt auf führende Anbieter in der IT-Technologie, ausgesuchte IT-Infrastrukturtechnik-Anbieter sowie E-Mail-Provider und Spieleplattformbetreiber. Es wird auch das verwendete Tool zur Analyse vorgestellt.

In Kapitel 4 wird die Analyse der gewählten Anbieter unter Nutzung des bereits genannten Tools umgesetzt und beschrieben.

Kapitel 5 stellt die Auswertung der durchgeführten Umfrage dar. Abschließend erfolgt ein kurzes Fazit zur Umfrage.

Kapitel 6 soll der Betrachtung der Bewertbarkeit von Wiederherstellungsmethoden dienen. Es wird analysiert, ob es möglich ist, Wiederherstellungsmethoden gegeneinander in ein Ranking zu stellen und somit eine Aussage über die Reife der jeweiligen Methode zu geben.

In Kapitel 7 werden die aus Kapitel 4 und 5 gewonnen Erkenntnisse diskutiert. Abschließend folgen in Kapitel 8 ein Fazit und ein Ausblick.

## 2. Grundlagen

In diesem Kapitel werden notwendige Grundlagen zum Verständnis der Master-Thesis erläutert. Hierbei werden die Zusammenhänge im Identity and Access Management und der Wiederherstellungsmethoden erklärt. Abschließend werden einige Gefahren und Angriffe auf Wiederherstellungsmethoden dargestellt.

### 2.1. Identity and Access Management

Identity and Access Management sorgt für eine zentrale Verwaltung von Identitäten und Zugriffsrechten auf verschiedene Systeme und Anwendungen. Es bildet einen Oberbegriff für alle notwendigen Prozesse und Anwendungen, die für die Verwaltung von Identitäten und Zugriffsrechten eingesetzt werden[6]. Hierzu zählen alle benötigten Applikationen, Systeme und Ressourcen. Identity und Access Management Systeme sind in der Lage, in Echtzeit Rechte und Rollen zu vergeben oder zu entziehen. Eine der wichtigsten Aufgaben eines Identity and Access Managements besteht also darin, die Zugriffsrechte der Benutzer zu verwalten, damit das betreffende System den Benutzer authentifizieren und autorisieren kann[6].

Die Begriffe Authentifikation und Autorisierung werden in den folgenden Kapiteln näher betrachtet. Bei der Vergabe von Rollen und Rechten sollte immer auf das Need-to-know-Prinzip geachtet werden. Informationen, die für den Benutzer nicht von Belang sind, sollten diesem auch nicht zur Verfügung stehen[7].

Hilfestellung zur Einrichtung eines Identity and Access Managements bietet unter anderem das IT-Grundschutz-Kompendium des Bundesamt für Sicherheit in der Informationstechnik (BSI). Im Baustein ORP.4: Identitäts- und Berechtigungsmanagement werden im Kapitel 3 Anforderungen Informationen gegeben, die bei der Umsetzung von Regelungen für ein Identity and Access Management helfen können[8].

Das Identity and Access Management lässt sich in zwei Bereiche aufteilen, ein als Verwaltungsteil zu bezeichnender Bereich Identitätsmanagement (Identity Management) und einen Nutzungsteil, das Zugriffsmanagement (Access Management)[9].

---

Das Identitätsmanagement hat die Aufgabe als Identity Provider, einen Bestand von digitalen Identitäten zu verwalten. Diese Form des Managements erzeugt, aktualisiert und archiviert alle das System betreffenden Identitäten. Das Zugriffsmanagement hat die Aufgabe, den durch das Identitätsmanagement verwalteten Identitäten nach Prüfung der Voraussetzungen den Zugriff auf IT-Ressourcen zu gewähren. Es dient somit als Service Provider[9].

Ein Teil des Zugriffsmanagements ist die Identifikation, bei der ein Benutzer seine Identität gegenüber einem IT-Dienst oder System nachweist. Dies geschieht über die im Identitätsmanagement hinterlegte digitale Identität. Für natürliche Personen ist dies die Benutzererkennung. Bei technischen Komponenten erfolgt eine Personalisierung, eine eindeutige Zuordnung der IT-Komponente. Damit eine digitale Identität im Identitätsmanagement hinterlegt wird, muss die natürliche Person oder die IT-Komponente registriert werden. Hierfür werden Informationen der natürlichen Person oder der IT-Komponente im System hinterlegt und es wird ein Authentisierungsmerkmal erzeugt, damit eine sichere Wiedererkennung gewährleistet werden kann[9].

### **2.1.1. Autorisierung und Authentifizierung**

Authentifizierung und Autorisierung sind grundlegende Begriffe im Zusammenhang mit Identity und Access Management. Authentifizierung beschreibt das Verfahren, mit dem ein Benutzer seine Identität an einem System bestätigt[10]. Als Benutzer werden in diesem Zusammenhang die Anwender eines Systems und alle Objekte, die im Auftrag eines Anwendenden aktiv sind, bezeichnet. Den Nachweis der Identität erbringt der Benutzer durch die Präsentation bestimmter Informationen (Authentifizierungsmethode), zum Beispiel Benutzererkennung und Passwort. Sind diese Informationen korrekt, so wird dem Benutzer der Zugang zum System gewährt[11]. Abbildung 2.1 zeigt beispielhaft den Ablauf einer Authentifikation.

Je nach geforderter Sicherheitsstufe kann die Eingabe der Informationen aus einem oder mehreren Faktoren bestehen, dies wird in einem späteren Kapitel (siehe 2.1.3) noch erläutert. Authentifizierungsmethoden lassen sich in verschiedene Klassen unterteilen[13]:

Authentifizierung durch Wissen - Der Benutzer hat Wissen über ein Passwort, eine PIN oder zum Beispiel die Antwort auf eine bestimmte Frage. Je nach Komplexität des jeweiligen Wissens finden sich einfachere oder schwierigere Angriffspfade auf diese Authentifikationsmöglichkeit. Einfache Passwörter (siehe 2.1.2) lassen

---

## Authentifikation

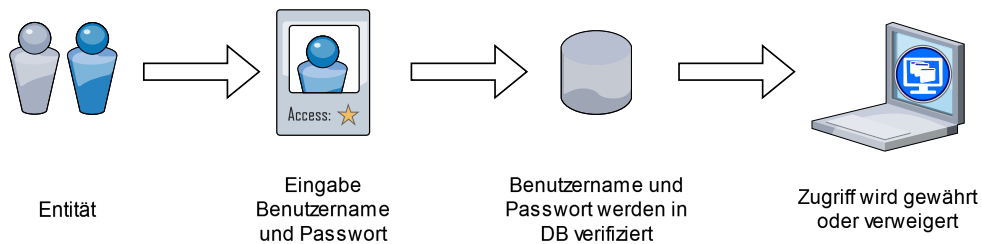


Abbildung 2.1.: Authentifikation [12]

sich mittels Brute-Force-Attacke schnell überwinden, Antworten auf Fragen zum persönlichen Umfeld des Benutzers können anhand von eigenen Aussagen in Social-Media-Kanälen entnommen werden[13][14].

**Authentifizierung durch Besitz** - Der Benutzer besitzt ein zusätzliches Gerät, Smartphone oder Hardware-Token, auf welchem Identifikationsparameter gespeichert sind. Diese Identifikationsparameter können bei Anforderung durch ein System abgerufen werden. Als Beispiel sei hier die Nutzung eines TAN-Generator in Kombination mit der EC-Karte zur Authentifikation im Online-Banking genannt[3].

**Authentifizierung durch Sein** - Der Benutzer nutzt seine physischen Gegebenheiten, um sich an einem System zu authentifizieren. Maßnahmen hierfür sind Iris-Scanner, Fingerabdruck-Scanner, Gesichts- und Stimmerkennung. Diese Maßnahmen können auch in Kombination angewendet werden, wodurch die Qualität der Authentifizierung gesteigert werden kann[11].

**Zusätzliche unterstützende Faktoren** - Zur Beurteilung der Echtheit des Benutzers können auch noch weitere Informationen herangezogen werden, unter anderem die verwendeten Endgeräte des Benutzers, bereits erfolgte Transaktionen des Benutzers (Reputation) oder der Standort und die Zeit des Authentifizierungsprozesses[13].

Mit dem Begriff Autorisierung wird ein Prozess beschrieben, welcher prüft, auf welche Informationen oder Datenobjekte ein Benutzer zugreifen darf oder welche Handlungen auf diesen Informationen erfolgen dürfen (Zugriffsrecht)[10][11]. Durch die Autorisierung werden Rechte vergeben, es wird jedoch keine Identität bestätigt. Somit kann eine Authentifizierung ein Faktor für eine Autorisierung sein, jedoch kann durch eine Autorisierung keine Identifikation von Benutzern oder Geräten

erfolgen[10]. In der folgenden Abbildung 2.2 ist beispielhaft der Ablauf einer Autorisierung dargestellt:

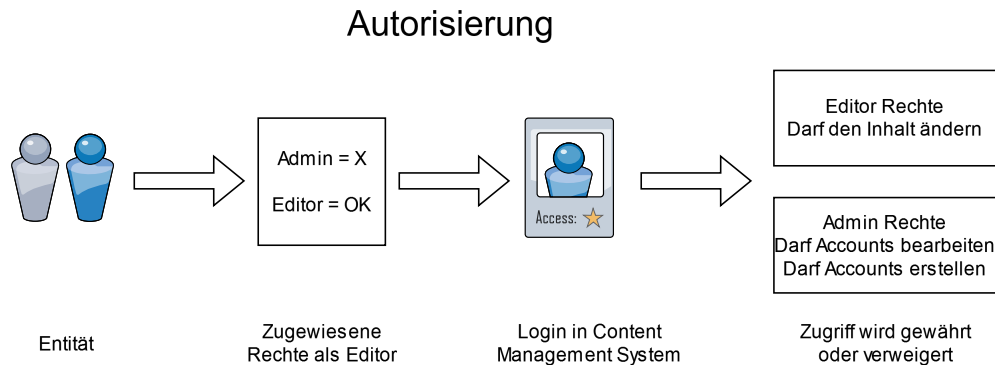


Abbildung 2.2.: Autorisierung [12]

## 2.1.2. Passwörter

Eines der gängigsten und bekanntesten Verfahren der Authentifikation eines Benutzers gegenüber einem System ist die Nutzung einer eindeutigen Kennung, zum Beispiel Benutzername oder ID, und eines dazugehörenden Passwortes. Dieses Passwort sollte nur dem Benutzer bekannt sein, da es als Geheimnis zwischen System und Benutzer gilt[11]. Auf der Seite des Systems muss sicher gestellt werden, dass dieses Geheimnis vor unautorisiertem Zugriff geschützt wird. In den meisten Fällen werden hierzu kryptographische Verfahren beziehungsweise kryptographische Hashfunktionen eingesetzt, damit die Vertraulichkeit der gespeicherten Passwörter auf dem System gewährleistet wird[11].

Bei der Erstellung sicherer Passwörter gibt es mehrere Ansätze. Das BSI und Verbraucherzentralen geben hierfür Hilfestellungen[15][16]:

Lange und weniger komplexe Passwörter

Die Länge des Passwortes soll mindestens 25 Zeichen sein und es sollen nur zwei Zeichenarten verwendet werden, z.B. Groß- und Kleinbuchstaben

Kurze und komplexe Passwörter

Die Mindestlänge des Passwortes beträgt 8 Zeichen und es sollen vier Zeichenarten kombiniert werden (Groß- und Kleinschreibung, Zahlen und Sonderzeichen)



Für jede Art der Passwörterstellung gilt, dass persönliche Angaben (Namen, Geburtsdaten oder ähnliches) zu vermeiden sind und das gewählte Passwort nicht in einem Wörterbuch zu finden sein soll.

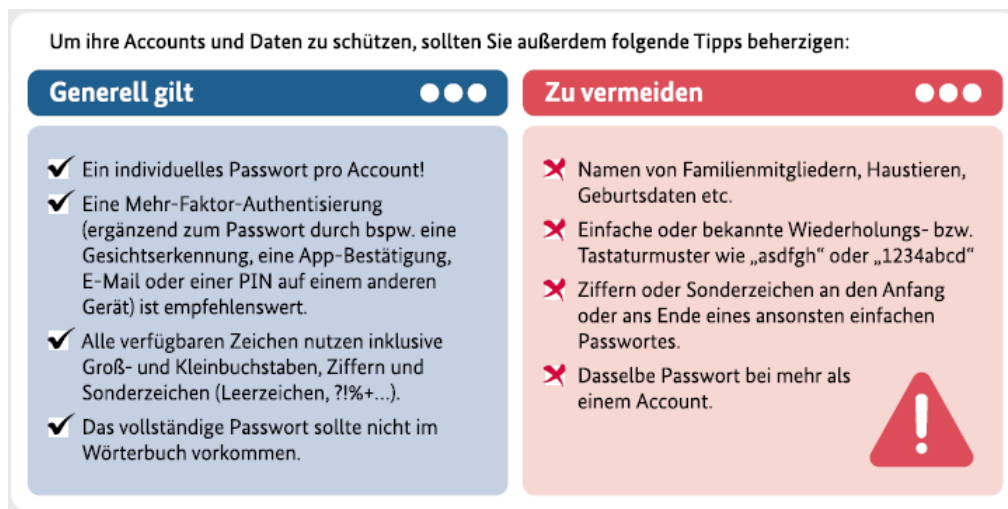


Abbildung 2.3.: Tipps für sichere Passwörter[17]

Frühere Empfehlungen wie Passwörter regelmäßig zu ändern (z.B. alle 3 Monate) werden heutzutage nicht mehr unterstützt, da die Vorgaben teilweise dazu führten, dass die Benutzer Passwörter nur minimal veränderten, damit sie sich die Passwörter leichter merken konnten[16]. Des Weiteren sollte der Benutzer vermeiden, ein Passwort für mehrere Konten zu verwenden. Um die sich hieraus ergebende Komplexität zu verwalten, gibt es die Möglichkeit, Passwort-Manager zu verwenden. Diese bilden eine sichere Ablage für Passwörter und unterstützen den Benutzer bei der Erstellung hinreichend komplexer Passwörter. Einige Passwort-Manager bieten auch eine Online-Synchronisierung an, was die Nutzung auf mehreren Geräten vereinfacht.

Entgegen aller Empfehlungen und Vorgaben verwenden viele Benutzer leicht zu erratende Passwörter. Jährlich wird eine Liste mit den am häufigsten verwendeten Passwörtern herausgegeben. Diese Liste wird durch Daten gespeist, die aus im Darknet gehandelten Listen entnommen werden[13][18][19].

Tabelle 2.1.: Auswahl häufiger Passwörter 2023

123456789	password
12345678	password1
hallo	admin123
1234567890	iloveyou
1234567	qwerty

---

### 2.1.3. Multifaktor Authentifizierung

Bei einer Multifaktor Authentifizierung werden mehrere Authentifizierungsverfahren in Kombination genutzt. Ziel dieser Art der Authentifikation ist ein höheres Level an Sicherheit und Vertrauenswürdigkeit. Es soll hierbei auf die Nutzung unterschiedlicher und unabhängiger Verfahren geachtet werden[13].

Eine der häufigsten Varianten ist die Zweifaktor-Authentifizierung (2FA). Die Zweifaktor-Authentifizierung nutzt zwei unabhängige und unterschiedliche Faktoren für den Nachweis der Echtheit der digitalen Identität des Benutzers oder der IT-Komponente. Die häufigste Variante bildet die Nutzung von Wissen, ein Passwort oder eine PIN und der Nachweis des Besitzes eines Hardware-Sicherheitsmoduls, zum Beispiel eine Smartcard oder ein USB-Token[13].

Bei einer Multifaktor-Authentifizierung wird der Grad der Sicherheit noch weiter erhöht, indem mehr als nur zwei Faktoren für die Authentifizierung verlangt werden. Hierbei können folgende Faktoren genutzt werden:

- Nachweis des Besitzes eines Hardware-Sicherheitsmoduls
- Nachweis von Wissen des Benutzers, zum Beispiel Passwort oder PIN
- Körperliches Charakteristikum, wie zum Beispiel ein Fingerabdruck oder die Stimme
- Nachweis durch das Verhalten des Benutzers, genutzte Technologien oder auch Ort des Zugriffs

Zusätzliche Technologien für die Authentifizierung stellen One-Time-Passwörter (OTP), Besitz einer SIM-Karte (SMS an die zugehörige Nummer) oder der Besitz von QR-Codes dar.

### 2.1.4. Risikobasierte Authentifizierung

Risikobasierte Authentifizierung dient zur Stärkung der Passwortauthentifizierung. Dieser Ansatz überwacht Merkmale, die sich auf das Loginverhalten während der Eingabe des Passwortes beziehen[20]. Unterscheiden sich die beobachteten Merkmale signifikant zu dem bekannten Verhalten, werden durch die risikobasierte Authentifikation weitere zusätzliche Informationen erfragt, zum Beispiel die Lösung eines CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)[21], Verifikation per E-Mail oder auch OTP.

---

In der Umsetzung wird während des Login-Vorgangs das Verhalten des Benutzers analysiert. Je nach System werden hier unter anderem Faktoren wie der geografische Standort, die IP-Adresse des Benutzers, das verwendete Endgerät oder die Nutzung eines Proxy-Server bewertet. Der berechnete Risikowert wird als quantifiziertes Maß für die Wahrscheinlichkeit gewertet, ob es sich um einen legalen oder illegalen/böswilligen Vorgang handelt[22]. Hierbei wird in drei Kategorien unterschieden:

Verbindung mit geringem Risiko - Der Benutzer wird bei einem geringen Risiko nicht aufgefordert zusätzliche Informationen anzugeben. Erfolgt der Anmeldeversuch zum Beispiel von einem bekannten Standort mit einer bekannten IP, wird dieser Anmeldeversuch als risikoarm eingestuft. Auch die Nutzung eines Virtual Privat Network (VPN) wird als risikoarm eingestuft.

Verbindung mit mittlerem Risiko - Bei Berechnung eines mittleren Risiko werden vom Benutzer weitere Informationen eingefordert. Beispiele sind hierfür die Beantwortung dem Benutzer bekannter Fragen oder die Verifikation per E-Mail. Ein Auslöser hierfür kann die Nutzung eines bislang nicht verwendeten Endgeräts sein[22].

Verbindung mit hohem Risiko - Wird bei einer Anmeldeanfrage ein hohes Risiko berechnet, muss der Benutzer weitere Authentifizierungsverfahren nutzen oder es wird automatisch der Zugriff verweigert. Ein Auslöser hierfür kann ein Anmeldeversuch aus einem Land mit vielen bekannten Hackerangriffen sein.

Einer der Vorteile im Vergleich zur Vorgabe von Multifaktor Authentifizierung für den Benutzer bei der risikobasierten Authentifizierung ist, dass erst nach der Berechnung des Risikos weitere Faktoren verlangt werden. Dies kann zu einer höheren Bewertung der Benutzerfreundlichkeit eines Systems führen[22].

### **2.1.5. Single-Sign-On**

Single-Sign-On (SSO) ist eine Technologie, die es Benutzern erlaubt, nach einmaliger Anmeldung an einer zentralen Institution Zugang zu diversen Onlinediensten zu erhalten[23]. Die Technologie Single-Sign-On soll Benutzern den Umgang mit mehreren Services und Anwendungen erleichtern. In der Regel benötigt ein Benutzer für jeden Service oder jede Anwendung eine Kennung mit dazugehörigem Passwort. Aufgrund der Vielzahl dieser Services und Anwendungen müssen sich die Benutzer auch eine Vielzahl an Zugangsdaten merken. Single-Sign-On bietet die Möglichkeit, dies

zu vereinfachen, indem der Benutzer sich an einer zentralen Instanz authentifiziert und anschließend zu allen an diese Instanz gekoppelten Services Zugang erhält, ohne sich erneut zu authentifizieren[24]. Abbildung 2.4 stellt den allgemeinen Ablauf des Verfahrens SSO dar.

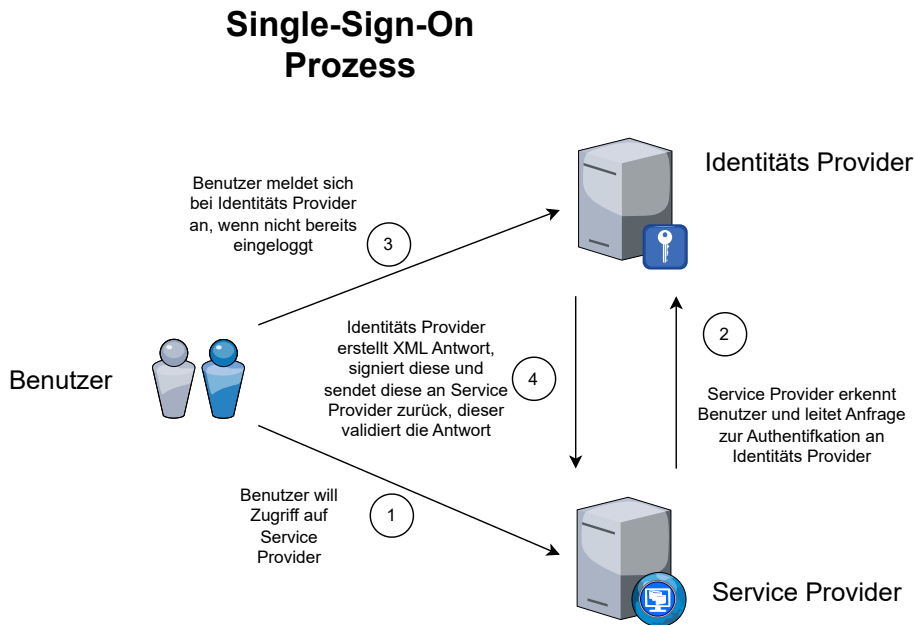


Abbildung 2.4.: Ablauf des Single-Sign-On [25][26]

Es gibt drei verschiedene Typen des Single-Sign-On:

#### 1. Web Single-Sign-On

Web Single-Sign-On ermöglicht es dem Benutzer nach der initialen Anmeldung weitere Web-Dienste zu benutzen, ohne sich erneut Authentifizieren zu müssen. Die Anmeldung stellt eine Vertrauensbasis zwischen der authentifizierenden Instanz und dem Browser des Benutzer her.

#### 2. Legacy Web Single-Sign-On

Legacy Web Single-Sign-On wird auch als Unternehmens Single-Sign-On bezeichnet[23]. Legacy Single-Sign-On ermöglicht es dem Benutzer sich nicht nur bei Web-Services zu authentifizieren, sondern auch bei weiteren Anwendungen des Unternehmens.

#### 3. Federated Single-Sign-On

Federated Single-Sign-On erweitert den Ansatz von Single-Sign-On, indem es dem Benutzer ermöglicht, nach erfolgter Authentifizierung an der eigenen Domäne auch Zugriff auf Services einer weiteren verbundenen Domäne zu erhalten[23]. Beispiele hierfür finden sich in der Nutzung von z.B. eines Google oder Facebook Accounts für weitere Onlinedienste.

---

Vorteile des Single-Sign-On sind, dass der Benutzer sich weniger Zugangsdaten merken oder abspeichern muss. Das verwendete Passwort muss nur einmal übertragen werden, somit wird auch für die Übertragung die Sicherheit erhöht[24].

Ein Nachteil besteht in der Möglichkeit, dass das Single-Sign-On als Single Point of Failure gesehen werden kann. Verliert der Benutzer seine Authentifizierungsdaten, so hat dieser keinen Zugriff mehr auf alle angeschlossenen Dienste. Werden die Authentifizierungsdaten durch einen Angreifer entwendet oder abgefangen, so hat der Angreifer Zugriff auf alle angeschlossenen Dienste[24].

### **2.1.6. Zero Trust-Ansatz**

Der Zero Trust-Ansatz ist ein Cyber-Sicherheitsmodell, bei dem weder internen noch externen Entitäten in einem Netzwerk Vertrauen gewährt wird[13]. Im Gegensatz zum Modell der Perimeter-Sicherheit, bei dem sämtlichen internen Entitäten vertraut wird und lediglich die externe Kommunikation überprüft wird, wird bei Zero Trust die gesamte Kommunikation, intern wie extern, kontrolliert und auf Angriffe untersucht. Jede Entität im Netzwerk muss sich bei jeder Anfrage authentifizieren. Dies führt zu vielen zusätzlichen Maßnahmen, da keine Entität im Netzwerk ohne Sicherheitsmaßnahmen bestehen darf, hilft jedoch bei der Einschränkung von Auswirkungen von externen Angriffen, da diese nach dem Eindringen in das Netzwerk weiterhin gegen Sicherheitsmaßnahmen agieren müssen. Somit wird durch diesen Ansatz eine höhere Sicherheit gegen Advanced Persistent Threats (APT) gewährleistet[13].

### **2.1.7. Fast Identity Online**

Fast Identity Online (FIDO) ist ein Satz offener und lizenzfreier Standards und Protokolle zur sicheren und komfortablen Authentifizierung. Die maßgebliche Entwicklung wurde durch die FIDO-Alliance durchgeführt. FIDO ermöglicht passwortlose 2FA basierend auf der Public-Key-Kryptographie[27].

Im Folgenden wird erläutert, wie der Prozess zur Nutzung von FIDO abläuft. Während der Registrierung bei einem Onlinedienst erzeugt der Benutzer auf seinem Endgerät ein kryptographisches Schlüsselpaar. Der private Teil des Schlüssels verbleibt geheim beim Benutzer, der öffentliche Teil des Schlüssels wird beim Onlinedienst hinterlegt. Dieses Schlüsselpaar wird von FIDO als Passkey bezeichnet[28].

Möchte der Benutzer sich jetzt beim Onlinedienst anmelden, muss dieser sich lokal an seinem Endgerät verifizieren. Dieser Vorgang kann durch ein biometrisches

Merkmal, z.B. der Scan des Fingerabdrucks, Eingabe einer PIN oder durch einen FIDO-Secret-Key erfolgen. Anschließend erfolgt ein Abgleich des Passkey-Paares durch Challenge-Response-Verfahren[29]. Abbildung 2.5 stellt exemplarisch den Ablauf des Challenge-Response-Verfahrens von FIDO dar.

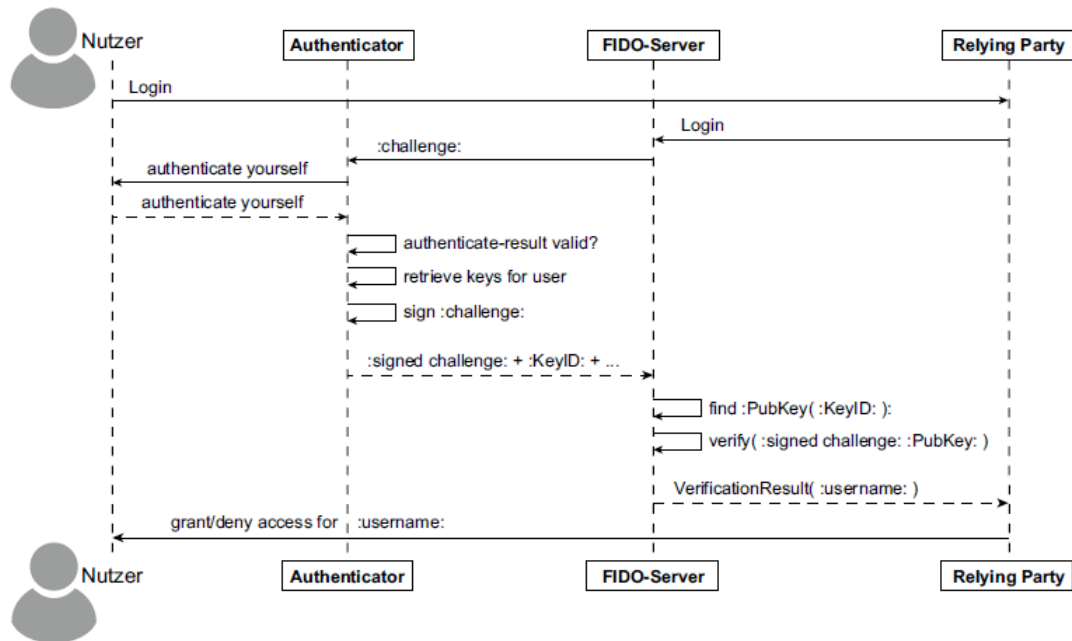


Abbildung 2.5.: Ablauf Challenge-Response-Verfahren FIDO[13]

## 2.2. Wiederherstellungsmethoden

Der Fokus dieser Master-Thesis liegt auf den Wiederherstellungsmethoden für Benutzer-Accounts. Diese Wiederherstellungsmethoden helfen einem Benutzer, der seine primären Authentifizierungsfaktoren verloren oder anderweitig nicht mehr verfügbar hat, Zugang zum jeweiligen Onlinedienst zu erhalten und die primäre Methode zu erneuern[2].

Wiederherstellungsmethoden sind also als „Notfall-Zugang“ zu einem Account zu sehen. Die Umsetzung kann auf verschiedene Weisen erfolgen, wie etwa Passwörter, Codes, E-Mail Verifikation oder weitere Varianten, die im Folgenden noch weiter erklärt werden. Weitere Methoden zur Authentifikation bei einer Wiederherstellung können der Anruf einer Hotline-Nummer, postalische Authentifikation oder auch die Nutzung einer Video-App sein. Diese Varianten sind jedoch nicht im Fokus dieser Arbeit und werden daher nicht weiter erläutert. In verschiedenen Betrachtungen dieses Themas wird wiederholt darauf hingewiesen, dass die Umsetzungen der Wieder-

---

herstellungsmethoden Schwächen beinhalten[2][14]. In den folgenden Abschnitten werden einige Umsetzungen für Wiederherstellungsmethoden dargestellt.

### 2.2.1. Wiederherstellungsmethode Code oder Codeliste

Die erste Variante von Wiederherstellungsmethoden ist die Nutzung von Codes oder Codelisten. Dem Benutzer wird nach dem Einrichten der primären Authentifikationsmethode die Möglichkeit gegeben, den Account durch einen Code oder eine Codeliste abzusichern. Diesen Code oder Codeliste kann sich der Benutzer abspeichern oder ausdrucken. Im Falle des Starts des Wiederherstellungsvorgangs wird der Benutzer nach dem Code oder eines Codes aus der Liste gefragt.

Als Beispiel sei hier die Authentifizierung der Plattform GitHub genannt. GitHub ist ein Online Dienstleister zur Speicherung von Quellcode. Auf GitHub können die Benutzer mit anderen Benutzern zusammenarbeiten und ihren Code teilen[30]. Als primäre Authentifikation wird dem Benutzer eine Zwei-Faktor-Authentifizierung angeboten[31]. Als erster Faktor dient ein Passwort, welches der Benutzer eigenständig wählt. Der zweite Faktor ist ein Code, der entweder durch eine Anwendung auf dem mobilen Endgerät des Benutzers generiert oder dem Benutzer per SMS zu gesendet wird. Die Wiederherstellungsmethode für den GitHub-Account ist eine Codeliste mit 16 Einträgen, die der Benutzer sich unter seinen Account-Einstellungen herunterladen, ausdrucken oder in einem Passwort-Manager speichern kann (siehe Abbildung 2.6)[32]. Mit jedem Wiederherstellungsvorgang wird ein Code der Liste verbraucht. Der Benutzer kann sich in seinen Account-Einstellungen jederzeit eine neue Liste erzeugen, hierdurch wird die zuvor erstellte Liste ungültig.

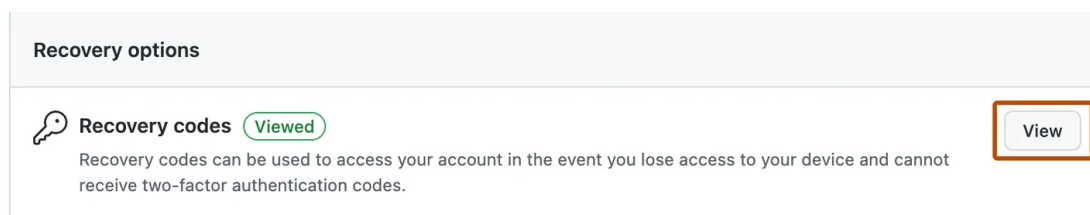


Abbildung 2.6.: GitHub Codeliste[32]

### 2.2.2. Wiederherstellungsmethode soziale Authentifikation

Als nächste Variante der Wiederherstellungsmethode wird die soziale Authentifikation erläutert. Diese Methode findet vor allem in sozialen Netzwerken Anwendung, wie z.B. Facebook, MySpace oder StayFriends. Die Benutzer dieser Plattformen vernetzen sich mit anderen Benutzern und pflegen so den Kontaktaufbau und -erhalt über digitale Medien[33]. Auch wenn der Kontakt zu bisher nicht bekannten Personen seltener

---

vorkommt, wird er jedoch nicht ausgeschlossen.

Die Wiederherstellungsmethode über den social graph (sozialen Graphen) nutzt die Verbindung zwischen den verschiedenen Accounts der Benutzer. Jeder Benutzer hat für seinen Account eine Liste, welche andere Benutzer enthält, die diesem als Freund zugeordnet sind. Diese Liste wird durch das versenden von Anfragen an andere Benutzer oder die Bestätigung eingehender Anfragen durch den Besitzer des Accounts befüllt. Wird im Falle des Wiederherstellungsvorgangs die Authentifizierung über den social graph gewählt, so muss der Benutzer entweder Fragen zu seinen Kontakten beantworten oder es werden Codes (secrets) an verschiedene vom Benutzer ausgewählte Kontakte versendet, die in Kombination dem Benutzer wieder Zugriff auf seinen Account ermöglichen[14].

Als Beispiel für die Wiederherstellungsmethode mittels sozialer Authentifikation sei die Variante von Facebook genannt. Verliert ein Benutzer bei Facebook sein primär genutztes Endgerät oder die primären Authentifizierungsfaktoren, kann er als Wiederherstellungsmethode die Verifikation über den social graph wählen. Der Benutzer muss bei dieser Variante aus 100 Vorschlägen von Kontakten aus seiner Freundesliste drei zugeordnete andere Benutzer auswählen. Die angebotene Liste wird nach jeder Auswahl verkleinert. Eine genaue Erklärung für den zugrundeliegenden Algorithmus gibt es nicht[14]. An jeden dieser Kontakte wird nun ein 4-stelliger Code versendet und dem anfordernden Benutzer wird an seine hinterlegte E-Mail-Adresse eine E-Mail zu gesendet, in der der Benutzer über den Start des Vorgangs und die drei gewählten Benutzer informiert wird. Die Übergabe der drei Codes soll möglichst über ein separates Medium erfolgen, z.B. über das Telefon[14].

### **2.2.3. Wiederherstellungsmethode persönliche Fragen /**

#### **Sicherheitsfragen**

Die Wiederherstellungsmethode durch persönliche Fragen oder Sicherheitsfragen ist eine der ältesten und bekanntesten Methoden. Viele Onlinedienste nutzen Fragen wie „Wie lautet der Mädchenname Ihrer Mutter?“ als Wiederherstellungsmethode[1]. Häufig werden hier mehrere Fragen bei der Account-Erstellung eingefordert[34]. Es gibt zwei Haupttypen von Sicherheitsfragen:

Systemdefinierte Sicherheitsfragen - Fragen dieser Art basieren auf Informationen, die dem Anbieter des Onlinedienstes bereits vorliegen, z.B. das Geburtsdatum oder die Adresse des Benutzers.



---

Benutzerdefinierte Sicherheitsfragen - Dem Benutzer werden eine Auswahl an Fragen vorgeschlagen und dieser kann hieraus wählen. Es kann auch die Option geben, dass der Benutzer die Frage selber formulieren kann[35].

Zur Wiederherstellungsmethode über persönliche Fragen / Sicherheitsfragen gibt es einige wissenschaftliche Betrachtungen. Bonneau et al.[36] haben in ihrer Untersuchung 2015 ermittelt, dass die Nutzung von Sicherheitsfragen ein geringeres Sicherheitslevel bietet als die Nutzung von benutzergewählten Passwörtern. Dies ergibt sich aus den Angaben persönlicher Daten, die Benutzer in sozialen Netzwerken vornehmen und die sich somit leichter ermitteln lassen. Auch Social Engineering Angriffe führen zu einer Schwächung dieser Wiederherstellungsmethode[37].

In einer weiteren Studie zeigen Hang et al.[38], dass bei einer dynamischen Nutzung von Informationen zum Verhalten des Benutzers Sicherheitsfragen ein gutes Sicherheitslevel bieten können. Micallef and Arachchilage[39] verfolgen einen Ansatz, der Gamification nutzt, um persönliche Fragen sicherer zu gestalten. Beide genannten Publikationen beziehen sich auf mobile Endgeräte.

#### **2.2.4. Wiederherstellungsmethode E-Mail oder SMS basiert**

Ähnlich der Wiederherstellungsmethode über persönliche Fragen / Sicherheitsfragen gehört auch die Nutzung von hinterlegten E-Mail-Adressen zu den bekannteren Methoden. In diesem Abschnitt werden sowohl die Methode per E-Mail als auch per SMS betrachtet, da beide Methoden einen Faktor Benutzen, bei dem der Benutzer eine E-Mail-Adresse / Telefonnummer hinterlegt. An diese E-Mail-Adresse oder Telefonnummer wird im Fall der Account-Wiederherstellung ein Code oder Link versendet, mit dem der Benutzer sich authentifizieren kann[2].

In einer Publikation analysieren Innocenti et al.[40] die Sicherheit von verschiedenen E-Mail-basierten Wiederherstellungsmethoden. Die Autoren stellen unter anderem dar, dass Account Takeover Attacks ein Risiko für diese Art der Wiederherstellung sind. Snyder und Kanich[41] sowie Li et al.[42][43] haben sich ebenfalls mit dem Problem des E-Mail-Accounts als Single-Point-of-Failure auseinander gesetzt. Beide kommen zu dem Schluss, dass E-Mail-Accounts nicht ausreichend abgesichert sind und ein Risiko darstellen in Bezug auf Angriffe gegen Wiederherstellungsmethoden.

Ein Beispiel für die Wiederherstellung per SMS ist der E-Mail-Provider WEB.DE.

---

Während der Account-Erstellung wird der Benutzer zur Passwort-Wiederherstellung per SMS um die Angabe seiner Mobilfunknummer gebeten (vgl. Abbildung 2.7).

**Passwort** i

Passwort wählen

i Mindestens 8 Zeichen - am besten einen Satz oder eine Mischung aus Buchstaben, Symbolen und Zahlen verwenden

Passwort wiederholen

**Passwort-Wiederherstellung per SMS** i

Mobilfunknummer

DE +49 v

Abbildung 2.7.: Eingabe Mobilfunknummer WEB.DE Registrierung[44]

### 2.2.5. Wiederherstellungsmethode Token basiert

Bei der Token basierten Wiederherstellungsmethode wird analog zur primären Authentifizierung mit Fast Identity Online für die Wiederherstellung der öffentliche Teil eines kryptographischen Schlüssel hinterlegt. Pöhn et al.[2] bewerten diese Wiederherstellungsmethode als beste Methode. Ihrer Auswertung nach ist die Sicherheit durch die Verwendung eines Token mit am höchsten, da diese Token weder vergessen noch durch Phishing abgefangen werden können. Zu der gleichen Bewertung kamen auch Kunke et al.[45].

Weiterhin wird die Verwendbarkeit als sehr einfach bewertet, da der Benutzer die Authentifikation durch einfaches Drücken eines Knopfes erledigen kann[45]. Schwarz et al.[46] haben in ihrer Arbeit das Konzept von FIDO erweitert und die Komponente einer eID hinzugefügt.

Die Wiederherstellungsmethode durch Token bietet den Vorteil, dass keine persönlichen Informationen hinterlegt werden müssen und auch der Faktor des Vergessens von Informationen, wie z.B. bei Passwörtern oder PIN, entfällt. Es wird jedoch eine Kooperation des jeweiligen Onlinedienst Anbieters zur Nutzung der Technologie benötigt.

---

## 2.3. Cyberangriffe auf Wiederherstellungsmethoden

Wie bei den primären Authentifikationsmethoden gibt es auch für die Wiederherstellungsmethoden einen hohen Anreiz für Cyberkriminelle an Informationen hierzu zu gelangen. Wie bereits in der Einleitung erwähnt, ist eine Wiederherstellungsmethode im Vergleich zur primären Authentifikation meist nur mit einem Faktor gesichert. Somit ist der Aufwand für Cyberkriminelle, Zugriff auf den jeweiligen Account zu bekommen, im Vergleich zur primären Authentifikationsmethode geringer. In den folgenden Kapiteln werden einige Beispiele dargestellt, wie Cyberkriminelle versuchen an Informationen zu Wiederherstellungsmethoden zu gelangen.

### 2.3.1. Social Engineering

Bei der Cyberangriffsart Social Engineering werden menschliche Eigenschaften wie z.B. Hilfsbereitschaft, Vertrauen oder Respekt vor Autorität ausgenutzt[13][47]. Ein zentrales Merkmal bei einer Social Engineering Attacke ist die Täuschung. Somit ist der grundlegende Vorgang des Betruges oder der Täuschung keine neue Erfindung in der Menschheitsgeschichte. Cyberkriminelle, die über Social Engineering an Informationen kommen wollen, versuchen dem Opfer unabsichtlich oder absichtlich diese Informationen zu entlocken. Der Angreifer kann sich als vermeintlicher Bekannter oder Administrator eines Dienstes ausgeben und unter verschiedenen Vorwänden, z.B. ein fingierter IT-Sicherheitsvorfall, versuchen Daten von seinem Opfer zu erhalten[47].

Die Vorgehensweise ist hierbei variabel. Der Angreifer kann direkt mit dem Opfer in Kontakt treten, im realen Leben oder per Telefonanruf. Diese Formen erfordern jedoch ein gewisses Geschick des Angreifers in der Kommunikation mit seinem Gegenüber.

Weniger aufwändig gestaltet sich das Social Engineering über E-Mail, Messenger Dienste oder Social Media. Viele Benutzer von Social Media Angeboten teilen bereitwillig viele Informationen über sich selbst, Angehörige oder sogar ihren Arbeitgeber. Häufig muss der Angreifer nur ein Nutzer des selben Social Media Angebotes sein, um hier Informationen ausspähen zu können. Durch die Verknüpfung von Informationen aus verschiedenen Social Media Angeboten ist ein Angreifer in der Lage, sich ein komplexes Bild zu seinem Opfer zu erstellen[47].

Eine weitere bekannte Methode des Social Engineering ist das Phishing per E-Mail. Beim Phishing bereitet der Angreifer eine E-Mail so auf, dass das Opfer denkt, diese E-Mail kommt vom jeweils vorgetäuschten Dienst oder Absender. Diese

---

E-Mails werden von einer E-Mail-Adresse des Angreifers mit einer vorgetäuschten Absenderadresse an viele Empfängeradressen gesendet. Den Vorgang mit der vorge-täuschten Absenderadresse nennt man Spoofing. Häufig werden in diesen E-Mails Links eingebettet, die das Opfer auf eine vermeintliche Seite eines Onlinedienst Anbieters weiterleiten und dort die Eingabe von Accountdaten einfordern. Wenn das Opfer auf diesen Link herein fällt, stellt es dem Angreifer diese Informationen zur Verfügung. Bei dieser Art des Phishing geht es dem Angreifer darum, dass ein gewisser Prozentsatz der Opfer auf diese Täuschung herein fällt, jedoch nicht um eine hundertprozentige Erfolgsquote[47][48].

Eine spezielle Form des Phishing ist das Spear-Phishing (vom englischen spear = Speer)[48]. Beim Spear-Phishing verfolgt der Angreifer nicht das Ziel, eine Masse an Opfern zu erreichen, sondern gezielt Organisationen oder Firmen anzugreifen. In seltenen Fällen werden hierbei auch spezielle Personen oder Rollen direkt angegriffen, z.B. die Finanzabteilung eines Konzern oder CEO's verschiedener Organisationen (CEO-Fraud)[47].

### **2.3.2. Trusted Friend Attacke**

Die Trusted Friend Attacke ist eine spezielle Form des Social Engineering. Javed et al.[14] entwickelten diesen Angriff gegen Facebooks Trusted Friends Mechanismus. Der Trusted Friends Mechanismus erlaubt es Benutzern der Plattform Facebook mittels social graph im Falle des Verlustes der primären Authentifikationsfaktoren die Wiederherstellung durchzuführen. Der Benutzer muss bei dieser Form der Wiederherstellung aus einer durch die Plattform Facebook vorgegebenen Liste von Freunden des Benutzers in 3 Iterationen jeweils eine Person auswählen. Die Liste wird nach jeder Auswahl auf die Hälfte reduziert. Nach der letzten Auswahl wird den ausgewählten Personen je ein vierstelliger Code sowie dem anfordernden Benutzer eine E-Mail mit den drei gewählten Personen zu gesendet[14]. Der anfordernde Benutzer kann nach Erhalt der drei Code-Teile mit dem gesamten Code seinen Account wiederherstellen.

Die Trusted Friend Attacke funktioniert nun unter anderem deswegen, da viele Benutzer Freundschaftsanfragen von Unbekannten annehmen. Der Angreifer muss mindestens drei Accounts unter seiner Kontrolle mit dem Account des Opfers verbunden haben. Anschließend muss der Angreifer den Wiederherstellungsprozess starten. Hierbei hat der Angreifer die Option, eine neue E-Mail zu registrieren (die Vorbedingungen hierzu sind nicht öffentlich)[14] oder der Angreifer hat Zugang zur im Account hinterlegten E-Mail-Adresse (diese Option ermöglicht nicht die Wiederherstellung über Trusted Friends, entfällt in diesem Fall folglich). Wenn der Trusted

---

Friends Prozess gestartet ist, wählt der Angreifer drei Accounts unter seiner Kontrolle für den Vorgang aus. Hierzu sind noch einige weitere Vorbereitungen notwendig[14]. Der Angreifer benötigt zur Durchführung die ID des „selected friend“, um diese mit Hilfe von POST-Daten Manipulation zur Auswahl eines bestimmten Accounts für die Wiederherstellung nutzen zu können. Facebook bietet ein Entwickler-Tool an, mit dessen Hilfe diese Informationen ausgelesen werden können[49]. Der Angreifer führt dies für alle drei benötigten Accounts durch und ist nun in der Lage, die Wiederherstellungscodes zu erhalten.

### **2.3.3. Account Takeover Attacken**

Eine weitere Bedrohung für Wiederherstellungsmethoden stellen Account Takeover Attacken dar. Account Takeover Attacken können auf verschiedene Arten erfolgen. Die Varianten beziehen Eindrigen durch Gewalt (Brute Force), Nutzung von bekannten Informationen (Credential Stuffing) sowie direkte Angriffe auf Online-Sitzungen (Session Hijacking) mit ein. Die einzelnen Techniken werden im Folgenden erläutert.

Brute Force - Ein Angriff mit Brute Force Technik ist der Versuch eines Angreifers, Zugang zu einem fremden Account zu bekommen, ohne dass der Angreifer Kenntnis von den benötigten Zugangsdaten hat. Der Angreifer versucht bei einer Brute Force Attacke systematisch die passende Kombination für die Zugangsdaten zu erraten. Dies erfolgt meistens durch eine wiederholte oder iterative Eingabe von Passwörtern[50]. Eine spezielle Variante der Brute Force Attacke ist der Wörterbuchangriff[13]. Hierbei nutzt der Angreifer bereits vorhandene Passwortlisten und versucht durch die Abarbeitung der Liste den Zugang zu erlangen. Diese Variante ist nach Pohlmann[13] erfolgversprechend, da viele Nutzer einfache Passwörter verwenden und die Anzahl der zu prüfenden Passwörter geringer ist, als bei der Brute Force Attacke.

Credential Stuffing - Credential Stuffing ist eine spezielle Variante der Brute Force Attacke[51]. Beim Credential Stuffing wird ähnlich zum Wörterbuchangriff auf bereits verfügbare Daten zurückgegriffen. Das Credential Stuffing nutzt Kombinationen von Benutzername und Passwort, die bereits in der Vergangenheit durch ein Datenleck öffentlich gemacht wurden. Häufig werden im Darknet Listen von Benutzer-Passwort-Listen angeboten. Nachdem der Angreifer sich diese Listen verschafft hat, kann dieser den Inhalt gegen das gewählte Ziel einsetzen. Auch beim Credential Stuffing ergibt sich die Erfolgsquote durch die häufige Bequemlichkeit der Benutzer, für viele Zugänge im Internet gleiche oder nur minimal abgewandelte Zugangsdaten zu nutzen.

Session Hijacking - Bei der Angriffsvariante Session Hijacking hat der Angreifer das Ziel, eine bestehende Sitzung eines Benutzers zu übernehmen. Mit einer Sitzung (engl. session) ist in der Informationstechnologie der Zeitraum gemeint, in dem ein Benutzer mit einem System oder einer Anwendung agiert. Bei einer Netzwerk- oder Internetverbindung erfolgt diese Verbindung über ein vorgegebenes Protokoll. Zur Erkennung eines Benutzers benötigt ein Webserver eine Methode, um diesen eindeutig zuordnen zu können. Nach der erfolgreichen Authentifikation des Benutzers und des zugehörigen Clients, wird dem Client ein Sitzungstoken (Session ID) zugewiesen[52]. Ein Angreifer kann, sofern er sich im selben Netzwerk befindet, versuchen diesen Sitzungsaufbau mit technischen Mitteln abzuhören (z.B. durch die Nutzung des Tools Wireshark<sup>1</sup>. Abbildung 2.8 zeigt einen schematisierten Ablauf des Session Hijacking[53]).

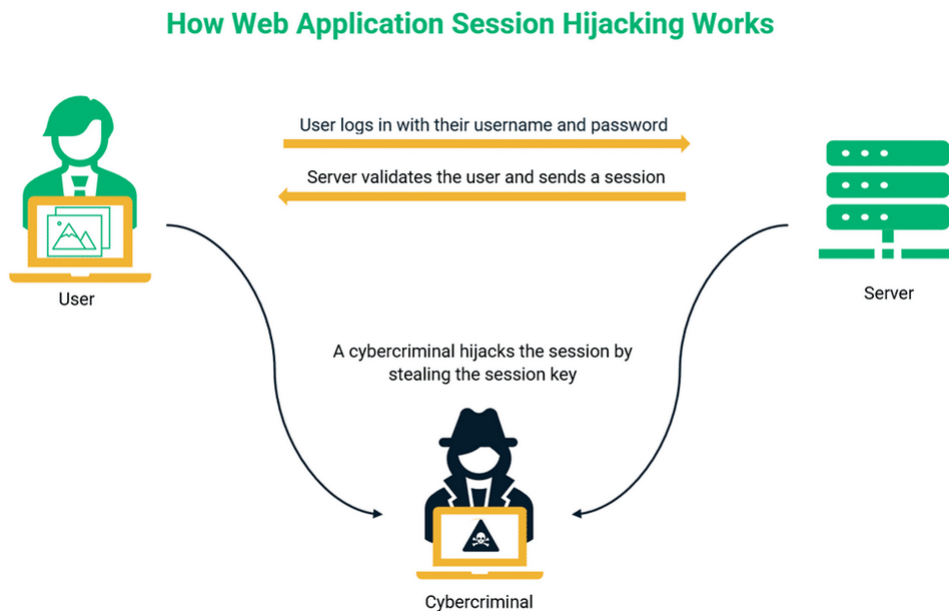


Abbildung 2.8.: Darstellung eines Session Hijacking Angriff[54]

<sup>1</sup>Wireshark ist ein Open-Source Netzwerk-Tool zur Analyse von Datenströmen in Netzwerken. Es kann zur Überwachung und Analyse von Datenpaketen verwendet werden.

### 2.3.4. Aktuelle Cyberangriffe auf Wiederherstellungsmethoden

In diesem Kapitel wird ein aktuelles Beispiel für einen Angriff auf die Wiederherstellungsmethode eines Online Dienstes dargestellt. Ende des Jahres 2023 erfolgte eine Kampagne gegen die Wiederherstellungsmethode des Social Media Anbieters Instagram[55]. Zur Absicherung der Accounts seiner Benutzer bietet Instagram seinen Benutzern die Möglichkeit der 2FA für die primäre Authentifikation an[56]. Der Benutzer erhält eine Liste mit fünf acht-stelligen Nummern (siehe Abbildung 2.9).

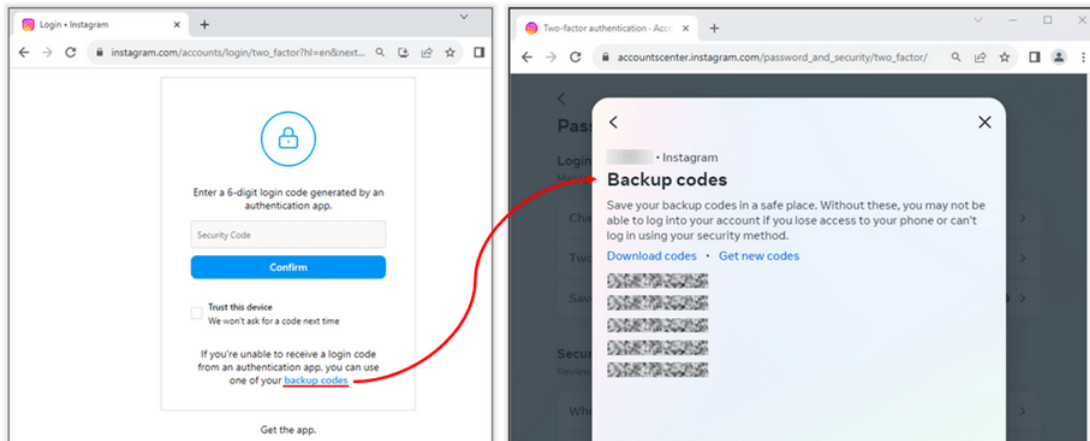


Abbildung 2.9.: Wiederherstellungscodes Instagram[57]

Die Angreifer der Attacke gegen Instagram wollten durch das Erlangen der Wiederherstellungsfaktoren der Nutzer diesen Schutz umgehen. Der Angriff erfolgte mittels einer Phishing-E-Mail, die den Eindruck erwecken sollte von Instagrams Muttergesellschaft Meta abgesendet worden zu sein, dargestellt in Abbildung 2.10.

Die Autoren der Seite Trustwave verweisen auf einige Hinweise, die die E-Mail als nicht authentisch ausweisen, unter anderem die nicht zu Meta gehörende Absenderdomain und die Weiterleitung auf eine Google Notification URL durch Betätigen der verlinkten Schaltfläche in der E-Mail[57]. Benutzer, die dem Link aus der E-Mail folgen, werden auf eine vermeintliche Seite von Meta geleitet, die als Brücke zur eigentlichen Phishing Webseite dient. Die Angreifer werden bei Nutzung der Seite über den Zugriff informiert. Der Benutzer wird zur Eingabe seines Benutzernamen sowie des zugehörigen Passwortes aufgefordert. Alle eingegebenen Daten werden nach anschließender Bestätigung an die Angreifer gesendet. Anschließend wird der Benutzer zur Eingabe seines Backup Codes aufgefordert, siehe 2.11.

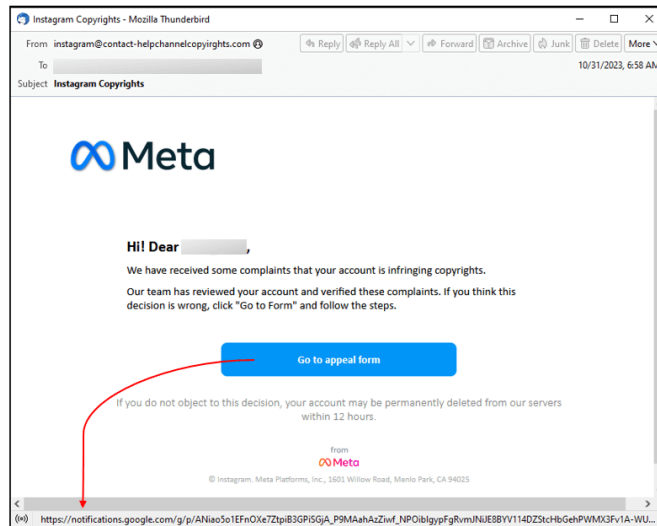


Abbildung 2.10.: Phishing E-Mail Instagram[57]

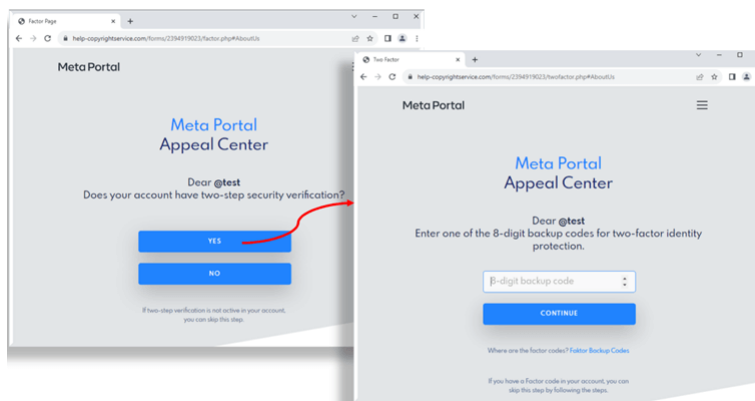


Abbildung 2.11.: Phishing Seiten für Instagram Backup Codes[57]

Es folgen weitere Seiten, auf denen versucht wird, an weitere Daten des Benutzers zu gelangen, wie z.B. Telefonnummer oder E-Mail-Adresse.

Weitere Beispiele für Phishing Angriffe zeigt das BSI[58]. Oftmals sind auch hier die versendeten E-Mails täuschend ähnlich zu den E-Mails des eigentlichen Anbieters. Meist geht es um eine einfache Bestätigung oder Aktualisierung von z.B. Datenschutzvereinbarungen zwischen dem Anbieter und dem Benutzer. Die E-Mails enthalten einen Link, der den Benutzer zur vermeintlichen Webseite des Anbieters leitet und dort die Eingabe der Authentifizierungsfaktoren fordert.

Auch die Weiterentwicklung der Künstlichen Intelligenz birgt Gefahren. Künstliche Intelligenz kann Cyberkriminellen helfen, authentischere Texte oder auch Grafiken zu erstellen, die es dem Benutzer schwieriger machen, diese Inhalte als manipulierte Inhalte zu erkennen[59].



## 2.4. Analyse Tool

### 2.4.1. Sicherheit

Zur Analyse der Sicherheit der Wiederherstellungsmethoden wurde der Account Access Graph (AAG) Analyser verwendet[60]. Pöhn et al.[2] verwendeten den AAG zur Analyse von Multi-Account-Dashboards. Für den AAG wurden sowohl für die primären Authentifikationsmethoden als auch für die Wiederherstellungsmethoden Reifegradmodelle (maturity models) entwickelt. Das Modell für die Wiederherstellungsmethoden wird in Tabelle 2.2 beschrieben.

Im AAG können für einen Account die Wege der primären Authentifikation und der Wiederherstellung nebeneinander modelliert werden. Die Graphen bestehen aus einem Kopf, welcher den jeweiligen Dienstleister darstellt. Mit Hilfe von Operatoren und Authentifikatoren werden die einzelnen Wege aufgebaut. Jede Authentifikator hat grundsätzlich einen Wert zugewiesen, welcher sich am Reifegradmodell orientiert. Die Skala geht vom Wert 1 (niedrigster) bis Wert 5 (höchster). So hat zum Beispiel ein Authentifikator der Wiederherstellung mit der Eigenschaft E-Mail oder SMS basiert den Wert 2 (siehe F2 Tabelle 2.2). Der Operator „&“ leitet den höchsten Wert an die nächste Entität weiter, der Operator „|“ gibt den niedrigsten Wert weiter. Abbildung 2.12 zeigt eine beispielhafte Darstellung für einen Graphen.

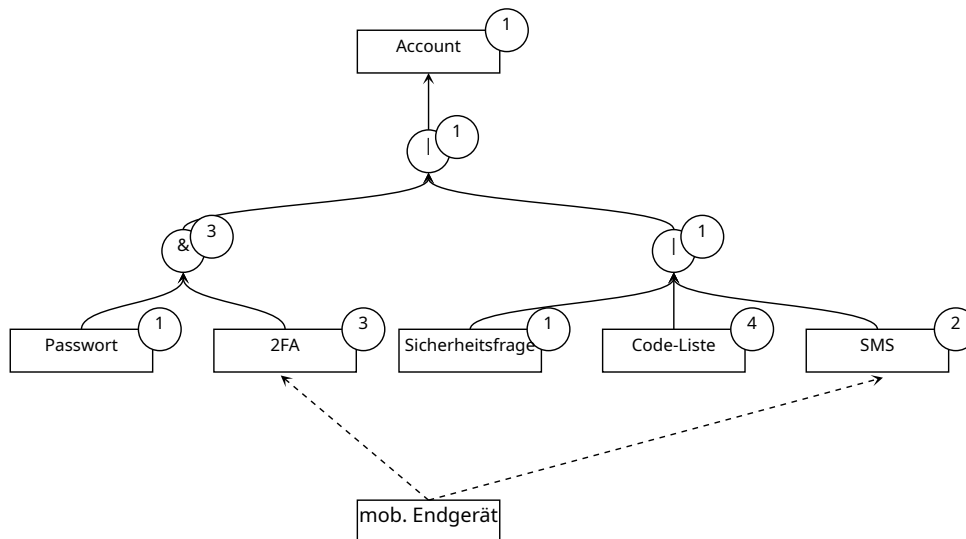


Abbildung 2.12.: Beispiel für einen AAG Sicherheit

Tabelle 2.2.: Reifegradmodell Wiederherstellung AAG

Level	Mechanism group	Mechanism	Exemplary security risks	Exemplary accessibility risks
F5	Token-based	Backup token	Token swap or attack on underlying security / applied software	Lost, broken, or otherwise currently unavailable token
F4	Recovery code-based	Backup code	Device or storage compromise	Forgotten, deleted, or never remembered code
F3	Trustee-based	Code or AuthN via several mostly pre-defined trustees	Social engineering or man in the middle	Not possible (e.g., forgotten) or available
F2	SMS-based	Code via SMS	SIM-swapping or hijacking, stolen device, or social engineering	Lost device, forgotten PIN noticed during reboot, or device lockout
	Email-based	Reset emails with old/new password or URL link	Credential stuffing, general account takeover, device compromise, or other human-in-the-middle	Deleted/deactivated email account or delay in delivery during each usage
F1	Question-based	Security question(s) or puzzle	Social engineering, found on the Internet or otherwise guessable	Forgotten answer or wrong semantic

### 2.4.2. Zugänglichkeit

Der AAG bietet weiterhin die Möglichkeit die Accessibility oder Zugänglichkeit eines Accounts graphisch darzustellen. Pöhn et al.[2] beschreiben in ihrer Veröffentlichung die Berechnung wie folgt:

1. Eine Quelle mit  $k$  ausgehenden Pfeilen hat den Wert von  $1/k$
2. Für die Operatoren „|“ =  $\omega$  und „&“ =  $\alpha$ , jeder mit direkten Vorgänger  $n_1, \dots, n_k$ , lauten die Formeln:

$$acc(\omega) = \sum_{i=1}^k acc(n_i) \quad acc(\alpha) = \min_{i=1, \dots, k} acc(n_i)$$

3. Für einen (nicht-Operator) Knoten  $n$  mit direkten Vorgängern  $n_1, \dots, n_k$  lautet die Formel:

$$acc(n) = \sum_{i=1}^k acc(n_i)$$

Abbildung 2.13 zeigt einen Beispielgraphen für die Werte bezogen auf die Zugänglichkeit.

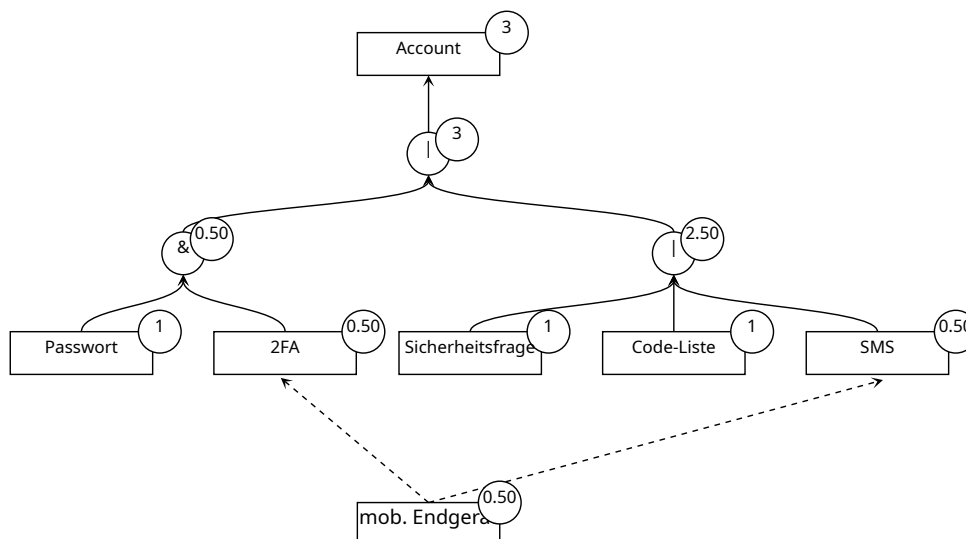


Abbildung 2.13.: Beispiel für einen AAG Zugänglichkeit

Die Zugänglichkeit wird nach folgenden Risikowerten eingeordnet:

- $0 \leq acc < 1$ : hohes Risiko (der Verlust von einem Token kann den Account unzugänglich machen)
- $1 \leq acc < 2$ : mittleres Risiko (ein Token kann verloren werden)
- $acc \geq 2$ : geringes Risiko (ein Token kann verloren werden)

## **3. Bestandsaufnahme und Methode**

Das Kapitel Bestandsaufnahme und Methode besteht aus zwei Abschnitten. Im ersten Abschnitt Bestandsaufnahme werden die für diese Arbeit benötigten Accounts angelegt und vorbereitet. In einem zweiten Schritt werden die zu den jeweiligen Accounts gehörigen Wiederherstellungsmethoden dargestellt.

Im zweiten Teil dieses Kapitels wird die zur Auswertung genutzte Methode beschrieben. Hierbei wird zum einen ein Graphen-Tool verwendet (siehe 2.4) und zum Anderen eine Umfrage (siehe 3.4.1) zu Wiederherstellungsmethoden erstellt.

### **3.1. Einschränkung und Auswahl der zu bewertenden Accounts**

Für die Durchführung der Bewertung der Wiederherstellungsmethoden von verschiedenen Anbietern wurde eine Auswahl getroffen. Hierfür lassen sich einige Begründungen anführen. Eine begrenzte Auswahl von Beispielen ermöglicht eine tiefergehende und fokussiertere Betrachtung des Sachverhaltes[61]. Eine gezielte Auswahl von Beispielen ermöglicht nach Maxwell [62] eine genauere Darstellung des Zusammenhangs der erzielten Ergebnisse. Ein weiterer Faktor ist die Machbarkeit, da der Zeitraum der Bearbeitung dieser Master-Thesis begrenzt ist und somit eine sinnvolle Einschränkung der Beispiele notwendig ist.

Für die Auswahl wurden bekannte Namen von Dienstleistern ausgewählt, z.B. Amazon oder Google. Betrachtet werden sollten aber auch E-Mail-Provider, eine Spieleplattform sowie ein Netzwerktechnikanbieter. Viele Nutzer haben Accounts bei E-Mail-Providern und nutzen diese somit auch, wenn gefordert, als Wiederherstellungsadressen. Wenn dieser Account jedoch nicht ausreichend gesichert ist, bietet dies Angreifern ein leichte Möglichkeit einen Account zu übernehmen indem vorher der Mail-Account gekapert wird. Der Anbieter Web.de wird in dieser Analyse als ein Beispiel der vielen Anbieter betrachtet.

Die Spieleplattform wurde ausgewählt, weil diese heutzutage nicht nur rein zur

---

Verwaltung von digitalen Spielen genutzt werden, sondern auch als Social Media Plattformen Anwendung finden und somit mehr Bedeutung und Anwendungsbereiche für die Benutzer bieten.

Der Anbieter für Netzwerktechnik wurde gewählt, weil immer mehr Benutzer ihre Heimnetzwerke selber gestalten. Hierfür stehen verschiedenste Plattformen zur Verfügung, die durch die Nutzung von Apps und Webapplikationen dem Benutzer die Verwaltung und den Zugriff auf sein Heimnetzwerk gewähren. Auch dies sind für Angreifer relevante Ziele, da hier schnell Zugriff auf viele Geräte erlangt werden kann, die wiederum für weitere schadhafte Handlungen verwendet werden können.

## **3.2. Erstellung von Accounts**

Für die Erstellung der Accounts wurden folgende Systeme genutzt:

- PC mit Windows 10 Pro Betriebssystem, Firefox Browser (Version 127.0 bis 129.2), 1&1 Festnetzanschluss Internetzugang
- Laptop mit Ubuntu 24.04 LTS, Firefox Browser (Version 127.0 bis 129.2), Congstar (Telekom-Netz) Mobilfunknetz Internetzugang
- Google Pixel 8 Pro, Web.de App, Steam App, SMS-Nutzung, Congstar (Telekom-Netz) Mobilfunknetz Internetzugang
- MacBook Air 13 Zoll, macOS Big Sur Version 11.7.10

Zur Verwaltung der primären Authentifikationsfaktoren wurde das Tool KeePass genutzt[63]. Alle benötigten Passwörter wurden durch KeePass generiert und zu jedem Account wurde ein Eintrag in KeePass erstellt.

### **3.2.1. Account Amazon**

Der erste Account wurde beim Onlinedienstanbieter Amazon erstellt. Zur Registrierung wurde die durch die Hochschule vorhandene E-Mail-Adresse „s.alfeis@stud.hs-wismar.de“ genutzt. Nach der Eingabe des Namens des Benutzers, der E-Mail-Adresse und des Passwortes wurde eine Bestätigung der E-Mail-Adresse durch zusenden eines OTP eingefordert. Zur Absicherung des Accounts wurde in den Einstellungen die Zwei-Faktor-Authentifizierung aktiviert. Genutzt wurde hierfür der Google Authenticator[64].

In den Sicherheitseinstellungen des Amazon Accounts kann auch die Nutzung

---

eines Passkey zur Authentifizierung eingestellt werden. Die Umsetzung ist hierbei mittels Hardware-Token oder Software-Passkey über ein mobiles Endgerät möglich. Für die Arbeit an dieser Master-These wurde ein USB-Token der Firma Token2 verwendet[65]. Mit Hilfe des Manager Tools des Token2 kann der Passkey angezeigt werden (siehe Abbildung 3.1).

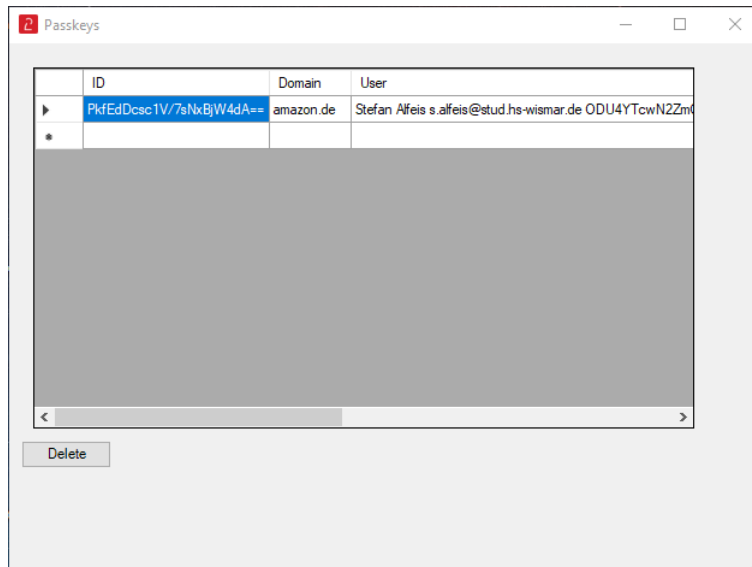


Abbildung 3.1.: Token2 Manager Passkey für Amazon

### 3.2.2. Account Apple

Der Account beim Anbieter Apple wurde mit der E-Mail-Adresse „sXXXXX.aXXXXX@XXX.de“ erstellt. Die Versuche einen Account mit der Studien-E-Mail-Adresse einen Account zu erstellen waren nicht erfolgreich. Für die Erstellung des Accounts wurde ein Macbook Air von 2013 genutzt. Als zweiter Faktor für die Authentifikation wurde die Telefonnummer „017X / XXXXX118“ hinterlegt. Zum Abschluss der Erstellung wurde eine Verifikations-E-Mail an die hinterlegte E-Mail-Adresse gesendet (siehe Abbildung 3.2).

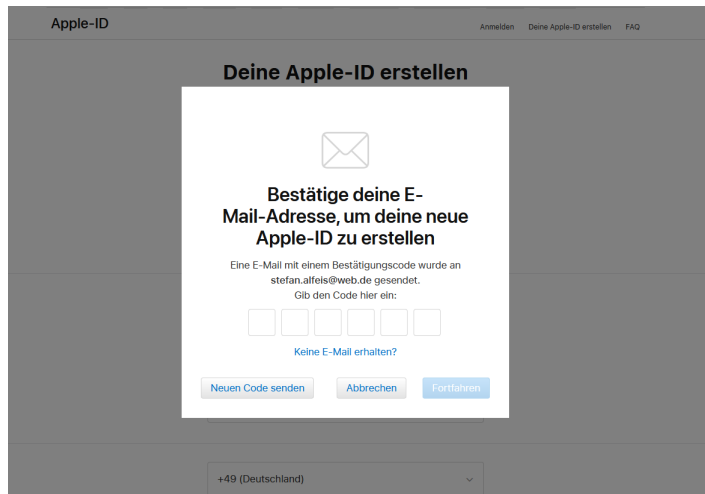


Abbildung 3.2.: Erstellung Apple ID

In den Sicherheitseinstellungen des Apple Accounts kann ein Wiederherstellungsschlüssel aktiviert werden (siehe Abbildung 3.3).

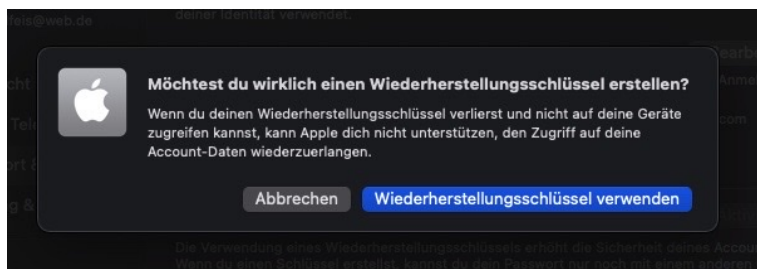


Abbildung 3.3.: Schlüssel erstellen Apple

Dieser hilft dem Benutzer, sollte er keinen Zugriff mehr auf die mit seinem Account verknüpften Endgeräte haben (siehe Abbildung 3.4).

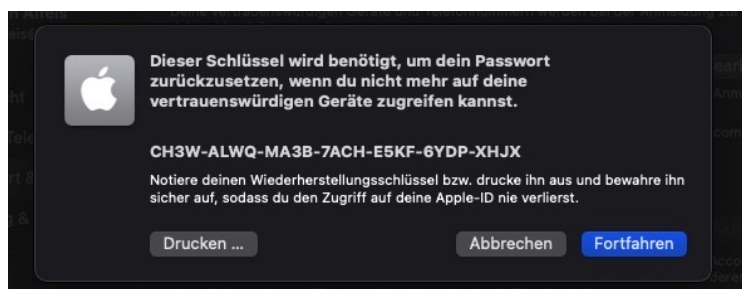


Abbildung 3.4.: Schlüssel Apple

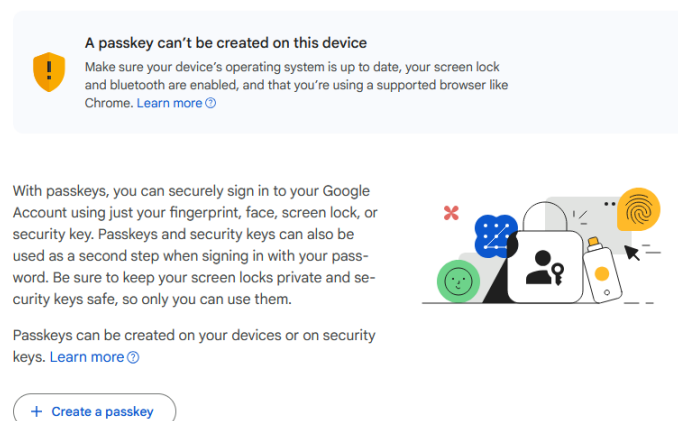
---

Nach der Anmeldung des Apple Accounts auf dem Macbook konnte dieses Macbook als zweiter Faktor zur Authentifikation für Vorgänge den Account betreffend genutzt werden.

### 3.2.3. Account Google

Die Erstellung des Accounts beim Anbieter Google erfolgte für folgende Google-Adresse: „alfeisstefan@gmail.com“. Im Verlauf der Accounterstellung wurde auch nach einer E-Mail-Adresse zur Kontowiederherstellung gefragt. Hierfür wurde die Adresse „s.alfeis@stud.hs-wismar.de“ hinterlegt. Nach der Erstellung des Accounts wurde in den Sicherheitseinstellungen zusätzlich zur E-Mail-Adresse sowohl eine Telefonnummer „017X / XXXXX118“ zur Wiederherstellung gespeichert als auch eine Liste mit Wiederherstellungs-Codes generiert. Für den Google Account war auch eine Option zur Einrichtung der Nutzung eines Passkey vorhanden. Diese Option konnte jedoch nur mit einem Mobilien Endgerät umgesetzt werden, die Einrichtung an einem PC war nicht möglich (vgl. Abbildung 3.5).

#### ← Passkeys and security keys



**A passkey can't be created on this device**  
Make sure your device's operating system is up to date, your screen lock and bluetooth are enabled, and that you're using a supported browser like Chrome. [Learn more](#)

With passkeys, you can securely sign in to your Google Account using just your fingerprint, face, screen lock, or security key. Passkeys and security keys can also be used as a second step when signing in with your password. Be sure to keep your screen locks private and security keys safe, so only you can use them.

Passkeys can be created on your devices or on security keys. [Learn more](#)

[+ Create a passkey](#)

Abbildung 3.5.: Passkey Einstellung Google



Da kein separates Gerät zur Verfügung stand, wurde diese Option hier nicht getestet. Abbildung 3.6 zeigt die Einstellungen, welche für die Sicherheit des Google Accounts vorgenommen wurden.

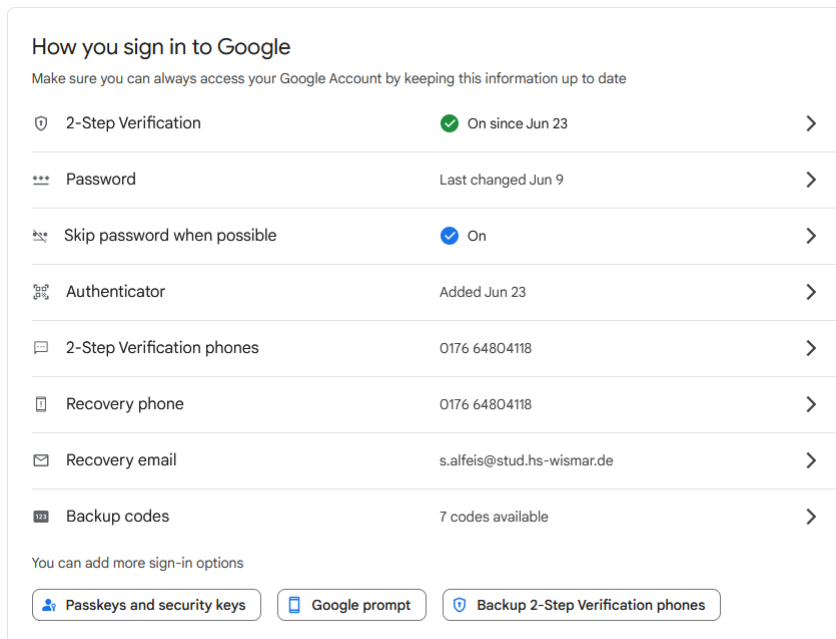


Abbildung 3.6.: Sicherheitseinstellungen Google

### 3.2.4. Account Microsoft

Es wurde versucht, beim Anbieter Microsoft einen Account für die Zwecke dieser Master-Thesis zu erstellen. Die Erstellung war jedoch nicht erfolgreich, trotz der Verwendung unterschiedlicher E-Mail-Adressen für die Registrierung. Die Registrierung wurde am 09.06.2024, 15.06.2024 und 26.07.2024 gestartet. Abbildung 3.7 zeigt, mit welcher Darstellung der Vorgang jedes Mal endete. Auch ein Versuch einen anderen Browser (Opera-Browser) zu nutzen führte nicht zum Erfolg.



Abbildung 3.7.: Erstellung Account Microsoft

### 3.2.5. Account Meta

Die Erstellung des Accounts bei Meta erfolgte ebenfalls mit der E-Mail-Adresse „s.alfeis@stud.hs-wismar.de“. Es wurde nach erfolgter Erstellung die Zwei-Faktor-Authentifizierung aktiviert. Abbildung 3.8 zeigt die verfügbaren Optionen. Auch für Meta wurde der Google Authenticator als zweiter Faktor freigeschaltet. Während der Aktivierung der 2FA hat der Benutzer die Option neben der Nutzung einer Authenticator-App auch seine Telefonnummer zu hinterlegen. An diese Nummer kann dann durch Meta ein Code für den zweiten Faktor gesendet werden. Weiterhin besteht die Option eine Code-Liste zu generieren, die im Falle des Verlustes des gekoppelten Telefons dem Benutzer Zugang zum Account verschaffen sollen.

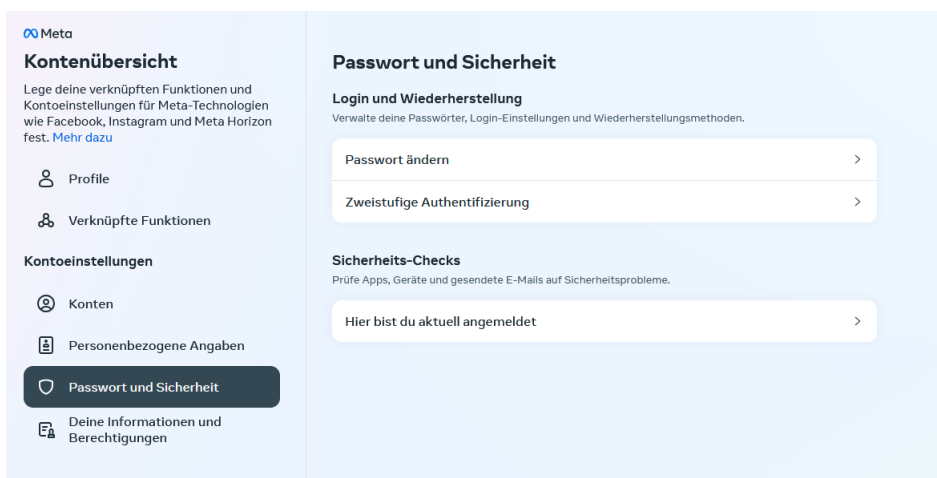


Abbildung 3.8.: Sicherheitseinstellungen Account Meta

### 3.2.6. Account Web.de

Im Verlauf der Accounterstellung beim Anbieter Web.de wurde folgende neue E-Mail-Adresse generiert: „masterthesis.stefan@web.de“. Auch für Web.de wurde die Zwei-Faktor-Authentifizierung aktiviert. Web.de fordert hierfür die Installation der proprietären App „Web.de“ (vgl. Abbildung 3.9).

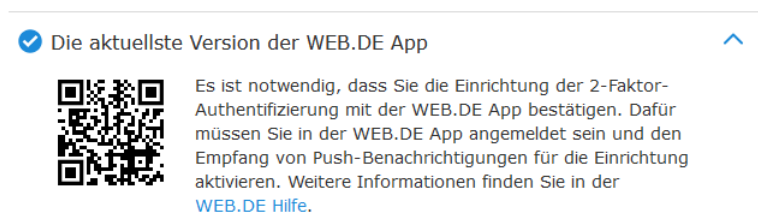


Abbildung 3.9.: Nutzung Web.de App für 2FA

Mit Hilfe dieser App kann eine Authenticator-App zum Account hinzugefügt werden. Für diesen Account wurde die Telefonnummer „017X / XXXXX118“ hinterlegt, die auch auch für die Wiederherstellung genutzt werden kann. Weiterhin ist es möglich eine zweite E-Mail-Adresse für eine Wiederherstellung zu hinterlegen.

### 3.2.7. Account Ubiquiti Unifi

Für die Erstellung des Accounts beim Anbieter Ubiquiti wurde ebenfalls die E-Mail-Adresse „s.alfeis@stud.hs-wismar.de“ verwendet. Es wurde für den primären Zugang die Zwei-Faktor-Authentifizierung aktiviert. Dies kann über die proprietäre App „Unifi Verify“ oder einen anderen Authenticator umgesetzt werden. Hier wurde der Google Authenticator verwendet. Alle vorgenommenen Einstellungen sind in Abbildung 3.10 dargestellt.

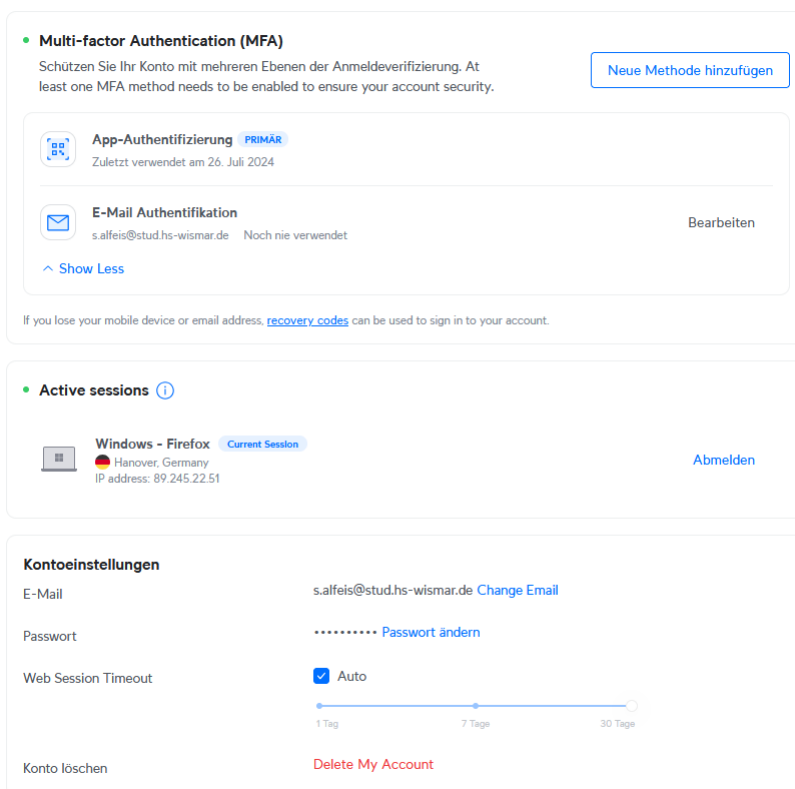


Abbildung 3.10.: Sicherheitseinstellungen Ubiquiti

In den Sicherheitseinstellungen des Accounts kann zudem eine Code-Liste generiert werden, für den Fall, dass die E-Mail-Adresse oder die mobile App nicht mehr verfügbar sind. Diese Code-Liste wird als PDF Datei ausgegeben und kann physisch ausgedruckt oder digital hinterlegt werden.

---

### 3.2.8. Account Steam

Für die Online-Spiele-Plattform Steam wurde ebenfalls ein Account mit Hilfe der E-Mail-Adresse „s.alfeis@stud.hs-wismar.de“ erstellt. In den Account-Einstellungen kann „Steam Guard“ aktiviert werden. Steam Guard dient der Absicherung des Accounts, hier kann entweder die Zusendung eines Codes auf eine E-Mail-Adresse oder die Nutzung der Steam-Mobile-App eingestellt werden. Während der Einrichtung der App auf dem Mobilien Endgerät wird ein Code angezeigt, der für die Wiederherstellung des Accounts oder den Transfer des Authentifikators genutzt werden kann (siehe Abbildung 3.11).

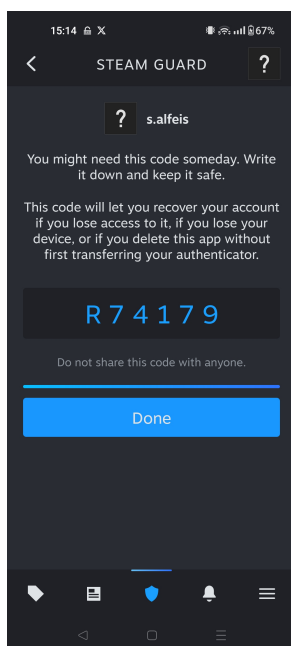


Abbildung 3.11.: Steam Guard Code

### 3.2.9. Account Facebook

Für die Durchführung der Evaluation wurde ebenfalls ein Facebook Account erstellt. Die Sicherheitseinstellungen für einen Facebook Account werden jedoch über eine Seite des Dienstleisters Meta getätigt. Da ein Account beim Dienstleister Meta bereits Bestandteil dieser Analyse ist, wurden keine weiteren Schritte bezüglich der Auswertung von Facebook unternommen.

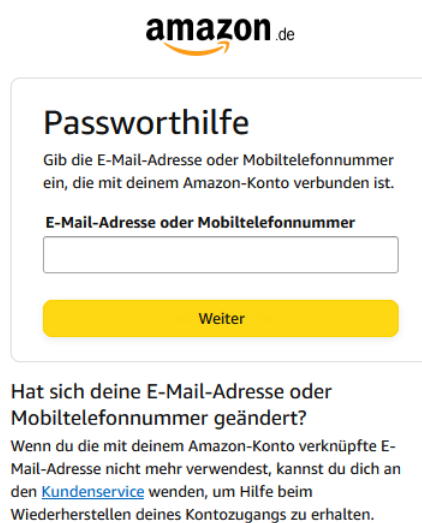
---

### 3.3. Umsetzung von Wiederherstellungsmethoden

Die folgenden Kapitel beschreiben die zu den erstellten Accounts gehörenden Wiederherstellungsmethoden. Die Durchführung der Wiederherstellung erfolgte jeweils im privaten Modus des Firefox Browser. Hiermit sollte eine eventuelle Nutzung von während der Erstellung genutzten Cookie-Daten vermieden werden[66][67]. Als Startpunkt wurde je nach Option des Anbieters „Passwort vergessen“ gewählt.

#### 3.3.1. Wiederherstellung Amazon

Die Wiederherstellungsmethode beim Onlinedienst Amazon wurde in zwei Schritten durchgeführt. Im ersten Durchlauf erfolgte für den Account die Wiederherstellung ohne einen Passkey. Die Wiederherstellung wird mittels Zusendung eines Einmal-Passwortes (OTP) an eine E-Mail-Adresse oder per SMS durchgeführt. Wenn ein Benutzer die Wiederherstellungsmethode bei Amazon startet, wird zunächst nach der hinterlegten E-Mail-Adresse oder Telefonnummer zu dem betreffenden Account gefragt (vgl. Abbildung 3.12).



amazon.de

**Passworthilfe**

Gib die E-Mail-Adresse oder Mobiltelefonnummer ein, die mit deinem Amazon-Konto verbunden ist.

**E-Mail-Adresse oder Mobiltelefonnummer**

Weiter

Hat sich deine E-Mail-Adresse oder Mobiltelefonnummer geändert?

Wenn du die mit deinem Amazon-Konto verknüpfte E-Mail-Adresse nicht mehr verwendest, kannst du dich an den [Kundenservice](#) wenden, um Hilfe beim Wiederherstellen deines Kontozugangs zu erhalten.

Abbildung 3.12.: Start Wiederherstellung Amazon

An diese E-Mail-Adresse oder Telefonnummer wird ein OTP gesendet, welches anschließend die Möglichkeit zur Eingabe eines neuen Passwortes freischaltet (siehe Abbildungen 3.13 3.14).

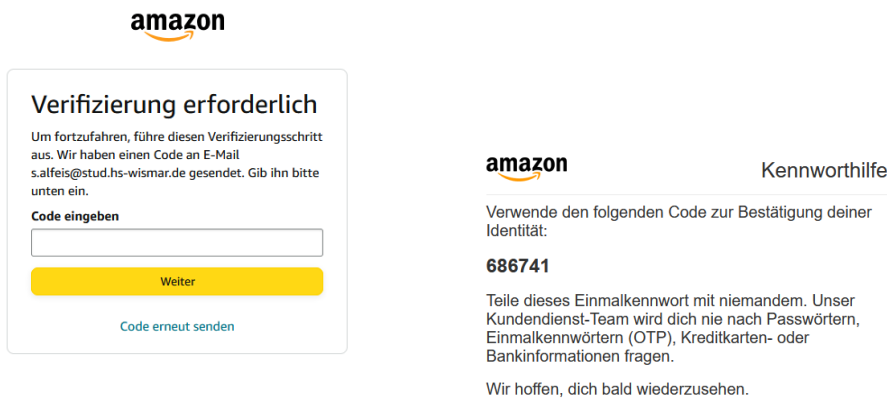


Abbildung 3.13.: Fenster zur Eingabe OTP Amazon

Abbildung 3.14.: Reset E-Mail Amazon

Abbildung 3.15 zeigt die Eingabemaske, welche nach der Eingabe des OTP dem Benutzer angezeigt wird. Nach der erfolgten Eingabe kann der Benutzer sich wieder mit den neu erstellten Daten anmelden.

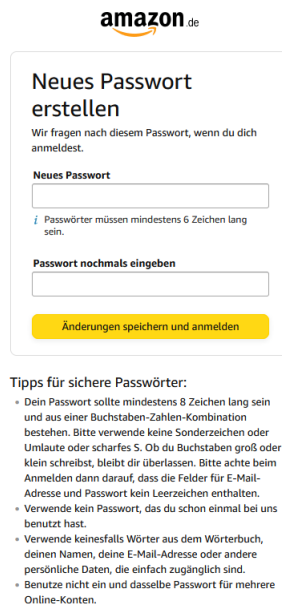
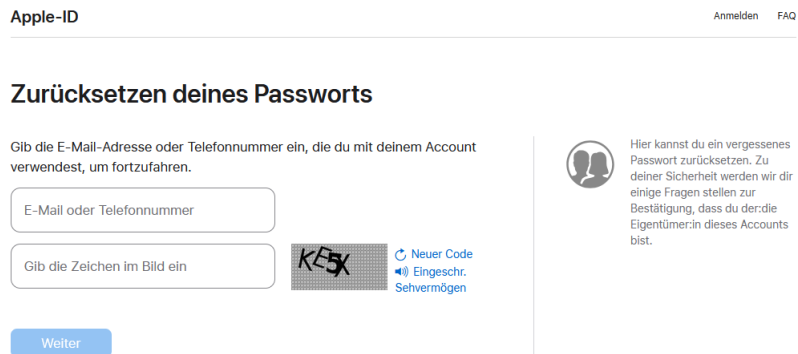


Abbildung 3.15.: Erstellung neues Passwort Amazon

Im zweiten Durchlauf war die Verwendung des Passkeys aktiviert. Auch hier war die Wiederherstellung nur über die hinterlegte E-Mail-Adresse oder Telefonnummer möglich.

### 3.3.2. Wiederherstellung Apple

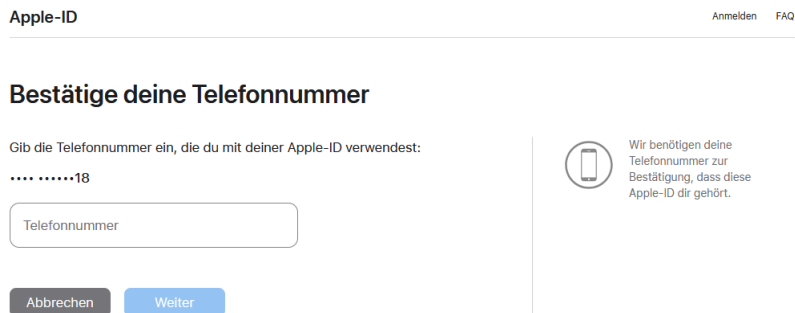
Der Online Dienstleister Apple bietet mehrere Möglichkeiten einen Account wieder herzustellen, wenn dem Benutzer die primären Authentifikationsfaktoren nicht mehr zugänglich sind. Auf der Webseite „appleid.apple.com/sign-in“ kann über eine Verlinkung die Seite „iforgot.apple.com/sign-in“ aufgerufen werden.



The screenshot shows the Apple ID password reset page. At the top left is 'Apple-ID' and at the top right are links for 'Anmelden' and 'FAQ'. The main heading is 'Zurücksetzen deines Passworts'. Below it, a text prompt asks for an email address or phone number. There are two input fields: one for 'E-Mail oder Telefonnummer' and another for 'Gib die Zeichen im Bild ein' (with a CAPTCHA image showing 'KEX'). To the right of the second field are links for 'Neuer Code', 'Eingeschr. Sehvermögen', and 'Sehvermögen'. A blue 'Weiter' button is at the bottom left. On the right side, there is an icon of two people and a text block explaining that a forgotten password can be reset and that security questions will be asked to verify ownership.

Abbildung 3.16.: Apple Zurücksetzen eines Passwortes

Abbildung 3.17 zeigt die Eingabe der zum Account gehörenden E-Mail-Adresse oder Telefonnummer. Die Eingabe muss durch ein CAPTCHA bestätigt werden. Für diesen Durchlauf wurde die Option E-Mail-Adresse verwendet. Im Folgenden Schritt muss die zur Apple-ID gehörende Telefonnummer eingegeben werden.



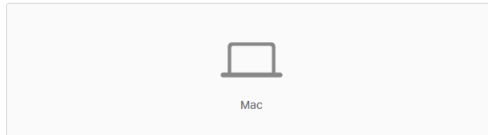
The screenshot shows the Apple ID phone number verification page. At the top left is 'Apple-ID' and at the top right are links for 'Anmelden' and 'FAQ'. The main heading is 'Bestätige deine Telefonnummer'. Below it, a text prompt asks for the phone number. There is a text input field for 'Telefonnummer' and a CAPTCHA consisting of a series of dots followed by the number '18'. At the bottom left are two buttons: 'Abbrechen' and 'Weiter'. On the right side, there is an icon of a smartphone and a text block explaining that the phone number is needed for verification.

Abbildung 3.17.: Apple Wiederherstellung 2

Anschließend öffnet sich ein Fenster (vgl. Abbildung 3.18), welches den Benutzer an ein zur Apple-ID gehörendes Gerät verweist.

### Schau nach einer auf deinem Mac angezeigten Benachrichtigung

Eine Nachricht mit Anweisungen wurde an deinen Mac gesendet. Verwende diese, um das Zurücksetzen deines Passworts abzuschließen.



[Benötigst du ausführlichere Anweisungen?](#) >  
[Keinen Zugriff auf deinen Mac?](#)



Am einfachsten und sichersten ist es, dein Passwort mithilfe deines Apple-Geräts zurückzusetzen. Es hilft bei der Bestätigung, dass die Anfrage wirklich von dir stammt.

Abbildung 3.18.: Apple Wiederherstellung 3

Auf dem zur Apple-ID gehörenden Gerät öffnet sich im Anschluss ein Pop-Up-Fenster, welches den Benutzer zur Wiederherstellung des Passwortes leitet (vgl. Abbildung 3.19). Hierfür ist das für das Gerät gesetzte Passwort notwendig. Nach der Eingabe und Bestätigung kann der Benutzer ein neues Passwort für die Apple-ID vergeben.

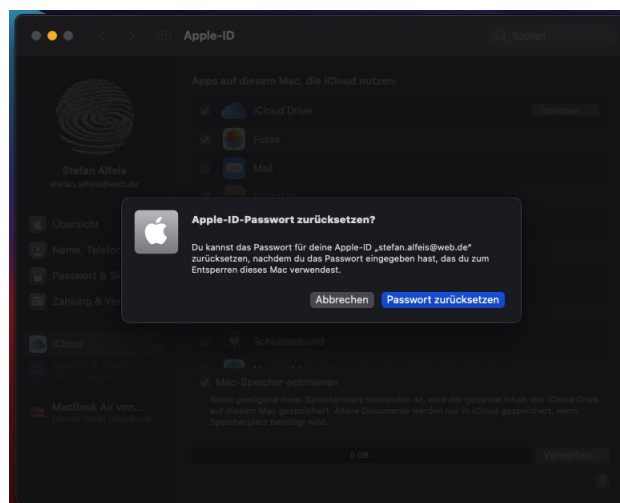


Abbildung 3.19.: Apple Wiederherstellung 4

Sollte der Benutzer nicht mehr im Besitz eines mit der Apple-ID verbundenen Gerätes sein, kann dieser auf andere Geräte zurückgreifen. Hierfür stehen dem Benutzer 3 Optionen zur Verfügung (vgl. Abbildung 3.20):

- Nutzung eines neuen Apple Gerät
- Nutzung eines iOS-Gerätes einer anderen Person
- Nutzung eines iOS-Gerätes aus einem Apple Store



## Verwende ein anderes Apple-Gerät, um dein Passwort zurückzusetzen.



### Passwort zurücksetzen während der Anmeldung auf einem neuen Gerät

Du kannst dein Passwort über den Anmeldebildschirm auf deinem neuen iPhone, iPad, iPod touch oder Mac zurücksetzen.

Weiter



### Ein iOS-Gerät einer anderen Person verwenden

Wenn ein:e Freund:in oder Familienmitglied über ein iPhone, iPad oder einen iPod touch verfügt, kannst du dein Passwort mit diesem Gerät zurücksetzen.

Weiter



### Ein iOS-Gerät in einem Apple Store verwenden

Wenn du einen Apple Store in der Nähe hast, kannst du dort ein anderes iPhone, iPad oder einen anderen iPod touch verwenden, um dein Passwort zurückzusetzen.

Weiter

Abbildung 3.20.: Apple Wiederherstellung 5

Bei einem neuen Gerät hat der Benutzer die Wahl, mit Hilfe der Verlinkung „Vergessen“ die Wiederherstellung zu starten oder, wenn er bereits das Gerät ohne Apple-ID gestartet hat über die Einstellungen den Vorgang zu beginnen (vgl. Abbildung 3.21).

## Passwort zurücksetzen während der Anmeldung auf einem neuen Gerät.

Stelle sicher, dass dieses Gerät iOS 11 oder macOS High Sierra (oder neuer) verwendet.



### Auf einem iPhone, iPad oder iPod touch

- ① Wenn du bei der Einrichtung aufgefordert wirst, dich mit deiner Apple-ID anzumelden, tippe auf den „Vergessen“-Link. Tippe anschließend auf „Apple-ID oder Passwort vergessen“ und folge den Anweisungen auf dem Bildschirm.
- ② Wenn du die Anmeldung mit deiner Apple-ID bei der Einrichtung übersprungen hast, öffne „Einstellungen“, tippe auf „Beim [Gerät] anmelden“ > „Noch keine Apple-ID oder hast du sie vergessen?“ und folge anschließend den Anweisungen auf dem Bildschirm. Für iOS 10.2 (oder älter) tippe auf „iCloud“ > „Apple-ID oder Passwort vergessen“ und folge den Anweisungen auf dem Bildschirm.

Abbildung 3.21.: Apple Wiederherstellung 6

Wird das Gerät einer anderen Person genutzt, kann der Benutzer hier „iforgot.apple.com/sign-in“ (bei iOS Version 17 oder neuer) aufrufen oder über die App „Apple Support“ (bei iOS Version 15 oder neuer) den Wiederherstellungsvorgang starten (vgl. Abbildung 3.22).

## Dein Passwort mit dem Apple-Gerät einer anderen Person zurücksetzen

Stelle sicher, dass auf dem Apple-Gerät, das du dir ausleihst, iOS 15 oder iPadOS 15 (oder neuer) installiert ist.



Auf einem Apple-Gerät mit iOS 17 oder iPadOS 17 oder neuer

- 1 Rufe [iforgot.apple.com](https://iforgot.apple.com) auf.
- 2 Tippe auf „Passwort zurücksetzen“ und befolge dann die Schritte auf deinem Bildschirm.

Auf einem Apple-Gerät mit iOS 15 oder iPadOS 15 (oder neuer)

- 1 Öffne die „App Store“-App. Suche dort nach „Apple Support“ und lade die App herunter.
- 2 Öffne die Support-App von Apple. Scrolle nach unten zu „Support-Tools“.
- 3 Tippe auf „Passwort zurücksetzen“ und befolge dann die Schritte auf deinem Bildschirm.

Zurück

Abbildung 3.22.: Apple Wiederherstellung 7

Bei der Verwendung eines Gerätes aus dem Apple Store muss ebenfalls die App „Apple Support“ für die Wiederherstellung verwendet werden.

### 3.3.3. Wiederherstellung Google

Der Online Dienstleister Google bietet folgende Möglichkeiten für die Wiederherstellung eines Accounts an (vgl. Abbildung 3.23):

- Bestätigung über die App Google Authenticator
- Eingabe eines achtstelligen Back-up-Codes
- Sendung eines Bestätigungscode an eine alternative hinterlegte E-Mail-Adresse
- Sendung eines Bestätigungscode an eine hinterlegte Telefonnummer
- mit anderer Anmeldeoption versuchen

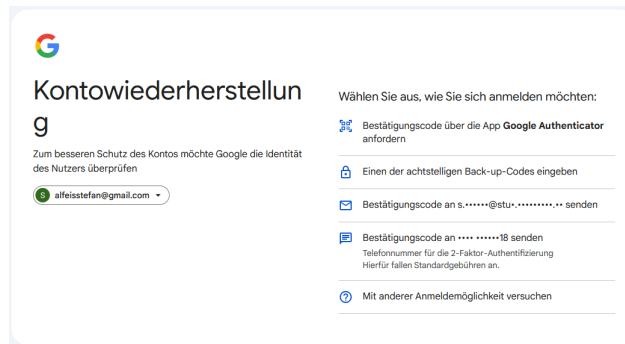


Abbildung 3.23.: Wiederherstellungsmethoden Google

Als erste Option wurde die Methode Bestätigung über die App Google Authenticator durchgeführt. Der Prozess fordert den Benutzer auf, den aktuellen Code aus dem Google Authenticator einzugeben (vgl. Abbildung 3.24).

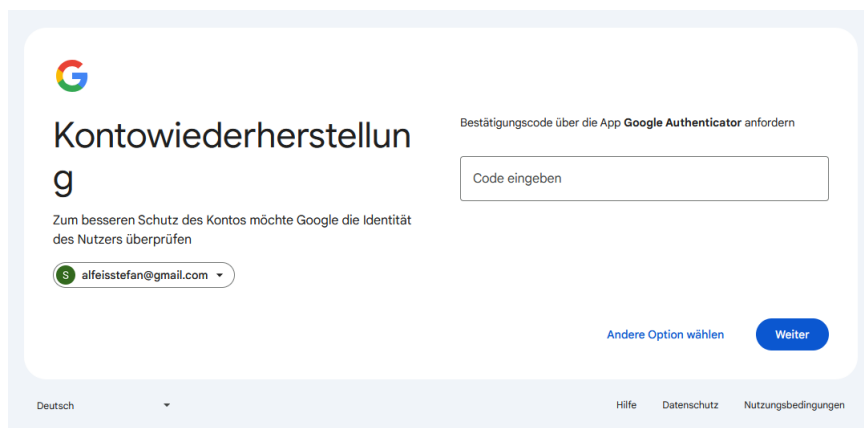


Abbildung 3.24.: Codeeingabe Google Authenticator

Der nächste Schritt bietet dem Benutzer die Möglichkeit ein neues Passwort für den Account zu vergeben (siehe Abbildung 3.25). Der Benutzer kann jedoch auch durch Betätigung der “Weiter“ Schaltfläche direkt zu seinem Konto gelangen.

Die zweite Option der Wiederherstellung ist die Eingabe eines achtstelligen Back-up-Codes aus der im Account generierten Liste. Nach der Eingabe eines der Codes wird auch hier dem Benutzer die Option ein neues Passwort zu vergeben oder direkt zum Account zu gehen gegeben. Analog erfolgt die Durchführung des Prozesses für die Methode durch SMS oder E-Mail.

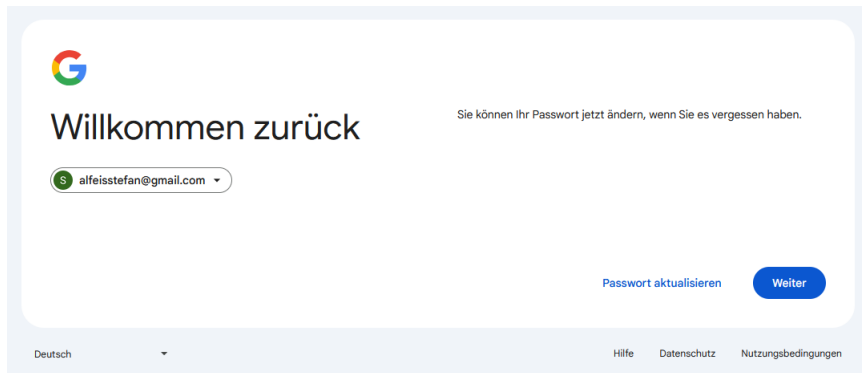


Abbildung 3.25.: Erstellen neues Passwort Google

Die Option „mit anderer Anmelde­möglichkeit anmelden“ fragt nach einem älteren Passwort, an welches sich der Benutzer noch erinnern kann (vgl. Abbildung 3.26). Nach Eingabe eines alten Passwortes wird der Benutzer aufgefordert eine E-Mail-Adresse einzugeben, an die Google einen Bestätigungscode versenden kann. Im An-

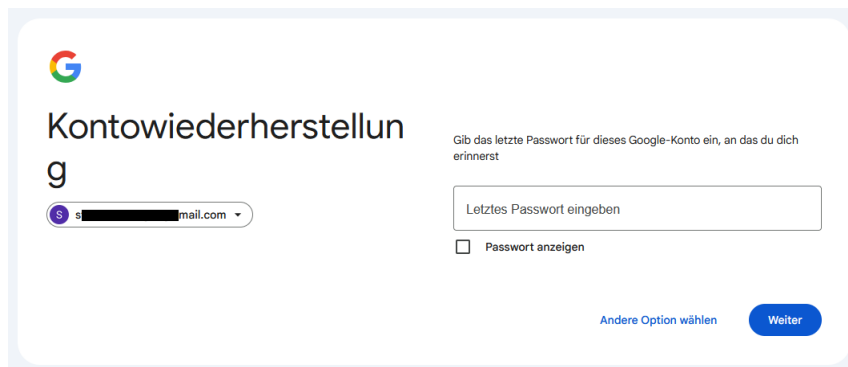


Abbildung 3.26.: Eingabe altes Passwort Google

schluss an die Eingabe einer E-Mail-Adresse erscheint ein Fenster im Browser, welches den Benutzer informiert, dass innerhalb der nächsten 48 Stunden ein Anmelde­link an die eingegebene Adresse versendet wird. Zeitgleich werden an die im Konto hinterlegten E-Mail-Adressen identische E-Mails versendet, die den Benutzer über den Wiederherstellungsversuch informieren. Der Benutzer hat hier durch die Betätigung eines Links die Möglichkeit, den Vorgang abubrechen. Nach Erhalt der E-Mail kann der Benutzer über den in der E-Mail enthaltenen Link das Passwort für den Account ändern (siehe Abbildung 3.27).

---

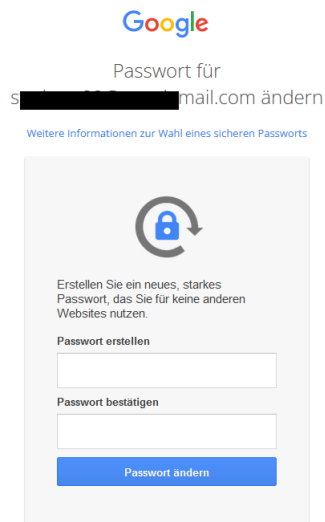


Abbildung 3.27.: Eingabe neues Passwort Google

Abschließend erhält der Benutzer wieder Zugriff zu seinem Account.

### 3.3.4. Wiederherstellung Microsoft

Die Durchführung der Wiederherstellung war im Selbstversuch nicht möglich, da kein Account für Microsoft erstellt werden konnte (siehe Kapitel 3.2.4 Microsoft).

Anhand der Beschreibung auf der Microsoft Support Seite[68] stellt sich der Ablauf der Wiederherstellung wie folgt dar: Der Benutzer kann zuerst wählen, ob er den notwendigen Überprüfungscode per E-Mail oder Telefonnummer erhalten möchte. Anschließend erhält der Benutzer auf das gewählte Medium eine E-Mail bzw. eine SMS mit dem benötigten Code. Diesen Code kann der Benutzer nun im Browser eingeben. Im Anschluss hat der Benutzer die Möglichkeit ein neues Passwort zu vergeben. Es kann weiterhin ein Wiederherstellungscodes für den Account generiert werden, für den Fall, dass alle weiteren Faktoren nicht mehr verfügbar sind.

Weitere Optionen zur Wiederherstellung können über den Kontakt zum Microsoft Support Team angefragt werden.

### 3.3.5. Wiederherstellung Meta

Die Wiederherstellung des Accounts bei Meta erfolgt über die für den Account genutzte E-Mail-Adresse. Wird der Vorgang gestartet, muss der Benutzer zunächst seine E-Mail-Adresse eingeben. An diese wird dann ein Code versendet (siehe Abbildungen 3.28 und 3.29).

**Passwort vergessen?**

Bitte gib deine E-Mail-Adresse ein. Wir senden dir dann einen Code, mit dem du auf dein Konto zugreifen kannst. Wenn du dich mit [Facebook](#) oder [Instagram](#) anmeldest, setze stattdessen das Passwort für das entsprechende Konto zurück.

E-Mail-Adresse

Konto finden

Abbildung 3.28.: Eingabe E-Mail  
Meta

**Konto bestätigen**

Wir haben einen Code an s.alfeis@stud.hs-wismar.de gesendet. Gib diesen Code hier ein, um dein Konto zu bestätigen.

Bestätigungscode

Keinen Zugriff mehr auf diese E-Mail-Adresse?

Weiter

Code erneut senden

Abbildung 3.29.: Eingabe Code  
Meta

Nach Eingabe des zu gesendeten Codes wird der Benutzer auf eine Seite zur Eingabe eines neuen Passwortes weitergeleitet. Abschließend wird die Eingabe eine Authentifizierungscode der gekoppelten App verlangt. Ist die Authentifizierung erfolgreich, wird der Prozess abgeschlossen.

Wenn ein Benutzer keinen Zugriff mehr auf seine E-Mail-Adresse hat, bietet Meta die Option an, direkt mit einem Mitarbeiter in Verbindung zu treten[69]. Diese Option wird im Rahmen dieser Master-Thesis nicht weiter evaluiert.

### 3.3.6. Wiederherstellung Web.de

Der Wiederherstellungsvorgang für den E-Mail-Provider web.de startet mit der Abfrage des betroffenen Accounts. Hierfür kann die E-Mail-Adresse oder der Benutzername angegeben werden (vgl. Abbildung 3.30). Zur Absicherung gegen Anfragen durch nicht-menschliche Systeme wird eine Sicherheitsfrage in Form eines CAPTCHA gestellt.

**Passwort vergessen?**

Kein Problem! Hier können Sie Ihr altes Passwort zurücksetzen und ein neues anlegen.

E-Mail-Adresse oder Nutzernamen

E-Mail-Adresse oder Nutzernamen eingeben

Sicherheitsabfrage



[Anderes Wort anzeigen](#)

Bitte geben Sie die Zeichen aus dem Bild ein. Damit wird sichergestellt, dass die Anfrage für ein neues Passwort von einem Menschen angestoßen wird.

Wort aus Bild eingeben

Weiter

Abbildung 3.30.: Start Wiederherstellung web.de

---

Anschließend kann der Benutzer die Methode wählen, mit der er die Wiederherstellung durchführen möchte. Zur Auswahl stehen hier (vgl. Abbildung 3.31):

- Wiederherstellung per SMS
- Wiederherstellung per E-Mail an Account, z.B. durch Nutzung der web.de App
- Wiederherstellung durch im Browser gespeicherte Passwörter
- Wiederherstellung durch Identitätsprüfung

## Passwort vergessen?

Um wieder Zugriff auf Ihr Postfach zu erhalten, wählen Sie eine der folgenden Möglichkeiten:

**Per SMS** ?

Freischalt-Code für ein neues Passwort an mein Mobiltelefon senden: +491\*\*\*\*\*118

**Senden**

---

**Per E-Mail an masterthesis.stefan@web.de**

Nutzen Sie alternative Zugriffsmöglichkeiten auf Ihr WEB.DE Postfach, z. B. über die WEB.DE Mail App – und haben Sie noch Zugriff darüber? Dann können wir Ihnen einen Freischalt-Link für ein neues Passwort an Ihre WEB.DE E-Mail-Adresse senden: masterthesis.stefan@web.de

**Senden**

---

**Im Browser gespeicherte Passwörter anzeigen**

Falls Sie Ihr WEB.DE Passwort in Ihrem Browser oder E-Mail-Programm gespeichert haben, können Sie es wieder anzeigen lassen. Weitere Informationen dazu finden Sie in der [WEB.DE Hilfe](#).

---

Keine der Optionen kommt für mich infrage!  
[Weiter zur Identitätsprüfung](#)




Abbildung 3.31.: Abfrage Account web.de

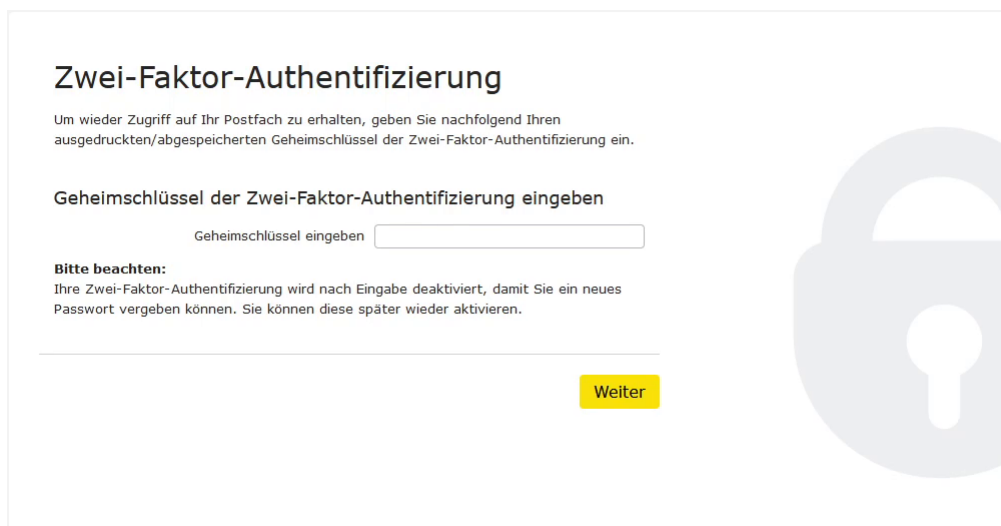
Im ersten Durchlauf wurde die Methode per SMS gewählt. Es wurde eine SMS mit einem Code an die im Account hinterlegte Telefonnummer versendet. Abbildung 3.32 zeigt die Eingabemaske.



The screenshot shows a web page titled "Bitte SMS-Nachrichten prüfen". Below the title, it says "Wir haben eine SMS mit einem Freischalt-Code an Ihr Mobiltelefon gesendet." The main heading is "Freischalt-Code eingeben". Below this, it says "Geben Sie bitte hier den Code ein, den wir an die Rufnummer +491\*\*\*\*\*118 gesendet haben:". There is a text input field labeled "Code" containing the value "298639". Below the input field, there are two buttons: "Passwort vergessen neu starten" (a blue link) and "Code bestätigen" (a yellow button). On the right side of the page, there is a large, light gray padlock icon.

Abbildung 3.32.: Eingabe Code aus SMS web.de

Nach der erfolgten Eingabe des Codes aus der SMS wird durch den Prozess die Eingabe des Geheimschlüssels der Zwei-Faktor-Authentifizierung gefordert (siehe Abbildung 3.33). Es wird darauf hingewiesen, dass durch diesen Vorgang die Zwei-Faktor-Authentifizierung deaktiviert wird und später manuell wieder aktiviert werden muss.



The screenshot shows a web page titled "Zwei-Faktor-Authentifizierung". Below the title, it says "Um wieder Zugriff auf Ihr Postfach zu erhalten, geben Sie nachfolgend Ihren ausgedruckten/abgespeicherten Geheimschlüssel der Zwei-Faktor-Authentifizierung ein." The main heading is "Geheimschlüssel der Zwei-Faktor-Authentifizierung eingeben". Below this, there is a text input field labeled "Geheimschlüssel eingeben". Below the input field, there is a section titled "Bitte beachten:" with the text "Ihre Zwei-Faktor-Authentifizierung wird nach Eingabe deaktiviert, damit Sie ein neues Passwort vergeben können. Sie können diese später wieder aktivieren." Below this text, there is a yellow button labeled "Weiter". On the right side of the page, there is a large, light gray padlock icon.

Abbildung 3.33.: Eingabe Geheimschlüssel 2FA web.de



---

Abschließend wird der Benutzer zur Eingabe eines neuen Passwortes aufgefordert (siehe Abbildung 3.34). Im Anschluss an die Erstellung des neuen Passwortes wird der Benutzer wieder zur Login-Seite von web.de geleitet und kann den Account wieder nutzen.



Abbildung 3.34.: Eingabe neues Passwort web.de

Im zweiten Durchlauf wurde die Methode Wiederherstellung per E-Mail durchgeführt. Es wurde automatisiert eine E-Mail mit einem Link zur Wiederherstellung des Passwortes an den Account versendet. In der web.de App konnte die E-Mail geöffnet und der Vorgang gestartet werden. Nach Betätigung des Links wird man in den Browser des mobilen Endgerätes weitergeleitet. Es wird der Benutzername des Accounts abgefragt, für den die Wiederherstellung erfolgen soll. Im Anschluss an die Eingabe leitet der Prozess den Benutzer direkt zur Eingabe eines neuen Passwortes weiter. Die Abbildungen 3.35 und 3.36 zeigen diesen Vorgang.

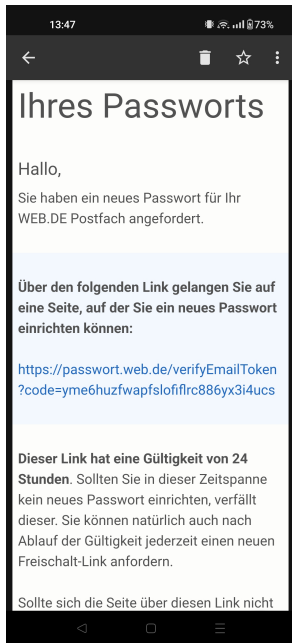


Abbildung 3.35.: web.de App

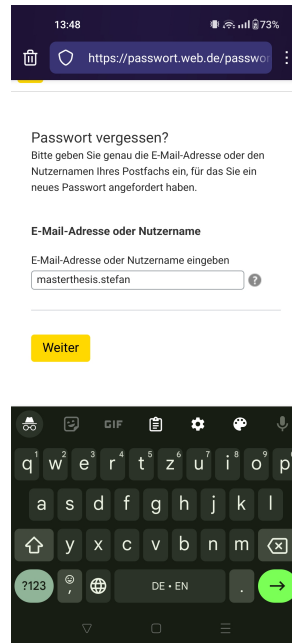


Abbildung 3.36.: Eingabe Name

Die letzte Wiederherstellungsmethode durch persönliche Identifizierung wurde im Rahmen dieser Master-Thesis nicht betrachtet. Web.de gibt an, dass hierfür ein Personalausweis, ein Smartphone mit Kamera inklusive der App „IDnow“ sowie eine alternative E-Mail-Adresse benötigt werden[70].

### 3.3.7. Wiederherstellung Ubiquiti Unifi

Der Prozess der Wiederherstellung beim Dienstleister Ubiquiti startet mit der Abfrage der E-Mail-Adresse, die mit dem betreffenden Account verbunden ist (siehe Abbildung 3.37).

An diese Adresse wird nun eine E-Mail mit einen Link zur Zurücksetzung des Passwortes versendet. Abbildung 3.38 zeigt einen Ausschnitt aus der erhaltenen E-Mail. In dieser E-Mail sind auch Daten über den Ursprung der Anfrage zur Zurücksetzung des Passwortes enthalten.

Im Anschluss an die Eingabe eines neuen Passwortes wird der Benutzer wieder zur Anmeldeseite von Ubiquiti geleitet.

Der zweite Pfad der Wiederherstellung eines Ubiquiti Accounts bezieht sich auf die Zwei-Faktor-Authentifizierung. Hat der Benutzer keinen Zugriff mehr auf die mit seinem Account gekoppelte App oder das mobile Gerät, kann er per E-Mail einen Code anfordern oder einen der vorab erstellten Recovery Codes nutzen, um Zugang zu seinem Account zu bekommen (vgl. Abbildung 3.39).

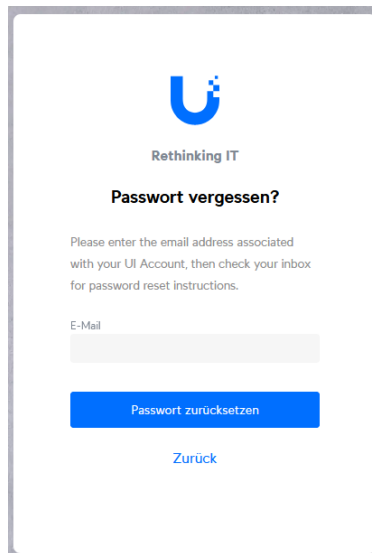


Abbildung 3.37.: Start Wiederherstellung Ubiquiti

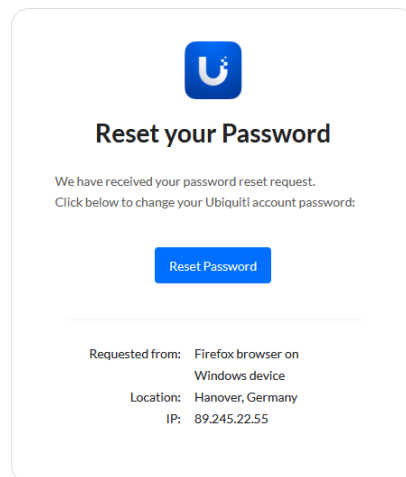


Abbildung 3.38.: E-Mail mit Link Ubiquiti

Hat der Benutzer auch diese beiden Optionen nicht mehr verfügbar, weist der Dienstleister den Benutzer freundlich darauf hin, dass er keine weitere Möglichkeit hat seinen Account wieder zu erlangen und ein neuer Account erstellt werden muss (vgl. Abbildung 3.40).

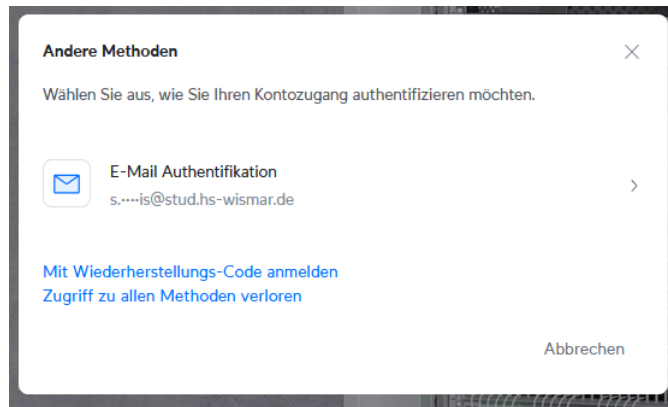


Abbildung 3.39.: Methoden für Verlust 2FA Ubiquiti

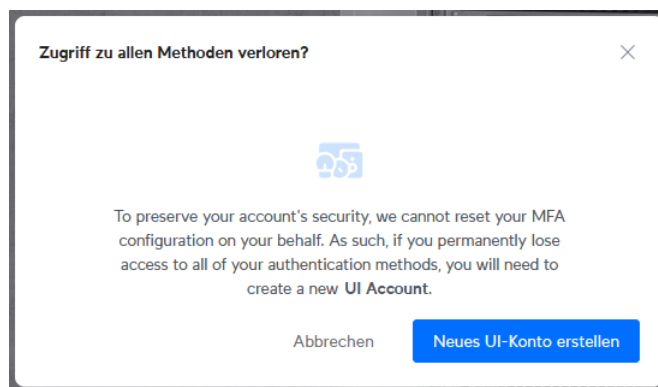


Abbildung 3.40.: Verlust aller 2FA Ubiquiti

### 3.3.8. Wiederherstellung Steam

Für die Wiederherstellung beim Onlinedienstleister Steam werden verschiedene Optionen angeboten (vgl. Abbildung 3.41):

- Accountname oder Passwort vergessen
- Account wurde gestohlen
- Benutzer erhält keinen Steam-Guard-Code
- Steam-Mobile-Authenticator wurde gelöscht oder verloren

Für die Option „Accountname oder Passwort vergessen“ startet die Wiederherstellung mit der Abfrage der zum Account gehörenden E-Mail-Adresse. Zusätzlich muss ein CAPTCHA ausgefüllt werden. Abbildung 3.42 zeigt die Eingabemaske aus dem Fenster des Browsers.

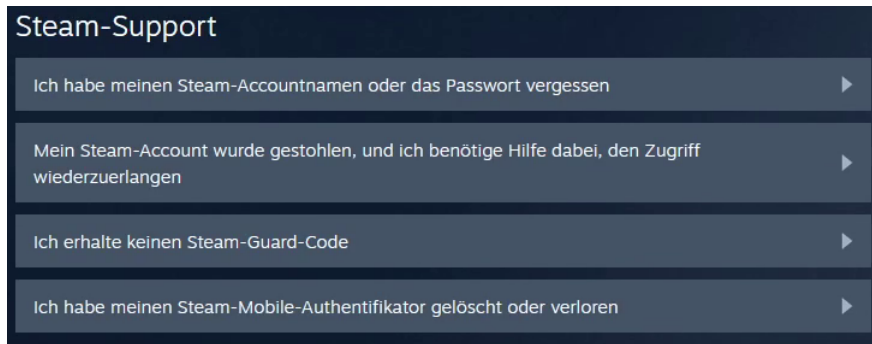


Abbildung 3.41.: Start Wiederherstellung Steam



Abbildung 3.42.: Eingabe E-Mail-Adresse Steam

Nach Eingabe der Daten öffnet sich ein neues Fenster, welches dem Benutzer die Auswahl bietet, entweder eine Bestätigung über die gekoppelte Steam-Mobile-App anzufragen oder eine weitere Option aufzurufen. Wird die Bestätigung per App ausgewählt, wird dem Benutzer ein Code angezeigt. Der Benutzer muss jetzt die Steam-App auf seinem mobilen Gerät öffnen und in den Optionen den Punkt „Bestätigungen“ auswählen. Hier wird dem Benutzer eine Nachricht angezeigt, in der ebenfalls der Code sichtbar ist. Bestätigt der Benutzer den Code, öffnet sich im Browser des Computers ein neues Fenster, welches den Accountnamen anzeigt. Hier hat der Benutzer vier Optionen zur Auswahl:

- Passwort zurücksetzen
- E-Mail-Adresse zurücksetzen
- Steam-Mobile-Authenticator entfernen
- Hilfe zu einem anderen Account

Bei Auswahl einer der ersten drei Optionen wird der Benutzer zu einer Seite weitergeleitet, die die Option, bietet einen Code an die mit dem Account gekoppelte E-Mail-Adresse zu senden. Die zweite Auswahlmöglichkeit besagt, dass der Benutzer keinen Zugriff mehr auf die E-Mail-Adresse hat und leitet den Benutzer zu einer Seite weiter, auf der das Passwort zum Account eingegeben werden kann. Wird hier die Option „Ich habe mein Passwort vergessen“ ausgewählt, führt der Prozess den Benutzer zu einer Seite mit einem Fragebogen. Der Benutzer wird aufgefordert, einige Informationen zu seinem Account anzugeben, um sich zu verifizieren. Abbildung 3.43 zeigt einen Ausschnitt dieses Fragebogens.

The image shows a dark-themed web form for recovering a Steam account. At the top, there is a breadcrumb trail: "Startseite > Account suchen > Steam-Support kontaktieren". Below this, the main heading reads "Lassen Sie uns den Zugriff auf Ihren Account wiederherstellen!". A sub-heading explains: "Bevor wir Ihren Account wiederherstellen können, müssen wir sicherstellen, dass Sie tatsächlich der Besitzer sind. Sie können diesen Vorgang beschleunigen, indem Sie unten so viele Informationen angeben, wie möglich." The form contains several input fields with associated labels and instructions:

- Ihre aktuelle E-Mail-Adresse (zur Kontaktaufnahme)**: A text input field.
- Erzählen Sie uns jetzt von Ihrem Steam-Account ...**: A section header.
- Wie lautet der Anmelde-name des Accounts, den Sie wiederherstellen möchten?**: A text input field. To its right, a note states: "Dies ist ein Pflichtfeld. Wenn Sie sich nicht an Ihren Accountnamen erinnern können, versuchen Sie, sich an Ihren Anzeigenamen zu erinnern."
- Wie lautet die erste E-Mail-Adresse, die mit Ihrem Account verknüpft wurde?**: A text input field. To its right, a note asks: "Können Sie sich nicht an die erste erinnern? Geben Sie bitte die älteste, an die Sie sich erinnern können, an."
- Geben Sie eine mit Ihrem Account verknüpfte Telefonnummer an**: A text input field. To its right, a note says: "Vielleicht haben Sie eine Telefonnummer mit Ihrem Account verknüpft, die bei der Wiederherstellung helfen kann."

Abbildung 3.43.: Fragebogen Steam

Wählt der Benutzer bei der Frage nach der Bestätigung durch die gekoppelte App 3.3.8 die zweite Option aus, erhält er die Optionen der Verifikation durch einen Code per SMS oder die Angabe, dass er auch keinen Zugriff mehr zur hinterlegten Telefonnummer hat. Bei Auswahl der ersten Option wird ein Code an die Telefonnummer versendet. Bei Auswahl der zweiten Option kann der Benutzer erneut aus zwei Optionen wählen, in diesem Fall die Zusendung eines Codes an die hinterlegte E-Mail-Adresse oder auch hier die Auswahl, dass kein Zugriff mehr besteht. Bei Auswahl der Option, dass kein Zugriff mehr auf die E-Mail-Adresse besteht, landet der Benutzer erneut auf der Seite zu Eingabe seines Passwortes. Wählt der Benutzer hier die Option „Ich habe mein Passwort vergessen“, wird der Benutzer auch hier zum Fragebogen weitergeleitet.

---

## 3.4. Methode

In den folgenden Abschnitten werden die Methoden beschrieben, die verwendet werden, um die Wiederherstellungsmethoden zu analysieren und zu bewerten. Es wird hierbei sowohl auf bereits existierende Anwendungen (siehe Kapitel 2.4 Analyse Tool) zurückgegriffen als auch eine Online-Umfrage erstellt.

### 3.4.1. Benutzer-Umfrage

Ein Bestandteil der Analyse von Wiederherstellungsmethoden soll eine Benutzer-Umfrage sein. Ziel dieser Umfrage ist es zu evaluieren, welche Wiederherstellungsmethoden den Benutzern bekannt sind und mit welchen dieser Methoden die Benutzer bereits in Berührung gekommen sind. Weiterhin soll mit Hilfe dieser Umfrage ein Bild erstellt werden, welche Akzeptanz bei den Benutzern vorhanden ist im Bezug auf Komplexität bei Wiederherstellungsmethoden.

Methodisch wird die Umfrage nach dem Mixed-Methods-Ansatz aufgebaut[71]. Der Mixed-Methods-Ansatz ist eine Kombination aus qualitativer und quantitativer Forschung. In der qualitativen Forschung wird der Fokus verstärkt auf die individuelle Antwort gelegt und es werden mehr Freitextantworten ausgewertet. Die quantitative Forschung ist auf messbare Werte und Zahlen ausgelegt. Hierbei wird meist mit Multiple-Choice- oder skalierbaren Fragen gearbeitet[72].

Die Umsetzung der Umfrage erfolgte als Online-Umfrage. Diese Methode wurde gewählt, da hierdurch die Umfrage schnell und mit verhältnismäßig geringem Aufwand erstellt werden konnte. Weiterhin kann eine Online-Umfrage einfach an die Teilnehmenden verteilt werden, da hier nur die Weitergabe einer Verlinkung zu der Umfrage notwendig ist. Zur Umsetzung einer Online-Umfrage gibt es verschiedene Anbieter. Für die Umfrage im Rahmen dieser Master-Thesis wurde die Webseite „empirio“ gewählt. „empirio“ bietet im Vergleich zu anderen Anbietern einen größeren kostenlosen Funktionsumfang bezogen auf die Erstellung und Art der Fragestellung an. Telefonische, postalische oder Face-to-Face-Umfragen wurden aufgrund des benötigten Zeitaufwands nicht in die Auswahl genommen[72].

Im Folgenden werden die Fragestellungen der Umfrage aufgeführt und erläutert. Zu Beginn der Umfrage wurde eine Informationsseite erstellt, die den Teilnehmenden Auskunft darüber geben sollte, um welche Fragestellung es bei der Umfrage geht und welche Inhalte zu erwarten sind.

---

Inhalt der Informationsseite:

Ziel dieser Umfrage ist es, eine Übersicht bezüglich der Nutzung und Kenntnis von Wiederherstellungsmethoden bei Onlinezugängen zu erstellen.

Wenn sich ein Benutzer einen Onlinezugang erstellt, so werden häufig Maßnahmen abgefragt, damit im Falle des Verlustes der Zugangsdaten, der Benutzer sich hierauf wieder Zugriff verschaffen kann. Bei manchen Accounterstellung wird dies nicht gleich zu Anfang abgefragt, sondern kann erst nach erfolgreicher Anmeldung in den Einstellungen des Accounts geändert werden.

Bekannte Beispiele sind persönliche Fragen, wie „Nennen Sie den Mädchennamen Ihrer Mutter“ oder die Möglichkeit eine Telefonnummer zu hinterlegen, an welche im Falle der Wiederherstellung eine SMS versendet wird.

Hinweis: Die hier erhobenen Daten werden ausschließlich für die Erstellung einer Master-Thesis verwendet.

### **Frage 1: Wie alt sind Sie?**

Die erste Frage diente zur Einleitung in den Fragebogen. Die Fragestellung sollte während der Auswertung der Umfrage dazu dienen eine eventuelle Einordnung bezogen auf das Alter, die Kenntnisse und die Vorstellungen oder Wünsche der Teilnehmenden geben zu können. Die Frage wurde als Multiple-Choice-Frage erstellt mit den Auswahlmöglichkeiten < 20 Jahre, 21-30 Jahre, 31-40 Jahre, 41-50 Jahre, 51-60 Jahre, 61-70 Jahre und > 70 Jahre.

### **Frage 2: Welche Erfahrung haben Sie mit Informationstechnologien?**

Die zweite Frage sollte in Zusammenhang mit Frage 1 Auskunft über die Vorkenntnisse bezogen auf Informationstechnologie der Teilnehmenden geben. Die Frage wurde als Multiple-Choice-Frage erstellt mit den Antwortmöglichkeiten:

- Einsteiger (Erste Kontakte durch Schule oder nur gelegentliche Nutzung)
- Grundlegende IT-Kenntnisse (Hauptsächliche Nutzung von Office-Programmen Schule oder Arbeit)
- Erweiterte Kenntnisse (Schulungen oder Fortbildungen in speziellen Themen der IT)
- Fachkenntnisse (Ausbildung oder Studium in der IT, berufliche Tätigkeit in der IT)



---

### **Frage 3: Welche der folgenden Wiederherstellungsmethoden kennen Sie?**

Frage 3 ist die erste Frage mit direktem Bezug zu Wiederherstellungsmethoden. Die Teilnehmenden hatten bei dieser Frage die Möglichkeit der Mehrfach-Auswahl. Folgende Antworten wurden vorgegeben:

- Passwort, Code oder Code-Liste
- E-Mail oder SMS
- persönliche Frage oder Sicherheitsfrage
- Token (Nutzung eines kryptographischen Schlüssel)

### **Frage 4: Haben Sie bei einem der folgenden Anbieter einen Benutzeraccount?**

Diese Frage stellte direkten Bezug zu einigen in der Master-Thesis betrachteten Anbietern her. Die Antworten konnten als Mehrfach-Auswahl gegeben werden.

- Google
- Apple
- Microsoft
- Amazon
- Facebook
- E-Mail-Provider (Web.de, GMX oder ähnliche)
- kein Account beiden genannten Optionen

### **Frage 5: Welche Wiederherstellungsmethode haben Sie für den / die Anbieter gewählt? (Wenn mehrere Möglichkeiten zutreffen, bitte "Andere" auswählen und in der nächsten Frage beantworten)**

Durch Frage 5 sollte erfasst werden, welche Art der Wiederherstellungsmethode die Teilnehmenden beim jeweiligen Anbieter gewählt haben. Es wurden die Möglichkeiten aus Frage 3 aufgegriffen und durch weitere Optionen ergänzt. Wie in der Fragestellung beschrieben, sollten die Anwender, wenn mehrere Methoden beim Anbieter gewählt wurden, diese Auswahl in der folgenden Frage 6 beantworten. Dies war nötig, da eine Fragestellung mit mehreren Stufen nicht als Mehrfach-Auswahl möglich war. Die Antworten waren folgendermaßen aufgebaut (jeweils für Google, Apple, Microsoft, Amazon, Facebook und E-Mail-Provider):

- 
- Passwort, Code oder Code-Liste
  - E-Mail oder SMS
  - persönliche Frage oder Sicherheitsfrage
  - Token (Nutzung eines kryptographischen Schlüssels)
  - Andere
  - nicht (mehr) bekannt
  - kein Account

**Frage 6: Wenn in der vorherigen Frage „Andere“ ausgewählt wurde, welche Methode wird verwendet? (Bitte Anbieter nennen)**

Frage 6 baut inhaltlich auf Frage 5 auf und wurde als Freitext Antwort formuliert. Die Frage diente zur Beschreibung, wenn eine Variante zur Wiederherstellung genutzt wurde, die nicht bereits als Antwort vorgegeben wurde.

**Frage 7: Haben Sie schon einmal für einen Onlinezugang eine Wiederherstellung durchgeführt oder durchführen müssen?**

Mit Frage 7 wurde erhoben, ob die Teilnehmenden bereits einmal ein Wiederherstellung bei einem Onlinezugang durchgeführt haben. Die Antwortmöglichkeiten waren Ja oder Nein als Multiple-Choice-Antwort.

**Frage 8: Wenn Frage 7 mit Ja beantwortet wurde, welche Methode wurde für die Wiederherstellung angewendet? (Bitte Anbieter und Methode nennen)**

Frage 8 baut direkt auf Frage 7 auf und diente der genaueren Beschreibung des Wiederherstellungsvorgangs. Es war ein Freitext Feld für die Antwort vorgegeben.

**Frage 9: Wenn Frage 8 beantwortet wurde, wie zufrieden waren Sie mit der gewählten / geforderten Methode? (1 Daumen = unzufrieden, 5 Daumen = sehr zufrieden)**

Diese Frage sollte Auskunft über die persönliche Wahrnehmung der Teilnehmenden im Bezug auf den Vorgang der Wiederherstellung geben. Als Antwortmöglichkeit wurde eine Skala mit den Werten von 1 bis 5 vorgegeben, wobei 1 für „unzufrieden“ und 5 für „sehr zufrieden“ stand.

---

**Frage 10: Was ist Ihnen wichtiger, wenn Sie an Wiederherstellungsmethoden denken, Sicherheit oder Bedienbarkeit?**

Mit Frage 10 sollte ein Stimmungsbild der Teilnehmenden eingeholt werden, inwiefern den Teilnehmenden der Punkt Sicherheit, Bedienbarkeit oder beides wichtig ist. Die Frage wurde mit Multiple-Choice-Antwort gestellt.

- Sicherheit
- beides
- Bedienbarkeit
- keine Angabe

**Frage 11: Wären Sie bereit für eine höhere Sicherheit bei Wiederherstellungsmethoden zusätzliche technische Maßnahmen in Kauf zu nehmen? (z.B. eine Handy-App, USB-Token oder ähnliches)**

Die letzte Frage dieser Umfrage zielte auf die Bereitschaft der Teilnehmenden ab, zusätzliche technische Maßnahmen für mehr Sicherheit bei Wiederherstellungsmethoden zu akzeptieren. Die Antwortmöglichkeit war als Multiple-Choice-Antwort gestellt:

- Ja
- Nein
- Weiß nicht



Durch die optionale Nutzung beider Authentifikationswege für die primäre Authentifikation wird hier der Sicherheitswert 2 priorisiert. Gleiches gilt für den Pfad der Wiederherstellungsmethoden, sodass sich als Gesamtsicherheitswert für die Sicherheit des Amazon Accounts der Wert 2 ergibt. Wichtig zu erwähnen ist, dass es keine gesonderte Wiederherstellung gibt, wenn die Option Passkey für die primäre Authentifikation gewählt wurde.

#### 4.1.2. Sicherheitsbewertung Apple

Die Wiederherstellung für einen Apple Account bietet, wie in Kapitel 3.3.2 beschrieben, mehrere Optionen. Jedoch verlaufen die Optionen im Falle der Nutzung eines anderen Gerätes, welches nicht im Besitz des Benutzers ist, vom Ablauf her gesehen gleich zur Methode, wenn der Benutzer seine eigenen Geräte nutzt. Deswegen wurde diese Option nur mit einer Authentifikation moduliert. Der Weg, wenn der Benutzer im Besitz aller notwendigen Geräte und Werte ist, wurde ausführlich modelliert. Die Authentifikationen E-Mail plus CAPTCHA und Telefonnummer haben den Sicherheitswert 2 bekommen. Die reine Kenntnis einer Telefonnummer wurde schlechter bewertet als der Besitz eines Gerätes, daher dieser Wert.

Das mit dem Apple Account gekoppelte Gerät wurde mit dem Sicherheitswert 3 bewertet. Dieser Sicherheitswert wurde angelehnt an den Sicherheitswert aus der primären Authentifikation gewählt. Somit ergibt sich für den gesamten Pfad der Wiederherstellung der Sicherheitswert 3. Da auch der Pfad für die primäre Authentifikation mit insgesamt 3 bewertet wurde ergibt sich für den Dienstleister Apple der Sicherheitswert 3 (vgl. Abbildung 4.2).

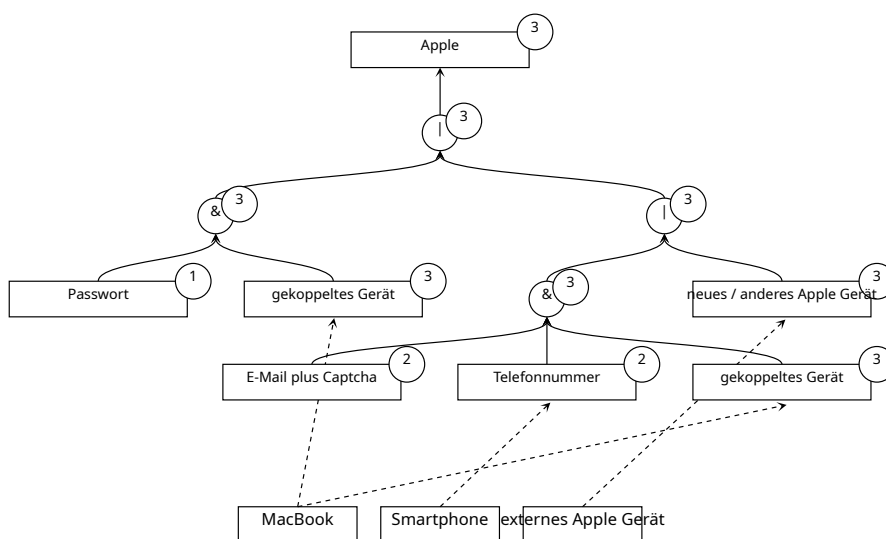


Abbildung 4.2.: AAG Apple Sicherheit

### 4.1.3. Sicherheitsbewertung Google

Der Internetdienstleister Google bietet verglichen mit den anderen in dieser Master-Thesis getesteten Anbieter zusammen mit dem Dienstleister Steam die meisten Wege für eine Wiederherstellung des Accounts. Die Pfade der Wiederherstellung per E-Mail und SMS wurden mit dem Sicherheitswert 2 bewertet, der Pfad der Wiederherstellung durch Nutzung eines OTP mit dem Sicherheitswert 3 und die Nutzung einer Code-Liste wurde mit dem Sicherheitswert 4 bewertet.

Auffällig war hier, dass Google auch die Option bietet ein älteres für den Account genutztes Passwort für die Wiederherstellung zu nutzen. Dieser Pfad wurde mit dem Sicherheitswert 1 bewertet, da dies potentiell die Möglichkeit bietet, dass Angreifer hier, anhand einer Wörterbuch-Attacke mit öffentlich gemachten Passwörtern, eine Möglichkeit haben den Account zu übernehmen. Es werden E-Mails mit Informationen über den Vorgang an die im Account angegebenen E-Mail-Adressen versendet. In diesen E-Mails ist ein Link zum Abbruch des Vorgangs enthalten. Die Möglichkeit der Nutzung eines alten Passworts wird trotzdem als eine unsichere Methode eingestuft. Folglich ist die Wertung dieser Methode mit dem Sicherheitswert 1 gerechtfertigt. Der Gesamtsicherheitswert für den Pfad der Wiederherstellung wird somit mit dem Sicherheitswert 1 gewertet.

Für den Pfad der primären Authentifikation ergibt sich der Sicherheitswert von 2. Zustande kommt dieser Sicherheitswert durch die Wertung 1 für die Nutzung eines Passwortes in Kombination mit entweder einem OTP mit dem Sicherheitswert 3 oder der Zusendung eines Codes per SMS mit dem Sicherheitswert 2.

Der Gesamtsicherheitswert für den Dienstleister Google ergibt in Kombination der primären Authentifikation und der Wiederherstellung 1 (vgl. Abbildung 4.3).

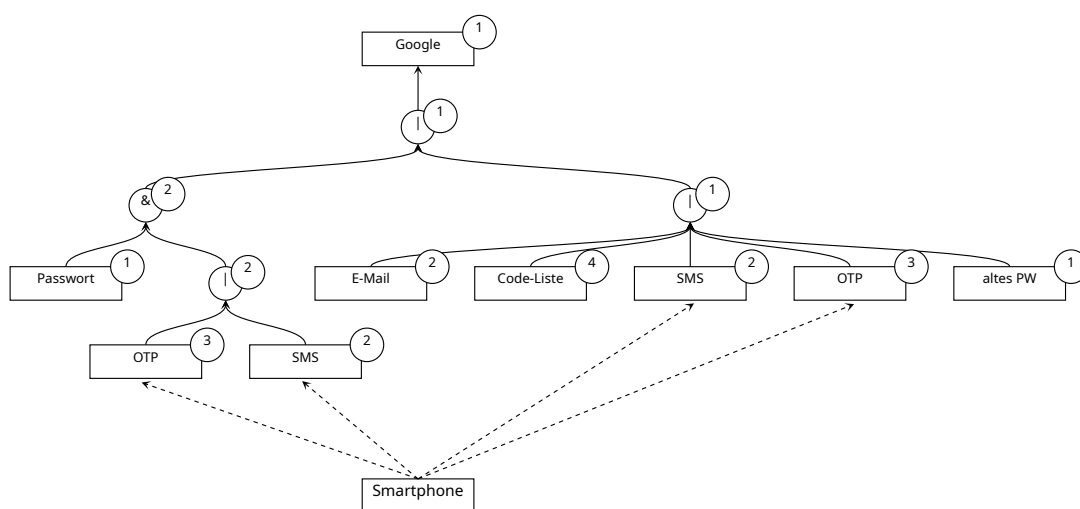


Abbildung 4.3.: AAG Google Sicherheit

#### 4.1.4. Sicherheitsbewertung Microsoft

Wie bereits im Kapitel 3.3.4 Wiederherstellung Microsoft beschrieben, war die Wiederherstellung nicht im Selbstversuch möglich. Die Erstellung des AAG erfolgte somit anhand der Informationen von der Supportseite von Microsoft[68].

Der Pfad der primären Authentifikation wurde mit dem Sicherheitswert 3 bewertet, weil für beide Optionen der Anmeldung als zweiter Faktor die Nutzung eines OTP eingestellt werden kann. Anhand der Beschreibung auf der Support Seite von Microsoft sind die Wiederherstellungsmethoden per E-Mail oder SMS mit Code möglich. Beide erhalten gemäß der Wertung des AAG den Sicherheitswert 2. Die Gesamtbewertung von Microsoft erfolgt mit dem Sicherheitswert 2 aufgrund der Wiederherstellungsmethoden. Abbildung 4.4 zeigt das Graphenmodell und die Bewertungen.

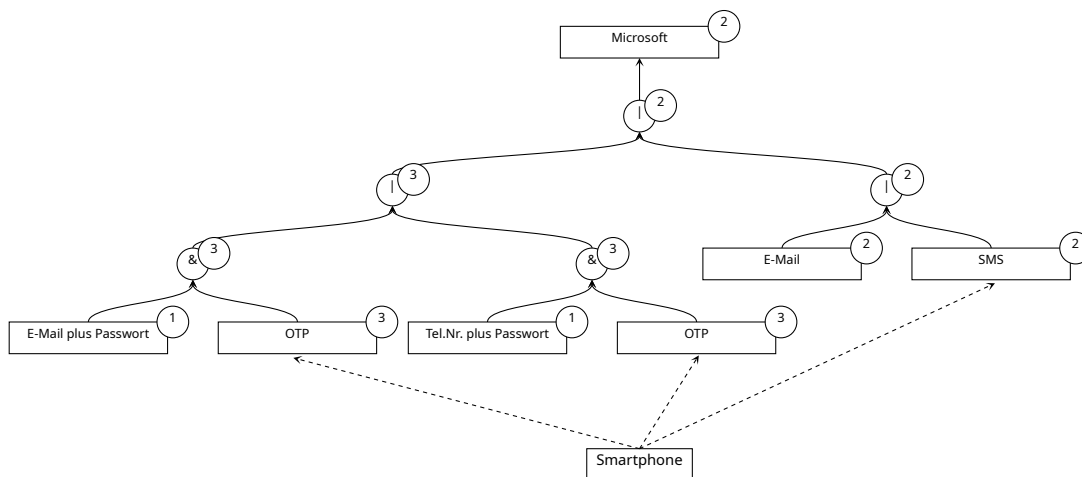


Abbildung 4.4.: AAG Microsoft Sicherheit

#### 4.1.5. Sicherheitsbewertung Meta

Der Pfad der primären Authentifikation bei Meta hat als Sicherheitswert den Gesamtsicherheitswert 2 bekommen (vgl. Abbildung 4.5). Dieser ergibt sich aus der Wertung 1 für die Nutzung eines Passwortes in Kombination mit einem OTP, welches den Sicherheitswert 3 erhält, oder der Nutzung des SMS-Dienstes als zweiten Faktor (Wertung 2).

Für die Wiederherstellung bietet Meta nur eine Methode an, die Wiederherstellung per E-Mail. Diese erhält gemäß AAG Reifegradmodell einen Sicherheitswert von 2. Auch hier wird nach der Änderung des Passwortes die Eingabe eines OTP gefordert, welches den Sicherheitswert von 3 erhält. Alternativ kann auch ein Code

aus einer vorab generierten Code-Liste benutzt werden (Wertung 4). In Kombination wird dieser Pfad mit 3 bewertet, was zu einem Gesamtsicherheitswert von 2 für Meta führt.

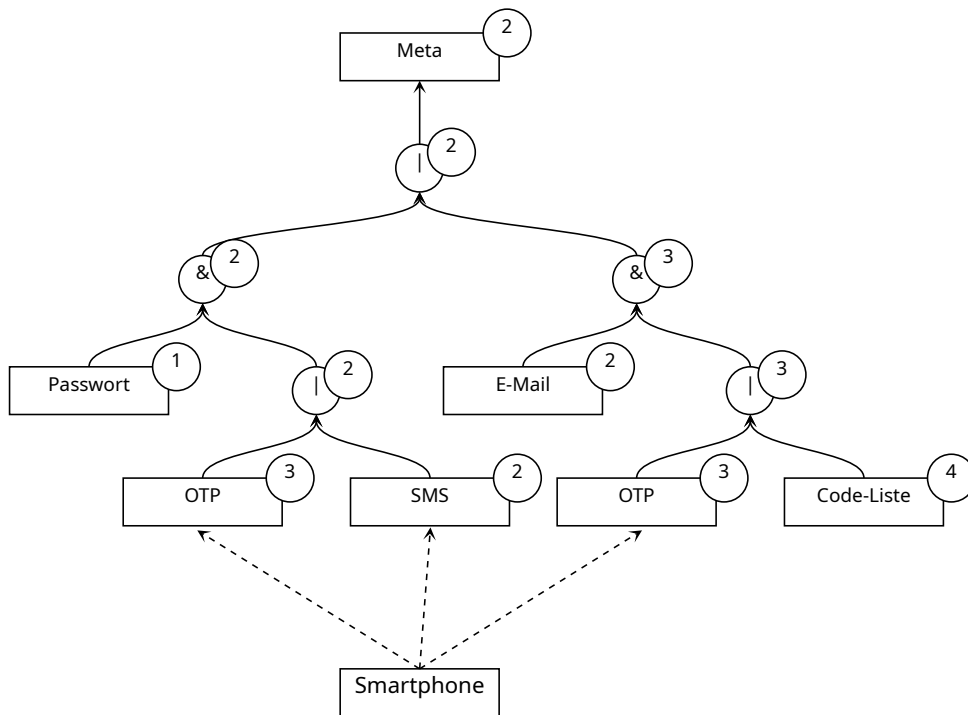


Abbildung 4.5.: AAG Meta Sicherheit

#### 4.1.6. Sicherheitsbewertung Web.de

Für den E-Mail-Provider web.de gibt es drei Pfade für die Wiederherstellung. Wie bereits bei den vorhergehenden Bewertungen werden auch hier die Pfade per E-Mail und SMS jeweils mit dem Sicherheitswert 2 bewertet. Der dritte Weg ist die Nutzung der mit dem Account gekoppelten mobilen App, welche den Sicherheitswert 3 erhält. Die proprietäre web.de App erhält hier den gleichen Wert wie die Methode OTP, da auch hier vorab im Account die Nutzung eingerichtet werden muss und keine Relation zur Telefonnummer besteht (vgl. Abbildung 4.6).

Die primäre Authentifikation wird mit dem Sicherheitswert 3 bewertet. Dies ergibt sich aus der Wertung 1 für die Nutzung eines Passwortes und der Wertung 3 für die Nutzung eines OTP. Die Gesamtsicherheitswertung für den E-Mail-Provider web.de ist mit dem Sicherheitswert 2 erfolgt.



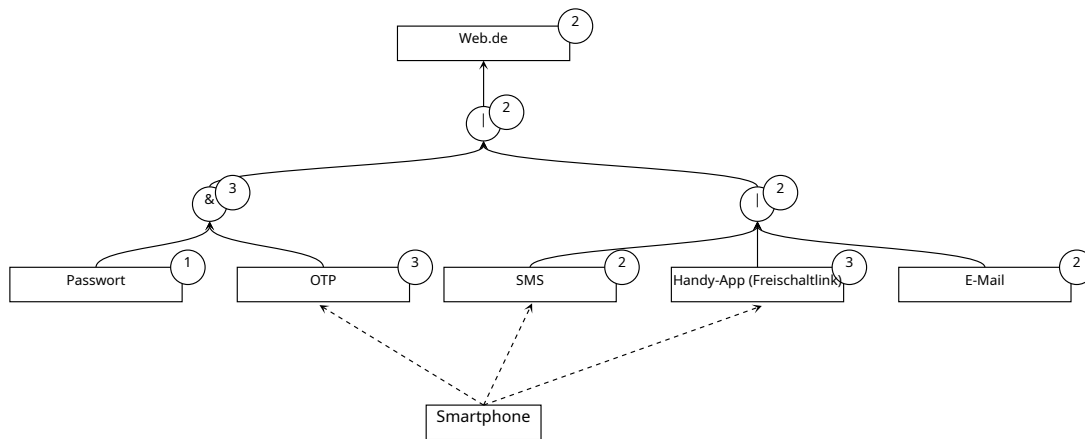


Abbildung 4.6.: AAG Web.de Sicherheit

#### 4.1.7. Sicherheitsbewertung Ubiquiti Unifi

Ubiquiti Unifi bietet den Benutzern für die Wiederherstellung wie in Kapitel 3.3.7 beschrieben zwei Optionen. Der erste Pfad für die Wiederherstellung des Passwortes erhält durch die Kombination von E-Mail mit Link zur Wiederherstellung und der Authentifikation per App den Sicherheitswert 3. Der zweite Pfad bezieht sich auf den Verlust der Authentifizierungs App. Hierfür wird eine Code-Liste generiert, was mit dem Sicherheitswert von 4 bewertet wird.

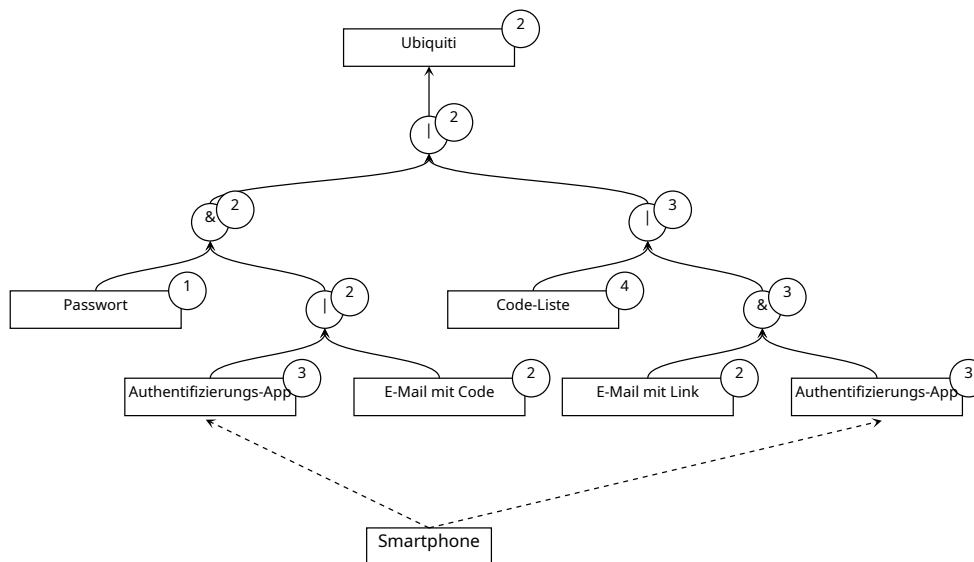


Abbildung 4.7.: AAG Ubiquiti Sicherheit

Die primäre Authentifikation für Ubiquiti Unifi erhält den Sicherheitswert von 2. Diese Wertung entsteht durch die Nutzung der Authentifikations App (Sicherheitswert 3) oder der Bestätigung per E-Mail mit Code (Sicherheitswert 2). Die Nutzung des Passwortes wird mit dem Sicherheitswert 1 gewertet. In Kombination aller Sicherheitswerte

im AAG erhält Ubiquiti Unifi einen Gesamtsicherheitswert von 2. Abbildung 4.7 zeigt den zugehörigen Graphen.

#### 4.1.8. Sicherheitsbewertung Steam

Die Modellierung der Plattform Steam im AAG ergab für Steam den Gesamtsicherheitswert 2 (vgl. Abbildung 4.8). Die primären Pfade der Authentifikation wurden mit den Sicherheitswerten 3 für Passwort und Verifikation über die Steam App bewertet. Den Sicherheitswert 3 erhielt ebenfalls die Authentifikation durch Scannen des QR-Codes auf der Anmeldeseite von Steam durch die Steam App.

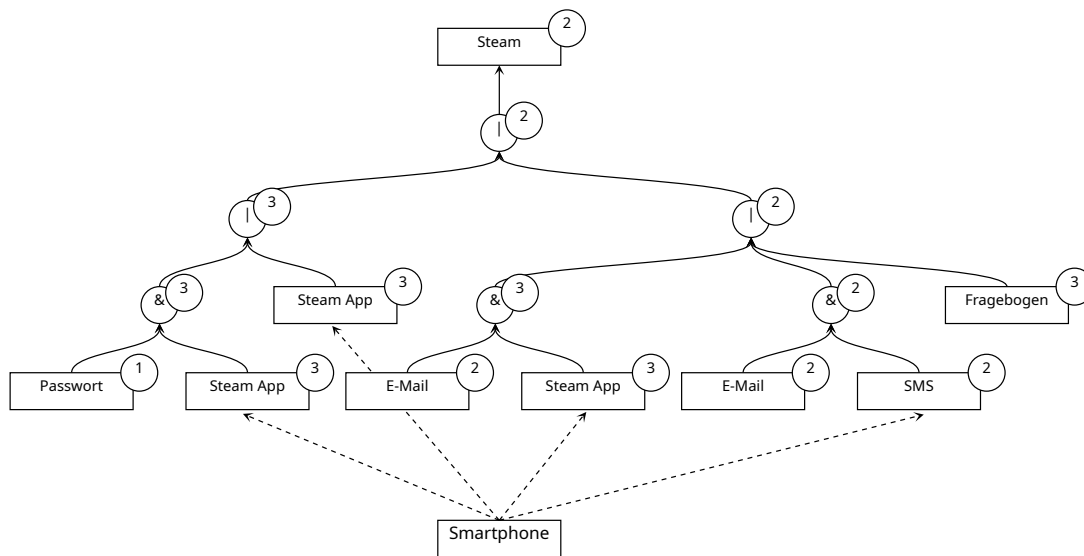


Abbildung 4.8.: AAG Steam Sicherheit

Der Pfad der Wiederherstellung wird insgesamt mit dem Sicherheitswert 2 bewertet. Die Pfade E-Mail in Kombination mit der Steam App und E-Mail mit Nutzung des Fragebogens werden mit dem Sicherheitswert 3 gewertet. Der Pfad mit E-Mail und SMS erhält die Sicherheitswertung von 2.

## 4.2. Analyse der Zugänglichkeit

Dieser Abschnitt setzt sich mit den Werten des AAG für die Zugänglichkeit der analysierten Verfahren der Anbieter auseinander. Die hieraus gewonnenen Ergebnisse fließen ebenfalls in die Bewertung in Kapitel 6 ein.

### 4.2.1. Zugänglichkeitsbewertung Amazon

Die Abbildung 4.9 des Graphen für den Anbieter Amazon zeigt, dass das Gerät Smartphone vier Verbindungen zu Faktoren hat. Hierdurch ergibt sich der Zugänglichkeitswert 0,25 für das Gerät und die betroffenen Faktoren. Die Berechnung für den ersten Pfad der primären Authentifikation ergibt den Zugänglichkeitswert 0,50, bestehend aus Passwort und entweder OTP oder SMS, die Berechnung für den zweiten Pfad ergibt 0,25, bestehend aus Passkey und OTP. Somit ergibt sich für die primäre Authentifikation ein Zwischenwert von 0,75. Der Pfad der Wiederherstellung führt zu einem Zwischenwert von 1,25, sodass sich ein Gesamtzugänglichkeitswert von 2 für den Anbieter Amazon berechnet. Gemäß der Einstufung der Risikowerte besteht somit ein geringes Risiko für diesen Account, d. h. es können ein oder mehrere Authentifizierungstoken verloren gehen, ohne den Zugang zum Account vollständig zu verlieren.

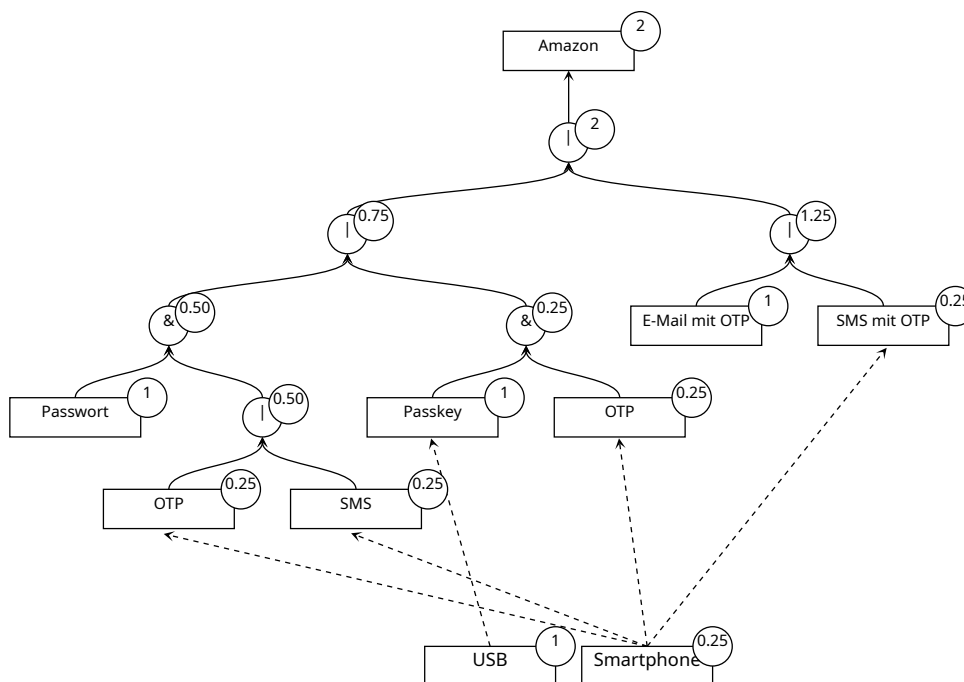


Abbildung 4.9.: AAG Amazon Zugänglichkeit

## 4.2.2. Zugänglichkeitsbewertung Apple

Der Anbieter Apple erhält gemäß der Analyse durch den AAG für die primäre Authentifikation einen Zugänglichkeitswert von 0.50. Dieser Zugänglichkeitswert kann jedoch noch erhöht werden (auf 0.83)<sup>1</sup>, wenn man mehrere Geräte mit dem Apple Account koppelt, z.B. ein Smartphone. Dies gilt auch für die Authentifikation „gekoppeltes Gerät“ im Pfad der Wiederherstellung. Für den ersten Pfad der Wiederherstellung bestehend aus E-Mail, Telefonnummer und einem gekoppelten Gerät ergibt sich der Zugänglichkeitswert 0.50 für die Zugänglichkeit. Der zweite Pfad neues oder anderes gekoppeltes Gerät erhält den Zugänglichkeitswert 1. Somit ergibt sich ein Zwischenwert von 1.50 für die Wiederherstellung. Der Gesamtzugänglichkeitswert für den Anbieter Apple beträgt, wie bereits für Amazon, ebenfalls den Zugänglichkeitswert 2 und somit ein geringes Risiko (vgl. Abbildung 4.10).

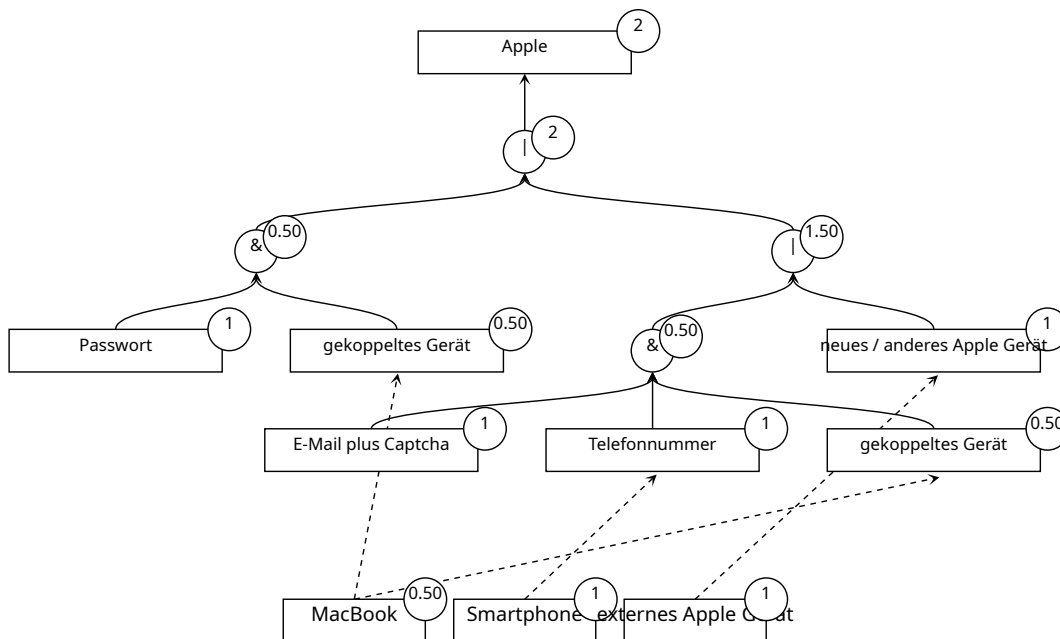


Abbildung 4.10.: AAG Apple Zugänglichkeit

<sup>1</sup>Die Berechnung hierfür erfolgte ebenfalls im AAG und kann im Anhang nachvollzogen werden, siehe A.1

### 4.2.3. Zugänglichkeitsbewertung Google

Der Gesamtzugänglichkeitswert der Zugänglichkeit für den Anbieter Google beträgt 4 (vgl. Abbildung 4.11). Dieser hohe Zugänglichkeitswert ergibt sich durch die vielen Optionen im Pfad der Wiederherstellung. Der Pfad der Wiederherstellung alleine erhält eine Bewertung von 3.50. Der Pfad der primären Authentifikation wird ähnlich der Pfade von Amazon oder Apple mit 0.50 bewertet. Dieser Zugänglichkeitswert ergibt sich aus der Nutzung von Passwort in Verbindung mit einem OTP oder einer SMS. Der Gesamtzugänglichkeitswert von 4 führt ebenfalls zu einem geringen Risiko, es können also mehrere Token verloren werden.

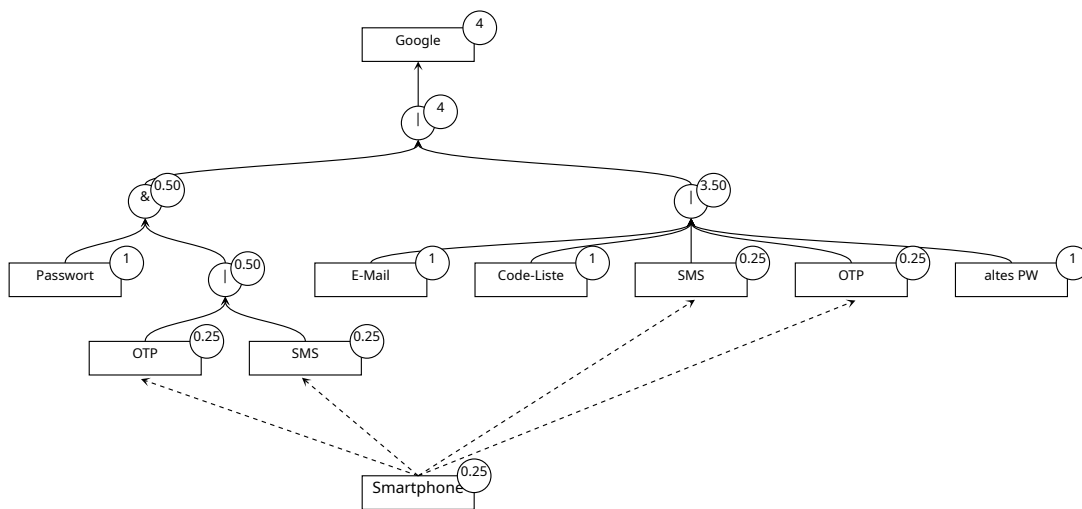


Abbildung 4.11.: AAG Google Zugänglichkeit

#### 4.2.4. Zugänglichkeitsbewertung Microsoft

Die primäre Authentifikation für den Anbieter Microsoft wird mit 0.67 bewertet. Dieser Zugänglichkeitswert entsteht dadurch, dass das mit dem Account gekoppelte Smartphone drei Verbindungen im Graphen hat und somit den Zugänglichkeitswert 0.33 erhält. Durch die Nutzung eines OTP als zweiten Faktor für beide Pfade der primären Authentifikation und die damit entstehende Verbindung zum Smartphone, werden beide Pfade einzeln mit je 0.33 bewertet. Der Zugänglichkeitswert für die Wiederherstellung lautet 1.33, weil hier entweder der Pfad per E-Mail oder per SMS genutzt werden kann. Insgesamt erhält der Anbieter Microsoft einen Zugänglichkeitswert von 2 für die Zugänglichkeit (vgl. Abbildung 4.12).

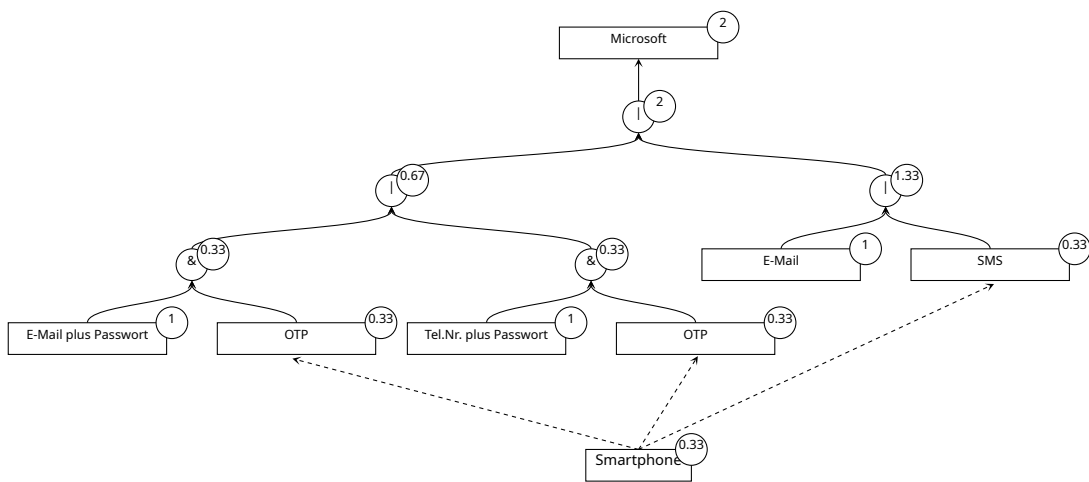


Abbildung 4.12.: AAG Microsoft Zugänglichkeit

## 4.2.5. Zugänglichkeitsbewertung Meta

Der Anbieter Meta erhält in der Gesamtbewertung der Zugänglichkeit den Zugänglichkeitswert 1,67. Der Pfad der primären Authentifikation erhält den Zugänglichkeitswert 0,67. Diese Bewertung entsteht durch die Nutzung eines Passwortes (Zugänglichkeitswert 1) und die Bestätigung des Passwortes durch entweder OTP oder SMS (in Kombination Zugänglichkeitswert 0,67). Die Wiederherstellung wird mit dem Zugänglichkeitswert 1 bewertet. Gemäß Einstufung kann also ein Token für den Zugang verloren werden, ohne den kompletten Zugang zum Account zu verlieren. Abbildung 4.13 zeigt den Graphen für den Anbieter Meta.

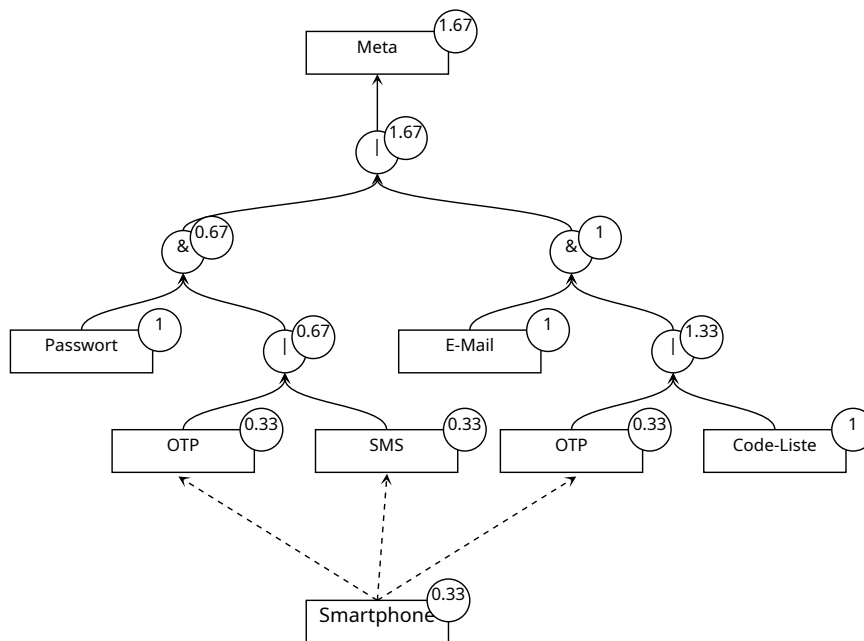


Abbildung 4.13.: AAG Meta Zugänglichkeit

## 4.2.6. Zugänglichkeitsbewertung Web.de

Der Pfad der Wiederherstellung für den Anbieter Web.de wird im AAG mit 1.67 bewertet. Dieser Zugänglichkeitswert entsteht durch die Einzelwerte 0.33 für SMS, 0.33 für die Web.de App und den Zugänglichkeitswert 1 für die Nutzung einer alternativen E-Mail-Adresse. In Abbildung 4.14 ist erkennbar, dass das gekoppelte Smartphone den Zugänglichkeitswert 0.33 erhält, da es drei Verknüpfungen zu Faktoren hat. Der Pfad der primären Authentifikation wird mit dem Zugänglichkeitswert 0.33 bewertet, sodass sich ein Gesamtzugänglichkeitswert von 2 für den Anbieter Web.de ergibt. Gemäß Einstufung entsteht hier ein geringes Risiko.

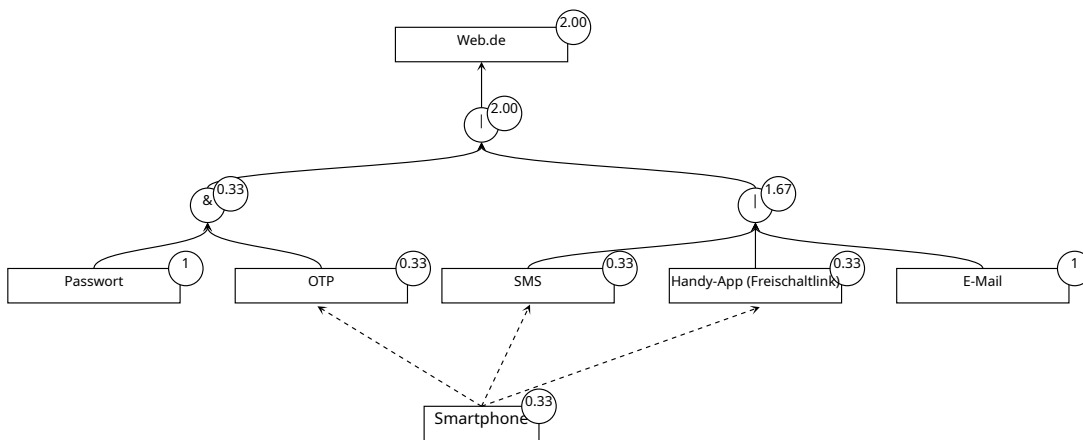


Abbildung 4.14.: AAG Web.de Zugänglichkeit



## 4.2.7. Zugänglichkeitsbewertung Ubiquiti Unifi

Der Anbieter Unifi ist der erste, der für die primäre Authentifikation einen Zugänglichkeitswert größer oder gleich 1 erhält, in diesem Fall genau 1. Dies entsteht durch den Pfad der zweiten Faktoren, welcher mit 1.50 bewertet wird. Der Pfad der Wiederherstellung wird im AAG ebenfalls mit dem Zugänglichkeitswert 1.50 bewertet. Somit ergibt sich ein Gesamtzugänglichkeitswert von 2.50 für Unifi (vgl. Abbildung 4.15). Auch Unifi wird mit einem geringen Risiko für den Verlust der Zugänglichkeit bewertet.

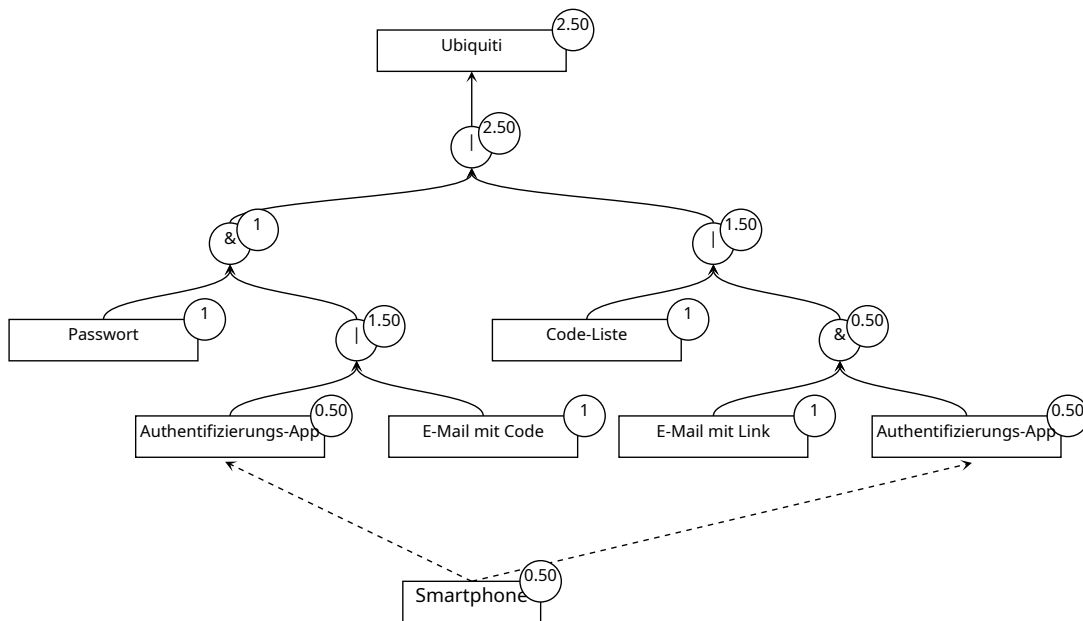


Abbildung 4.15.: AAG Ubiquiti Unifi Zugänglichkeit

## 4.2.8. Zugänglichkeitsbewertung Steam

Zum Abschluss erfolgte die Bewertung der Zugänglichkeit des Anbieters Steam. Obwohl Steam viele Optionen sowohl in der primären Authentifikation als auch bei den Wiederherstellungsmethoden bietet, erfolgt die Gesamtzugänglichkeitsbewertung nur mit dem Zugänglichkeitswert 2. Diese ergibt sich aus der Verteilung der Nutzung des mit dem Account gekoppelten Smartphones (vgl. Abbildung 4.16). Das Smartphone hat je zwei Pfeile in Richtung primäre Authentifikation und Wiederherstellung. Hierdurch ergibt sich für die primäre Authentifikation der Zwischenwert 0.50 und für die Wiederherstellung der Zwischenwert 1.50. Auffällig ist, dass bei Verlust des gekoppelten Smartphones nur noch der Weg über den Fragebogen offen bleibt, da alle weiteren Pfade Verbindungen zu dem Gerät aufweisen.

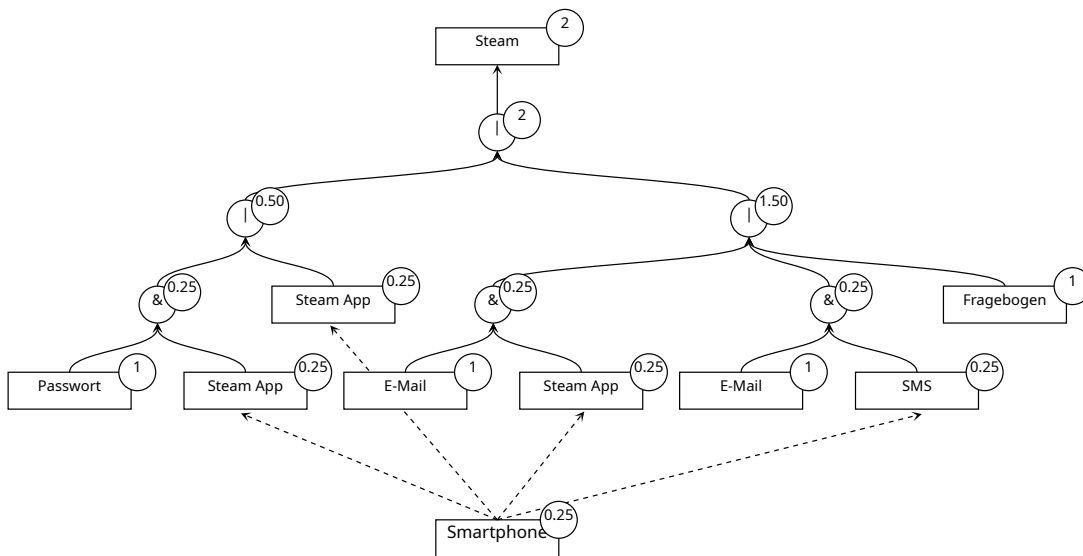


Abbildung 4.16.: AAG Steam Zugänglichkeit

# 5. Umfrage

## 5.1. Auswertung der Umfrage

Die Benutzerumfrage war vom 01.07.2024 bis zum 22.07.2024 aktiv geschaltet. In dieser Zeit wurde die Umfrage 132 mal aufgerufen, 51 Personen beendeten die Umfrage. Die durchschnittliche Dauer der Bearbeitung der Umfrage lag bei 04:12 Minuten.

### 5.1.1. Frage 1 „Wie alt sind Sie?“

An der Umfrage nahmen Teilnehmer aus jeder der vorgegebenen Altersgruppen teil (vgl. Abbildung 5.1). Die Mehrheit der Teilnehmer kam aus dem Bereich zwischen 31 und 50 Jahren (insgesamt 31 Teilnehmer).

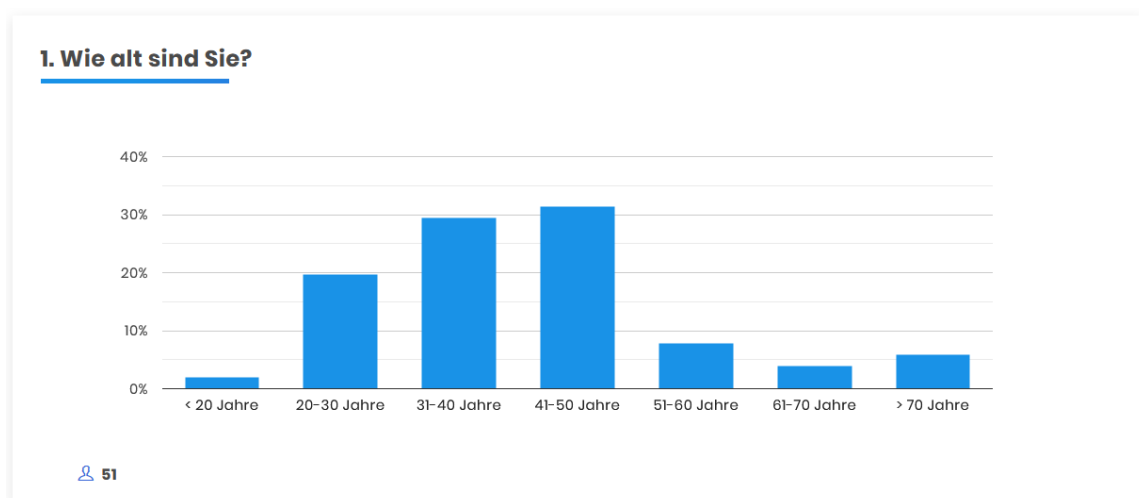


Abbildung 5.1.: Frage 1: Wie alt sind Sie?

Die Teilnehmenden bilden einen guten Schnitt durch das Altersspektrum, auch wenn es nicht dem aktuellen demografischen Wandel in Deutschland entspricht[73].

### 5.1.2. Frage 2 „Welche Erfahrung haben Sie mit Informationstechnologien?“

Frage 2 diente zur Einschätzung der Erfahrung der Teilnehmer im Bezug auf Informationstechnologie. Abbildung 5.2 zeigt die graphische Darstellung der Ergebnisse. 30 Teilnehmer gaben an, Fachkenntnisse im Bereich der Informationstechnologie zu besitzen, 8 Teilnehmer wählten erweiterte Kenntnisse aus, 10 Teilnehmer wählten grundlegende Kenntnisse aus und 3 Teilnehmer gaben an Kenntnisse auf dem Niveau Einsteiger zu besitzen.

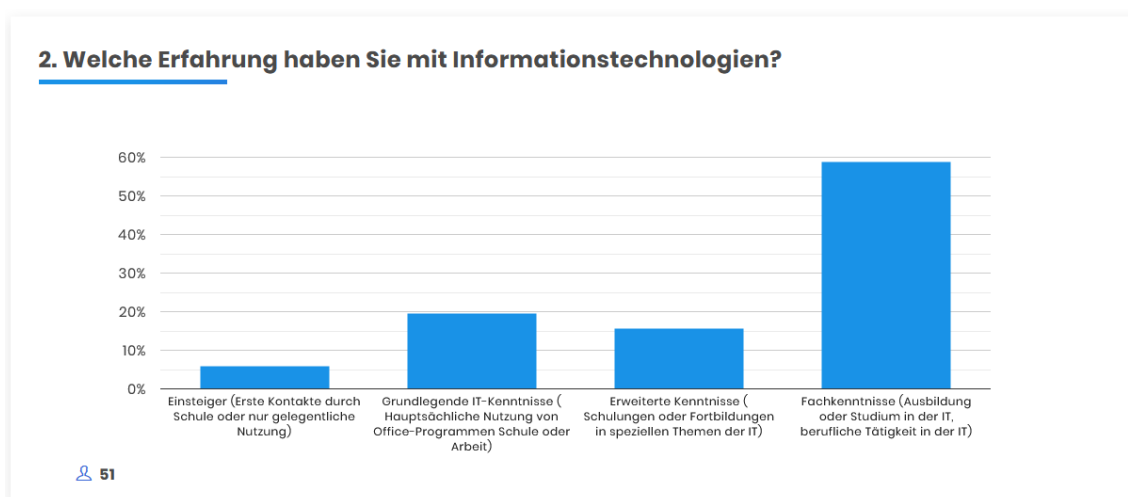


Abbildung 5.2.: Frage 2: Welche Erfahrung haben Sie mit Informationstechnologien?

Auch wenn die Mehrheit der Teilnehmer Fachkenntnisse besitzt, kann trotzdem eine differenzierte Aussage getroffen werden, da gut 47% der Teilnehmer mit weniger Fachwissen die Umfrage befüllten. Teilnehmer, die angaben Einsteigerkenntnisse zu besitzen, waren den Altersbereichen unter 20 Jahren, zwischen 20 und 30 Jahren sowie 41 bis 50 Jahren zu zuordnen. Teilnehmer, die angaben grundlegende Kenntnisse zu besitzen, wählten die Option ab 31 bis über 70 Jahre alt zu sein aus. Teilnehmer mit erweiterten Kenntnissen waren dem Altersbereich 20 bis 50 Jahren zuzuordnen. Die Teilnehmer, die sich selbst mit Fachkenntnissen einschätzten, gaben an zwischen 20 und 70 Jahren alt zu sein.

### 5.1.3. Frage 3 „Welche der folgenden Wiederherstellungsmethoden kennen Sie?“

Ziel von Frage 3 war es, zu erfassen, welche Wiederherstellungsmethoden im Teilnehmerkreis bekannt sind. Das Umfrageergebnis zeigt, dass die Varianten E-Mail und SMS sowie persönliche oder Sicherheitsfrage jeweils 49 Teilnehmern bekannt sind.

Die Methode Passwort, Code oder Code-Liste wurde von 48 Teilnehmern ausgewählt. Die Wiederherstellungsmethode Token wurde nur von 34 Teilnehmern ausgewählt (vgl. Abbildung 5.3).

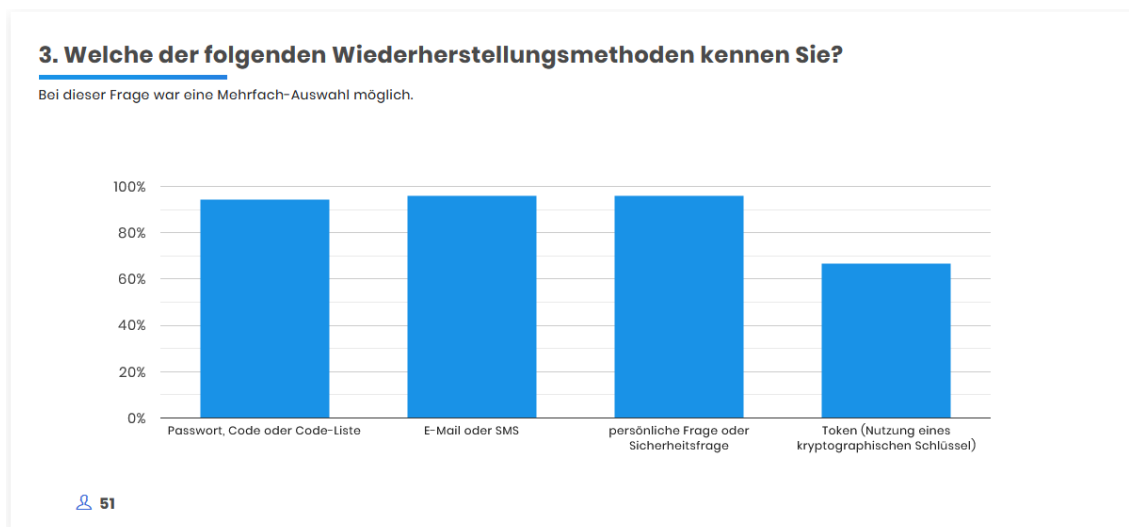


Abbildung 5.3.: Frage 3: Welche der folgenden Wiederherstellungsmethoden kennen Sie?

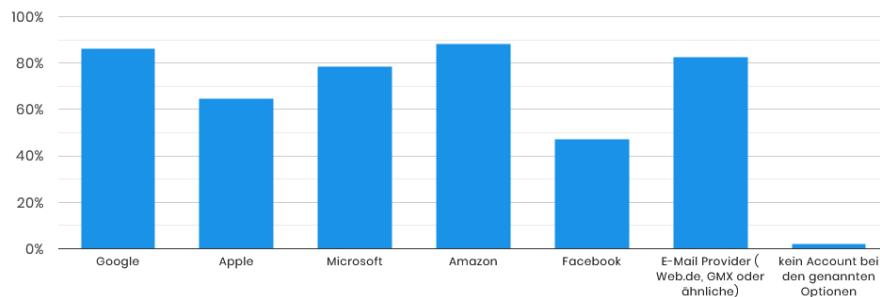
Unter den Teilnehmenden, die angaben Fachkenntnisse zu besitzen, wählten 7 Teilnehmer die Option aus die Wiederherstellungsmethode Token nicht zu kennen. 11 Teilnehmer aus den Bereichen grundlegende und erweiterte Kenntnisse gaben an, die Methode Token zu kennen. Diese Zahlen wurden aus den Rohdaten der Ergebnisse entnommen (siehe Anhang A.3). Aus dem Ergebnis dieser Frage lässt sich ableiten, dass die persönliche Qualifikation der Teilnehmer nicht zwingend auf den Kenntnisstand der Technologie schließen lässt.

#### 5.1.4. Frage 4 „Haben Sie bei einem der folgenden Anbieter einen Benutzeraccount?“

Frage 4 diente zur Erstellung einer Übersicht, welche Accounts die Teilnehmenden besitzen. Abbildung 5.4 zeigt die graphische Auswertung. Das Ergebnis zeigt, dass ca. 80% der Teilnehmer einen Account bei Google, Microsoft, Amazon oder einem E-Mail-Provider besitzen. 33 Teilnehmer gaben an einen Apple Account zu besitzen und 24 Teilnehmer besitzen einen Facebook Account. Lediglich ein Teilnehmer, der angab jünger als 20 Jahre alt zu sein, wählte aus keinen Account bei den angegebenen Dienstleistern zu besitzen.

#### 4. Haben Sie bei einem der folgenden Anbieter einen Benutzeraccount?

Bei dieser Frage war eine Mehrfach-Auswahl möglich.

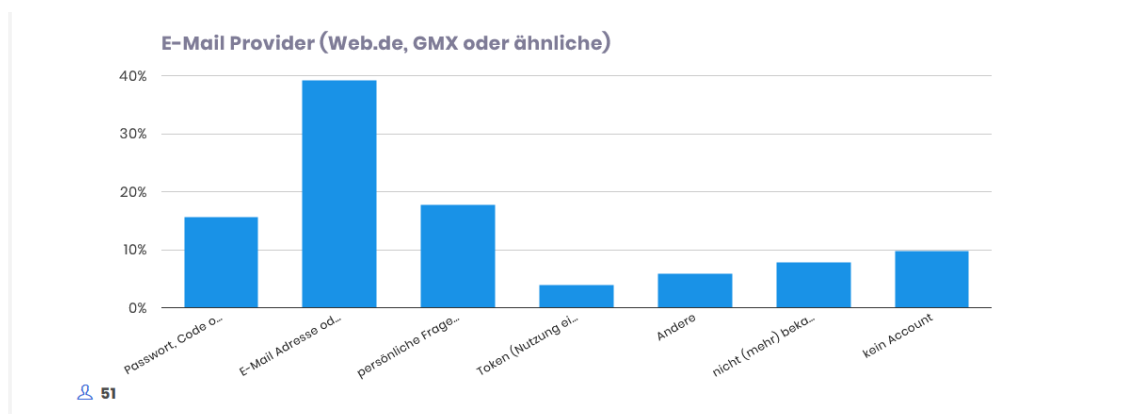


51

Abbildung 5.4.: Frage 4: Haben Sie bei einem der folgenden Anbieter einen Benutzeraccount?

#### 5.1.5. Frage 5 „Welche Wiederherstellungsmethode haben Sie für den / die Anbieter gewählt?“

Frage 5 sollte zur Erfassung der verwendeten Wiederherstellungsmethoden dienen. Die Methode per E-Mail-Adresse oder SMS war bei allen Diensten am häufigsten ausgewählt worden. Zwischen 4 bis 7 Teilnehmer wussten je nach Anbieter nicht mehr, welche Methode sie ausgewählt hatten. Am zweit meisten wurde die Methode Passwort, Code oder Code-Liste ausgewählt. Bei den E-Mail-Providern gaben 9 Teilnehmer an die Wiederherstellungsmethode persönliche Frage oder Sicherheitsfrage zu verwenden (vgl. Abbildung 5.5). Bei den anderen Anbietern wurde diese Methode seltener oder gar nicht gewählt. Tabelle 5.1 zeigt die Anzahl der Antworten zu den jeweiligen Varianten.



51

Abbildung 5.5.: Frage 5: Welche Wiederherstellungsmethode haben Sie für den / die Anbieter gewählt?

Tabelle 5.1.: Ergebnis Frage 5

	Passwort, Code oder Codeliste	E-Mail- Adresse oder SMS	persönl. Frage oder Sicher- heits- frage	Token	Andere	nicht (mehr) bekannt	kein Account
Amazon	7	30	3	3	0	5	3
Apple	8	16	0	3	3	5	16
E-Mail- Provider	8	20	9	2	3	4	5
Facebook	5	12	1	1	3	5	24
Google	5	26	2	3	4	6	5
Microsoft	3	23	4	4	3	7	7

Auffällig ist, dass bei allen Anbietern die Methode E-Mail-Adresse oder SMS am häufigsten gewählt wurde. Die zweit häufigste Methode verteilt über die Anbieter ist die Nutzung von Passwörtern oder Codes. Token wurden von den Teilnehmern weniger eingesetzt.

#### 5.1.6. Frage 6 „Wenn in der vorherigen Frage „Andere“ ausgewählt wurde, welche Methode wird verwendet? (Bitte Anbieter nennen)“

Diese Frage diente zur Beschreibung der Wiederherstellungsmethode, wenn in Frage 5 nicht die verwendete Methode aufgeführt wurde. Die Antworten lassen leider darauf schließen, dass die Frage nicht präzise genug formuliert wurde. Die Intention der Frage war, dass die Teilnehmer den Anbieter (Google, Apple oder anderen Zutreffenden) nennen und dann die hierzu eingestellte Methode beschreiben. Gegebene Antworten, wie z.B. „Diverse“, „Auswahl über Freundesliste“ oder „Notizbüchlein“, bestätigen diese Vermutung. Lediglich zwei Teilnehmer gaben erwartete Antworten, „Google passwort und Email, Web.de passwort und Email, Microsoft passwort und emai“ (in der Antwort fehlen Buchstaben) und „Microsoft Authenticator“.

### 5.1.7. Frage 7 „Haben Sie schon einmal für einen Onlinezugang eine Wiederherstellung durchgeführt oder durchführen müssen?“

Mit dieser Frage sollte erfasst werden, wie viele der Teilnehmer bereits einmal eine Wiederherstellung zu einem Onlinezugang durchgeführt haben, entweder freiwillig oder unfreiwillig durch Verlust oder Vergessen der primären Authentifikationsfaktoren. Knapp 75% der Teilnehmer gaben an, bereits einmal diesen Vorgang durchgeführt zu haben (vgl. Abbildung 5.6).

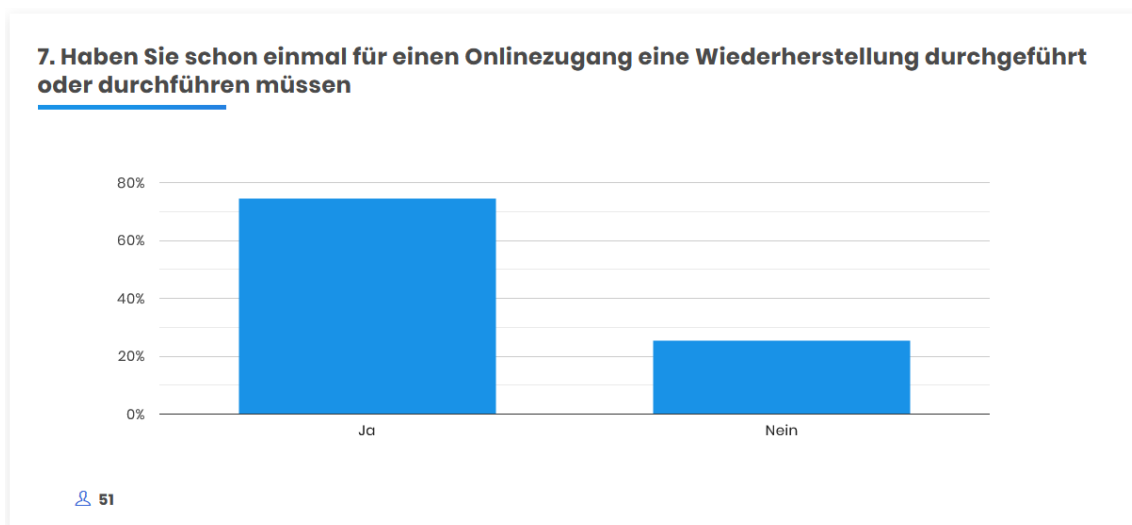


Abbildung 5.6.: Frage 7: Haben Sie schon einmal für einen Onlinezugang eine Wiederherstellung durchgeführt oder durchführen müssen?

### 5.1.8. Frage 8 „Wenn Frage 7 mit Ja beantwortet wurde, welche Methode wurde für die Wiederherstellung angewendet? (Bitte Anbieter und Methode nennen)“

Frage 8 bot den Teilnehmern die Option, die jeweilige Methode des Wiederherstellungsvorgangs zu beschreiben, wenn Frage 7 mit „Ja“ beantwortet wurde. Unter den Antworten waren unter anderem die Methode E-Mail oder SMS vertreten für Google, Amazon, Facebook, Microsoft oder E-Mail-Provider. Ein Teilnehmer nannte auch das Beispiel PayPal und Wiederherstellung per E-Mail-Adresse. Ein weiteres Beispiel war die Wiederherstellung eines Facebook Accounts durch die Trusted Friend Methode. Ein Teilnehmer gab an, dass ein zugehöriger E-Mail-Account gehackt wurde und er somit gezwungen war, alle verknüpften Onlinezugänge zu bearbeiten. Hierbei mussten auch Verfahren wie Post-Ident oder Sicherheitsfrage per Telefon genutzt werden.



---

**5.1.9. Frage 9 „Wenn Frage 8 beantwortet wurde, wie zufrieden waren Sie mit der gewählten / geforderten Methode? (1 Daumen = unzufrieden, 5 Daumen = sehr zufrieden)“**

Mit Frage 9 wurde die persönliche Empfindung des Teilnehmenden zum Vorgang der Wiederherstellung aus Frage 8 abgefragt. Bei der Beantwortung der Frage gab es 3 Wertungen, obwohl bei Frage 7 mit „Nein“ geantwortet wurde. Diese Antworten wurden manuell aus der Auswertung gefiltert. Die Mehrheit der Teilnehmer gab an mit der Wiederherstellungsmethode zufrieden (4) oder sehr zufrieden (5) gewesen zu sein. 9 Teilnehmer wählten die Wertung 3 und somit eine neutrale Meinung. Je ein Teilnehmer war nicht zufrieden (2) und unzufrieden (1).

Der Teilnehmer, der die niedrigste Wertung vergeben hat, hatte in Frage 8 geantwortet bei Facebook die Methode Trusted Friend genutzt zu haben. Der Teilnehmer mit der Wertung 2 gab an, per SMS einen Zugangscodes erhalten zu haben. Leider fehlt hier die Angabe des Dienstleisters. Unter den beiden hohen Wertungen war mehrheitlich die Methode per E-Mail oder SMS genutzt worden, es waren aber auch eine Sicherheitsfrage, die Nutzung eines Codes und eines Token darunter.

**5.1.10. Frage 10 „Was ist Ihnen wichtiger, wenn Sie an Wiederherstellungsmethoden denken, Sicherheit oder Bedienbarkeit?“**

Frage 10 sollte die persönliche Meinung der Teilnehmer erfragen, in wie weit den Teilnehmern zum Thema Wiederherstellungsmethoden Sicherheit, Bedienbarkeit oder beides wichtig ist. Die meisten der Teilnehmer (33) wählten die Option „beides“, 16 Teilnehmer wählten „Sicherheit“ und 2 Teilnehmer gaben an, dass ihnen Bedienbarkeit am wichtigsten ist. Die folgende Abbildung 5.7 zeigt das Ergebnis dieser Frage in graphischer Darstellung.

Die Teilnehmer, die Bedienbarkeit als wichtiger gewählt haben, haben angegeben Fachkenntnisse in der Informationstechnologie zu haben und wählten bei Frage 9 die Wertungen 3 und 5 aus.

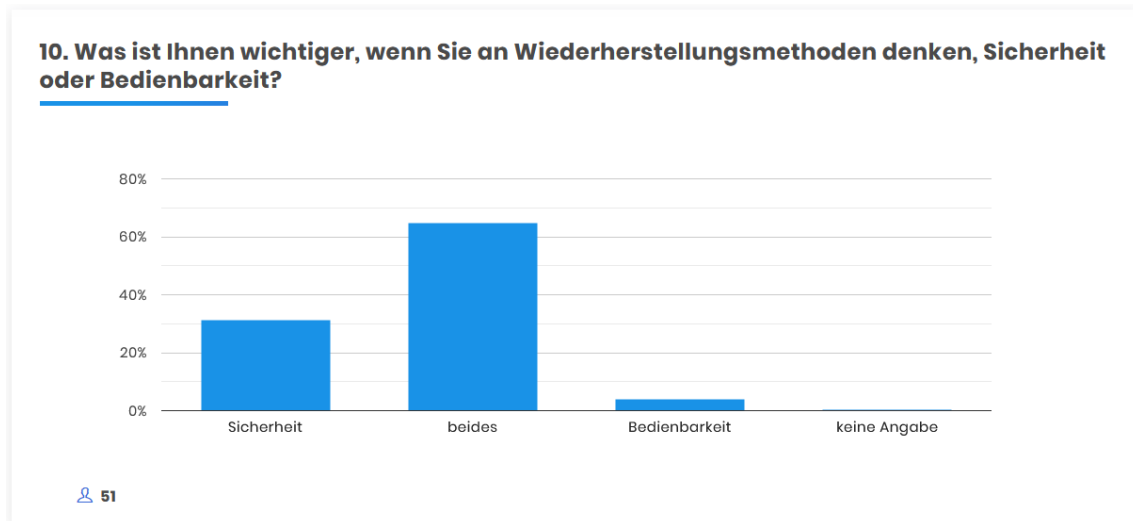


Abbildung 5.7.: Frage 10: Was ist Ihnen wichtiger, wenn Sie an Wiederherstellungsmethoden denken, Sicherheit oder Bedienbarkeit?

### 5.1.11. Frage 11 „Wären Sie bereit für eine höhere Sicherheit bei Wiederherstellungsmethoden zusätzliche technische Maßnahmen in Kauf zu nehmen? (z.B. eine Handy-App, USB-Token oder ähnliches)“

Mit der letzten Frage der Umfrage wurde die Bereitschaft der Teilnehmer erfasst, ob diese für eine höhere Sicherheit bereit wären, zusätzliche technische Maßnahmen in Kauf zu nehmen (vgl. Abbildung 5.8). 41 Teilnehmer beantworteten diese Frage mit „Ja“, 8 Teilnehmer wählten „Weiß nicht“ und 2 Teilnehmer wählten die Option „Nein“. Die beiden Teilnehmer, die „Nein“ angaben, hatten in Frage 2 ausgewählt grundlegende Kenntnisse und Fachkenntnisse zu besitzen.

## 5.2. Fazit der Umfrage

Durch die Umfrage konnte ein Stimmungsbild der Teilnehmer zum Thema Wiederherstellungsmethoden gewonnen werden. Den Teilnehmern waren die meisten der vorgegebenen Methoden bekannt, unabhängig davon, wie der eigene Wissensstand zum Thema Informationstechnologie angegeben wurde. Die Wiederherstellungsmethode per E-Mail oder SMS war am häufigsten bei der Frage nach der Umsetzung für eigene Accounts angegeben. Viele der Teilnehmer hatten bereits Erfahrung mit dem Thema Wiederherstellungsmethode in der Form, dass sie aktiv eine Wiederherstellung durchführen mussten. Hierbei wurden unterschiedliche Methoden genutzt und die große Mehrheit war mit der geforderten Methode (am häufigsten E-Mail oder SMS) zufrieden.

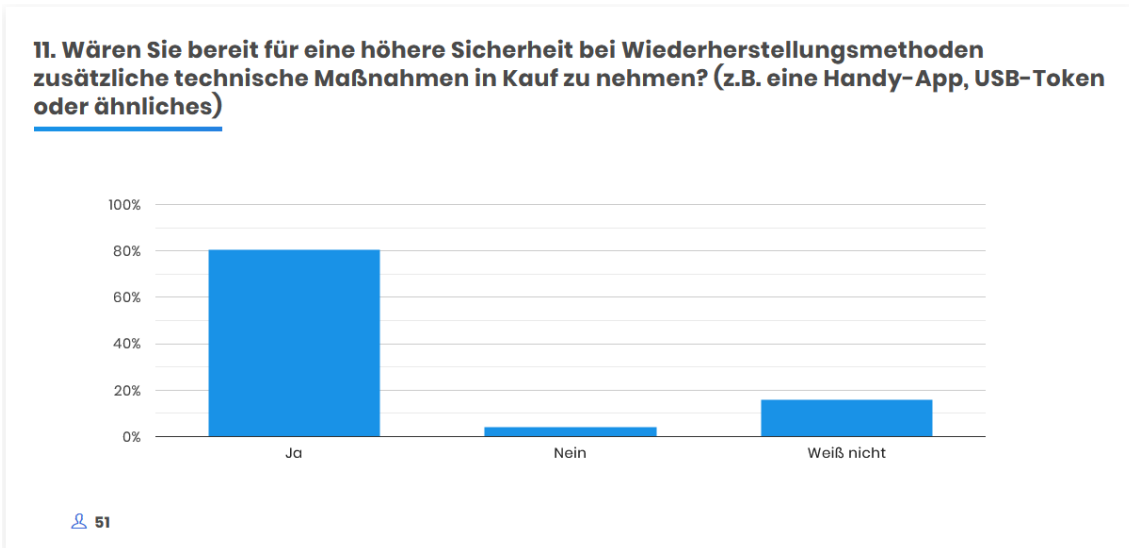


Abbildung 5.8.: Frage 11: Wären Sie bereit für eine höhere Sicherheit bei Wiederherstellungsmethoden zusätzliche technische Maßnahmen in Kauf zu nehmen? (z.B. eine Handy-App, USB-Token oder ähnliches)

Ein klares Bild zeichnet sich auch bei der Frage zur Sicherheit und Bedienbarkeit ab. 33 Teilnehmer wünschen sich beides, 16 Teilnehmer legten den Fokus auf das Thema Sicherheit und nur 2 Teilnehmer wählten die Bedienbarkeit vor den anderen Optionen. Ebenso klar war die Meinung der Teilnehmer zur Nutzung zusätzlicher technischer Maßnahmen, um die Sicherheit zu erhöhen. 41 Teilnehmer stimmten hier mit „Ja“, 8 Teilnehmer waren sich unsicher und wählten „Weiß nicht“ und nur 2 Teilnehmer wären nicht bereit zusätzliche technische Maßnahmen zu nutzen.

## 6. Bewertbarkeit von Wiederherstellungsmethoden

In diesem Kapitel soll eine Bewertung der Wiederherstellungsmethoden erfolgen. Diese Bewertung bezieht sich zum einen auf die theoretischen Vorgaben für die Methoden, zum anderen werden die Erkenntnisse aus der Analyse und der Umfrage mit einbezogen. Die Umfrage soll die Anforderungen der Benutzer an die Benutzbarkeit stützen.

Kriterien für die Bewertung der Wiederherstellungsmethoden werden der Sicherheitswert, die Benutzbarkeit, die Erreichbarkeit, die gewonnenen Erkenntnisse aus der Umfrage und der eigenständig durchgeführten Wiederherstellungsversuche, sowie die Verfügbarkeit der Methode sein. Zu unterscheiden ist bei der Bewertung, dass es quantifizierte Werte gibt, der Sicherheitswert, die Benutzbarkeit und die Erreichbarkeit sowie „softe“ Werte, die Erkenntnisse aus der Umfrage, die eigenständig durchgeführten Wiederherstellungsversuche und die Verfügbarkeit der Methode.

Die Sicherheitswerte ergeben sich analog zum Reifegradmodell des AAG (vgl. Tabelle 6.1):

Tabelle 6.1.: Sicherheitsbewertung

Methode	Bewertung
persönliche / Sicherheitsfragen	1
SMS	2
E-Mail	2
soziale Authentifikation	3
Code / Code-Liste	4
Token	5

Die Methode mit der höchsten Sicherheit hat den höchsten Wert erhalten (5), die Methode mit der geringsten Sicherheit den kleinsten Wert (1)[2].

---

Für die Bewertung der Benutzbarkeit wurden folgende Werte festgelegt (vgl. Tabelle 6.2):

Tabelle 6.2.: Bewertung Benutzbarkeit

Methode	Bewertung
Benutzer hat Informationen im Gedächtnis	4
Benutzer hat Informationen online oder auf mobilem Gerät zur Verfügung	3
Benutzer bekommt durch den Dienstleister während des Vorgangs Daten	2
Benutzer hat einen Code, eine Code-Liste oder Token	1

Die den Methoden zugewiesenen Werte stellen hier die Komplexität für den Benutzer dar. Beim Reifegradmodell des AAG hat die sicherste Methode den höchsten Wert erhalten, analog hierzu erhält die für den Benutzer einfachste Methode bei der Benutzbarkeit den höchsten Wert.

Als einfachste Methode für den Benutzer wird das Behalten von Informationen im Gedächtnis gesetzt. Der Benutzer benötigt keine externen Mittel, um die Informationen abzurufen.

Die zweite Stufe stellen Informationen dar, die der Benutzer online abrufen oder auf einem mobilen Gerät zur Verfügung hat.

Die dritte Stufe bilden Informationen, die der Benutzer während des Vorgangs der Wiederherstellung durch den Dienstleister vorgegeben bekommt dar, z.B. bei Trusted Friends Vorschläge aus der Freundesliste.

Die vierte Stufe stellen Informationen dar, die der Benutzer geheim ablegen soll, zum Beispiel Code-Listen (entweder zu Hause oder verschlossen im Büro) oder aber auch Token auf USB-Sticks. USB-Sticks können auch als mobile Geräte zählen, jedoch werden diese hier anders gewertet, weil der Benutzer z.B. sein Smartphone nahezu immer bei sich führt und hier eine besondere Aufmerksamkeit für aufgebracht wird. Ein USB-Stick ist kleiner als ein Smartphone und kann somit einfacher übersehen, verlegt oder verloren werden.

Die Erreichbarkeit der Methode wurde in 3 Kategorien unterteilt (vgl. Tabelle 6.3):

Tabelle 6.3.: Bewertung Erreichbarkeit

Ablage	Bewertung
Gedächtnis des Benutzers	4
Onlinedienste (E-Mail etc)	3
Mobile Geräte (USB Token, Smartphone)	2
Ablage zu Hause / Büro	1

Das Gedächtnis des Benutzers wurde am höchsten bewertet, weil hierfür keine externen Hilfsmittel notwendig sind. Onlinedienste erhalten die Wertung 3, da hier irgendein online-fähiges Gerät benötigt wird, es muss nicht ein Gerät des Benutzers sein. Die Wertung 2 wird für mobile Geräte vergeben, die der Benutzer mit sich führen kann, z.B. sein Smartphone. Die niedrigste Wertung von 1 erhält die Ablage der Information zur Wiederherstellung zu Hause oder im Büro. Diese Ablage ist ortsgebunden, da es nicht empfohlen wird z.B. eine Liste mit Wiederherstellungscodes dauerhaft mit sich zu führen.

Die Bewertung der Wiederherstellungsmethoden anhand der vorab erläuterten Kriterien stellt sich wie folgt dar (vgl. Tabelle 6.4):

Tabelle 6.4.: Bewertung Methoden

Methode	Sicherheitswert	Benutzbarkeit	Erreichbarkeit
persönliche / Sicherheitsfragen	1	4	4
SMS	2	3	2
E-Mail	2	3	3
soziale Authentifikation	3	2	3
Code / Code-Liste	4	1	1
Token	5	1	2

Das Kriterium Verfügbarkeit bezieht sich in dieser Betrachtung auf die Möglichkeit der Nicht-Verfügbarkeit einer Methode. Benutzer haben während ihres digitalen Lebens häufig mehr als eine E-Mail-Adresse. Als Beispiel hat ein Benutzer während seines Studiums eine E-Mail-Adresse erhalten. Mit dieser Adresse hat er sich einen

---

Account bei einem Onlinedienstleister erstellt. Diesen Account nutzt er auch nach seinem Studium weiter, hat jedoch vergessen die E-Mail-Adresse zu aktualisieren und nach Beendigung seines Studiums keinen Zugriff mehr auf diese Adresse. Somit ist ihm der Weg der Wiederherstellung mithilfe der E-Mail-Adresse verwehrt.

Ein weiteres Beispiel ist die Nutzung eines Smartphones für eine Wiederherstellung. Es kann sowohl die Telefonnummer als Wiederherstellungsmethode angegeben werden als auch eine App auf dem Smartphone hierfür genutzt werden. Wechselt der Benutzer nun z.B. seine Telefonnummer und hat keinen Zugriff mehr auf diese oder der Benutzer verliert sein Smartphone durch Verlegen oder Diebstahl, sind auch diese Methoden nicht mehr umsetzbar.

Möglich sind demnach folgende Szenarien:

- physischer Verlust eines mobilen Gerätes (Code-Liste geschreddert, Smartphone gestohlen)
- Verlust von (Zugangs)-Daten (Datenbank der Passwortverwaltung gelöscht, Vergessen der Informationen)
- gelöschter / nicht mehr erreichbarer Account
- Wechsel der postalischen Adresse

Ordnet man diese Kriterien den Wiederherstellungsmethoden zu, so ergibt sich folgendes Bild (es sind hier nur einige Beispiele aufgeführt, vgl. Tabelle 6.5):

Tabelle 6.5.: Verfügbarkeit von Wiederherstellungsmethoden

Methode	Szenario
persönliche / Sicherheitsfragen	Verlust von (Zugangs)-Daten möglich durch Vergessen
SMS	Verlust von (Zugangs)-Daten durch Wechsel der Telefonnummer oder physischer Verlust eines mobilen Geräte
soziale Authentifikation	gelöschter / nicht mehr erreichbarer Account einer Person aus der Freundesliste
Code / Code-Liste	Verlust von (Zugangs)-Daten durch Löschen der Datenbank der PW-Verwaltung oder physischer Verlust durch versehentliches schreddern der Code-Liste
Token	Verlust von (Zugangs)-Daten durch Löschen der Daten auf dem USB-Stick oder physischer Verlust des USB-Stick

Es gibt für jede Methode Möglichkeiten, die den Zugriff verhindern können. Persönliche oder Sicherheitsfragen können so gestellt sein, dass die Beantwortung der Frage nicht eindeutig für den Benutzer ist. Als Beispiel kann eine Frage nach dem Namen des ersten Haustiers des Benutzers lauten. Hatte der Benutzer nun mehrere Haustiere, an die er sich als seine ersten erinnert, so kann er hier die falsche Antwort geben. Die weiteren Szenarien sind bereits oben beschrieben worden.

Aus der Umfrage, die für diese Master-Thesis durchgeführt wurde, ergibt sich, dass 3/4 der Teilnehmer bereits Erfahrungen mit einer Wiederherstellung gesammelt haben. Die Nutzung von E-Mail oder SMS zur Wiederherstellung wurde positiv bewertet, aber auch die Nutzung von Token oder Codes (siehe 5.1.9). Aus Frage 10 ergibt sich, dass sich gut 64% der Benutzer eine Balance zwischen Sicherheit und Bedienbarkeit wünschen. Ein Drittel der Befragten legt den Fokus auf die Sicherheit (siehe 5.1.10). Auch sind 80% der Befragten gewillt, zusätzliche technische Maßnahmen in Kauf zu nehmen, wenn diese Maßnahmen die Sicherheit der Wiederherstellung erhöhen (siehe 5.1.11).

Die Durchführung der Wiederherstellungen für die ausgewählten Dienstleister hat gezeigt, dass es eine Vielzahl von unterschiedlichen Varianten in den Umsetzungen der Methoden gibt. Bis auf zwei Anbieter, Meta und Microsoft, bieten alle Dienstleister



---

mehrere Wege für die Wiederherstellung an. Durch die verschiedenen Kombinationen hat jedoch es jedoch kein Anbieter geschafft, einen Sicherheitswert über 3 für die Wiederherstellungsmethoden zu erreichen.

## 7. Diskussion und Empfehlung

Die Betrachtung und Durchführung der Wiederherstellungsmethoden hat gezeigt, dass es verschiedene Varianten in der Umsetzung der einzelnen Methoden gibt. Viele der betrachteten Dienstleister bieten mehrere Methoden für die Durchführung an und gehen somit auf die verschiedenen Bedürfnisse der Benutzer ein.

Im Reifegradmodell zur Sicherheit der einzelnen Methoden des AAG wird dargestellt, dass es für die unterschiedlichen Methoden auch Risiken gibt. Fragen-basierte Wiederherstellungsmethoden sind anfällig für Social Engineering Angriffe oder können durch das Online-Verhalten der Benutzer geschwächt werden, wenn diese Informationen teilen, die für die Beantwortung der Fragen genutzt werden können.

E-Mail-basierte Wiederherstellungsmethoden bieten eine Reihe von Angriffspunkten, angefangen bei Angriffen auf Passwörter wie Wörterbuch-Attacken oder andere Brute-Force-Attacken, Ausspäh-Attacken wie Man-In-The-Middle-Attacken oder Phishing oder auch Account Takeover Angriffe. Ein jüngeres Beispiel zeigt, dass die Gefahr durch Phishing akut ist[74]. Der Einzelhändler Pepco hat durch E-Mail-Spoofing (die Angreifer gaben sich als legitime Mitarbeiter aus) ca. 15,5 Millionen Euro verloren. Auch wenn hier nicht direkt Zugangsdaten erbeutet wurden, zeigt dieses Beispiel doch, wie professionell Angriffe dieser Art aufgebaut sind. Die Mitarbeiter von Check Point haben eine Liste für das erste Quartal des Jahres 2024 veröffentlicht, in der prozentual Firmen und Anbieter aufgeführt werden, welche besonders im Fokus von Phishing Angriffen stehen[75]. Oben in dieser Liste sind u.a. Microsoft, Google und LinkedIn aufgeführt, es finden sich aber auch DHL, Amazon oder Facebook unter den Betroffenen.

SMS-basierte Wiederherstellungsmethoden sind ebenfalls anfällig für Social Engineering Angriffe. Aber auch Spoofing-Attacken (Angreifer maskiert eigene Telefonnummer) oder der Verlust des Smartphones zusammen mit der SIM-Karte können hier Gefahren darstellen.

Die soziale Authentifikation kann ebenfalls durch Social Engineering angegrif-

fen werden. Weiterhin ist auch hier der Benutzer eine Gefahr für die Sicherheit des eigenen Accounts, da viele Benutzer Freundschaftsanfragen von ihnen unbekanntem Personen akzeptieren.

Codes oder Code-Listen können verloren, vernichtet oder offen gelegt werden und Token-basierte Wiederherstellungsmethoden können durch Attacken auf die zugrundeliegende Sicherheitsstruktur oder Software angegriffen werden. Weiterhin kann durch die Weiterentwicklung von künstlicher Intelligenz und Quantencomputer Technologie heute noch nicht abgesehen werden, wie sich die Sicherheit der kryptographischen Algorithmen in der Zukunft darstellt.

Viele der betrachteten Anbieter setzen die Wiederherstellung durch Zusendung eines Codes an eine E-Mail-Adresse oder per SMS an eine Telefonnummer um. Diese Option für sich alleine birgt nur eine eingeschränkte Sicherheit, da potentiell der adressierte E-Mail-Account oder die zur Telefonnummer gehörende SIM-Karte nicht mehr im Besitz des eigentlichen Besitzers sein kann. Der Dienstleister Meta erweitert diesen Vorgang um die Forderung der Eingabe eines OTP zusätzlich zur Zusendung eines Codes per E-Mail. Die Nutzung eines zweiten Faktors kann für eine Wiederherstellungsmethode die Sicherheit erhöhen, ohne den Aufwand und die Bedienbarkeit für den Benutzer in der Komplexität wesentlich zu erhöhen. Viele Dienstleister bieten oder fordern die Nutzung eines zweiten Faktors bereits für die primäre Authentifikation. Dieser Ansatz sollte auch für die Wiederherstellung übernommen werden.

Tabelle 7.1.: Anbieter und Wiederherstellungsmethoden

	Code oder Codeliste	Soziale Authentifikation	pers. Fragen und Sicherheitsfragen	E-Mail oder SMS	Token
Amazon				X	
Apple	X			X	
Google	X			X	
Microsoft	X			X	
Meta	X			X	
Web.de	X			X	
Ubiquiti	X			X	
Unifi					
Steam	X			X	

---

Tabelle 7.1 stellt eine Verknüpfung zwischen den in Kapitel 2.2 beschriebenen möglichen Methoden und den in der Durchführung verfügbaren Methoden je Anbieter dar. Hierbei fällt auf, dass jeder Anbieter mindestens die Methode per E-Mail oder SMS zur Verfügung stellt. Auch die Verwendung eines Codes oder einer Code-Liste wird von fast allen Anbietern angeboten. Im Fall von Web.de und Meta wird diese jedoch explizit für den Verlust der 2FA Option genutzt. Sollte beim Anbieter Amazon der Zugriff auf den 2FA-Faktor nicht mehr möglich sein, so muss der Benutzer einen Identitätsnachweis an Amazon übersenden und auf Freischaltung warten. Dieser Vorgang kann laut Amazon 1-2 Tage dauern[76].

Die Methoden soziale Authentifikation, persönliche Fragen oder Sicherheitsfragen und Token wurden in der Durchführung von keinem Anbieter für die Wiederherstellung offeriert. Auf der einen Seite ist der Entfall der Methode der Fragen positiv zu bewerten, da gemäß Bewertungsmatrix 2.2 diese Methode einen geringen Wert für die Sicherheit erhält. Andererseits hat kein Anbieter die Option angeboten, einen Passkey oder anderen Token für die Wiederherstellung zu nutzen. Hier sollten die Anbieter nachziehen, da durch diese Methode die Sicherheit eines Accounts deutlich erhöht werden kann. Dies trifft jedoch auch nur zu, wenn schwächere Methoden nicht gleichzeitig zugelassen werden. Als Beispiel sei hier der Anbieter Google erwähnt.

In Abbildung 4.3 ist nachvollziehbar, dass Google die Option Code-Liste anbietet und für diese Methode einen Wert von 4 erhält. Da jedoch weitere Methoden genutzt werden, u.a. die Möglichkeit zur Eingabe eines älteren / vormals genutzten Passwortes besteht, wird der Gesamtwert für die Wiederherstellung für Google auf den Wert 1 reduziert.

Ein weiterer Faktor, der auf das Niveau der Sicherheit der Wiederherstellungsmethode Einfluss haben sollte, ist die mögliche Mehrfachnutzung eines Accounts für verschiedene Angebote. Bekannte Beispiele sind Amazon, Facebook / Meta, Google oder Apple. Viele Anbieter von Onlinediensten ermöglichen es den Benutzern die bereits vorhandenen Accounts für den Zugang zum Angebot des Anbieters zu nutzen. Durch diese Möglichkeit wird die Anforderung an die Sicherheit eines solchen Accounts deutlich erhöht, weil eine potentielle Kompromittierung des Accounts weitreichende Folgen für den Benutzer haben kann. Für Accounts dieser Art sollte darauf geachtet werden, dass neben der Absicherung der primären Authentifikation auch die Wiederherstellungsmethode nicht nur auf einem Faktor beruht.

Ein Ziel dieser Master-Thesis war es zu prüfen, in wie weit die Sicherheit einer Wiederherstellungsmethode mit der Verwendbarkeit und Erreichbarkeit angeglichen werden kann. Die Benutzerumfrage hat gezeigt, dass die meisten Benutzer gewillt

---

sind, für eine höhere Sicherheit den Aufwand zusätzlicher Maßnahmen in Kauf zu nehmen. Da der Vorgang der Wiederherstellung im Gegensatz zur primären Authentifikation auch nicht regelmäßig durchgeführt werden sollte, sondern nur im Fall des Verlustes der primären Authentifikationsfaktoren, wird die Empfehlung gegeben, entweder eine Wiederherstellungsmethode zu verwenden, die als Methode an sich bereits eine höhere Sicherheit inhärent hat oder eine Kombination von Methoden wie z.B. Versendung eines Codes per E-Mail und die Eingabe eines OTP oder die Bestätigung durch eine mit dem Account gekoppelte App (siehe 3.3.8).

Vermieden werden sollte die Option von z.B. der Nutzung einer Code-Liste und als ein weiterer Weg nur die Zusendung eines Wiederherstellungscodes per E-Mail (siehe 3.3.3). Auch die Frage nach einem vormals genutzten Passwort sollte vermieden werden (siehe 3.3.3). Dies birgt eine große Gefahr für den Account, da zum einen für Angreifer viele Passwörter im DarkNet verfügbar sind, zum anderen Benutzer häufig dasselbe Passwort für mehrere Zugänge benutzen.

Die Verwendung von Codes oder Code-Listen bietet eine vergleichsweise hohe Sicherheit, auch wenn hier der Aufwand für den Benutzer höher ist, da er diese Faktoren nicht immer sofort zur Verfügung hat.

Die Nutzung von Token war bei der Durchführung in dieser Master-Thesis von keinem Dienstleister angeboten worden. Hier besteht Potential, da die Einrichtung dieser Maßnahme analog zur Nutzung als primäre Authentifikation nicht wesentlich komplexer ist, als die Einrichtung eines zweiten Faktors für die Authentifikation. Durch die Möglichkeit Token auf USB-Sticks mit zwei Anschlussmöglichkeiten zu speichern, wird die Bedienbarkeit auch für mobile Geräte ermöglicht[65].

Die folgende Graphik 7.1 zeigt eine Empfehlung für die Umsetzung von Wiederherstellungsmethoden. Hierbei muss klar unterschieden werden, ob es sich um einen Account handelt, welcher für Multi-Authentifikation<sup>1</sup> oder Single-Sign-On genutzt werden kann oder einen Account, der nur für die Nutzung eines Anbieters genutzt wird.

---

<sup>1</sup>hiermit ist gemeint, das ein Account für mehrere Onlinezugänge genutzt wird, wurde bei Pöhn et al.[2] „account network“ bezeichnet

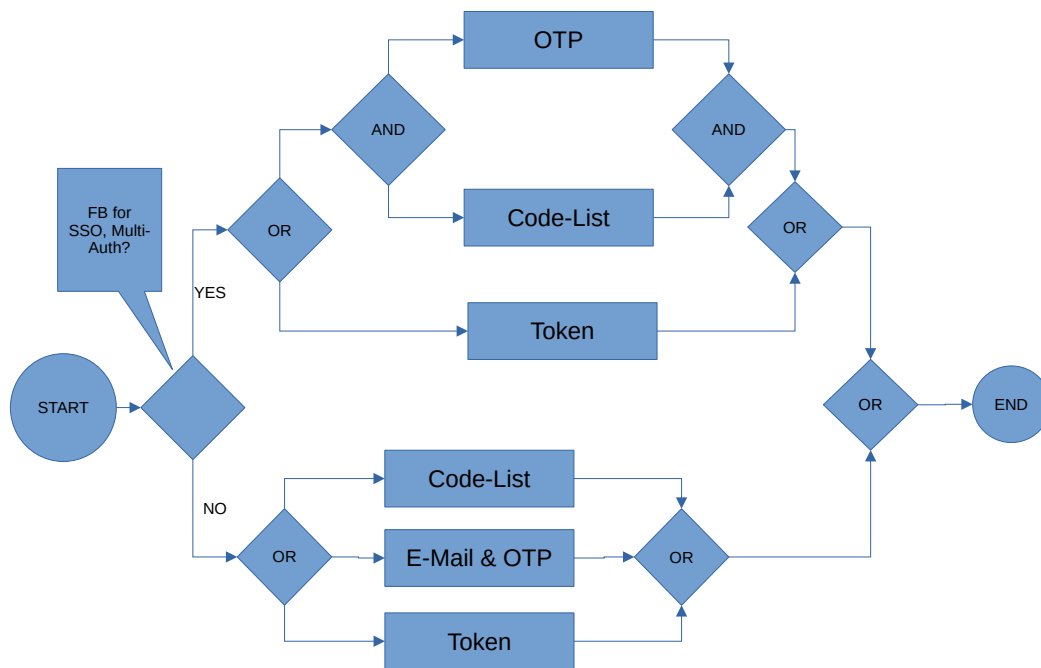


Abbildung 7.1.: Diagramm Empfehlung

Im letzteren Fall sollte es ausreichen, die Wiederherstellungsmethode aus den Optionen Code-Liste oder Code, E-Mail und OTP oder die Nutzung eines Token umzusetzen. Kann der Account des Anbieters oder Onlinedienstleisters für mehrere Authentifikationen genutzt werden, so sollte eine stärkere Variante der Wiederherstellungsmethode umgesetzt werden. Als Optionen werden hier die Nutzung eines Token oder die Kombination von Code-Liste oder Code und OTP empfohlen.

Bei der Nutzung eines Token sollte darauf geachtet werden, dass ein separates Gerät genutzt wird, sollte auch die primäre Authentifikation per Token gewählt werden. Die hierdurch geschaffene Redundanz erhöht die Sicherheit gegen Verlust und Missbrauch durch den Verlust der primären Authentifikation. Die Abbildungen 7.2 und 7.3 zeigen, dass der Wert für die Zugänglichkeit sich erhöht, wenn ein separater USB-Stick für den Wiederherstellungstoken verwendet wird.

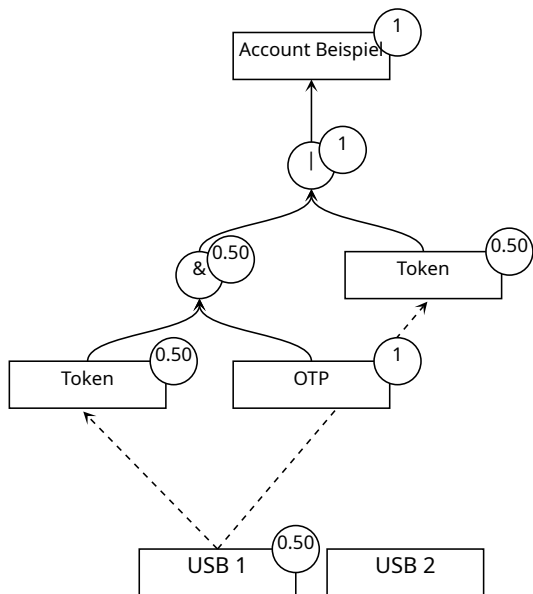


Abbildung 7.2.: Zugänglichkeit 1  
Tokenspeicher

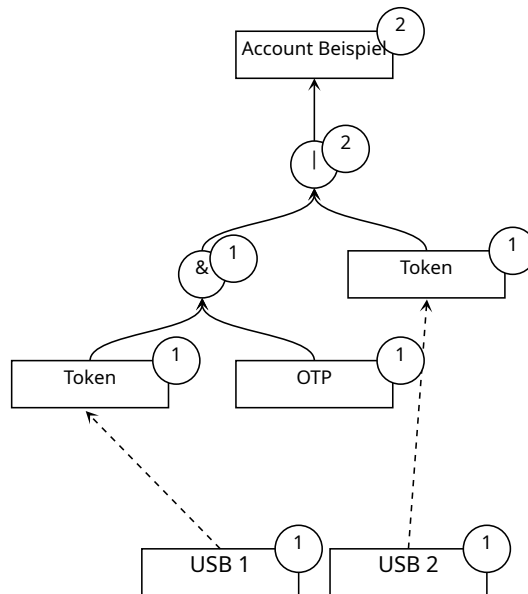


Abbildung 7.3.: Zugänglichkeit 2  
Tokenspeicher

Die Variante der Wiederherstellungsmethode Code-Liste oder Code in Kombination mit OTP bietet ebenfalls eine hohe Stufe der Sicherheit. Es werden zwei Faktoren verwendet, die beide gemäß der Bewertung der Sicherheit höhere Werte erhalten[2]. Somit stehen den Anbietern Optionen zur Auswahl, die die Sicherheit der Wiederherstellungsmethode auf ein gutes Niveau heben, jedoch den Aufwand für den Benutzer nicht zu stark erhöhen.

Als letztmögliche Wiederherstellungsmethode sollten die Anbieter die Option der persönlichen Verifikation vorhalten. Sollte ein Benutzer alle anderen Authentifikations- und Wiederherstellungsfaktoren nicht mehr zur Verfügung haben, muss dem Benutzer noch die Möglichkeit gegeben werden, den Nachweis seiner Person z.B. durch Videotelefonie oder vergleichbare Methoden zu erbringen.

# 8. Fazit und Ausblick

## 8.1. Fazit

In dieser Master-Thesis wurden verschiedene Wiederherstellungsmethoden verglichen und ihre Umsetzungen sowie mögliche Angriffsvektoren dargestellt. Es erfolgte eine Betrachtung der Umsetzung der Wiederherstellungsmethoden bei ausgewählten Anbietern sowie eine Analyse der jeweiligen Umsetzungen mit Hilfe des Account Access Graph Tools.

Die Bestandsaufnahme in Kapitel 3 zeigte, dass die verschiedenen Methoden bei den Anbietern in unterschiedlichen Varianten umgesetzt werden. Die Nutzung von zusätzlichen Geräten zur Verifikation des Benutzers wurde hier positiv im Sinne der Sicherheit empfunden. Negativ fiel die Option eines Anbieter auf, ältere Passwörter für die Wiederherstellung abzufragen. Auffällig war in der Analyse (siehe Kapitel 4), dass eine größere Auswahl an Methoden nicht zu einem höheren Wert in der Sicherheit führte. Die Untersuchung der Zugänglichkeit zeigte, dass in den aktuellen Umsetzungen der Anbieter meistens ausreichend alternative Wege vorhanden sind. Nur in einem Fall bestand das Risiko bei Verlust eines Faktors den Zugang zum Account ganz zu verlieren (vgl. Kapitel 4.2.5).

Die Auswertung der Benutzerumfrage (siehe 5) zeigte, dass den meisten Benutzern das Thema Sicherheit wichtiger ist im Vergleich zu einer einfacheren Bedienung. Auch sind viele Benutzer bereit, weitere technische Maßnahmen in Kauf zu nehmen, wenn sich dadurch die Sicherheit für eine Wiederherstellungsmethode erhöht.

Als Ergebnis aus der Analyse in Kombination mit den Bewertungen zur Benutzbarkeit und Erreichbarkeit kann festgehalten werden, dass es viele mögliche Umsetzungen für Wiederherstellungsmethoden gibt. Die Anbieter sollten jedoch genau prüfen, welche Methoden für ihren jeweiligen Account sinnvoll sind. Accounts, die für verschiedene Authentifikationen auf unterschiedlichen Seiten genutzt werden können, sollten besser abgesichert werden, als Accounts, die diesen Faktor nicht unterstützen. Eine abschließende Empfehlung für Umsetzungen von Wiederherstellungsmethoden konnte gegeben werden.



---

## 8.2. Ausblick

Die in dieser Master-Thesis gewonnenen Erkenntnisse können einen Ansatz bieten, wie Anbieter ihre Wiederherstellungsmethoden umsetzen oder verbessern sollten. Eine einheitliche Empfehlung ist nicht möglich, da die Varianz der Methoden und die jeweilige Stufe der Sicherheit zu groß ist. Für die Zukunft bleibt es weiter wichtig, neue Technologien zu betrachten und die bestehenden Methoden zu hinterfragen. Die Nutzung von Token als Wiederherstellungsmethode erscheint als eine sichere Variante, da die Technik hier immer mehr Anwendungsmöglichkeiten bietet. Aktuell ist diese Methode jedoch noch nicht im Fokus der Anbieter.

Es bleibt ebenfalls abzuwarten, welche Einflüsse zukünftig die Themen künstliche Intelligenz und Quantencomputer im Bereich der Wiederherstellungsmethoden haben werden. FIDO (siehe 2.1.7) und andere Varianten können ebenfalls in der Zukunft Optionen zur Umsetzung von Wiederherstellungsmethoden bieten.

# Literaturverzeichnis

- [1] Ruhr Universität Bochum Prof. Dr. Markus Dürmuth. Passwörter sicherer machen. URL: <https://news.rub.de/wissenschaft/2016-06-23-informationstechnik-passwoerter-sicherer-machen>, (abgerufen am 13.05.2024).
- [2] Daniela Pöhn, Nils Gruschka, Leonhard Ziegler, and Andre Büttner. A framework for analyzing authentication risks in account networks. *Computers & Security*, 135:103515, 2023.
- [3] Bundesamt für Sicherheit in der Informationstechnik. Zwei-faktor-authentisierung. URL: <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung.html?nn=909630> (abgerufen am 14.04.2024).
- [4] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why older adults (don't) use password managers. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 73–90. USENIX Association, August 2021.
- [5] Ian Baker. Account takeover attacks surge by over 300 percent. URL: <https://betanews.com/2023/09/27/account-takeover-attacks-surge-by-over-300-percent/> (abgerufen am 21.01.2024).
- [6] Peter Schmitz Stefan Luber. Was ist identity- and access management (iam)? URL: <https://www.security-insider.de/was-ist-identity-and-access-management-iam-a-612910/>, (abgerufen am 01.05.2024).
- [7] R.S. Sandhu and P. Samarati. Access control: principle and practice. *IEEE Communications Magazine*, 32(9):40–48, 1994.
- [8] Bundesamt für Sicherheit in der Informationstechnik. Orp.4: Identitäts- und berechtigungsmanagement. URL: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium\\_Einzel\\_PDFs\\_2021/02\\_ORP\\_Organisation\\_und\\_Personal/ORP\\_\\_4\\_Identitaets\\_und\\_Berechtigungsmanagement\\_Editon\\_2021.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP__4_Identitaets_und_Berechtigungsmanagement_Editon_2021.pdf?__blob=publicationFile&v=2), (abgerufen am 01.05.2024).

- 
- [9] Eberhard von Faber. *IT und IT-Sicherheit in Begriffen und Zusammenhängen*. Springer Vieweg Wiesbaden, Springer Fachmedien Wiesbaden, 2021.
- [10] Auth0 by Okta. Authentifizierung und autorisierung im vergleich. URL: <https://auth0.com/de/intro-to-iam/authentication-vs-authorization> (abgerufen am 14.04.2024).
- [11] Claudia Eckert. *IT-Sicherheit, Konzepte - Verfahren - Protokolle*. De Gruyter Oldenbourg, Berlin, Boston, 2018.
- [12] OneLogin. Was ist identity and access management (iam)? URL: <https://www.onelogin.com/de-de/learn/iam>, (abgerufen am 18.05.2024).
- [13] Norbert Pohlmann. *Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Springer Vieweg Wiesbaden, Springer Fachmedien Wiesbaden, 2022.
- [14] Ashar Javed, David Bletgen, Florian Kohlar, Markus Dürmuth, and Jörg Schwenk. Secure fallback authentication and the trusted friend attack. In *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 22–28, 2014.
- [15] Bundesamt für Sicherheit in der Informationstechnik. Sichere passwörter erstellen. URL: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html), (abgerufen am 28.04.2024).
- [16] Verbraucherzentrale. Starke passwörter – so geht’s. URL: <https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/starke-passwoerter-so-gehts-11672>, (abgerufen am 28.04.2024).
- [17] Bundesamt für Sicherheit in der Informationstechnik. Bsi-basisschutz: Sichere passwörter. URL: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere\\_passwoerter\\_faktenblatt.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=4), (abgerufen am 21.05.2024).
- [18] Hasso-Plattner-Institut. 123456789 ist das beliebteste passwort 2023 in deutschland. URL: <https://hpi.de/news/jahrgaenge/2023/123456789-ist-das-beliebteste-passwort-2023-in-deutschland.html>, (abgerufen am 12.05.2024).

- 
- [19] NordPass. Top 200 der gängigsten passwörter. URL: <https://nordpass.com/de/most-common-passwords-list/>, (abgerufen am 12.05.2024).
- [20] Stephan Wiefling. *Usability, security, and privacy of risk-based authentication*. doctoralthesis, Ruhr-Universität Bochum, Universitätsbibliothek, 2023.
- [21] Carnegie Mellon University. Captcha: Telling humans and computers apart automatically. URL: <http://www.captcha.net/>, (abgerufen am 12.05.2024).
- [22] Rahul Awati. Risikobasierte authentifizierung (rba). URL: <https://www.computerweekly.com/de/definition/Risikobasierte-Authentifizierung-RBA>, (abgerufen am 12.05.2024).
- [23] Tayibia Bazaz and Aqeel Khalique. A review on single sign on enabling technologies and protocols. *International Journal of Computer Applications*, 151:18–25, 10 2016.
- [24] Peter Luber, Stefan und Schmitz. Definition sso - was ist single sign-on (sso)? URL: <https://www.security-insider.de/was-ist-single-sign-on-sso-a-631479/>, (abgerufen am 24.06.2024).
- [25] Ivan Lee. Single sign-on - what is it? how does sso work? URL: <https://www.wallarm.com/what/single-sign-on-what-is-it>, (abgerufen am 22.08.2024).
- [26] Bundesamt für Sicherheit in der Informationstechnologie BSI. Single-sign-on. URL: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Single-Sign-On/single-sign-on\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Single-Sign-On/single-sign-on_node.html), (abgerufen am 22.08.2024).
- [27] FIDO Alliance. Why fido? URL: <https://fidoalliance.org/>, (abgerufen am 21.05.2024).
- [28] Bundesamt für Sicherheit in der Informationstechnik. Schafft die passwörter ab?! URL: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html), (abgerufen am 21.05.2024).
- [29] FIDO Alliance. How passkeys work. URL: <https://fidoalliance.org/how-fido-works/>, (abgerufen am 21.05.2024).

- 
- [30] GitHub Inc. Informationen zu github und git. URL: <https://docs.github.com/de/get-started/start-your-journey/about-github-and-git#informationen-zu-github>, (abgerufen am 18.05.2024).
- [31] GitHub Inc. Informationen zur zwei-faktor-authentifizierung. URL: <https://docs.github.com/de/authentication/securing-your-account-with-two-factor-authentication-2fa/about-two-factor-authentication>, (abgerufen am 21.05.2024).
- [32] GitHub Inc. Wiederherstellungsmethoden bei der zwei-faktor-authentifizierung konfigurieren. URL: <https://docs.github.com/de/authentication/securing-your-account-with-two-factor-authentication-2fa/configuring-two-factor-authentication-recovery-methods>, (abgerufen am 18.05.2024).
- [33] Bernadette Kneidinger-Müller. *Soziale Netzwerk Seiten*, pages 67–73. Springer Fachmedien Wiesbaden, Wiesbaden, 2020.
- [34] Microsoft. Einrichten von sicherheitsfragen als Überprüfungsmethode. URL: <https://support.microsoft.com/de-de/account-billing/einrichten-von-sicherheitsfragen-als->
- [35] Okta Swaroop Sham. Sicherheitsfragen: Best practices, beispiele und ideen. URL: <https://www.okta.com/de/blog/2021/03/security-questions/>, (abgerufen am 21.05.2024).
- [36] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In *Proceedings of the 24th International Conference on World Wide Web, WWW '15*, page 141–150, Republic and Canton of Geneva, CHE, 2015. International World Wide Web Conferences Steering Committee.
- [37] Crowdstrike. 10 arten von social-engineering-angriffen. URL: <https://www.crowdstrike.de/cybersecurity-101/types-of-social-engineering-attacks/>, (abgerufen am 21.05.2024).
- [38] Alina Hang, Alexander De Luca, and Heinrich Hussmann. I know what you did last week! do you? dynamic security questions for fallback authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15*, page 1383–1392, New York, NY, USA, 2015. Association for Computing Machinery.
- [39] Nicholas Micallef and Nalin Asanka Gamagedara Arachchilage. Changing users' security behaviour towards security questions: A game based learning approach.

---

In *2017 Military Communications and Information Systems Conference (Mil-CIS)*, pages 1–6, 2017.

- [40] Tommaso Innocenti, Seyed Ali Mirheidari, Amin Kharraz, Bruno Crispo, and Engin Kirda. You’ve got (a reset) mail: A security analysis of email-based password reset procedures. In Leyla Bilge, Lorenzo Cavallaro, Giancarlo Pellegrino, and Nuno Neves, editors, *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 1–20, Cham, 2021. Springer International Publishing.
- [41] Peter Snyder and Chris Kanich. One thing leads to another: Credential based privilege escalation. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, CODASPY ’15, page 135–137, New York, NY, USA, 2015. Association for Computing Machinery.
- [42] Yue Li, Haining Wang, and Kun Sun. Email as a master key: Analyzing account recovery in the wild. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pages 1646–1654, 2018.
- [43] Yue Li, Zeyu Chen, Haining Wang, Kun Sun, and Sushil Jajodia. Understanding account recovery in the wild and its security implications. *IEEE Transactions on Dependable and Secure Computing*, 19(1):620–634, 2022.
- [44] web.de. Registrierung. URL: [https://registrierung.web.de/#.pc\\_page.tarifvergleich.index.teaser\\_1.registrierung](https://registrierung.web.de/#.pc_page.tarifvergleich.index.teaser_1.registrierung), (abgerufen am 21.05.2024).
- [45] Johannes Kunke, Stephan Wiefeling, Markus Ullmann, and Luigi Lo Iacono. Evaluation of account recovery strategies with fido2-based passwordless authentication, 2021.
- [46] Fabian Schwarz, Khue Do, Gunnar Heide, Lucjan Hanzlik, and Christian Rossow. Feido: Recoverable fido2 tokens using electronic ids. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS ’22, page 2581–2594, New York, NY, USA, 2022. Association for Computing Machinery.
- [47] Bundesamt für Sicherheit in der Informationstechnik. Social engineering – der mensch als schwachstelle. URL: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html), (abgerufen am 26.05.2024).

- 
- [48] Bundesamt für Sicherheit in der Informationstechnik. Phishing & smishing auf dem Vormarsch. URL: [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html), (abgerufen am 26.05.2024).
- [49] Facebook. Graph api explorer tool. URL: <https://developers.facebook.com/tools/explorer>, (abgerufen am 11.08.2024).
- [50] Mitre Att&ck. Brute force. URL: <https://attack.mitre.org/techniques/T1110/>, (abgerufen am 02.06.2024).
- [51] Mitre Att&ck. Brute force: Credential stuffing. URL: <https://attack.mitre.org/techniques/T1110/004/>, (abgerufen am 02.06.2024).
- [52] OWASP. Session hijacking attack. URL: [https://owasp.org/www-community/attacks/Session\\_hijacking\\_attack#](https://owasp.org/www-community/attacks/Session_hijacking_attack#), (abgerufen am 02.06.2024).
- [53] Wireshark. Wireshark. URL: <https://www.wireshark.org/>, (abgerufen am 02.06.2024).
- [54] Encryption Consulting Subhayu Roy. What is session hijacking? URL: <https://www.encryptionconsulting.com/what-is-session-hijacking/>, (abgerufen am 02.06.2024).
- [55] Bleeping Computer Bill Toulas. New phishing attack steals your instagram backup codes to bypass 2fa. URL: <https://www.bleepingcomputer.com/news/security/new-phishing-attack-steals-your-instagram-backup-codes-to-bypass-2fa/>, (abgerufen am 02.06.2024).
- [56] Instagram. Dein instagram-konto mit zweistufiger authentifizierung sichern. URL: <https://help.instagram.com/566810106808145>, (abgerufen am 02.06.2024).
- [57] Trustwave Diana Solomon. Instagram phishing targets backup codes. URL: <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/instagram-phishing-targets-backup-codes/>, (abgerufen am 02.06.2024).
- [58] Bundesamt für Sicherheit in der Informationstechnik. Aktuelle beispiele für phishing-angriffe. URL:

---

<https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Aktuelle-Beispiele-fuer-Phishing/aktuelle-beispiele-fuer-phishing.html>, (abgerufen am 31.07.2024).

- [59] Handelsblatt. Immer mehr cybercrime – verbrecher nutzen ki. URL: <https://www.handelsblatt.com/technik/it-internet/europol-immer-mehr-cybercrime-verbrecher-nutzen-ki/100054626.html>, (abgerufen am 31.07.2024).
- [60] Andre Büttner. research-tool. URL: <https://github.com/Multi-Account-Dashboard/research-tool>, (abgerufen am 07.07.2024).
- [61] W.C. Booth, G.G. Colomb, and J.M. Williams. *The Craft of Research, Third Edition*. Chicago Guides to Writing, Editing, and Publishing. University of Chicago Press, 2009.
- [62] J.A. Maxwell. *Qualitative Research Design: An Interactive Approach: An Interactive Approach*. Applied Social Research Methods. SAGE Publications, 2013.
- [63] KeePass. KeePass password safe. URL: <https://keepass.info/>, (abgerufen am 15.06.2024).
- [64] Google. Google authenticator. URL: <https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=de&pli=1>, (abgerufen am 24.07.2024).
- [65] Token2. Token2 - security is easy. URL: <https://www.token2.com/home>, (abgerufen am 24.07.2024).
- [66] Mozilla Firefox. Privater modus – kontrolle über die von firefox gespeicherten daten behalten. URL: <https://support.mozilla.org/de/kb/privater-modus>, (abgerufen am 22.08.2024).
- [67] Mozilla Firefox. Häufige irrtümer über das surfen im privaten modus. URL: <https://support.mozilla.org/de/kb/haufige-missverstandnisse-surfen-im-privaten-modus>, (abgerufen am 22.08.2024).
- [68] Microsoft. Zurücksetzen eines vergessenen kennworts für ihr microsoft-konto. URL: <https://support.microsoft.com/de-de/account-billing/zur%C3%BCcksetzen-eines-vergessenen-kennworts-f%C3%BCr-ihr-microsoft-konto-eff4f067-5042-c1a3-fe72-b04d60556c37>, (abgerufen am 28.07.2024).



- 
- [69] Meta Communityforums. Lost my email account. URL: <https://communityforums.atmeta.com/t5/Get-Help/Lost-my-email-account/td-p/1005754>, (abgerufen am 28.07.2024).
- [70] Web.de. Persönliche identifizierung: Ablauf. URL: <https://hilfe.web.de/account/idcheck.html>, (abgerufen am 27.07.2024).
- [71] Udo Kelle. *Mixed Methods*, pages 153–166. Springer Fachmedien Wiesbaden, Wiesbaden, 2014.
- [72] Lea Pfeiffer, Franziska und Genau. Umfrage als wissenschaftliche methode durchführen. URL: <https://www.scribbr.de/methodik/umfrage-wissenschaftliche-methode/>, (abgerufen am 06.07.2024).
- [73] DESTATIS Statistisches Bundesamt. Demografischer wandel. URL: [https://www.destatis.de/DE/Themen/Querschnitt/Demografischer-Wandel/\\_inhalt.html](https://www.destatis.de/DE/Themen/Querschnitt/Demografischer-Wandel/_inhalt.html), (abgerufen am 23.07.2024).
- [74] Zeljka Zorz. European retailer pepco loses €15.5 million in phishing (possibly bec?) attack. URL: <https://www.helpnetsecurity.com/2024/02/28/pepco-phishing-bec-attack/>, (abgerufen am 26.08.2024).
- [75] Check Point. Microsoft and google top the list in q1 2024 phishing attacks: Check point research highlights a surge in cyber threats. URL: <https://blog.checkpoint.com/security/microsoft-and-google-top-the-list-in-q1-2024-phishing-attacks-check-point-research-highlights-a-surge-in-cyber-threats/>, (abgerufen am 26.08.2024).
- [76] Amazon. Konto nach fehlgeschlagener zwei-faktor-authentifizierung wiederherstellen. URL: <https://www.amazon.de/gp/help/customer/display.html?nodeId=GU3SL3GTHLHPDQ2H>, (abgerufen am 26.08.2024).

# Abbildungsverzeichnis

2.1. Authentifikation [12]	6
2.2. Autorisierung [12]	7
2.3. Tipps für sichere Passwörter[17]	8
2.4. Ablauf des Single-Sign-On [25][26]	11
2.5. Ablauf Challenge-Response-Verfahren FIDO[13]	13
2.6. GitHub Codeliste[32]	14
2.7. Eingabe Mobilfunknummer WEB.DE Registrierung[44]	17
2.8. Darstellung eines Session Hijacking Angriff[54]	21
2.9. Wiederherstellungscode Instagram[57]	22
2.10. Phishing E-Mail Instagram[57]	23
2.11. Phishing Seiten für Instagram Backup Codes[57]	23
2.12. Beispiel für einen AAG Sicherheit	24
2.13. Beispiel für einen AAG Zugänglichkeit	26
3.1. Token2 Manager Passkey für Amazon	29
3.2. Erstellung Apple ID	30
3.3. Schlüssel erstellen Apple	30
3.4. Schlüssel Apple	30
3.5. Passkey Einstellung Google	31
3.6. Sicherheitseinstellungen Google	32
3.7. Erstellung Account Microsoft	32
3.8. Sicherheitseinstellungen Account Meta	33
3.9. Nutzung Web.de App für 2FA	33
3.10. Sicherheitseinstellungen Ubiquiti	34
3.11. Steam Guard Code	35
3.12. Start Wiederherstellung Amazon	36
3.13. Fenster zur Eingabe OTP Amazon	37
3.14. Reset E-Mail Amazon	37
3.15. Erstellung neues Passwort Amazon	37
3.16. Apple Zurücksetzen eines Passwortes	38
3.17. Apple Wiederherstellung 2	38
3.18. Apple Wiederherstellung 3	39

---

3.19. Apple Wiederherstellung 4 . . . . .	39
3.20. Apple Wiederherstellung 5 . . . . .	40
3.21. Apple Wiederherstellung 6 . . . . .	40
3.22. Apple Wiederherstellung 7 . . . . .	41
3.23. Wiederherstellungsmethoden Google . . . . .	42
3.24. Codeeingabe Google Authenticator . . . . .	42
3.25. Erstellen neues Passwort Google . . . . .	43
3.26. Eingabe altes Passwort Google . . . . .	43
3.27. Eingabe neues Passwort Google . . . . .	44
3.28. Eingabe E-Mail Meta . . . . .	45
3.29. Eingabe Code Meta . . . . .	45
3.30. Start Wiederherstellung web.de . . . . .	45
3.31. Abfrage Account web.de . . . . .	46
3.32. Eingabe Code aus SMS web.de . . . . .	47
3.33. Eingabe Geheimschlüssel 2FA web.de . . . . .	47
3.34. Eingabe neues Passwort web.de . . . . .	48
3.35. web.de App . . . . .	49
3.36. Eingabe Name . . . . .	49
3.37. Start Wiederherstellung Ubiquiti . . . . .	50
3.38. E-Mail mit Link Ubiquiti . . . . .	50
3.39. Methoden für Verlust 2FA Ubiquiti . . . . .	51
3.40. Verlust aller 2FA Ubiquiti . . . . .	51
3.41. Start Wiederherstellung Steam . . . . .	52
3.42. Eingabe E-Mail-Adresse Steam . . . . .	52
3.43. Fragebogen Steam . . . . .	53
4.1. AAG Amazon Sicherheit . . . . .	59
4.2. AAG Apple Sicherheit . . . . .	60
4.3. AAG Google Sicherheit . . . . .	61
4.4. AAG Microsoft Sicherheit . . . . .	62
4.5. AAG Meta Sicherheit . . . . .	63
4.6. AAG Web.de Sicherheit . . . . .	64
4.7. AAG Ubiquiti Sicherheit . . . . .	64
4.8. AAG Steam Sicherheit . . . . .	65
4.9. AAG Amazon Zugänglichkeit . . . . .	66
4.10. AAG Apple Zugänglichkeit . . . . .	67
4.11. AAG Google Zugänglichkeit . . . . .	68
4.12. AAG Microsoft Zugänglichkeit . . . . .	69
4.13. AAG Meta Zugänglichkeit . . . . .	70

---

4.14. AAG Web.de Zugänglichkeit . . . . .	71
4.15. AAG Ubiquiti Unifi Zugänglichkeit . . . . .	72
4.16. AAG Steam Zugänglichkeit . . . . .	73
5.1. Frage 1: Wie alt sind Sie? . . . . .	74
5.2. Frage 2: Welche Erfahrung haben Sie mit Informationstechnologien? . . . . .	75
5.3. Frage 3: Welche der folgenden Wiederherstellungsmethoden kennen Sie? . . . . .	76
5.4. Frage 4: Haben Sie bei einem der folgenden Anbieter einen Benutzeraccount? . . . . .	77
5.5. Frage 5: Welche Wiederherstellungsmethode haben Sie für den / die Anbieter gewählt? . . . . .	77
5.6. Frage 7: Haben Sie schon einmal für einen Onlinezugang eine Wiederherstellung durchgeführt oder durchführen müssen? . . . . .	79
5.7. Frage 10: Was ist Ihnen wichtiger, wenn Sie an Wiederherstellungsmethoden denken, Sicherheit oder Bedienbarkeit? . . . . .	81
5.8. Frage 11: Wären Sie bereit für eine höhere Sicherheit bei Wiederherstellungsmethoden zusätzliche technische Maßnahmen in Kauf zu nehmen? (z.B. eine Handy-App, USB-Token oder ähnliches) . . . . .	82
7.1. Diagramm Empfehlung . . . . .	93
7.2. Zugänglichkeit 1 Tokenspeicher . . . . .	94
7.3. Zugänglichkeit 2 Tokenspeicher . . . . .	94
A.1. Zugänglichkeit Apple AAG 2. gek. Gerät . . . . .	110
A.2. Frage 5: Google . . . . .	111
A.3. Frage 5: Amazon . . . . .	111
A.4. Frage 5: Apple . . . . .	112
A.5. Frage 5: Facebook . . . . .	112
A.6. Frage 5: Microsoft . . . . .	112

# Tabellenverzeichnis

2.1. Auswahl häufiger Passwörter 2023 . . . . .	8
2.2. Reifegradmodell Wiederherstellung AAG . . . . .	25
5.1. Ergebnis Frage 5 . . . . .	78
6.1. Sicherheitsbewertung . . . . .	83
6.2. Bewertung Benutzbarkeit . . . . .	84
6.3. Bewertung Erreichbarkeit . . . . .	85
6.4. Bewertung Methoden . . . . .	85
6.5. Verfügbarkeit von Wiederherstellungsmethoden . . . . .	87
7.1. Anbieter und Wiederherstellungsmethoden . . . . .	90

# Abkürzungsverzeichnis

2FA .....	Zwei Faktor Authentifizierung
AAG .....	Account Access Graph
APT .....	Advanced Persistent Threat
ATO .....	Account takeover attacks
BSI .....	Bundesamt für Sicherheit in der Informationstechnik
CAPTCHA .....	Completely Automated Public Turing test to tell Computers and Humans Apart
CEO .....	Chief Executive Officer
FIDO .....	Fast Identity Online
IAM .....	Identity and Access Management
IP .....	Internet Protocol
IT .....	Informationstechnologie
OS .....	Operating System
OTP .....	One-Time-Password
PC .....	Personal Computer
PIN .....	Persönliche Identifikationsnummer
QR .....	Quick Response
SIM .....	Subscriber Identity Module
SMS .....	Short Message Service
SSO .....	Single-Sign-On
USB .....	Universal Serial Bus
VPN .....	Virtual Privat Network

# A. Anhang

## A.1. Weitere Darstellungen des AAG

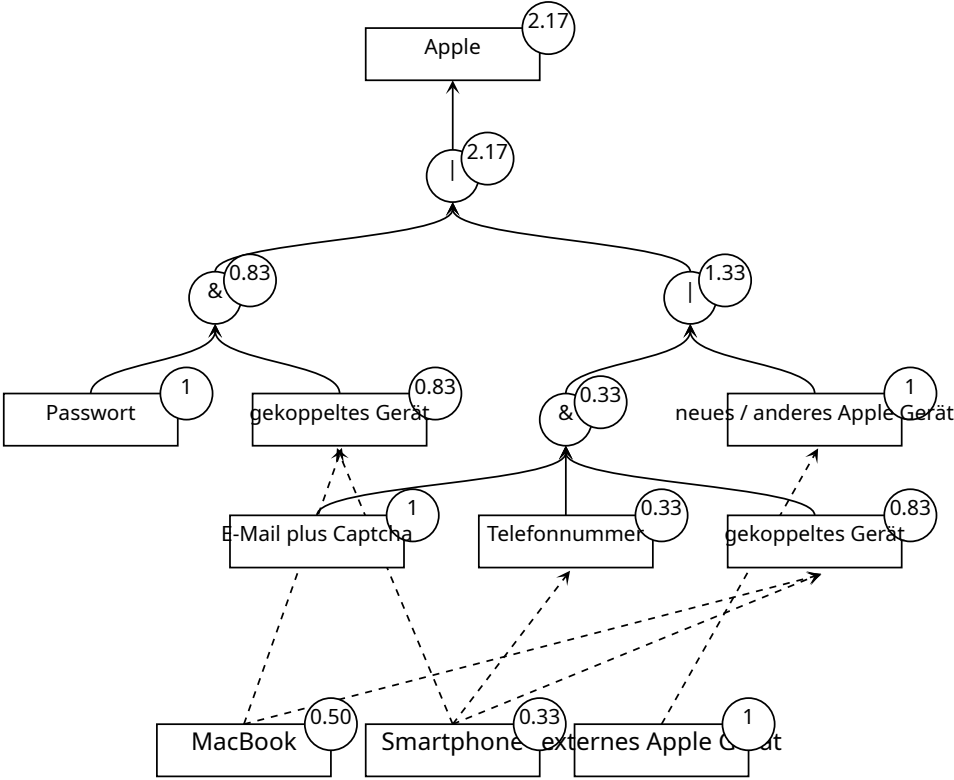


Abbildung A.1.: Zugänglichkeit Apple AAG 2. gek. Gerät

## A.2. Bilder aus Benutzerumfrage



Abbildung A.2.: Frage 5: Google

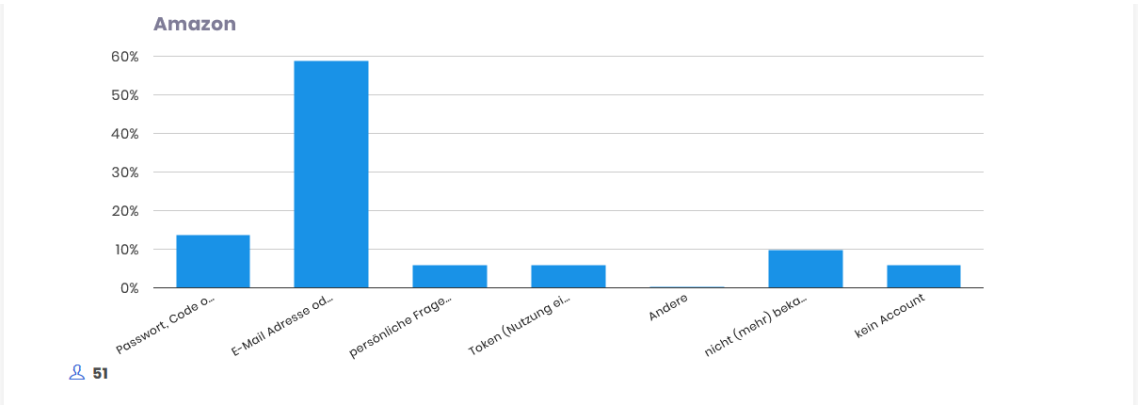


Abbildung A.3.: Frage 5: Amazon



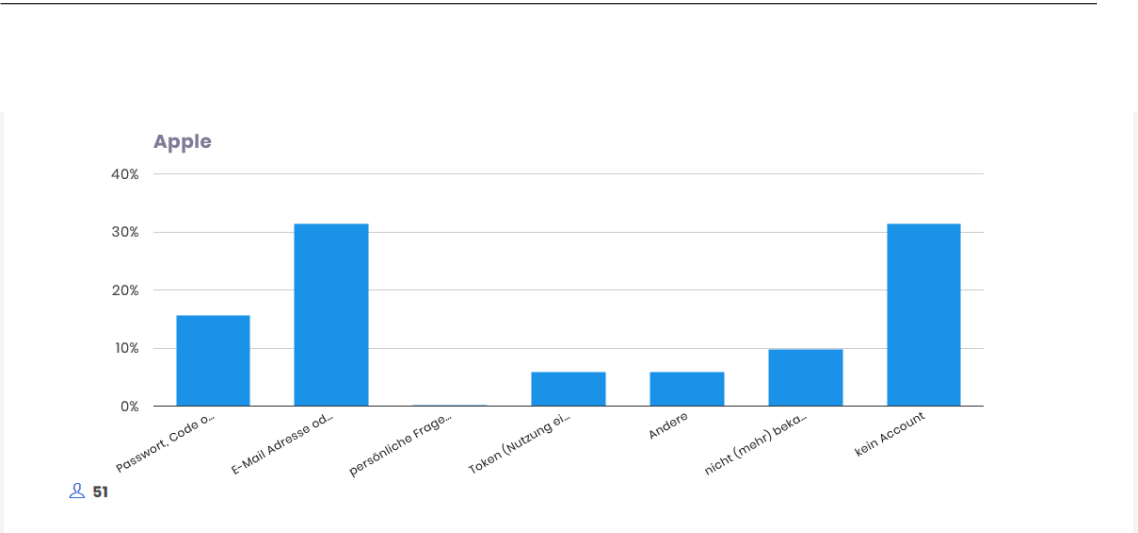


Abbildung A.4.: Frage 5: Apple

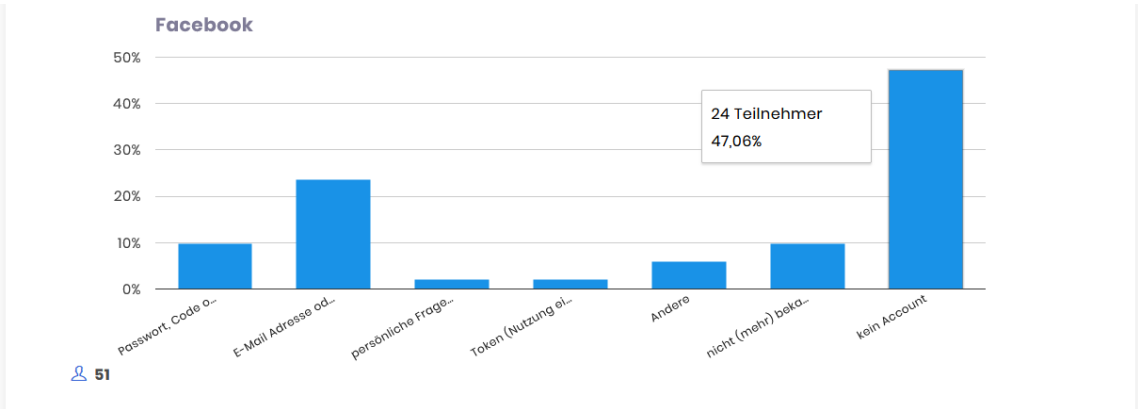


Abbildung A.5.: Frage 5: Facebook

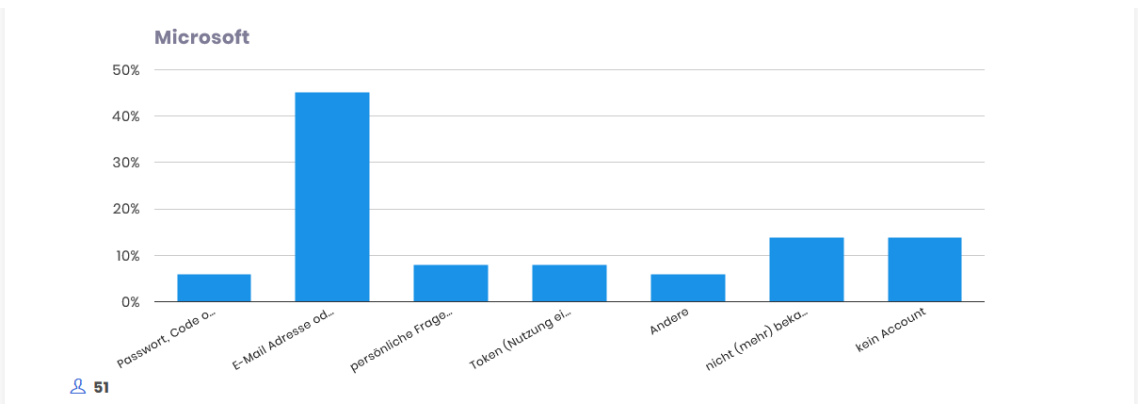


Abbildung A.6.: Frage 5: Microsoft

---

### **A.3. Rohdaten zur Benutzerumfrage**

Unter folgendem Link sind die Rohdaten der Umfrage einsehbar:

 Rohdaten Benutzerumfrage