LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Department “Institut für Informatik”
Lehr- und Forschungseinheit Medieninformatik
Prof. Dr. Heinrich Hußmann

Bachelorarbeit

Verbesserung von verbalem Echtzeitfeedback bei der Passwortselektion

Caroline Olsienkiewicz
caroline.olsi@gmail.com

Bearbeitungszeitraum: 13.07.2016 bis 30.11.2016
Betreuer: Tobias Seitz
Verantw. Hochschullehrer: Prof. Dr. Heinrich Hußmann

Zusammenfassung

Die Erstellung eines neuen Passwortes ist für die meisten Menschen keine leichte Aufgabe. Es sollte schwer zu erraten sein, meist bestimmten Richtlinien entsprechen und vor allem einfach zu merken sein. In den meisten Unternehmen beziehungsweise Organisationen kommt hinzu, dass die Mitarbeiter gezwungen werden, ihre Passwörter regelmäßig zu ändern, um die Sicherheit zu erhöhen. Dies kann zu einer generellen Frustration durch Überforderung der Mitarbeiter führen, was wiederum eine Gefährdung der Sicherheit zur Folge haben kann. Dieses Gefühl der Frustration senkt die Motivation und Kreativität der Mitarbeiter bei der Passworterstellung. Sie wählen schwächere Passwörter.
Es wurde eine qualitative Studie durchgeführt, um zu erfahren, wie solche Arbeitnehmer bei der Passwortselektion unterstützt werden können und die Ergebnisse analysiert. Diese Studie ergab, dass bereits ein einfaches Feedback-System genügt, um die User bei dieser Aufgabe zu unterstützen. In dieser Arbeit wurde ein solches einfaches System getestet und aufgrund der Ergebnisse dieser Studie auf den Nutzer eingehend verbessert. Es wurde erkannt, dass die Hauptprobleme der User primär bei der Ideenfindung für starke Passwörter sowie der Vorstellung ihrer Stärke liegen. Während sich frühere Arbeiten hauptsächlich auf die technischen Aspekte solcher Systeme konzentrierten, liegt der Fokus dieser Arbeit beim Nutzer. Das resultierende Programm stellt eine Unterstützung in diesen Punkten dar und erleichtert dem Anwender erfolgreich die Aufgabe der Passworterstellung.

Abstract

The creation of strong web-passwords represents a problem for most people. Password are supposed to be strong and not easy to guess. Additionally, in most cases it has to respect certain password-creation policies. And with all that, the user has also to be able to remember it.
Companies and organizations put an even greater burden on users by forcing them to change their work-passwords regularly. This can lead to frustration and coping-mechanisms as reuse of passwords and choosing the weakest password that still fulfills all the creation-policies, which puts the companies security at risk.
In order to identify how to assist users best with the critical task of password-creation, we conducted a qualitative online-study and used the Grounded Theory to analyze the results. It was shown that even a basic feedback-system can already be a significant help to the user. Such a basic system was tested and then improved by taking into account the users needs. While previous work focused primarily on the technical details of such programs, this work focusses on the user himself. It was shown that users would like to recieve help, especially regarding finding a suitable idea for a strong password and the users perception of password strength. The resulting feedback-system gives support where the user needs it and makes the creation process faster and easier for them.

Aufgabenstellung

BA - Verbesserung von verbalem Echtzeitfeedback bei der Passwortselektion

Um Informationen zu schützen werden weiterhin trotz bestehender Alternativen vorwiegend Passwörter eingesetzt, mit denen sich Nutzer an Systemen authentifizieren können. Jedoch, ist es für Nutzer nicht immer einfach sich starke Passwörter auszudenken, die gleichzeitig merkbar bleiben. Diesem Problem wurde in der Vergangenheit auf mehrfache Weise begegnet. Zum Beispiel helfen Passwort Manager dabei, eine Vielzahl von verschiedenen Passwörtern handhabbar zu machen. Viele Nutzer bestehen jedoch auf das Einprägen ihrer Zugangsdaten, damit sie die Passwörter jederzeit zur Verfügung haben und vor Angriffen auf die Passwortmanager geschützt sind. In diesem Fall wurde bisher versucht, den Nutzern Rückmeldungen auf Ihre Passwortwahl bereits während des Tippens zu geben. Dieser Ansatz zeigte vor allem bei der Selektion von Passwörtern bei wichtigen Zugängen Erfolg.

Mittlerweile existieren solche Feedbackmechanismen in verbaler und nonverbaler Form, wobei der nonverbale Ansatz deutlich häufiger anzutreffen ist, z.B. in Form von Passwort-Metern. Ein Grund hierfür könnte in der effektiven Formulierung des verbalen Feedbacks liegen. Diese Arbeit soll untersuchen, wie effektiv im Hinblick auf Nutzerempfinden verbales Feedback sein kann. Es soll ein bestehendes System getestet und ein Ansatz zur Lösung aufgezeigt werden. Hierbei soll der Fokus auf qualitativen Studien liegen, bei denen der Faktor Mensch die Hauptrolle spielt.

Zur Aufgabe gehören:
-Literraturrecherche zum Thema sichere und benutzbare Passwörter -Qualitative Vorstudie
-Erarbeitung eines Lösungsvorschlags
-Implementierung eines Systems, welches in einer Nutzerstudie verbales Feedback auf Passwörter in Echtzeit liefert
-Evaluierung des Lösungsvorschlags mit gängigen Methoden nutzerzentrierten Designs
-Schriftliche Ausarbeitung, wo das Projekt dokumentiert und die Ergebnisse beleuchtet werden.

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbstständig angefertigt, alle Zitate als solche kenntlich gemacht sowie alle benutzten Quellen und Hilfsmittel angegeben habe.

München, 29. November 2016

. . . . . .

Inhaltsverzeichnis

1 Einleitung

Heutzutage gibt es bereits eine Vielzahl neuartiger Mechanismen zur Nutzer-Authentifizierung. Beispiele hierfür sind physikalische Schlüssel wie Smart Cards oder Tokens, auf denen die Zugangsdaten gespeichert werden, sowie biometrische Schlüssel oder Ähnliches. Dennoch bleibt die Authentifizierung durch Passwörter die am meisten verwendete Methode. Sie ist kostengünstig und einfach zu implementieren. Von der Nutzerperspektive sieht das jedoch wie folgt aus. Es wird im Internet gesurft und mit der Zeit nach und nach werden mehr Benutzerkonten angelegt wie beispielsweise für E-Mail-Accounts, soziale Medien, oder Ähnliches. Für jedes dieser Konten wird nun ein Passwort benötigt. Ohne spezifisches Hintergrundwissen zur Passwortsicherheit wählt der User[1] ein Passwort, das er sich leicht merken kann und verwendet dieses auf anderen Seiten wieder, um sich möglichst wenige verschiedene Passwörter merken zu müssen. Oft wird bei einer Wiederverwendung das Passwort abgeändert [30]. Ein solches Passwort-Management kann zu einem Sicherheits-Problem führen. Simple Passwörter können bereits mithilfe eines handelsüblichen Computers innerhalb weniger Stunden erraten werden. Solche einfachen Passwörtern bestehen beispielsweise aus einem Wort, in welchem Buchstaben durch Ziffern oder Sonderzeichen ersetzt wurden [18]. Da mittlerweile als Nutzernamen häufig die E-Mail-Adresse verwendet wird, ermöglicht des Weiteren die Wiederverwendung von Passwörtern den Angreifern durch die Kenntnis eines Passwortes, mehrere Konten des gleichen Nutzernamens zu hacken [6]. Dieses Verhalten der User kann ausgenutzt werden, um unerlaubt an deren Daten zu gelangen und diese für gewinnbringende Zwecke zu verwenden. Um den Nutzer vor solchen Angriffen zu schützen, ist es wichtig, dieses Nutzer-Verhalten zu ändern.

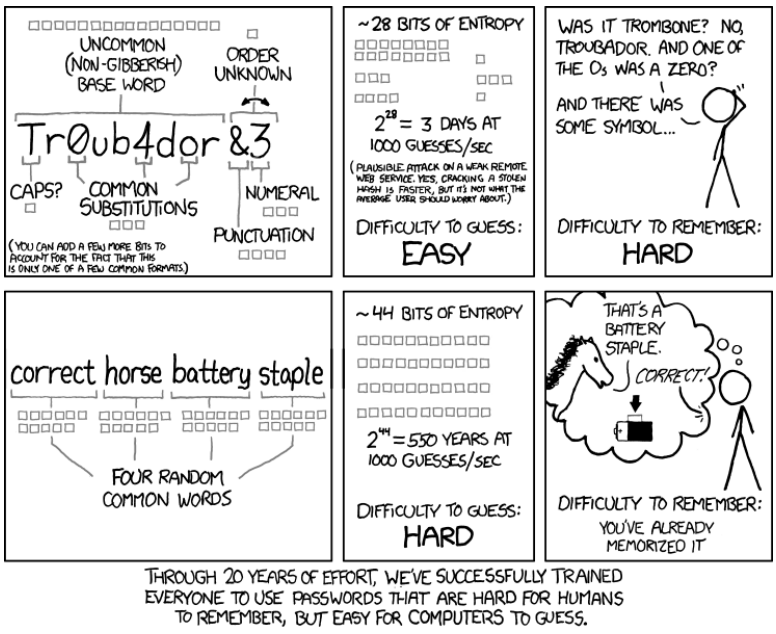

Abbildung 1.1: An diesem XKCD Comic wird gezeigt, dass viele Strategien zur Erstellung eines Passwortes nicht immer zu optimalen Ergebnissen führen. Es entstehen zwar relativ starke Passwörter, die Merkbarkeit und Usability wird dabei jedoch außer Acht gelassen [36].

Während die Vorhersehbarkeit der von Usern erstellten Passwörter oft dokumentiert wird und die am einfachsten zu Erratenden sogar in den Medien präsentiert werden [4, 33], wird vergleichsweise wenig Fokus darauf gelegt, den Nutzern zu helfen, starke Passwörter zu erstellen.

[1] Im weiteren Verlauf stehen die Bezeichnungen „der User“, „der Nutzer“, „der Anwender“, usw. stets für die männliche sowie die weibliche Person.

Sie werden mit dieser Aufgabe von den IT-Administratoren allein gelassen, da naiver Weise davon ausgegangen wird, dass die Nutzer sich eigenständig darum bemühen, ihre Daten gemäß zu schützen. Genau diese Aufgabe wächst und wird allerdings mit der wachsenden Anzahl an zu verwaltenden Passwörtern immer schwieriger zu bewältigen. Heutzutage besitzt jeder durchschnittlich 25 Online-Accounts, für die er bis zu acht mal am Tag ein Passwort eingeben muss [10]. Dies macht es nahezu unmöglich, für jeden Account ein mindestens gleich starkes und sicheres Passwort zu erfinden, das auch noch einfach zu merken ist. Bewältigungs-Strategien werden unausweichlich [30].
Der Mensch wird deshalb oft als Sicherheitsrisiko betrachtet. Von der Literatur wird ihm eine Nachlässigkeit und ein fehlendes Interesse unterstellt, wenn es um die Sicherheit eines Systems geht [1]. Er zeigt wenig Motivation, weshalb ihm strenge Richtlinien zur Passworterstellung vorgegeben werden sollen, um den System-Schutz zu gewährleisten [1, 2]. Diese Richtlinien konzentrieren sich oft auf nur eine einzige Form starker Passwörter: Drei bis vier verschiedene Zeichenklassen (Großbuchstaben, Kleinbuchstaben, Sonderzeichen, Ziffern) und eine Mindestlänge von acht Zeichen. Daraus resultierende Passwörter sind meist zwar stark doch eher schwer zu merken. Ist dies der richtige Weg? Es kommt die Frage auf, ob eine andere Herangehensweise nicht bessere Resultate erzeugen könnte: Passwörter die sowohl stark, als auch leichter zu merken sind. Abbildung 1.1 stellt eben diese Situation dar und liefert ein Beispiel, wie ein Passwort aussehen könnte, das sowohl sicher als auch merkbar ist. Ein Passwort, das lediglich aus drei aneinandergereihten Wörtern besteht, kann durch Eselsbrücken merkbar gemacht werden. Die Länge, der aufgereihten Wörter, bewirkt eine hohe Passwortstärke.
Zahlreiche Studien deuten darauf hin, dass die Nutzer grundsätzlich gewillt sind, sichere Passwörter zu erstellen [1, 2, 16, 17, 21]. Die strengen Vorgaben verursachen jedoch Frustration und nötigen die User zur Anwendung von Bewältigungs-Mechanismen. Es werden in vielen Fällen die einfachsten Passwörter erstellt, welche den Richtlinien entsprechen, zudem werden sie wiederverwendet und aufgeschrieben [30]. Dies führt oft zu sehr unsicheren Passwörtern und die Sicherheit des Systems wird tatsächlich gefährdet [1, 2, 16, 17, 21]. Diese Studien erläutern weiterhin, dass das Grundproblem nicht beim Anwender liegt. Der Fehler liegt darin, Letzteren bei der Erstellung solcher Richtlinien nicht mit einzubeziehen. Es sollte mehr auf den Nutzer eingegangen [9] und bei dieser Aufgabe der Passwort-Selektion unterstützt werden [27].
Adams und Sasse [17] zeigen zudem ein weiteres Problem auf: Zusätzlich zu bereits strikten Vorgaben wird in vielen Unternehmen beziehungsweise Organisationen eine regelmäßige Passwortänderung verlangt. Die Ideenfindung und Erstellung eines starken Passwortes wird zusätzlich dadurch erschwert, dass die Angestellten sich in regelmäßigen Abständen ein neues Passwort merken müssen. Dies führt zu Frustration unter den Mitarbeitern und Ausweich-Strategien wie beispielsweise die Wiederverwendung weniger Passwörter in einer Art Zyklus. Adams und Sasse stellen am Ende ihrer Arbeit Empfehlungen vor, was bei der Erstellung von Passwort-Richtlinien beachtet werden sollte, um unter Einbezug der User-Bedürfnisse die Sicherheit des Systems zu verstärken. Dem Nutzer sollte gezeigt werden, wie ein sicheres Passwort aussieht und anhand welcher Kriterien Eines erstellt werden kann, das leicht zu merken ist. Ur et al. [31] haben weiterhin herausgefunden, dass die Vorstellung der Nutzer von einem starken Passwort oft nicht der Realität entspricht. Sie erklären, dass ein gezieltes, datengesteuertes Feedback während der Passwort-Vergabe ein vielversprechender Ansatz ist, um dem User bei der richtigen Einschätzung der Stärke zu helfen.

Hier setzt diese Forschungsarbeit an. Es soll ein bereits bestehendes Feedback-System getestet und auf den Nutzer eingehend verbessert werden. Es existieren Internetseiten, die ein solches System zur Testung und Einschätzung der Stärke von Passwörtern anbieten [18, 20]. Doch die Bereitstellung solcher Systeme als Hilfe bei der Passwort-Selektion ist in der Praxis selten bis gar nicht zu finden [1, 2, 12]. Da die Situation in Unternehmen am schwerwiegendsten ist, konzentriert sich die Arbeit auf diesen bestimmten Anwendungsfall. Es soll ein System

konzipiert werden, das als grundlegende Hilfestellung verwendet werden kann, um den Nutzer bei der Erstellung und Ideenfindung von Passwörtern zu unterstützen, sowie seine Auffassung von starken Passwörtern richtigzustellen. Der Anwender steht dabei im Mittelpunkt der Forschung. Das Feedback des zu verbessernden Systems zielt darauf ab, Passwörter zu erstellen, die hauptsächlich durch ihre Länge stark werden. Es vermittelt, dass Stärke nicht ausschließlich von der Anzahl und Kombination verschiedener Zeichenklassen abhängt und welche Faktoren dazu beitragen, dass ein Passwort einem Angriff nicht standhält [35]. Auf dieser Grundlage baut das neue System auf und bindet Ansichten und Bedürfnisse der Nutzer mit ein. Während sich frühere Studien hauptsächlich auf überwiegend quantitative Daten fokussieren, wird in dieser Arbeit der Schwerpunkt auf das Empfinden des Users gesetzt. Dies wird durch die Erhebung qualitativer Daten gewährleistet. Durch zusätzliche quantitative Werte wird die Auswertung ergänzt.
Zu diesem Zweck wurde mithilfe einer Studie unter Anderem erforscht, welche unterstützenden Systeme bereits bestehen und wie diese Anwendung finden. Unter allen Studien-Teilnehmern gab es einzig Eine, die eine vergleichbare Art des direkten Feedback bei der Passworterstellung schilderte. Weiterhin wurde erneut gezeigt, dass die Nutzer direkte Hilfe benötigen. Ihnen fehlt das Wissen und die nötige Anregung, aus welchen Bestandteilen ein sicheres Passwort zusammengesetzt werden kann. Dieses auch noch so zu erstellen, dass es einfach zu merken ist, erscheint als die größte Schwierigkeit. Weiterhin bestätigen die Ergebnisse zum einen, dass zu strenge Richtlinien und vor allem die regelmäßige Passworterneuerungs-Maßnahmen den Anwender frustrieren und ihn dazu leiten, Passwörter wiederzuverwenden. Zum anderen wird erneut gezeigt, dass die Nutzer oftmals ein falsches Verständnis haben, bezüglich der Kriterien für ein starkes Passwort.
Die Arbeit besteht aus einer Vorstudie, in der die Herangehensweise der Hauptstudie in fünf persönlichen Interviews getestet und gefestigt wurde. Die Hauptstudie, eine qualitativ ausgelegte Online-Studie liefert die nötigen Ergebnisse, um das Feedback-System zu verbessern. Das daraus resultierende optimierte System wurde in einer anekdotisch aufgezogenen finalen Befragung der selben Teilnehmer wie in der Vorstudie getestet und positiv bewertet. Die Teilnehmer empfanden das vorgestellte Feedback-System als informativ und hilfreich bei der Erstellung eines starken Passwortes.

Die Arbeit ist in acht Teile gegliedert. Nach der Einleitung folgt die Erläuterung relevanter Studien und die Eingliederung der Arbeit in den aktuellen Forschungsstand.
Als nächstes wird das Forschungsthema näher erklärt und das Problem eingegrenzt. Da der Forschungsbereich breit gefächert ist und viele Ansatzmöglichkeiten bietet, wird der Anwendungsfall und die Motivation hierzu erläutert. Weiterhin werden der Aufbau und die Nutzeroberfläche des verwendeten Programms, sowie die Vorgehensweise der Vorstudie und ihre Ergebnisse geschildert.
Der vierte Teil der Arbeit präsentiert die Methodik der Hauptstudie. Außerdem wird beschrieben, wie die Teilnehmer rekrutiert wurden und der Aufbau des Fragebogens dargelegt. Abschließend wird die Prozedur der Studie und ihre Einschränkungen geschildert.
Die Darstellung der Ergebnisse erfolgt im fünften Teil. Dieser ist aufgeteilt in einen Abschnitt zu Demographie und Ausschlusskriterien der Teilnehmer, einen Abschnitt für die Präsentation der quantitativen und einen Weiteren für die der qualitativen Ergebnisse. Ein letzter Abschnitt beschreibt die Ergebnisse der Bewertung der Nutzererfahrung.
Im sechsten Teil werden die Ergebnisse interpretiert und ein Lösungsansatz vorgestellt. Die Erläuterung von Aufbau und Durchführung der Testung dieser Lösung erfolgt im siebten Teil. Im achten und abschließenden Teil dieser Arbeit werden alle Erkenntnisse zusammengefasst und ein Ausblick auf weitere Forschungsansätze gegeben.

2 Verwandte Arbeiten

In diesem Abschnitt wird ein Überblick über den aktuellen Forschungsstand gegeben und die Arbeit darin eingegliedert. Das Verhalten der Nutzer in Bezug auf Passwörter wurde bereits anhand einiger Studien erforscht und anschließend dokumentiert. Einen Teil dieser Arbeiten wird im Folgenden vorgestellt.

2.1 User-Verhalten im Umgang mit Passwörtern

In diesem Abschnitt werden die Arbeiten vorgestellt, die sich mit dem Verhalten von Nutzern bezüglich Passwörtern befassen.
Stobert und Biddle [30] haben durch eine qualitative Datenerhebung analysiert, wie User die Aufgabe bewältigen, ihre meist hohe Anzahl an Online-Konten mit den zugehörigen Passwörtern zu verwalten. Die Ergebnisse der insgesamt 27 Interviews führten zu dem Schluss, dass eine Art Lebenszyklus für Passwörter existiert, der eine Reihe progressiver Stadien umfasst, die ein Passwort durchläuft. Demnach werden Passwörter erstellt, dann einem Online-Konto zugewiesen und anschließend niedergeschrieben oder auswendig gelernt. Damit leben die Nutzer eine Weile, bis sie die Passwörter vergessen. Zur Erstellung eines neuen Passwortes, werden alte Passwörter wiederverwendet oder angepasst und der Zyklus wird fortgefahren. Dieser Zyklus wird in Abbildung 2.1 dargestellt.

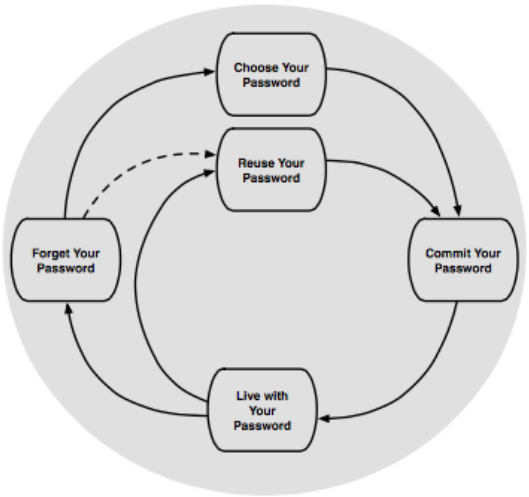

Abbildung 2.1: Passwort-Lebens-Zyklus nach Stobert und Biddle [30].

Die Arbeit zeigt, dass Nutzer nicht grundsätzlich alle Richtlinien zur Passworterstellung ablehnen und boykottieren, sondern lediglich versuchen mit den komplexen Vorgaben zurecht zu kommen. Dem soll bereits durch geringe Aufklärung über Passwort-Stärke und Sicherheitsfaktoren entgegengesteuert werden können.

Florêncio und Herley [10] haben die Web-Passwort-Gewohnheiten anhand einer großangelegten Online-Studie analysiert. Mithilfe einer Browser-Erweiterung, die von den Teilnehmern installiert wurde, konnte beobachtet werden, dass jeder Nutzer durchschnittlich 6,5 Passwörter besitzt, die jeweils für 3,9 Seiten verwendet werden. Insgesamt verwaltet jeder Teilnehmer ungefähr 25 Konten und tippt durchschnittlich acht mal am Tag ein Passwort ein. Es wurde weiterhin festgestellt, dass schwache Passwörter häufiger wiederverwendet werden. Zusätzlich führte die Studie zu der Erkenntnis, dass User sehr oft ihre Zugangsdaten vergessen und insgesamt

0,4% aller Anwender weltweit jährlich Opfer eines Phishing-Angriffs werden.
Ähnliche Ergebnisse lieferte eine Studie von Hayashi und Hong [15]. Es haben 20 Teilnehmer zwei Wochen lang Tagebuch über ihr Verhalten bezüglich Passwörtern geführt. Hierbei wurde zusätzlich erkannt, dass 60,3% der Testpersonen keine Hilfsmittel, wie beispielsweise Passwort-Manager oder Ähnliches verwenden und 84,3% aller Logins am eigenen Computer geschehen.

Hoonakker, Bornoe und Carayon [16] wollten mehr Informationen über das genaue Verhalten von Nutzern in Bezug auf die Computer- und Informations-Sicherheit sammeln und haben zu diesem Zweck zunächst Fokusgruppen organisiert und darauf aufbauend einen Fragebogen erstellt. Die Arbeit zeigt, dass nur sehr wenige Nutzer die bestmöglichen Passwort-Verfahrensweisen anwenden und tatsächlich starke Passwörter erstellen. Dieser kleine Teil der Befragten versuchte weder die strengen Richtlinien zu umgehen, noch durch unsicheres Verhalten, wie beispielsweise das Aufschreiben der Passwörter, mit ihnen umzugehen. Des Weiteren bestätigt diese Studie, dass die Nutzer prinzipiell gewillt sind, die strikten Passwort-Vorgaben einzuhalten, jedoch meist nicht in der Lage sind, sich daran zu halten.

In einer anderen Studie zeigen Herley und Florêncio [12] wie man ein großes Portfolio von Passwörtern am besten verwaltet. Sie stellen ein Modell vor, welches anhand einer realistischen Vorstellung von Angriffen, sowie einer objektiven Funktion über Verlust und Nutzer-Aufwand das Passwort-Management erleichtert. Es wurde mithilfe einer Formel errechnet, dass die Wiederverwendung von Passwörtern den Erinnerungsaufwand um ein Fünffaches verringert und es deshalb in großem Maße praktiziert wird. Das Modell beschreibt auf Grundlage dieser Ergebnisse eine Wiederverwendung, die durch geschicktes Gruppieren der Konten nach Wichtigkeit den Aufwand dort minimiert, wo er nicht unbedingt notwendig ist. Das bedeutet, je nach Sicherheitseinschätzung eines Kontos wird ein höherer oder geringerer Aufwand bei der Passworterstellung betrieben. Sie sagen außerdem, dass das Niederschreiben der Passwörter eine akzeptable Bewältigungsstrategie ist, wenn es korrekt ausgeführt wird.
In einer weiteren Arbeit zeigen sie [11], dass starke Passwörter gegen die meisten Arten von Angriffen machtlos sind. Sie bieten lediglich Schutz gegen Angriffe, in denen der Hacker versucht, das Passwort zu erraten. Man sollte daher eher Wert auf starke User-Identifikationsnummern (sogenannten „User-IDs“) setzen.

Die Wiederverwendung stellt einen großen Aspekt des Nutzer-Verhaltens dar. Das et al. [8] untersuchen in einer ihrer Arbeiten, was die Wiederverwendung von Passwörtern für Auswirkungen mit sich bringt. Sie haben erforscht, wie ein Angreifer ein bekanntes Passwort dazu verwenden kann, die Passwörter des gleichen Nutzers für andere Konten zu erraten und so den ersten Inter-Webseiten-Passwort-Errate-Algorithmus erstellt. Dieser schafft es, 30% der abgeänderten Passwörter innerhalb von 100 Versuchen zu erraten. Dies ist fast das doppelte von dem, was bereits existierende Algorithmen schaffen. Die Grundlage für den Algorithmus boten 100000 veröffentlichte Passwörter von elf verschiedenen Seiten.
Gemeinsam mit Herley stellt Bonneau in einer Arbeit die Geschichte des Passwortes dar [6]. Es wird ein Überblick über die verschiedenen Angriffsarten gegeben und wie man sich dagegen schützen kann und sollte.
Es werden hierfür Methoden empfohlen, wie eine Authentifizierung anhand weiterer Informationen wie beispielsweise die IP-Adresse des persönlichen Computers oder dessen Standort. Diese bieten Möglichkeiten einer zusätzlichen Identitätsbestätigung und somit mehr Sicherheit.

2.2 Richtlinien bei der Passworterstellung und ihre Auswirkungen

Eine Vorgabe von Richtlinien bei der Passworterstellung ist mittlerweile weit verbreitet. Sie werden den Anwendern vorgeschrieben, um starke und sichere Passwörter zu erzeugen. In diesem Abschnitt werden Arbeiten vorgestellt, die sich mit aus strikten Richtlinien resultierenden Passwörtern befassen und wie die Nutzer mit den Vorgaben zurecht kommen.

In einer 1997 von Adams, Sasse und Lunt durchgeführten Studie [2] wurde untersucht, wie die Passworterstellungs-Methoden von den Nutzern empfunden werden. In dem zweiteiligen Ablauf wurden zunächst 139 Mitarbeiter einer Firma beziehungsweise Internet-Nutzer aus verschiedenen Ländern zu ihrem Verhalten bezüglich Passwörtern befragt und welche Probleme bei der Passworterstellung entstehen. Im zweiten Teil wurde der Umgang mit Passwörtern in 30 Interviews mit Mitarbeitern zweier Firmen in Erfahrung gebracht. Dabei ging hervor, dass die meisten Probleme der Teilnehmer auf die hohe Anzahl ihrer Passwörter und der Häufigkeit ihrer Wiederverwendung zurückzuführen sind. Ob die Nutzer sich auf die Sicherheits-Maßnahmen einlassen, hängt von ihrer Einschätzung der zu schützenden Sicherheitsstufe ab. Zusätzlich müssen diese Maßnahmen vereinbar sein mit ihren Arbeits-Praktiken. Obwohl die vorgegebenen Methoden die Systeme sicherer machen sollten, bewirken sie in der Realität oft das Gegenteil. Durch zu hohe Anforderungen an die Nutzer, fühlen sich diese dazu gezwungen, die Richtlinien zu umgehen oder so anzuwenden, dass sie zurecht kommen. Dies verursacht oft unsichere Passwörter. Des Weiteren zeigt die Studie, dass Nutzer, die ihr Passwort oft ändern müssen, häufiger unsicherere Passwörter erstellen als Andere und diese ebenfalls häufiger aufschreiben.
In einer weiteren Arbeit berichten Adams und Sasse [1] über weitere Ergebnisse dieser selben Studie. Es wird gesagt, dass für die Sicherheits-Richtlinien ein nutzerorientiertes Design unbedingt notwendig ist, um die Sicherheit eines Systems tatsächlich gewährleisten zu können.

Eine weitere Tagebuch-Studie wurde von Inglesant und Sasse durchgeführt [17]. Sie konzentrierte sich auf die Situation in Firmen und Organisationen. Die Autoren wollten testen, wie Passwörter im Arbeitsumfeld verwendet werden und den Effekt erfassen, welchen die Sicherheitsvorschriften auf die tägliche Anwendung hat. Sie hat erneut ergeben, dass die Nutzer im Allgemeinen darauf bedacht sind, sichere Passwörter zu erstellen, jedoch von den Sicherheitsanforderungen der Firmen gänzlich überfordert werden. Dies führt zu Unproduktivität in Bezug auf die Passwortselektion und wirkt sich negativ auf die Firmensicherheit aus.
Was die Nutzer über Passwort-Vorgaben denken und wie sie mit ihnen zurecht kommen behandelten Shay und Komanduri [29], sowie Cranor et al. [21] in zwei ähnlichen Studien. Zum einen wurde erkannt, dass die Vorgabe von lediglich einer Mindestlänge von 16 Zeichen die effektivste und für Nutzer angenehmste Richtlinie darstellt. Zum anderen bestätigen beide Studien, dass zu strenge Vorgaben zur Passworterstellung bei den Nutzern Frustration und Missmut hervorruft.
Weir et al. [34] haben die tatsächliche Effizienz dieser strikten Richtlinien getestet und gezeigt, dass die meisten Richtlinien schutzlos gegenüber Online-Attacken bleiben. Dies entspringt der Tatsache, dass die Nutzer versuchen mit diesen Richtlinien zurecht zu kommen und die einfachsten Passwörter wählen, die dennoch den Vorgaben entsprechen.

In einer anderen Studie konzentrieren sich Shay et al. [28] ebenfalls auf die Stärke der Passwörter, welche solche Passwort-Vorgaben hervorrufen und vergleichen diese. Sie wollten herausfinden, ob lange Passwörter sicher sein können und beweisen dies anhand eines Online-Experiments mit über 8000 Teilnehmern. Sie zeigen, dass Passwörter mit einer Länge von 20 Zeichen ebenso starke Passwörter erzielen, wie Passwörter mit 16 Zeichen, bestehend aus drei verschiedenen Zeichenklassen und die klassische Variante der Mindestlänge von acht Zeichen, bestehend aus vier verschiedenen Zeichenklassen. Letztere sind jedoch weitaus umständlicher in der Anwendung.

Eine weitere Form der Vorgabe stellt in vielen Fällen die regelmäßige Passworterneuerung dar. Diese findet hauptsächlich in Firmen und Organisationen Anwendung, um die Sicherheit ihrer Daten zu erzwingen. Zhang et al. [37] haben diese Technik erforscht und heraus gearbeitet, dass Angreifer mit der Kenntnis früherer Passwörter mindestens 41% der modifizierten Passwörter erraten können, auch wenn diese an sich stark sind.

2.3 Nutzerverständnis der Passwortstärke

Solche Passwort-Richtlinien führen oft nicht zu sicheren Passwörtern. Eben beschriebene Arbeiten zeigen einige Ursachen hierfür. Weitere Gründe liegen oft in der Auffassung der Nutzer, was ein starkes beziehungsweise schwaches Passwort überhaupt ausmacht. Im Folgenden werden Studien vorgestellt, die sich hiermit befassen.

Mithilfe einer Online-Studie mit 165 Teilnehmern haben Ur et al. getestet [31], inwieweit die Vorstellungen der Teilnehmer von starken Passwörtern der Realität entsprechen. Es wurde deutlich, dass die Nutzer viele unsichere Passwörter nicht identifizieren konnten und es ihnen unter Anderem nicht bewusst war, dass das Anhängen von Zahlen am Ende des Passwortes die Sicherheit nicht mehr verstärkt, als angehängte Buchstaben.

Um die Vorstellungen der Nutzer von starken Passwörtern richtigzustellen, wird oft versucht, mehr Wissen über Sicherheit zu verbreiten. Loutfi und Jøsang [23] haben das Passwortverhalten der Personen getestet, die dafür plädieren, die User mehr über die Passwort-Sicherheit aufzuklären und bewiesen, dass kognitives Wissen darüber in der Praxis nicht immer zu sicheren und praktischen Passwörtern führt. In diesem Fall waren diese Personen IT-Experten aus verschiedenen Unternehmen. Es wird gezeigt, dass zusätzliche Aufklärungsversuche von den Nutzern teilweise nicht aufgenommen werden kann aufgrund einer bereits existierenden Informationsüberflutung.
Was tatsächlich Wirkung zeigen und auf Dauer stärkere Passwörter hervorrufen kann, wird im Folgenden dargestellt.

2.4 Hilfestellung bei der Passworterstellung

Dieser Abschnitt befasst sich mit der Erleichterung der Passworterstellung durch aktive Hilfestellung während der Passwortvergabe. Er stellt gleichzeitig die für diese Forschungsarbeit wichtigsten Aspekte dar und bietet die Grundlage für die in dieser Arbeit durchgeführten Studien.

Wie eine Hilfestellung bei der Passworterstellung geleistet werden kann, behandeln Shay et al. [27] in einer weiteren Arbeit. Es wurde untersucht, welchen Einfluss Feedback und Anleitung bei der Passwortselektion auf die Usability und Sicherheit hat. Die Arbeit zeigt, dass gezieltes Feedback über die Inhalte eines starken Passwortes während der Passworterstellung zu starken Passwörtern und weniger Fehlversuchen führt. Werden die Teilnehmer Schritt für Schritt durch den Erstellungsprozess begleitet, führt dies zwar zu einer Verbesserung der Usability, ruft jedoch schwächere Passwörter hervor.
Eine Erleichterung durch Feedback in Form einer Stärke-Anzeige wird in einer Studie von Ur et al. erforscht [32]. Zu diesem Zweck haben sie 14 verschiedene Arten der Darstellung der Passwort-Stärke getestet und die Ergebnisse verglichen. Dabei wurde gezeigt, dass die sogenannten „Passwort-Meter“, basierend auf strengen Vorgaben, die stärksten Passwörter hervorrufen können, jedoch zu strikte Vorgaben den Nutzer frustrieren. Wichtig bei der Wahl der Anzeige ist außerdem eine visuelle Darstellung.
Einen weiteren Faktor bei der Erstellung von Richtlinien zur Passwortvergabe stellen die Charak-

tereigenschaften des Nutzers dar. Egelman und Peer [9] haben das bekannte „Big-5-Modell“ in Frage gestellt und legen nahe, dass die Charakter-Eigenschaften zur Entscheidungsfindung eine weitaus größere Rolle spielt.

Die Relevanz von effektiven Passwort-Vorgaben wird immer wieder betont. Eine auf den User abgestimmte Vorgabe bei der Passworterstellung kann die resultierende Stärke positiv beeinflussen. Hierzu schlagen Schechter et al. [26] ein Richtlinien-System vor, das dem Nutzer alle möglichen Arten von Passwörtern erlaubt, solange sie nicht zu den Passwörtern zählen, die durchschnittlich am häufigsten gewählt werden. Dies führte zu einer Verbesserung der Usability. Welches zu diesen Passwörtern gehört, errechnet eine Art „Orakel“, das mithilfe einer existierenden Datenstruktur namens „count-min sketch“ erstellt wurde.
Ebenfalls für die Verbesserung der Usability stellen Keith et al. [19] das Prinzip der Passphrasen vor. Diese besitzen eine einzige Vorgabe, nämlich eine Mindestlänge von 15 Zeichen. Es wurde gezeigt, dass die Nutzer diese Art von Passwörtern generell als schwieriger anzuwenden empfinden. Dies liegt hauptsächlich an ihrer Länge und den deshalb häufiger auftretenden Tippfehlern. Passphrasen sind jedoch insgesamt nicht schwerer zu merken als typische Passwörter. Zviran und Haga [38] haben zu diesem Thema das Konzept der kognitiven Passwörter untersucht. Diese Art der Authentifizierung besteht aus der Beantwortung zufällig gewählter Fragen, für welche ein Nutzer im Vorhinein Antworten gegeben hat. Die Ergebnisse zeigen, dass sich nach einer Zeitspanne von drei Monaten über 80% der Teilnehmer an alle Antworten erinnern konnten. Lediglich 23% dieser Fragen konnten von Verwandten und engen Freunden der Testpersonen richtig beantwortet werden.

Diese Forschungsarbeit baut auf den Ergebnissen dieser Studien auf und setzt die Forschung fort. Es wurde bereits viel zu dem Thema User und Passwörter erforscht, jedoch wurde wenig auf den Nutzer selbst eingegangen. Einige dieser Studien [27, 17, 31, 1, 2, 32] stellen fest, dass es wichtig für die Sicherheit ist, den Nutzer mit einzubeziehen und ihn bei der Passwortwahl zu unterstützen, liefern jedoch keinen konkreten Lösungsvorschlag. Genau diesen Lösungsvorschlag versucht diese Arbeit aufzuzeigen. Sie untersucht die Bedürfnisse der Nutzer bezüglich Hilfestellungen bei der Erstellung von Passwörtern mithilfe eines verbalen Echtzeitfeedbacks. Sie füllt somit die Lücke zwischen den bereits erforschten technischen Aspekten dieses Forschungsbereiches und den tatsächlichen Wünschen der Nutzer. Dies wird im nächsten Abschnitt präzisiert und näher erläutert.

3 Problemdarstellung

Der Forschungsbereich zur Erleichterung in Sachen Passworterstellung für Nutzer bei sicherheits- und datenschutzrelevanten Fragen ist breit gefächert und bietet viele verschiedene Anlaufstellen. Diese Arbeit beschränkt sich auf die Erleichterung der Passwortfindung durch ein verbales Feedback-System.
Im folgenden Abschnitt wird das Problem dieser Arbeit erläutert und ein Konzept vorgestellt.

3.1 Definition und Eingrenzung des Problems

Die Benutzererfahrung, allgemein bekannt als „User Experience“, ist bei der Neuerstellung von Passwörtern grundsätzlich schlecht [17]. Durch zu strikte Richtlinien bei der Passwortselektion werden die Angestellten unproduktiv und wählen oft das schwächste Passwort, das den Vorgaben entspricht und somit akzeptiert wird. Anforderungen können beispielsweise eine Mindestanzahl an Zeichen sein, die Vorgabe, mindestens ein Sonderzeichen zu verwenden oder Ähnliches. Diese Nutzererfahrung verschlechtert sich, je öfter man das Passwort ändern muss und je strenger die Vorgaben sind. Im privaten Gebrauch - Passwörter, die für private Konten wie E-Mail-Accounts, Soziale Medien oder Shopping-Seiten - ist man meist relativ frei in Bezug auf die regelmäßige Änderung seiner Passwörter. In den meisten Firmen oder Institutionen ist es jedoch üblich, eine regelmäßige Passworterneuerung vorzuschreiben [17]. Da die Vorgaben für diese Firmen-Passwörter meist ziemlich streng sind, führt dies zu Frustration und zwingt die Arbeitnehmer zu Bewältigungsmechanismen wie das Notieren der Passwörter auf Notiz-Zetteln oder die Wiederverwendung einer bestimmten Anzahl an Passwörtern [17].
Hier setzt diese Forschungsarbeit an. Sie konzentriert sich auf die Situation in Firmen und Institutionen. Es wurde in diesem Bereich bislang wenig Forschung betrieben und es besteht ein breites Feld an möglichen Testpersonen. Es wird angestrebt, die Benutzererfahrung der Mitarbeiter zu verbessern, indem ein schon existierendes Feedback-System optimiert wird, das die Angestellten bei der Passwortvergabe unterstützt. Dieses System ist die frei verfügbare Bibliothek „zxcvbn“. Dieses System eignet sich deshalb für diese Arbeit, da es eine Vielzahl an Informationen über ein eingegebenes Passwort liefert und Entscheidungs-Möglichkeiten anbietet, welche Rückmeldungen herausgefiltert werden sollen. Im nächsten Gliederungsunterpunkt wird eine genaue Beschreibung dieses Programms gegeben.

3.2 zxcvbn

Das System zxcvbn ist eine frei verfügbare Bibliothek, mit der sich die Stärke von Passwörtern abschätzen lässt. Es bietet dem Benutzer eine Reihe von Informationen über eine eingegebene Zeichenfolge. Ziel ist es, dem Nutzer mitzuteilen, wann ein gewähltes Passwort stark ist und andernfalls Vorschläge zu geben, wie es zu verbessern ist. Diese Bibliothek implementiert einen neuartigen Algorithmus, der auf der Erkennung von abgeänderten Passwörtern und weiteren Mustern basiert [35].
Zum Zwecke dieser Arbeit werden nicht alle der verfügbaren Funktionen in Gebrauch genommen. Der Nutzer soll zum einen nicht mit Informationen überhäuft werden. Es soll vermieden werden, dass er sich aufgrund zu vieler Angaben nicht auf alles im Einzelnen konzentrieren kann. Zum anderen dient die Forschungsarbeit der Verbesserung eines schon existierenden verbalen Feedback-Systems, was damit erreicht wird, eine Grundbasis an Informationen zu bieten, die im Nachhinein erweitert und verbessert wird. Im Folgenden werden die verwendeten Funktionen beschrieben.
Das Programm liefert während der Eingabe eines Passwortes, Hinweise und Tipps in Form von Sätzen zu diesem Passwort. Ein solcher Satz kann zum Beispiel lauten „Füge noch ein paar Wörter hinzu. Je ungebräuchlicher desto besser.“

Ferner beinhaltet das Programm ein englisches Wörterbuch, mit dem die Eingaben abgeglichen werden. Wird ein englisches Wort als Passwort eingegeben, welches in diesem Wörterbuch enthalten ist, wird eine Warnung in Form eines Satzes angezeigt, die besagt, dass das eingegebene Wort zu den am häufigsten verwendeten Passwörtern zählt. Eine solche Warnung kann sein: „Das ist ein häufig verwendetes Passwort."
Da das System aus dem englischen Sprachraum stammt, schien es sinnvoll, es für diesen Einsatzzweck zu übersetzen. Die Studie würde im deutschsprachigen Raum stattfinden, weshalb eine eventuelle Sprachbarriere ausgeschlossen werden sollte. Dies bedeutet, es wurden alle Hinweise und Warnungen in die deutsche Sprache umgewandelt, und zusätzlich ein deutsches Wörterbuch hinzugefügt. So werden dieselben Warnungen ebenfalls angezeigt, wenn das Passwort einem deutschen Wort entspricht. Diese Hinweise und Warnungen verändern sich, je mehr Zeichen eingetippt werden.
Zusätzlich wird durchgehend die Passwortstärke berechnet und bezieht sich immer auf die aktuelle Zeichenfolge. Die Berechnungen basieren auf der minimalen Anzahl an Versuchen, die man bräuchte, um das Passwort zu erraten. Die Berechnung dieser Anzahl wiederum stellt sich aus verschiedenen Komponenten zusammen und wird je nach Art des Passwortes unterschieden. Steht beispielsweise ein eingegebenes Passwort an Stelle 55 der am meisten verwendeten Passwörter, so berechnet das System die minimale Anzahl an Rate-Versuchen als 55. Die Verwendung verschiedener Zeichenklassen oder das Eingeben eines spiegelverkehrten Wortes erweitert jeweils diese Zahl um den Faktor 2. Dieser ergibt sich daraus, dass ein Angreifer beispielsweise bei einem spiegelverkehrt eingegebenen Passwort zwei Versuche bräuchte: einen für das Wort in korrekter Form und einen für das Wort rückwärts gelesen.
Das System liefert darüber hinaus noch einige weitere Informationen. Zum einen liefert es die Zeit in Sekunden, die ein Angreifer bräuchte, um das Passwort mit der sogenannten Methode der rohen Gewalt (besser bekannt als „Brute-Force Methode") zu erraten. Bei dieser Methode testet der Angreifer zu einer bekannten Kennung eine große Anzahl an möglichen Passwörtern. Darunter fallen alle bekannten Wörter aus dem oben genannten Wörterbüchern sowie Variationen und geringfügige Erweiterungen davon. Erweiterungen können angehängte Ziffern, Sonderzeichen oder Buchstaben sein. Weiterhin liefert es die Anzahl der Versuche, die der Angreifer benötigen würde und die Zeit als eine grobe Einschätzung wie schnell das Passwort geknackt werden kann. Die Methode der rohen Gewalt ist eine der einzigen Arten von Angriffen, gegen die ein Passwort tatsächlich standhalten kann. [6]

In einer Vorstudie sollte dieses System erstmals getestet werden. Diese in kleinem Rahmen abgehaltenen persönlichen Interviews sollten Aufschluss darüber geben, ob das System eine passende Grundlage für eine Verbesserung darstellt und inwieweit Möglichkeiten der Verbesserungen existieren.
Um das System im Rahmen dieser ersten Studie testen zu lassen, wurde es in eine Internetseite eingebettet. Diese Internetseite stellt die Benutzeroberfläche dar. Im nächsten Abschnitt wird der Aufbau dieser Seite geschildert.

3.3 HTML-Seite als Nutzeroberfläche für die Studie

Die Grundlage für diese Vorstudie bietet eine Oberfläche in Form einer Webseite. Diese wurde mit HTML5 erstellt und die deutsche Version der Bibliothek zxcvbn darin implementiert. Es werden während einer Passworteingabe, die Hinweise in Form von Sätzen angezeigt sowie die Warnungen und die Passwortstärke als eine Zahl von Null bis Vier. Der Fokus der Arbeit liegt auf dem verbalen Feedback-System, weshalb genau diese drei Informationen grundlegend sind. Dies soll eine grundlegende Hilfeleistung stellen, um die Passwortvergabe zu erleichtern. Die Internetseite ist schlicht und simpel gestaltet. Der Nutzer sollte nicht von zu viel unnötigem Design, Bildern oder Sonstigem abgelenkt werden, sondern sich auf das Wesentliche, nämlich die Erstellung

des Passwortes und die Hilfestellungen konzentrieren können. Die Seite besteht deshalb aus vier Hauptbereichen: der Überschrift; einem Einleitungstext, um den Studien-Teilnehmern zu erklären, was zu tun ist; dem Eingabetextfeld, in welches das Passwort eingegeben werden soll; und dem Ausgabebereich, in dem die Hinweise und Warnungen sowie die Passwortstärke als Zahl erscheinen, sobald man mit der Eingabe beginnt. Ein Bild dieser Seite zeigt Abbildung 3.1.

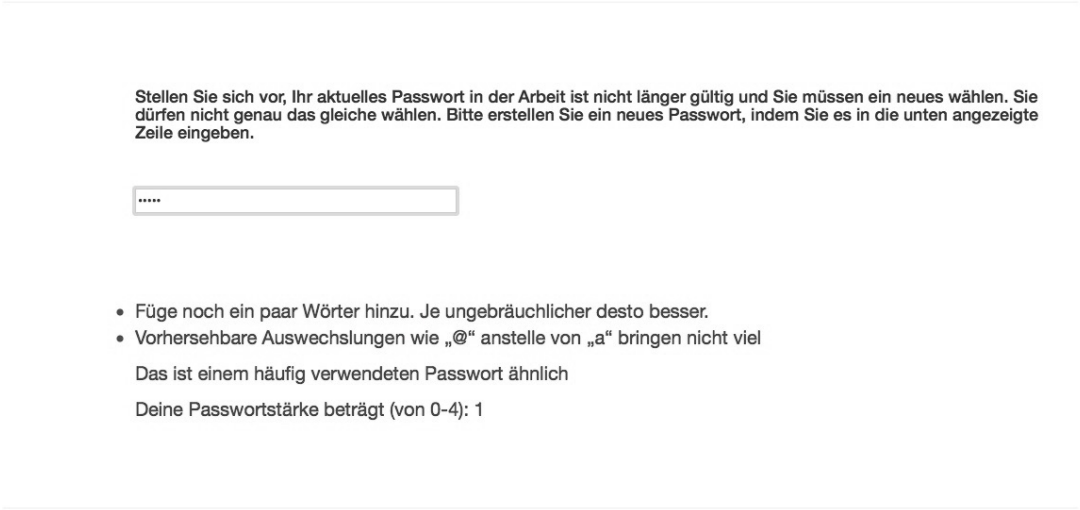

Abbildung 3.1: Aussehen der Internetseite für die Vorstudie

3.4 Vorstudie als erster Test für die Hauptstudie

Um die Herangehensweise an meine Studie zu testen und zu definieren, wurde im Vorhinein eine kurze Studie durchgeführt. Als nächstes wird der Ablauf dieser Studie beschrieben.

3.4.1 Beschreibung der Testpersonen und Ablauf der Befragung

Die Vorstudie bestand aus fünf Interviews mit Personen aus möglichst verschiedenen Beschäftigungsbereichen. Nielsen hat gezeigt, dass diese geringe Anzahl bei einer Testung der Usability von Systemen die besten Ergebnisse liefert [24].
Diese Vorstudie sollte dazu dienen, noch existierende Fehler und Schwachstellen im Konzept und der Internetseite zu erkennen und zu beheben. Des Weiteren sollte ein erster Eindruck darüber erlangt werden, ob die geplante Hauptstudie die erwünschten Ergebnisse liefern kann, um das Feedback-System verbessern zu können. Ziel war es, die Grundlagen für die Hauptstudie zu untersuchen: Wird die Webseite verstanden, wird die Aufgabenstellung verstanden und kann mit dieser Aufgabenstellung das richtige herausgefunden werden. Die Voraussetzungen für eine Befragung waren Folgende. Sie sollten sich nicht im Vorhinein mit dem Forschungsthema befasst haben und weiterhin in ihrer Arbeit ein Passwort verwenden, das sie regelmäßig ändern müssen. Insgesamt waren es fünf Personen (drei männlich, zwei weiblich, im Alter zwischen 26 und 53, Median = 46). Es war wichtig, möglichst verschiedene Beschäftigungsbereiche zu erreichen, um zu erkennen, wie die Passwort-Angelegenheiten in den verschiedenen Firmen geregelt sind (die Teilnehmer arbeiten im Lehrwesen, der Automobilbranche, der Fahrwerksentwicklung, der IT-Anwendungsentwicklung und im Bauwesen). Indem man erkennt, welche Gemeinsamkeiten es gibt und wo die Unterschiede liegen, ermöglicht dies, die spätere Hauptstudie darauf auszulegen.

Auch war es wichtig zu beobachten, wie sich jüngere Menschen im Gegensatz zu Älteren verhalten. Das könnte eventuelle Auswirkungen auf beispielsweise die Formulierung der Sätze des Feedbacks oder die Art der Anzeigen haben.
Den Teilnehmern wurden zunächst einige wenige Fragen als Einstieg gestellt, in denen ihre demographischen Angaben erhoben und ihre Situation in der Arbeit bezüglich Passwörtern in Erfahrung gebracht wurden. Als nächstes wurden sie gebeten, sich vorzustellen, sie seien in der Arbeit und es sei wieder an der Zeit, ihr Passwort zu erneuern. Dieses sollten sie auf der angelegten Internetseite erstellen. Im letzten Schritt wurden die Testpersonen zu dieser Aktion befragt, um herauszufinden, wie es ihnen ergangen ist und um das Programm zu evaluieren. Es sollte in Erfahrung gebracht werden, wie das Programm grundsätzlich ankommt, ob die Hinweise und Warnungen angenommen werden und welche Verbesserungen vorgenommen werden sollten, bevor die Hauptstudie gestartet würde.
Im Folgenden wird eine Beschreibung der Fragen gegeben und erläutert.

3.4.2 Aufbau des Fragebogens

Die Befragung wurde als semi-strukturierte Interviews durchgeführt. Die grundlegende Liste umfasst insgesamt 23 Fragen: drei demographische Angaben, elf einleitende Fragen, sechs Fragen zur Testdurchführung und drei abschließende Fragen. Die vollständige Liste dieser Fragen befindet sich in Appendix A.
Die einleitenden Fragen dienten zum einen dazu, die Testpersonen mit einfachen Fragen aufzuwärmen und zum anderen dazu, alle Grundinformationen über den Gebrauch von Passwörtern im Allgemeinen und am Arbeitsplatz zu liefern. Zusätzlich sollte klar werden, ob es bereits Hilfestellung in irgendeiner Form gab und in welchem Maße eine verbale Hilfestellung erwünscht war.
Die Fragen zur Testdurchführung bezogen sich direkt auf den Verlauf der Passworterstellung und das erschienene Feedback. Es sollte ein Bild darüber erlangt werden, wie die Testpersonen das Programm auffassten und wie sie damit zurecht kamen. Es wurde unter anderem gefragt, wie das Feedback empfunden wurde, inwieweit es Probleme beim Verständnis gab und ob es hilfreich war. Außerdem wurde die Frage gestellt, welche Hinweise die Teilnehmer/innen gerne gesehen hätten. Hier konnten die Befragten all ihre Gedanken äußern, die sie zum vorgestellten System hatten.
Der abschließende Teil diente zur Klärung offener Fragen der Testpersonen, bot Gelegenheit für Anmerkungen und dankte für die Teilnahme. Zusätzlich wurde die Frage gestellt, ob man bereit wäre, an einer Folgestudie teilzunehmen.
Je nach Teilnehmer oder Teilnehmerin wurden zu manchen Gelegenheiten weitere Fragen gestellt, weiter nachgehakt oder Fragen weggelassen, da sie schon an anderer Stelle beantwortet wurden. Das erlaubte es, individuell auf jeden Teilnehmer einzugehen und das Gewollte zu erfahren.
Im nächsten Abschnitt wird näher auf die wichtigsten Ergebnisse eingegangen.

3.5 Ergebnisse der Vorstudie

Zur Analyse der Vorstudie wurden die Antworten der Teilnehmer für die einzelnen Fragen und Bereiche gesammelt und zusammengefasst. Im Folgenden werden die daraus resultierenden Ergebnisse vorgestellt.

3.5.1 Ergebnisse der einleitenden Fragen

Nun folgt ein Überblick über die Ergebnisse der einleitenden Fragen.
Insgesamt wurde das Programm von allen verstanden. Drei Testpersonen müssen ihre Passwörter in der Arbeit in einem Zeitraum von vier bis sechs Wochen ändern, eine Person alle drei Monate und eine lediglich alle sechs Monate. Drei von ihnen fällt das Erstellen eines neuen Passwortes schwer, da ihnen die Ideen zu einem guten Passwort fehlen, welches sie sich dennoch merken können. Einem fällt es leicht, da er eine gute Taktik hat. Diese bestand darin, sich einen für ihn gut

merkbaren Satz auszudenken und jeweils die Anfangsbuchstaben jeden Wortes zu übernehmen. Der fünfte Teilnehmer besitzt drei bis vier Passwörter, die er fortlaufend wiederverwendet.
Die Richtlinien aller Befragten ähnelten sich in der Struktur: Bestimmte Anzahl an Zeichen, bestimmte Anzahl an Sonderzeichen, Ziffern, Großbuchstaben und/oder Kleinbuchstaben, keine Ähnlichkeit zu vorherigen Passwörtern.
Alle empfinden die Prozedur des regelmäßigen Passwort-Änderns als unangenehm und zeitaufwändig. Die Länge, die durchschnittlich gebraucht wird, um in der Arbeit das neue Passwort zu erstellen liegt bei drei der Probanden unter einer Minute. In diesen Fällen werden schon vorhandene Passwörter wiederverwendet oder eine gute Taktik angewendet. Die restlichen Teilnehmer brauchen einige Minuten für die Aufgabe. Der Grund sei die Ideenfindung für das neue Passwort. Vier der befragten Personen benötigen mindestens zwei oder drei Versuche für die Erstellung des neuen Passwortes. Das liegt meistens an nicht erfüllten Richtlinien. Die fünfte Person wiederum verhilft sich durch Wiederverwendung alter Passwörter. Zwei Teilnehmer erhalten nach der Zurückweisung der Eingabe in der Arbeit keine Rückmeldung, warum das Passwort nicht akzeptiert wurde. Eine Teilnehmerin erhält Rückmeldung, falls zu wenig Stellen oder Ziffern bzw. Sonderzeichen eingegeben wurden.
Lediglich eine Teilnehmerin berichtete, in der Arbeit eine Hilfestellung zur Erstellung des neuen Passwortes zu erhalten in Form eines Tipps, wie ein sicheres Passwort erstellt werden könne. Dieser Tipp änderte sich nie und wurde demnach auch selten angewendet, da man Bedenken hatte, das Passwort wäre sonst leichter zu erraten. Ansonsten konnte von keiner Hilfestellung berichtet werden.
Alle Teilnehmer waren sich sicher, Tipps in jeglicher Art könnten die regelmäßige Passworterstellung erleichtern und würden dies willkommen heißen.
Im Folgenden wird genauer auf die qualitativen Ergebnisse der Vorstudie eingegangen.

3.5.2 Bewertung des Feedback-Systems

Die Teilnehmer bewerteten das Feedback allgemein als positiv. Die Frage „Wie haben Sie das Feedback empfunden?“ lieferte die Stichworte „klar“, „hilfreich“ und „gut“. Jedoch war es für zwei Teilnehmer zu ungenau. Es erklärte nicht die Hintergründe der Hinweise, welche Wirkung sie auf die Passwortstärke haben und wurde deshalb nicht angewendet.
Vier von den fünf Personen änderten ihr Passwort so lange, bis die Passwortstärke maximal war und sagten, dies sei eine sehr positive Hilfestellung, da diese zu starken Passwörtern animierte. Außerdem verhalf dies zu einem Gefühl der Sicherheit. Es gäbe Vertrauen, ein sicheres Passwort gewählt zu haben. Zwei von ihnen fügten hinzu, dass sie sich jedoch mehr Informationen darüber wünschten, was diese Stärke bedeutete und auf welchen Hintergründen sie basierte. Ein Teilnehmer bemerkte, die Hinweise seien nicht sichtbar genug.
Die Frage, welche Art von Hinweisen man gerne gesehen hätte lieferte folgende Antworten. Zwei Personen wünschten sich eine Anzeige der vorgesetzten Richtlinien, die während der Eingabe abgehakt würden. Dies sollte zu einer schnelleren Passworterstellung führen und diese erleichtern. Wiederum zwei der befragten Personen erhielten gerne konkrete Vorschläge oder Beispiele, wie man ein sicheres und dennoch merkbares Passwort erstellen könnte. Eine Person wünschte sich Vorschläge zur Passwortzusammensetzung mit ausreichend Erklärung, welche Auswirkung die einzelnen Komponenten auf die Sicherheit des Passwortes haben.
Alle Testpersonen waren interessiert an einer Folgestudie und würden definitiv ein solches Feedback-System anwenden.

3.5.3 Positive Ergebnisse der Vorstudie als Grundlage für die Hauptstudie

Die Ergebnisse der Vorstudie bilden die Grundlage für die Hauptstudie. Trotz der geringen Teilnehmerzahl lassen sich bereits konkrete Verbesserungswünsche an das System erkennen.

Zum einen mehr Informationen allgemein. Die Nutzer möchten wissen, warum ihnen ein solcher Hinweis gegeben wird und was dahinter steckt. Sie vertrauen den Hinweisen nicht blind. Zum anderen wurde der Wunsch nach einer Hilfestellung geäußert, um die Prozedur des Passworterstellens zu erleichtern und zu beschleunigen. Es fehlen die Ideen dafür, wie man ein sicheres Passwort erstellt, das sich dennoch gut merken lässt. Es werden konkrete Beispiele benötigt, die einem die Ideenfindung erleichtert oder gar abnimmt. Dies fehlte bei dieser ersten Version des Systems. Zusätzlich wäre eine Anzeige der vorgegebenen Richtlinien eine weitere erwünschte Hilfe.
Diese Ergebnisse sollen anhand der Hauptstudie verfestigt und die Verbesserungsvorschläge konkretisiert werden.

4 Hauptstudie

Ziel der Arbeit ist es, das verbale Feedback-System des öffentlich zugänglichen Programms zxcvbn zu erweitern und zu verändern. Es soll die Nutzer bei der Passworterstellung bestmöglich unterstützen. Um herauszufinden, hinsichtlich welchen Aspekten das System verbessert werden kann, wurde eine Studie durchgeführt. Die Grundlage der Studie bietet die bereits erstellte Internetseite als Nutzeroberfläche, auf welcher die Teilnehmer den Test durchführen sollten. In diesem Kapitel wird zunächst die Herangehensweise und Methodik der Studie erläutert. Als nächstes folgt die Beschreibung der verwendeten Nutzeroberfläche. Im dritten Abschnitt werden die Hintergründe der Rekrutierung dargelegt. Der vierte Abschnitt umfasst den Aufbau und die Erläuterung des Fragebogens. Abschließend wird die Prozedur der Studie beschrieben.

4.1 Methodik

Die Hauptstudie ist eine Online-Studie. Es wurde eine qualitative Herangehensweise gewählt da es für diese Arbeit wichtig ist, herauszufinden, was die Teilnehmer denken. Es soll verstanden werden, was ihnen wichtig ist in Bezug auf die Passworterstellung. Zusätzlich soll herausgefunden werden, wie die Nutzererfahrung bewertet wird. Hierzu wurden einige Fragen als quantitativen Teil in die Studie mit eingebunden. Zu diesem quantitativen Teil gehören des weiteren die demographischen Angaben und Fragen zum Umgang mit Passwörtern im Allgemeinen sowie am Arbeitsplatz. Um möglichst viele verschiedene Teilnehmer aus verschiedenen Altersklassen und Beschäftigungsbereichen zu erreichen, schien die Wahl einer Online-Studie am sinnvollsten.
Die Kernfragen, auf die diese Studie aufbaut sind Freitext-Antworten. Sie sollen den Teilnehmern ermöglichen und sie dazu motivieren, ihre Gedanken und Meinungen möglichst ausführlich und genau darzulegen. Da dies eine qualitative Studie ist, ist es notwendig, so viel Informationen dazu zu sammeln, was die Testpersonen denken, um verstehen zu können wie sie handeln und weshalb sie so handeln. Bei einer Online-Studie hat man nicht die Möglichkeit mit weiteren Fragen „nachzuhaken“, weswegen es wichtig ist, ausführliche Antworten zu erhalten. Je detaillierter die Antwort ist, desto weniger Interpretation ist bei der späteren Auswertung von Nöten. Dies ist wichtig für die Repräsentativität der Ergebnisse.

4.1.1 Grounded Theory

Alle Freitext-Antworten wurden zusammengetragen und mit der Methode Grounded Theory nach Strauss und Corbin [7] analysiert. Bei dieser Methode werden die Antworten der Teilnehmer in drei Durchgängen immer wieder kodiert, um am Ende einen oder wenige Kern-Kodes zu formulieren. Die Verallgemeinerungsfähigkeit dieser Methode wird zum einen gesichert durch den Vorgang der kontinuierlichen Abstraktion. Je abstrakter das Konzept, vor allem je abstrakter die Hauptkategorie, desto weitläufiger wird die Theorie Anwendung finden können. Zum anderen definiert diese Methode eine Grundvoraussetzung, zu der die Daten gesammelt und woraus die Theorie entstehen konnte. Im Folgenden werden die einzelnen Durchgänge der Grounded Theory beschrieben.
Im offenen Kodieren werden alle Antworten der Teilnehmer zunächst zu einzelnen Kodes zusammengefasst. Diese Kodes werden dann im Axialen Kodieren gruppiert und diese Gruppen jeweils durch einen weiteren Kode benannt. Das Besondere in diesem zweiten Durchgang des Grounded Theory ist es, dass in einem nächsten Schritt eine zweite, unabhängige Person die Kodes aus dem offenen Kodieren nimmt und in die Gruppen des ersten Kodierers unterteilt, wie sie es für richtig hält. Anschließend wird verglichen, welche Kodes in welche Gruppen unterteilt wurden. Bei Unstimmigkeiten in den Verteilungen, werden diese besprochen und so eine endgültige Tabelle erstellt. Dieser weitere Schritt verhindert eine einseitige Interpretation der Ergebnisse und beugt Fehlinterpretationen vor. Diese zweite unabhängige Person sollte mit den Antworten des ersten Durchganges möglichst noch nicht vertraut sein und darf nicht in den Prozess des Axialen Kodie-

rens involviert gewesen sein.
Im dritten und letzten Durchlauf, dem selektiven Kodieren, werden die Gruppen jeweils zu einem Kern-Kode zusammengefasst. In einem letzten Schritt werden diese Kern-Kodes und alle Beobachtungen zusammengefasst, um eine Theorie zu formulieren. Diese Theorie repräsentiert die Endergebnisse der Studie. Diese Methodik zur Datenanalyse war sehr ähnlich zur der, die Stobert und Biddle in ihrer Arbeit verwenden [30].

4.1.2 Arithmetisches Mittel und Standardabweichung

Die quantitativen Ergebnisse werden mit jeweils dem arithmetischen Mittel und der jeweiligen Standardabweichung beschrieben. Es ist wichtig, einen generellen Überblick über die verschiedenen Aspekte der Passwort-Handhabung der Teilnehmer zu erlangen was hiermit erreicht werden kann.

4.1.3 Nutzererfahrungs-Fragebogen

Die Bewertung interaktiver Systeme ist eine wichtige Maßnahme im Rahmen benutzerorientierter Gestaltung. Deshalb war wichtig, das System ebenfalls evaluieren zu lassen. Für diese Evaluation, der sogenannten User Experience, diente der Fragebogen „AttrakDiff 2“ [14] als Vorbild und wurde für diese Studie zweckmäßig angepasst. Der Fragebogen besteht aus einer sieben-Punkte-Likert-Skala mit insgesamt 13 sich gegenüberstehenden Eigenschaftspaaren, einem sogenannten semantischen Differenzial. Dieses Semantische Differenzial beschreibt zwei verschiedene Aspekte der Nutzererfahrung: die hedonische Qualität (diese beziehen sich darauf, inwieweit ein System stimulierend wirkt und über die reine Nützlichkeit hinaus gehen) und die pragmatische Qualität (wie effektiv und effizient ist das System). Auch hier wurde jeweils das arithmetische Mittel berechnet, um so einen Überblick darüber zu erhalten, wie die Nutzer das Feedback-System erfassen. Die Eigenschaftspaare wurden bezüglich ihrer beschreibenden Qualität gegliedert und anschließend bewertet.

4.2 Internetseite

Die Internetseite wurde aus der Vorstudie direkt übernommen und wenig verändert, da eben dies in der Hauptstudie ermittelt werden sollte. An der Darstellung wurden die Farbe der Hinweise, Warnungen und der angezeigten Passwortstärke zu blau geändert, damit diese sich von den restlichen Textelementen unterscheiden und besser hervorgehoben werden. Dies geschah aufgrund der Resultate der Vorstudie. Um die Online-Studie zu ermöglichen, war es nötig, eine weitere HTML-Seite zu erstellen und die schon bestehende Seite sowie den Fragebogen in diese einzubetten.

Sie besteht aus einer initialen Seite, auf der die Teilnehmer begrüßt werden und ihnen der Ablauf der Studie erläutert wird. Durch einen Klick gelangt man auf die nächste Seite, auf der man die Frage beantworten muss, ob man in der Arbeit ein Passwort besitzt, das man regelmäßig ändern muss. Antwortet man mit einem Klick auf „Nein“, gelangt man auf eine Endseite, auf der erklärt wird, dass man nicht den Voraussetzungen für diese Studie entspricht. Beantwortet man die Frage jedoch mit „Ja“, wird man auf die schon beschriebene Passwort-Testseite geleitet. Von dieser Seite gelangt man durch einen weiteren Klick auf „Weiter zum Fragebogen“ zu einer nächsten Seite. Hier ist in einem in diese Seite eingebetteten Fenster der Fragebogen eingelassen. Bilder hiervon zeigen Abbildungen 4.1 und 4.2.

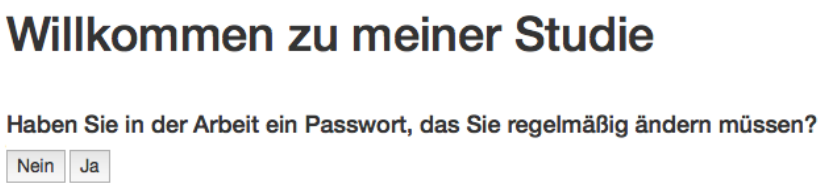

Abbildung 4.1: Anzeige, die nach der initialen Begrüßungsseite erscheint. Sie dient der Selektion der Teilnehmer, die den Kriterien für eine Teilnahme an der Studie entsprechen.

4.3 Rekrutierung

Der Anwendungsfall erfordert, dass alle Teilnehmer berufstätig sind. Dies schloss aus, die Testpersonen über den Universitäts-Email-Verteiler zu rekrutieren. Um möglichst viele Personen aus verschiedenen Altersklassen und Beschäftigungsbereichen zu erreichen, wurden die Dienste der Internet-Plattform Prolific in Anspruch genommen. Prolific [25] ist eine Plattform mit über 50000 Teilnehmern aus bis zu 147 Ländern und liefert somit die Möglichkeit, eine große Bandbreite in der Demographie der Befragten zu erlangen. Da diese Studie auf eine deutsche Nutzerbasis abzielt, wurde in der Studienbeschreibung auf Deutsch deutlich betont, dass man diese Studie nur machen sollte, wenn man Deutsch spricht. Als nächstes wurde eine Vorauswahl geschaltet, um Studenten und diejenigen auszuschließen, die momentan ohne feste Arbeitsstelle sind. Dies sollte verhindern, dass zu viele Teilnehmer die Studie beginnen, ohne sie abschließen zu können. Als zusätzliches Ausmustern von Testpersonen, dient die Frage auf der zweiten Seite meiner HTML-Oberfläche, wie oben beschrieben. Dies soll diejenigen Teilnehmer aussortieren, die zwar berufstätig sind, jedoch in ihrer Arbeit kein Passwort verwenden, das sie in regelmäßigen Abständen erneuern müssen.
Um die Ergebnisse einer Umfrage mit den Teilnehmern auf Prolific abgleichen zu können, bekommt jeder Prolific-Nutzer für jede Umfrage eine Identifikationsnummer, die im späteren Verlauf, als „Prolific-ID“ bezeichnet wird. Diese muss jeder Teilnehmer und jede Teilnehmerin im Fragebogen angeben. Am Ende jeder Umfrage muss man einen Link einfügen, der zurück auf die Prolific Seite führt. Dies stellt sicher, wann ein Teilnehmer die gesamte Umfrage tatsächlich durchgeführt und beendet hat. Des weiteren sichert Prolific so die Anonymität seiner Mitglieder.
Jeder Teilnehmer erhielt 1,30£ für einen vollständig und sinnvoll (aus den Antworten konnte herausgelesen werden, dass die Frage verstanden wurde) ausgefüllten Fragebogen. Teilnahmen mit zu vielen lückenhaften oder unsinnigen Antworten, wurden ohne Entgelt verworfen.

4.4 Fragebogen

In diesem Abschnitt wird zunächst die Erstellung des Fragebogens der Hauptstudie geschildert. Anschließend wird sein Aufbau und die Durchführung der Studie erläutert.

4.4.1 Limesurvey

Limesurvey ist eine kostenfreie Online-Umfrage-Plattform [22], die es ermöglicht, Online-Umfragen schnell und einfach zu entwickeln und durchzuführen. Aus diesem Grund war es sinn-

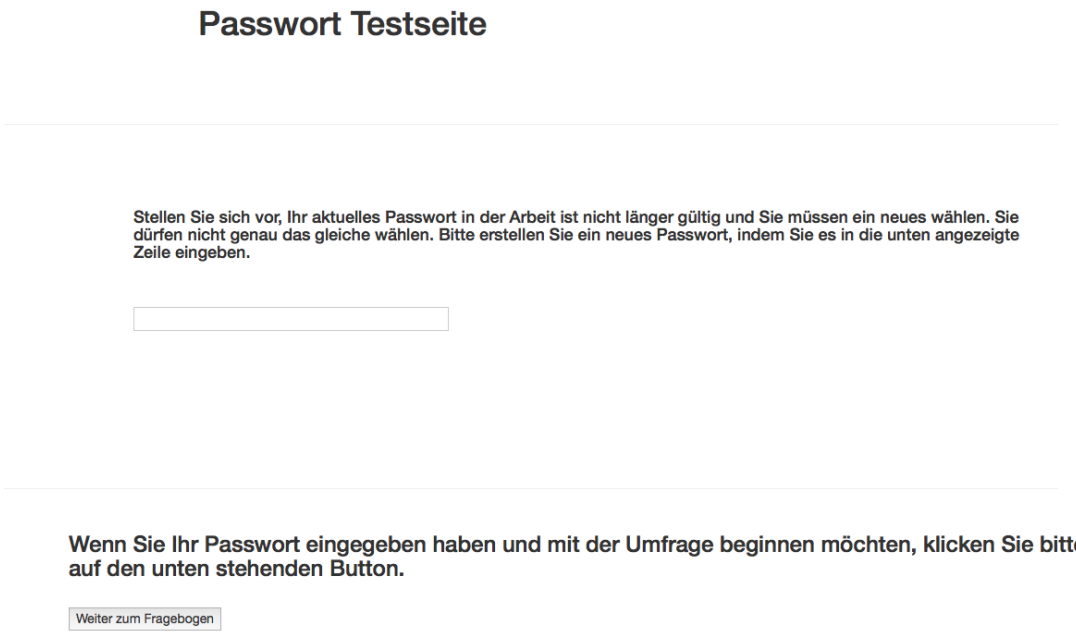

Abbildung 4.2: Seite der Hauptstudie, auf der das System getestet wird.

voll, diese Dienste für die Studie in Anspruch zu nehmen. Die Ergebnisse werden in einer Datenbank erfasst und lassen sich zur weiteren Auswertung exportieren. Der Fragebogen wurde mithilfe dieser Plattform erstellt und die Ergebnisse dort gesammelt. Im folgenden Abschnitt wird der Aufbau des Fragebogens und die Absichten der Fragen erläutert.

4.4.2 Aufbau und Erläuterung des Fragebogens

Der vollständige Fragebogen liegt in Appendix B vor.
Insgesamt besteht der Fragebogen aus 37 Fragen, die in sieben Gruppen gegliedert sind, wobei die letzte Gruppe lediglich einen abschließenden Link in einem Textfeld enthält.
Die erste Gruppe „Demographische Angaben“ enthält vier Fragen: eine Zeile zur Eingabe der Prolific-ID und jeweils eine Frage zu Geschlecht, Alter und Beschäftigungsbereich.
Die zweite Gruppe „Fragen zur Testdurchführung“ besteht aus elf Fragen, die sich direkt auf den zuvor durchgeführten Test beziehen. Sie beinhaltet die wichtigsten Fragen für diese Studie. Sie soll einerseits Aufschluss darüber geben, wie das Feedback bei den Nutzern ankommt und andererseits die Grundlage dafür liefern, wie das Feedback zu verbessern ist. Aus diesem Grund sind sechs dieser Fragen mit Freitext zu beantworten, die den Studien-Teilnehmern die Möglichkeit bieten und sie dazu ermutigen sollen, ihre Meinungen und Gedanken möglichst genau darzulegen.
Die dritte Fragegruppe „Fragen zum Passwort“ besteht aus sieben Fragen. Diese beziehen sich auf das im Test erstellte Passwort im Vergleich zu den Passwörtern, die die Teilnehmer generell in der Arbeit erstellen. Bei diesem Vergleich sollte festgestellt werden, wann die Teilnehmer das Feedback anwenden und in wiefern sie es tun. Dies soll die Ergebnisse der restlichen Antworten in Bezug auf das Feedback-System stützen. Die vierte Fragegruppe „Bewertung der User Experience“ beinhaltet lediglich eine sieben-Punkte-Likert-Skala, bei der sich 13 Wörterpaare gegenüberstehen und man mit den Zahlen eins bis sieben wählen kann, zu welchem der Begriffe man eher tendiert oder vollkommen zustimmt. Sie dient, wie der Name bereits sagt, der Bewertung der Nutzererfahrung mit den vorgegebenen Funktionen des Systems zxcvbn.
In der nächsten Fragegruppe „Allgemeine Fragen“ sind zwölf Fragen aufgeführt. Allen voran wurde hier eine Aufmerksamkeitsüberprüfung, ein sogenannter „Attention Check“, eingesetzt. Er

besteht aus einer Frage, die nichts mit der Studie zu tun hat. Man kann diese Frage lediglich richtig beantworten, wenn man die gesamte Erläuterung dieser Frage vollständig durchgelesen hat. Er soll dazu dienen, diejenigen Teilnehmer herauszufiltern, die den Fragebogen nicht gewissenhaft durchgehen, sondern nur überfliegen, um die Entlohnung zu erhalten. Wird diese Frage falsch beantwortet, ist die Umfrage so programmiert, dass die restlichen Fragen nicht mehr angezeigt werden und die Umfrage somit beendet wird. Die Ergebnisse dieser Umfrage-Teilnahmen ließen sich bei der Auswertung der Ergebnisse hierdurch leicht herausfiltern. Die restlichen Fragen in dieser Gruppe beziehen sich auf die Handhabung der Passwörter am Arbeitsplatz und den Umgang mit Passwörtern im Allgemeinen. Dies dient zum einen der Erkennung, wo die Probleme mit Passwörtern durchschnittlich liegen und sollen wiederum die spätere Interpretation der Ergebnisse stützen. Zum anderen dienen die Fragen in dieser Gruppe der Einschätzung, welche Arten von Unterstützung in Sachen Passwörtern es bereits gibt und wie die Nutzer die Aufgabe der Erstellung und Verwaltung all ihrer Passwörter bewältigen. Dies kann dabei helfen, Nutzerantworten besser zu verstehen und einordnen zu können.
Die sechste und vorletzte Gruppe besteht aus den 17 Fragen der Soziale-Erwünschtheits-Skala-17 (SES-17) [5]. Sie wurde mit aufgenommen, um eventuell erkennen zu können, wenn ein Teilnehmer nicht ehrlich war. Diese Skala misst die soziale Beeinflussung, das heißt, die Neigung eines Menschen, Fragen so zu beantworten, dass sie begehrenswerter auf andere wirken. Sind die Antworten eines Teilnehmers oder einer Teilnehmerin zu unglaubwürdig, sollte mithilfe dieser Skala gemessen werden können, wie sehr die Testperson danach strebt, das zu sagen, was ihrer Meinung nach die richtige Antwort ist. für die Zwecke dieser Studie wären solche Antworten jedoch unbrauchbar, weshalb sie verworfen wurden.
Im nachfolgenden Abschnitt wird der Ablauf der Studie geschildert.

4.5 Durchführung der Studie

Die Studie richtete sich an die Mitglieder der Online-Plattform Prolific. Wer den vorgegebenen Kriterien entsprach, konnte mit der Umfrage beginnen. Nach den in Unterpunkt 4.2 bereits beschriebenen Schritten wurde die Passwort-Testseite angezeigt. Hier wird in einem einleitenden Text der Anwendungsfall beschrieben und was zu tun ist. Der Text lautete wie folgt:

> „Stellen Sie sich vor, Ihr aktuelles Passwort in der Arbeit ist nicht länger gültig und Sie müssen ein neues wählen. Sie dürfen nicht genau das gleiche wählen. Bitte erstellen Sie ein neues Passwort, indem Sie es in die unten angezeigte Zeile eingeben."

Während der Passworteingabe erscheinen die Hinweise und Warnungen, sowie die Passwortstärke. Die Teilnehmer haben keine Zeitvorgabe, das neue Passwort zu erstellen. Nach der Passworterstellung können die Teilnehmer/innen mit der Beantwortung des Fragebogens beginnen, indem sie auf den Knopf „Weiter zum Fragebogen" drücken. Dieser erscheint in einem Fenster, das eingebettet in der Seite ist und lässt sich dort ausfüllen. Man hat hier zu jedem Zeitpunkt die Wahl, die Studie abzubrechen und die Antworten zu löschen. Auf der letzten Umfrageseite gelangt man durch einen abschließenden Link zurück auf die Plattform Prolific und kann dort die Studie beenden. Die Umfrage sollte zwischen 15 und 20 Minuten dauern.

4.6 Einschränkungen

Bei der Durchführung der Studie und der späteren Analyse der Daten gab es einige Aspekte, die erläutert werden müssen, bevor die Ergebnisse präsentiert werden. Zum einen gab es ein Problem mit der Sprache. Prolific ist eine britische Seite und ist international zugänglich. Die allgemeine Verständigungssprache ist deshalb Englisch. Da diese Studie jedoch auf Deutsch verfasst wurde, waren für eine Teilnahme ausreichende Deutschkenntnisse unbedingt notwendig. Eine solche

Vorauswahl zu programmieren, war über die Online-Plattform nicht geboten. Dies führte dazu, dass einerseits eine Vielzahl von Umfragen nicht abgeschlossen wurden. Andererseits gab es einen Großteil an Fragebögen, deren Antworten wenig bis keinen Sinn ergaben. Ein Teilnehmer hatte beispielsweise als Antwort Teile der Frage hinein kopiert. Ein weiterer Teilnehmer schrieb in allen Freitext-Antworten „GOOD“ oder „NICE“. Nur wenige Teilnehmer gaben sich die Mühe, die Fragen zu übersetzen und sie anschließend auf Englisch zu beantworten. Zum anderen eignete sich die Form einer Online-Umfrage nicht vollständig. In den Freitext-Antworten wurden die Gedanken in vielen Fällen nicht wie erhofft ausreichend erläutert. Dies hatte zur Folge, dass mehr Interpretationsarbeit geleistet werden musste, als es bei einer Studie mit persönlichen Interviews der Fall gewesen wäre.

Eine dritte Schwierigkeit ist während der Analyse der Daten aufgekommen. Bei der Auswertung der letzten Frage („Wie regelmäßig müssen Sie in der Arbeit Ihr Passwort ändern?“) wurde vier mal die Antwort „Nie“ angegeben. Da jedoch dies das voraussetzende Kriterium für eine Teilnahme an der Umfrage war, führt es zu den folgenden Annahmen. Die Teilnehmer hatten bei Beginn der Studie gelogen, um teilnehmen zu können. Andernfalls wurde die Frage eventuell nicht verstanden, beziehungsweise überlesen. Da jedoch die restlichen Fragen, sowie die Aufmerksamkeitsüberprüfung in allen vier Fällen korrekt und für den Zweck der Arbeit hilfreich beantwortet wurden, waren sie vor der Datenanalyse nicht aufgefallen und demnach nicht eliminiert worden. Der nachträgliche Ausschluss dieser vier Teilnahmen war nahezu unmöglich und hätte eine erneute vollständige Auswertung bedeutet. Es wurde entschieden, die Ergebnisse beizubehalten.
Schlussfolgernd wird erkannt, dass bei einer nächsten Studie genau auf solche Fälle explizit geachtet und eingegangen werden wird. Diese Fehler hätten vor der Analyse erkannt werden können. Des Weiteren wird empfohlen, Online-Studien möglichst auf Englisch abzuhalten, da dies den Teilnehmerbereich signifikant erweitert. Ebenso sinnvoller ist eine qualitative Datenerhebung im Rahmen persönlichen Interviews. Diese bewerkstelligen ein gezieltes Nachfragen, um die Antworten aller Teilnehmer nachvollziehen zu können.

Abschließend muss weiterhin beachtet werden, dass die Testpersonen die Passwörter nicht für den privaten Gebrauch erstellt haben. Die Motivation hinter dem Test und der Beantwortung des Fragebogens stellte für die meisten ausschließlich die finanzielle Entschädigung dar, was sich von einer persönlichen Motivation meist unterscheidet. Es kann demnach sein, dass im Fall einer privaten Verwendung des Systems, den einzelnen Features noch mehr Beachtung zugeteilt wird. Andererseits besteht die Möglichkeit, dass diejenigen Studienteilnehmer, denen bewusst war, dass der Fokus dieser Studie auf der Passworterstellung liegt, sich mehr Mühe dabei gegeben haben, als sie es normalerweise würden.
Im folgenden Kapitel werden die Ergebnisse der Hauptstudie vorgestellt.

5 Ergebnisse der Hauptstudie

In den folgenden Kapiteln werden die Ergebnisse der Studie aufgeführt. Es wird zunächst ein Überblick über die Demographie und die Gründe für einen Ausschluss der Fragebögen aus der Auswertung gegeben. Als Nächstes werden die Resultate des quantitativen Teils der Studie zusammengefasst. Dann folgt die Darstellung der qualitativen Ergebnisse. Abschließend werden die Nutzererfahrungen über das Systems dieser Studie vorgestellt.

5.1 Demographie und Ausschlusskriterien

Vor der ausführlichen Analyse der Ergebnisse, wurden alle Umfragebögen disqualifiziert, welche die Aufmerksamkeitsüberprüfung nicht bestanden hatten. Zusätzlich wurden die Kernfragen, die Fragen mit Freitext-Antworten, für jeden Fragebogen durchgegangen und diejenigen ausgeschlossen, welche diese Fragen ergebnislos oder gar nicht beantwortet hatten. Da diese Studie eine primär qualitative Studie ist, sind diese Fragen essentiell für eine spätere Lösungsfindung. Ein weiteres Ausschlusskriterium bestand in der Unvollständigkeit eines Fragebogens. Falls zu viele Fragen nicht beantwortet wurden oder die Umfrage unvollständig abgeschlossen worden war, wurden diese Teilnahmen ebenfalls disqualifiziert. Von anfänglichen 87 abgeschlossenen Umfragen, waren 40 verwendbar. Von diesen Teilnahmen waren 16 weiblich (40%) und 24 männlich (60%). Ihr Alter lag zwischen 20 und 53 Jahren. Die Beschäftigungsbereiche waren auf zwölf verschiedene Branchen verteilt, von denen die IT- und Internetbranche mit 15 Teilnehmern/innen vertreten war. Die Verteilung zeigt die Tabelle 5.1.
Der nächste Abschnitt liefert einen Überblick über die quantitativen Fragen der Studie.

BRANCHE	**ANZAHL**
Baugewerbe/- industrie	2
Bildungswesen	2
Elektrotechnik, Feinmechanik und Optik	1
Finanzdienstleister	2
Freizeit, Touristik, Kultur und Sport	2
Gesundheit und Soziale Dienste	3
Groß- und Einzelhandel	2
Hotel und Gastronomie	2
IT- und Internetbranche	15
Medien	5
Unternehmensberatung	1
Wissenschaft und Forschung	3

Tabelle 5.1: Verteilung der Beschäftigungsbereiche der Studien-Teilnehmer

5.2 Quantitative Ergebnisse

Im Anschluss an den demographischen Teil, waren sechs von elf Fragen mit Freitexten zu beantworten. Diese werden im nächsten Unterpunkt besprochen. Die restlichen fünf werden im Folgenden aufgeführt. Im weiteren Verlauf werden das arithmetische Mittel und die Standardabweichung mit „M“ beziehungsweise „SD“ bezeichnet.

Zweite Fragegruppe Auf die Frage hin, was sie für ein Feedback von dem System erhalten haben, erinnerten sich 32 (80%) Teilnehmer an die Passwortstärke als Zahl, 23 (57,5%) an Tipps in Form von Sätzen und 11 (27,5%) an Warnungen in Form von Sätzen. Es kreuzten 13 (32,5%) Personen ebenfalls die falsche Antwort „Balken, der wächst, wenn Passwort stärker wird“ an.

Auf was legen Sie Wert bei der Passworterstellung	**M**	**SD**
Erinnerbarkeit	4,20	1,11
Passwortstärle	4,05	1,18
Erfüllung der vorgegebenen Kriterien	3,70	1,14
Dass sie sich von Ihren anderen und vorherigen Passwörtern unterscheiden	3,60	1,24

Tabelle 5.2: Die Tabelle zeigt, auf was die Teilnehme bei der Erstellung eines neuen Passwortes Wert legen anhand des arithmetischen Mittels und der zugehörigen Standardabweichung

Die Teilnehmer empfanden die Hinweise als „fast immer verständlich“ (M=4,47[2] ; SD=1,01) und als „fast immer nachvollziehbar“ (M=4,36[3] ; SD=1,01). Als Nächstes sollten die Testpersonen sich vorstellen, sie bekämen das nächste Mal, wenn sie in der Arbeit das Passwort ändern müssten, ein solches Feedback wie in dieser Studie. Auf die Frage hin, wie sie darauf reagieren würden, antworteten 23 Personen (57,5%) mit „Ich würde es willkommen heißen.“ 20 Teilnehmer (50%) würden das Feedback anwenden und 13 (32,5%) es beachten. Zwei Personen würden das Feedback nicht beachten und weitere Zwei würden es nicht anwenden. Nun sollten die Teilnehmer mit Hilfe einer fünf-Punkte-Skala beschreiben, auf was sie bei der Passworterstellung am meisten Wert legen. Die Ergebnisse waren wie folgt: Am meisten Wert legen die Teilnehmer auf die Passwortstärke (M=4,05[4] ; SD=1,18) und die Erinnerbarkeit (M=4,20 ; SD=1,11). Etwas weniger legen sie auf die Erfüllung der Kriterien (M=3,70 ; SD=1,14) und darauf, dass sie sich von ihren anderen und vorherigen Passwörtern unterscheiden (M=3,60 ; SD=1,24). Tabelle 5.2 zeigt diese Ergebnisse zusammengefasst auf.

Dritte Fragegruppe In der dritten Gruppe „Fragen zum Passwort“ wurden die Teilnehmer zu den in der Studie erstellten und ihren Arbeits-Passwörtern befragt. Die Ergebnisse der ersten Frage „Welche Elemente haben Sie in Ihrem Passwort verwendet?“ sind in Abbildung 5.3 dargestellt. 70% der Befragten verwendeten Großbuchstaben, 92,5% Kleinbuchstaben, 50% hatten Sonderzeichen in ihrem Passwort und 82,5% verwendeten Ziffern. Lediglich 5% erstellten ihr Passwort durch ein Muster auf der Tastatur, 12,5% aus einem Datum, 7,5% ersetzten Buchstaben durch Ziffern und/oder Sonderzeichen. Wiederum 12,5% verwendeten einen Vornamen, 7,5% einen Nachnamen. Keiner der Befragten baute das Passwort auf einem Spitznamen auf. 32,5% der Passwörter bestanden aus einem Wort, hingegen nur 15% aus mehreren Wörtern. Wiederum lediglich 12,5% bestanden unter anderem aus einer Zahlenfolge und nur 5% aus einer Buchstabenfolge. Des Weiteren wurde erkannt, dass 42,5% der im Test erstellten Passwörter aus vier verschiedenen Zeichenklassen bestanden, 30% aus drei, 12,5% aus nur zwei Zeichenklassen und 10% aus einer einzigen. 2 Teilnehmer (5%) lieferten keine Angaben darüber, welche Art von Zeichen sie verwendet hatten. Der Grund für diese hohe Anzahl an verschiedenen Zeichenklassen in einem Passwort lässt sich durch den Anwendungsfall erläutern und wird in der Interpretation der Ergebnisse näher dargelegt. Im späteren Verlauf wird genauer erläutert, welche Vorgaben die Teilnehmer in der Arbeit für ihre Passwörter erhalten. Für die gleiche Frage, jedoch bezogen auf das Passwort in der Arbeit („Welche Elemente verwenden Sie in der Arbeit in Ihrem Passwort?“) werden die Ergebnisse ebenfalls in Abbildung 5.3 aufgezeigt.

Hier wurde festgestellt, dass diesmal 37,5% der Teilnehmer vier verschiedene Zeichenklassen angaben und 35% drei Zeichenklassen. Nur 15% verwenden zwei verschiedene Klassen und 5% eine einzige. Es lieferten diesmal 3 Teilnehmer (7,5%) keine Angaben über die Art der Zeichen,

[2] 1 = „unverständlich“, 2 = „nicht immer verständlich“, 3 = „neutral“, 4 = „fast immer verständlich“, 5 = „verständlich“

[3] 1 = „nicht nachvollziehbar“, 2 = „nicht immer nachvollziehbar“, 3 = „neutral“, 4 = „fast immer nachvollziehbar“, 5 = „nachvollziehbar“

[4] 1 = „keinen Wert“, 5 = „sehr viel Wert“

ELEMENT	Anzahl der Antworten - Test	Anzahl der Antworten - Arbeit
Großbuchstaben	28	30
Kleinbuchstaben	37	35
Sonderzeichen	20	19
Ziffern	33	32
Muster auf der Tastatur	2	2
Datum	5	7
Buchstabe durch Ziffern oder Sonderzeichen ersetzt	3	7
Vorname	5	5
Nachname	3	2
Spitzname	0	2
ein Wort	13	6
mehrere Wörter	6	8
Zahlenfolge	5	5
Buchstabenfolge	2	4

Tabelle 5.3: Diese Tabelle zeigt, wie viele Teilnehmer das jeweilige Element in ihrem Test-Passwort, sowie in ihrem Arbeits-Passwort verwendet haben.

die sie in der Arbeit in ihrem Passwort verwenden.
Die durchschnittliche Länge der Test-Passwörter betrug elf Zeichen (M=10,72 ; SD=4,84). Das kürzeste Passwort bestand aus einem Zeichen, das längste war 20 Zeichen lang. Ein Teilnehmer hat diese Frage nicht beantwortet. Die durchschnittliche Länge der Passwörter, die die Befragten in ihrer Arbeit erstellen beträgt zehn Zeichen (M=10,26 ; SD=4,52). Das Minimum lag ebenfalls bei eins und das Maximum bei 25. Die Verteilung der verschiedenen Längen zeigt Abbildung 5.1. Die Frage, welche Strategien zur Passworterstellung in der Studie angewandt wurden ergab, dass weniger als die Hälfte der Befragten ein komplett neues Passwort erstellt haben. Nur Wenige gaben an, eine Strategie verwendet zu haben. 17,5% gestanden, eines ihrer Passwörter wiederverwendet zu haben, 32,5% haben eines ihrer Passwörter modifiziert und 47,5% erstellten ein komplett neues Passwort. Einmal kam die Antwort, dass das Passwort auf den Anfangsbuchstaben jedes Wortes aus einem Satz basierte, den er oder sie sich gut merken kann. 22,5% der Teilnehmer bauten ihr Passwort auf einem Namen/Wort auf und haben Ziffern/Symbole hinten und/oder vorne angehängt. Nur zweimal basierte es auf einem Namen/Wort, in dem bestimmte Buchstaben durch Ziffern/Symbole ersetzt wurden. Wiederum zweimal setzte sich das Passwort aus einem Namen/Wort zusammen, in dem manche Buchstaben weggelassen wurden, sechs mal basierte es auf einem Wort, das aus einer anderen Sprache als Deutsch stammte. Keiner der Teilnehmer basierte das Passwort auf einer Adresse. Einmal wurde es auf Basis einer Telefonnummer erstellt und dreimal auf Basis eines Geburtsdatums. In den Bereich „Sonstiges“ wurden vier zusätzliche Antworten gegeben, auf was das erstellte Passwort basierte. Die Antworten lauteten wie folgt: „Frei gewählte Wörter“, „Mehrere Wörter + extra Zeichen“, „Passwort-Generator + Feedback“, „Teil der URL verwendet“. In Tabelle 5.4 wird die Verteilung dargestellt. Die Teilnehmer waren sich insgesamt „sicher“, ihr Passwort in ein paar Tagen erneut eingeben zu können (M= 4,23 ; SD=1,00). Abbildung 5.2 stellt die detaillierten Angaben der Teilnehmer hierzu dar.

Vierte Fragegruppe Die nächste Gruppe "Bewertung der User Experience“ wird im abschließenden Abschnitt aufgeführt und erläutert. Im Folgenden werden die Ergebnisse des nächsten Blocks „Allgemeine Fragen“ dargestellt.

Fünfte Fragegruppe In diesem fünften Fragenblock geht es um die Handhabung von Passwörtern. Die Frage nach den Passwortrichtlinien in der Arbeit ergaben Folgendes. Bei jeweils 60% der Befragten beinhalten die Vorgaben für das Passwort eine Mindestanzahl an Zeichen, eine Mindestanzahl an Großbuchstaben und eine Mindestanzahl an Kleinbuchstaben. Bei 40% gibt es die Vorgabe einer Mindestanzahl an Ziffern. Bei 32,5% darf das Passwort keine Ähnlichkeit zu vorherigen Passwörtern haben, bei 17,5% dürfen bestimmte Wörter nicht enthalten sein und bei

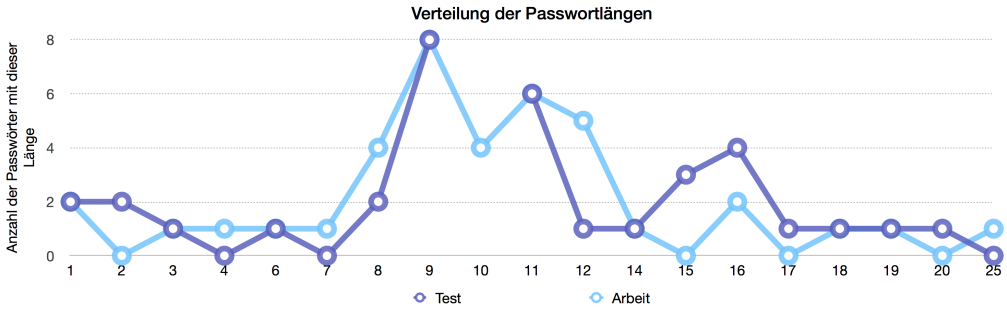

Abbildung 5.1: Verteilung der Passwort-Längen für das Test-Passwort, sowie ihr Passwort, das sie in der Arbeit verwenden. Die x-Achse gibt die Anzahl der Zeichen an, die y-Achse beschreibt die Anzahl der Teilnehmer, die ein Passwort mit dieser Länge erstellt haben.

ELEMENT	**Anzahl der Antworten**
Ich habe eines meiner Passwörter verwendet.	7
Ich habe eines meiner Passwörter modifiziert.	13
Ich habe ein komplett neues Passwort erstellt.	19
Das Passwort basiert auf ...	
... einem Namen/Wort und ich habe Ziffern/Symbole hinten und/oder vorne angehängt	1
... einem Namen/Wort und ich habe Ziffern/Symbole hinten und/oder vorne angehängt	9
... einem Namen/Wort, in dem ich Buchstaben weggelassen habe.	2
.. einem Wort, das aus einer anderen Sprache als Deutsch stammt.	6
... auf einer Adresse.	0
... einer Telefonnummer.	1
... einem Geburtstdatum.	3

Tabelle 5.4: Diese Tabelle beschreibt, wie viele Teilnehmer die angegebenen Strategien zur Passworterstellung anwenden.

einem Teilnehmer oder Teilnehmerin darf das Passwort gar keine Wörter enthalten. Bei 15% der Befragten gibt es eine Maximallänge. Fünf Teilnehmer waren sich der Richtlinien nicht sicher und drei gaben an, keine Richtlinien in der Arbeit zu erhalten.
Als Nächstes mussten die Testpersonen Sätze in einer fünf-Punkte-Likert-Skala bewerten, inwieweit sie auf sie zutreffen. Es wurden nicht alle Sätze von allen Befragten bewertet. Der Grund hierfür ist nicht bekannt. Da diese jedoch keine Pflichtfrage war, bestand die Möglichkeit, eine Antwort zu überspringen. Die Antworten mit den zugehörigen Werten des arithmetischen Mittels und der Standardabweichung sind in Tabelle 5.5 dargestellt. Insgesamt fällt es den Teilnehmern eher leicht, ein neues Passwort zu erstellen, weil sie eine gute Strategie haben. Teilweise werden die Passwörter wiederverwendet und ebenso teilweise sehen sich die Teilnehmer als kreativ in der Passworterstellung. Es fällt ihnen zum teilweise schwer, Passwörter zu erstellen, weil sie Schwierigkeiten haben, sich die Passwörter zu merken. Sie stimmen eher nicht zu, dass ihnen die Passworterstellung schwer fällt, weil sie keine gute Strategie haben. Die Tendenzen der sich gegenüberstehenden Aussagen stimmen überein.

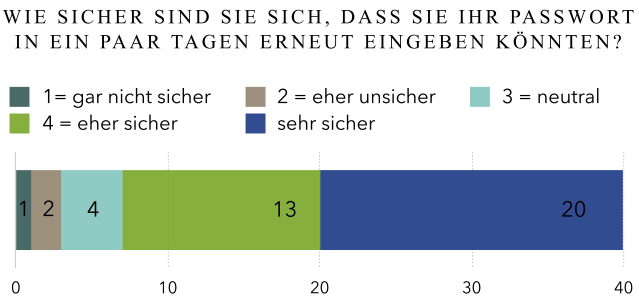

Abbildung 5.2: Verteilung der Teilnehmer-Antworten, wie sicher sie sich sind, ihr eben erstelltes Passwort in ein paar Tagen erneut eingeben zu können.

AUSSAGE	Ich stimme nicht zu (1)	Ich stimme eher nicht zu (2)	Ich stimme teilweise zu teilweise nicht zu (3)	Ich stimme eher zu (4)	Ich stimme ZU (5)	Arithmetisches mittel (M)	Standardabweichung (SD)
Mir fällt es leicht, ein neues Passwort zu erstellen, weil ...							
... ich eine gute Strategie habe	1	3	5	12	18	4,10	1,07
... ich meine eigenen Passwörter wiederverwende	5	3	12	10	9	3,38	1,30
... ich sehr kreativ bin	3	7	13	10	6	3,23	1,16
Mir fällt es NICHT leicht, ein neues Passwort zu erstellen, weil ...							
... ich nicht sehr kreativ bin	3	13	9	9	4	2,95	1,16
... ich mir Passwörter schwer merken kann	8	5	11	11	4	2,95	1,30
... ich keine gute Strategie habe	13	8	10	4	1	2,22	1,15

Tabelle 5.5: Diese Tabelle zeigt die Antworten der Teilnehmer auf und fasst sie mit dem jeweiligen arithmetischen Mittel und Standardabweichung zusammen.

In der darauffolgenden Frage wurden fünf verschiedene Strategien zur Passworterstellung gestellt. Es sollte beantwortet werden „Was ist Ihre Strategie zur Passworterstellung?“. 17 Teilnehmer (42,5%) setzen ihr Passwort aus bestimmten Wörtern zusammen. Vier Teilnehmer (10%) nehmen die Anfangsbuchstaben eines Satzes, den sie sich gut merken können. 18 Personen haben ein Passwort, das sie immer wieder abändern und erweitern, sechs verwenden ein Passwort eines anderen Accounts und lediglich fünf haben keine Strategie. Es wurden acht Antworten im Feld „Sonstiges:“ gegeben, die im Folgenden dargelegt werden. Zwei Teilnehmer verwenden einen Passwortmanager. Ein Teilnehmer oder Teilnehmerin fügt auf jeder neuen Internetseite zu einem bestehenden Passwort einen Teil des Namens oder eine Abkürzung dieser Seite hinzu, sodass er sich gut an das Passwort erinnern kann. Jemand anderes erklärte, verschiedene Kombinationen eines Passwortes zu verwenden, je nachdem, welchen Bezug er oder sie zu dieser Seite hatte. Eine weitere Strategie basierte auf Namen, die nicht die eigenen oder von Familienmitgliedern sind und mit Ziffern und Zeichen modifiziert werden. Zwei weitere Strategien basieren auf verschiedene Arten von Nummern. Die Antworten der Teilnehmer werden in Tabelle 5.6 aufgelistet.

Die Frage nach einer eventuellen Strategie, sich die Passwörter zu merken, ergab Folgendes. 13 Personen verwenden einen Passwort-Manager, Fünf notieren sich die Passwörter auf Notizblättern oder ähnlichem, vier verwenden zum Notieren ein digitales Notizblatt, also ein Textfile. Acht Personen merken sich die Passwörter durch Eselsbrücken und elf haben keine Strategie. Zusätzliche Antworten im Bereich „Sonstiges:“ ergaben für zwei Personen das explizite Einprägen der

Antworten im Feld „Sonstiges“ zur Frage: ***Was ist Ihre Strategie zur Passworterstellung?***
Für Internet etc. verwende ich einen Passwortmanager
I also create my password on a website based on website’s name (discrete enough so that no one can tell). This way I can remember the letters I always use and add words from website’s name to add on to that password.
I use different combinations based on the type of relationship I have with the site
Ich verwende Namen, die nicht meine eigenen sind oder in meiner Familie vorkommen, aber die ich mir gut merken kann und modifiziere diesen mit Zeichen und Ziffern.
Ordnungsnummer
Passwortmanager App
Sonderposten-ID- Nummer
Zufällige Tastaturanschläge, ergänzt mit einigen weiteren Zeichen

Tabelle 5.6: Diese Tabelle listet die acht Antworten der Teilnehmer im Feld „Sonstiges“ auf.

Passwörter. Insgesamt gaben 19 Teilnehmer (47,5%) zu, Passwörter für mehr als nur einen Zweck zu verwenden, 18 negierten dies (45%). Drei Personen gaben keine Antwort. Mithilfe der Methode der Grounded Theory wurde festgestellt, dass die Teilnehmer hauptsächlich entscheiden, welches ihrer Passwörter verwendet wird, je nach empfundener Wichtigkeit des Zwecks. Wichtige Daten werden durch als stark empfundene Passwörter geschützt. für weniger wichtige Zwecke genügt ein Schwächeres. über die Anzahl ihrer Passwörter gaben einzig acht Personen Auskunft. Zwei davon besitzen zwei bis drei Passwörter, vier von Ihnen haben vier, einer sieben bis acht und eine Person über zehn.
Die nächste Frage brachte die Erkenntnis, inwieweit die Teilnehmer bei der Passworterstellung in der Arbeit unterstützt werden. Die Ergebnisse zeigen, dass fünf Personen Hilfestellung vor der Eingabe des Passwortes erhalten, sechs während der Eingabe des Passwortes und lediglich drei nach der Eingabe des Passwortes. 28 Personen (70%) gaben an, keine Hilfestellung zu erhalten. Jeweils ein Teilnehmer oder Teilnehmerin erhält Hilfestellung vor und nach der Eingabe, vor und während der Eingabe und vor und nach der Eingabe. Zwei der Befragten erhalten Hilfestellung während und nach der Eingabe des Passwortes. Eine Erläuterung zur Weise, wie sie bei der Passworteingabe unterstützt wurden, gaben nur sieben Teilnehmer. Wie schon in der Vorstudie, gab eine der Teilnehmerinnen an, ein Feedback wie in dieser Studie zu erhalten. Ein weiterer Teilnehmer erhält Tipps zur Verwendung von verschiedenen Zeichenklassen, dass keine „normale[n] Wörter“ verwendet werden sollen und Hinweise zur Passwortstärke. Wiederum eine weitere Testperson erhält ebenfalls Hinweise zur Passwortstärke und eine Anzeige der Mindestvorgaben. Eine weitere Antwort lautete "Checkt das Passwort auf Ähnlichkeit und ob es alle nötigen Zeichen enthält.“ Ein anderes Mal wird ausschließlich ein Hinweis gegeben, wenn das neue Passwort dem alten entspricht. Die weiteren zwei Antworten beschreiben den Hinweis zum Aufbau des Passwortes, beziehungsweise die Angabe der Richtlinien.
Wie regelmäßig das Passwort in der Arbeit geändert werden muss, beschreiben die Tabelle 5.7 und die Abbildung 5.3. Wie oft dieses Passwort täglich eingegeben wird, zeigen die Tabelle 5.2 und das Diagramm in Abbildung 5.4.

WIE REGELMÄßIG ÄNDERN	**Anzahl der Antworten**
Alle 3-4 Wochen	4
Alle 6-8 Wochen	7
Alle 2-4 Monate	11
Alle 3-6 Monate	11
Häufiger	2
Seltener	1
Nie	4

Tabelle 5.7: Diese Tabelle beschreibt, in welchen regelmäßigen Abständen die Teilnehmer ihr Arbeits-Passwort ändern müssen.

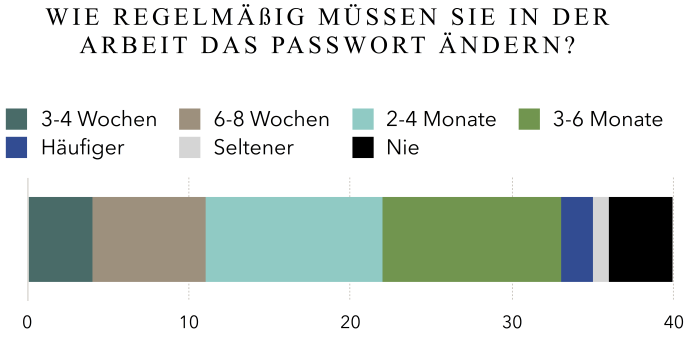

Abbildung 5.3: Darstellung der obigen Verteilung in einem Diagramm.

WIE OFT AM TAG	Anzahl der Antworten
1-2 mal	11
2-4 mal	9
4-6 mal	5
6-8 mal	7
Häufiger	7

Tabelle 5.8: Diese Tabelle beschreibt, wie oft die Teilnehmer ihre Passwörter am Tag durchschnittlich eingeben.

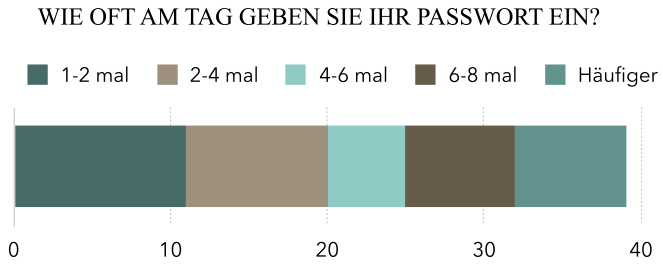

Abbildung 5.4: Darstellung letzterer Verteilung in einem Diagramm.

Sechste Fragegruppe Der letzte Teil des Fragebogens, der die soziale Erwünschtheit testet, zeigte wenig auffallenden Ergebnisse auf (M=9,19[5] ; SD=2,92). Sechs Teilnehmer erzielten einen ausreißenden Wert (Einer lag bei 3, Vier lagen bei 14 und Einer bei 16). Die Auswirkungen dieser Ergebnisse werden im folgenden Hauptkapitel erläutert.
Im nächsten Abschnitt werden die Haupterkenntnisse der Studie, die Ergebnisse der Grounded Theory dargelegt.

[5]Die höchste zu erreichende Zahl lag bei 17. Je höher das Ergebnis, desto höher ist die Soziale Erwünschtheit des Teilnehmers.

5.3 Qualitative Ergebnisse

Die Ergebnisse der Freitext-Antworten repräsentieren den Kernteil dieser Studie. Sie wurden mithilfe der Grounded Theory Methode nach Strauss und Corbin [7] analysiert. Dies ermöglichte es, die gesamten Antworten in fünf Kern-Kodes zusammenzufassen. Die Verbesserungswünsche der Teilnehmer an das existierende System umfassen die Erweiterung des derzeitigen Feedbacks durch mehr Information, die Ermutigung des Nutzers durch personalisiertere Hinweise und eine visuelle Darstellung der Passwortstärke. Des Weiteren sind die Teilnehmer der Meinung, es sei notwendig, die Nutzer allgemein mehr aufzuklären und äußerten Wünsche nach einer Änderung in den Passwortvorgaben.
Im Folgenden werden die einzelnen Schritte des Kodierungsvorganges beschrieben und deren Ergebnisse vorgestellt.

5.3.1 Offenes Kodieren

Der Vorgang der Grounded Theory wurde damit begonnen, alle zu analysierenden Fragen in einer Tabelle aufzureihen. Dann wurden nacheinander alle Antworten zu einem oder wenigen Kodes zusammengefasst und in die dazugehörigen Spalten eingefügt. So entstand eine Tabelle mit insgesamt 267 Kodes. Diese hohe Anzahl rührt daher, dass für jede Frage eine unterschiedliche Anzahl an Kodes erstellt wurde, je nach Ausführlichkeit der Antwort des Teilnehmers oder der Teilnehmerin. Auch wurden nicht zu allen Fragen stetig Antworten gegeben. Da nicht alle Fragen als Pflichtfragen programmiert waren, blieb es der Testperson überlassen, eine Antwort zu geben oder nicht.
Auffallend bereits in diesem ersten Schritt war eine tendenziell positive Einstellung der Teilnehmer gegenüber dem Programm. Begründung zur Aussage, „Ich würde es willkommen heißen“, bei der wiederkehrenden Passworterneuerung in der Arbeit ein solches Feedback wie in dieser Studie angezeigt würde, lieferte unter anderem Kodes wie „Definiert ein Minimum und hilft, es einzuhalten“ oder „Interesse an Kommentaren zur Sicherheit“. Die Aussage „Ich würde das Feedback beachten.“ ergab Kodes wie „Feedback mindert Frustration“ oder „Hilfe/Tipps während der Passworterstellung sorgen für besseres Passwort“. Ähnliche Antworten lieferten die Aussagen „Ich würde das Feedback anwenden“. Die negativen Aussagen „Ich würde das Feedback nicht beachten.“ und „Ich würde das Feedback nicht anwenden.“ wurden insgesamt vier mal angekreuzt. Die Begründungen zeigten, dass diese Teilnehmer keine Hilfe zur Passworterstellung benötigen. Die beiden Fragen zu Verbesserungsvorschlägen um das Feedback anwendbarer zu machen und nach Vorschlägen zur Erleichterung der Passwortneuerstellung, lieferten insgesamt 87 Kodes. Im nächsten Unterpunkt wird der zweite Durchgang, das axiale Kodieren und die resultierenden Ergebnisse beschrieben.

5.3.2 Axiales Kodieren

Nach dem Vorgang des offenen Kodierens folgte das axiale Kodieren. Hierbei wurden die Kodes jeder Frage jeweils in verschiedene Gruppen unterteilt. Die Gruppe wird durch einen zusammenfassenden Kode beschrieben. Für die weitere Zusammenfassen der Ergebnisse im späteren Verlauf der Auswertung, wurde versucht, möglichst für jede Frage ähnliche oder gleiche Kodes für die einzelnen Gruppen zu wählen. Ein zweiter Kodierer hat an dieser Stelle die Kodes des offenen Kodierens eigenständig nach seinem Verständnis in diese Gruppen einsortiert. Anschließend wurden die entstandenen Tabellen miteinander verglichen und Differenzen besprochen. Im gemeinsamen Einverständnis wurden sie daraufhin neu eingeordnet. Die Ergebnisse der resultierenden Tabelle lieferten für jede Frage zwischen drei und neun Gruppierungen. Einen Ausschnitt daraus zeigen die Tabellen 5.9 5.10. Im Folgenden werden diese Gruppen zugehörig zu ihren jeweiligen Fragen aufgeführt.

2. AXIALES KODIEREN	**Wie müsste man Ihrer Meinung nach das Feedback verbessern, dass es den Nutzern mehr nutzt bzw. dass Nutzer die Ratschläge befolgen?**
Erweiterung des derzeitigen Feedbacks durch mehr Informationen	Genau erklären, wie Passwort stärker wird
	Erklärung anbieten
	Vorschläge bringen
	Mehr kreatives Feedback
Feedback personalisieren	Persönlicher an Nutzer richten
	für alle Nutzer anwendbar machen
	Tipps hilfreicher als Warnungen
	Nutzer ermutigen ein starkes Passwort zu wählen
	Kunden Gefühl geben, alles richtig gemacht zu haben
Nutzer aufklären	Risiken nennen
	Folgen eines schlechten Passwortes erklären
	erklären, was passiert, wenn Passwort zu einfach
Visuelle Verbesserungen	Balken
	Farben (Rot, Gelb, Grün)
	Ziffern als Rubrik
	Visuelle Darstellung der Stärke
	Wachsender Balken mit mehr als 4 Stufen
	Balken mit Farben

Tabelle 5.9: Diese Tabelle zeigt einen Ausschnitt aus dem axialen Kodieren einer der Kern-Fragen. Links sind die Kategorien bzw. Oberbegriffe zu sehen, in der die Kodes unterteilt wurden. Rechts werden die jeweiligen Kodes dieser Kategorie aufgelistet.

Wie würden Sie reagieren, wenn das nächste Mal bei der Passworterneuerung in der Arbeit ein solches Feedback gegeben würde?
Die Begründungen zu dieser Aussage wurden in vier Gruppen unterteilt. Die Analyse bezog sich ausschließlich auf die Kodes der positiven Reaktionen („Ich würde es willkommen heißen.“, „Ich würde das Feedback anwenden.“, „Ich würde das Feedback beachten.“), da die negativen lediglich drei verschiedene Kodes aufwiesen, die sich nicht weiter gruppieren ließen.
Passwortstärke im Vordergrund. Die Kodes in dieser Rubrik beschreiben ein Interesse an der Passwortstärke. Dieses Interesse bezieht sich einerseits auf die Anzeige der Passwortstärke („Passwort so lange ändern, bis Stärke maximal“) oder andererseits darauf, dass das Feedback allgemein die Stärke des Passwortes erhöht und sicherstellt („Feedback hilft, stärkeres Passwort zu wählen, darum sehr willkommen“). Des Weiteren wurden in die Gruppe jegliche Kommentare zur Sicherheit aufgenommen („hilfreich, Anweisungen zur Verbesserung der Sicherheit zu erhalten“ oder „gut für Sicherheit“). Die Sicherheit eines Passwortes bezieht sich im Sinne der Studie auf die Passwortstärke und lässt sich somit hier eingliedern.
Generell positiv. Hier wurden alle Kodes eingefügt, die sich auf keinen bestimmten Aspekt des Feedbacks beziehen. Sie beschreiben eine grundsätzliche Zustimmung, ohne dabei ins Detail zu gehen („es ist hilfreich“, „es verbessert das Passwort“, etc.).
Neutral. Diese Gruppe beinhaltet Kodes, die in ihrer Aussage weder positiv noch negativ sind. Sie enthält einzig zwei Kodes: „Hilfreich, doch sollte einem selbst überlassen sein, ob man es anwendet“; „Beachten schon, aber eigene Passwörter immer recht sicher“.

Wie müsste man Ihrer Meinung nach das Feedback verbessern, dass es den Nutzern mehr nutzt bzw. dass Nutzer die Ratschläge befolgen?
Diese Frage war als Pflichtfrage programmiert, da sie für den Zweck der Studie essentiell war. Sie sollte hervorbringen, was sich die Nutzer allgemein unter einer guten Hilfestellung vorstellen und diente somit als Grundlage für die Verbesserung des bestehenden Feedback-Programms. Daher

lieferte sie am meisten Kodes, die in sieben Kategorien unterteilt wurden. Folgend werden die wichtigsten Kategorien aufgeführt. Keine Veränderung des derzeitigen Feedback-Systems. Die Kodes in dieser Gruppe weisen alle eine Zufriedenheit des derzeitigen Systems auf und nennen, keine Veränderungen zu benötigen („Dieses Feedback wird schon helfen“, „Glaubt an dieses Feedback“, etc.).
Erweiterung des derzeitigen Feedbacks durch mehr Informationen. Diese Antworten äußern den Wunsch nach mehr Informationen. Solche Informationen beziehen sich teilweise auf die Passwortstärke („Genau erklären, wie Passwort stärker wird“). Des Weiteren verlangen sie nach den Hintergründen, auf die das Feedback aufbaut („Gefühl geben, Feedback weiß, wovon es spricht“).
Feedback personalisieren und dadurch Nutzer ermutigen. Die Kodes dieser Gruppe beschreiben, dass die Hinweise nicht ausreichend an den Nutzer gerichtet werden. Es soll mehr auf den Nutzer eingegangen werden, um das Feedback effektiver werden zu lassen („Feedback für alle Nutzer anwendbar machen“). Wünsche nach konkreten Tipps wurden ebenfalls hier eingeordnet.
Nutzer aufklären. Der Nutzer soll über die Risiken eines Angriffes und die Folgen eines schwachen Passwortes informiert werden.
Visuelle Verbesserungen. Es wurden einige Verbesserungsvorschläge in Bezug auf die Darstellung des Feedbacks gegeben. Zum einen ergaben die Hinweise eine teilweise schlechte Resonanz („Anzeige der Hinweise deutlicher machen“). Zum anderen erwarten die Teilnehmer eine Darstellung der Passwortstärke in Form eines Balkens.

2. AXIALES KODIEREN	**Welche Vorschläge hätten Sie, um Ihnen die Passworterstellung zu erleichtern?**
Erweiterung des derzeitigen Feedbacks durch mehr Informationen	Einbindung, dass Großbuchstaben und Sonderzeichen auch Stärke erhöhen
	Sonderzeichen einbinden
	Zufälligkeit einbinden
	Auf Länge mehr eingehen
	Vorschlagen, mind. 1 Buchstaben zu verwenden
	Informieren über Sicherheit
Konkrete Beispiele geben, wie starke Passwörter erstellt werden können	Beispiele geben
	Formel zur Zusammenstellung von Passwörtern
	Lange Sätze vorschlagen, die man sich merken kann
	Beispiele konkretisieren (4 Ziffern auf Bezug auf Datum usw.)
	Nutzer zu langen Sätzen ermutigen
	Leichte Vorschläge bringen
Voraussetzungen für die Passworterstellung	Vorherige Passwörter anzeigen
	Ganze Sätze erlauben
	Zeichenbegrenzung aufheben
	Unsinnige Zeichenverbote aufheben
	Angabe der erlaubten Zeichen + Mindestvorgaben
	Nicht so oft ändern müssen

Tabelle 5.10: Zeigt wie vorherige Tabelle einige der Hauptkategorien des axialen Kodierens einer weiteren Frage (rechts) mit den jeweiligen Kodes (links).

Welche Vorschläge hätten Sie, um Ihnen die Passwortneuerstellung zu erleichtern? Diese Frage repräsentiert die zweite Kernfrage dieser Studie. Die Testpersonen sollten hier darlegen, in wiefern sie bei der Passworterstellung unterstützt werden wollen. Dies sollte eine weitere Grundlage für die Verbesserung des Systems liefern. Die Antwort-Kodes dieser Frage wurden in neun Gruppen unterteilt. Die wichtigsten Erkenntnisse sind Folgende.
Erweiterung des Feedbacks durch mehr Information. Wie schon in der vorhergehenden

Frage, lieferten die Antworten der Teilnehmer einige Kodes in Bezug auf die Erweiterung des Feedbacks. Das Feedback soll hauptsächlich mehr auf die Wirkung der Anwendung verschiedener Zeichenklassen eingehen („Sonderzeichen einbinden“, „Mehr Betonung dass spezielle Zeichen verwendet werden sollen statt nur mehr Wörter“).
Konkrete Beispiele geben, wie starke Passwörter erstellt werden können. Hier werden Wünsche nach Tipps geäußert, die helfen sollen, Ideen für Passwörter zu finden. Manche der Kodes beschreiben selbst Beispiele („Wort, das nur für Nutzer etwas bedeutet mit Ziffern“), andere verlangen danach („Beispiele geben“).
Passwortstärke im Vordergrund. Bei dieser Frage beinhaltet diese Gruppe konkrete Verbesserungswünsche in Bezug auf die Passwortstärke. Es soll mehr Informationen über die Stärke gegeben werden, sowie ihre visuelle Darstellung als Balken.
Anwendung dieses Systems. Auch bei dieser Frage gab es Teilnehmer, die das aktuelle System als gut befinden.
Voraussetzungen für die Passworterstellung. Einige Teilnehmer sind unzufrieden mit den Passwort-Vorgaben und bieten Änderungsvorschläge, die in dieser Gruppe gesammelt wurden. Diese Vorschläge beziehen sich auf die vorgesetzte Länge oder Verbote von Zeichen („Ganze Sätze erlauben“, „Zeichenbegrenzung aufheben“, „Unsinnige Zeichenvorgabe aufheben“), sowie auf die Anzeige der vorgesetzten Richtlinien („Vorherige Passwörter anzeigen“, „Angabe der erlaubten Zeichen + Mindestvorgaben“). Außerdem wurde der Wunsch geäußert, die Passwörter seltener ändern zu müssen.

Eine Reihe von Teilnehmern hat zu dieser Frage Antworten geliefert, die auf ein irrtümliches Verständnis der Frage hindeutet. Die Antworten beschrieben alle bestimmte Inhalte von Passwörtern. Antworten lauteten unter anderem „Verwenden Sie Zahlen und Sonderzeichen“ oder „Kombinationen aus Buchstaben, Zahlen, Sonderzeichen“. Ein Teilnehmer schrieb:

> „Ich denke, dass die stärksten Passwörter Zahlen haben müssen, Groß- und Kleinbuchstaben und Symbolen“

Dies führte zu der Annahme, die Frage sei so verstanden worden, man solle beschreiben, wie ein starkes Passwort erstellt wird. Die Antworten hierzu lieferten ein eindeutiges Ergebnis. Es besteht ein allgemeines Verständnis, dass ein starkes Passwort aus möglichst verschiedenen Zeichenklassen aufgebaut wird. Je mehr Sonderzeichen und Ziffern desto besser. Einmal wurde genannt, dass ein starkes Passwort durch Länge entsteht.

Warum unterscheiden sich die Passwörter von heute und aus der Arbeit in ihren Elementen und/oder der Länge?
Diese Frage wurde gestellt, falls sich die Angaben der beiden Passwortlängen unterschieden. Die Antwort-Kodes aus dem offenen Kodieren wurden sechs verschiedenen Kategorien zugewiesen, die in diesem Abschnitt erläutert werden.
Aufgrund des Feedbacks. Zwei Teilnehmer haben das Feedback angewandt, was dazu führte, dass sich die Passwörter in Länge und Elementen unterschieden.
Passwortstärke im Vordergrund. Die Kodes beschreiben hier, dass die Unterschiede aufgrund der angezeigten Passwortstärke entstanden sind. Die Teilnehmer wollten ein stärkeres Passwort erstellen, weshalb Unterschiede entstanden.
Sicherheit/Datenschutz. Dieser Oberbegriff beschreibt die Antwort-Kodes, die wegen eines Unterschiedes aufgrund von Schutzmaßnahmen entstanden. Teilnehmer wollten einerseits Ähnlichkeiten mit ihrem tatsächlichen Passwort ausschließen und sich selbst schützen. Andererseits wurde die Sicherheit erwähnt („für die Sicherheit“, „Vielfalt verschafft höhere Sicherheit“).
Mehr Kreativität möglich, wenn keine Vorschriften. Diese Gruppe lässt sich gut in Verbindung setzen mit den Wünschen nach Änderungen der Passwort-Vorgaben. Hier sammeln sich die

Antwort-Kodes, die besagen, dass durch das Fehlen jeglicher Richtlinien die Passworterstellung freier gestaltet werden konnte.
Neutral/Wichtigkeit. Die restlichen Kodes beschreiben neutrale Gründe, warum sich die Passwörter aus dem Test von denen aus der Arbeit unterscheiden. Die Teilnehmer hatten zum Teil keine Begründung oder wollten das Test-Passwort einfach halten.

Wie bewerten Sie die Notwendigkeit, regelmäßig die Passwörter zu ändern? Diese Frage diente der Einschätzung, inwieweit die Teilnehmer allgemein dazu gewillt sind, ihre Passwörter regelmäßig zu ändern. Dies könnte Einfluss darauf haben, wie das Feedback-System zu gestalten ist. Je geringer die Motivation das Passwort zu ändern ist, desto mehr Hilfe wird benötigt, um dem Nutzer die Aufgabe zu erleichtern. Insgesamt gab es drei Haupt-Kodes, in die die Antwort-Kodes kategorisiert wurden und im Laufe des Abschnitts dargelegt werden.
Negativ/Notwendig. Einige Kodes beschreiben negative Einstellungen mit der stetigen Änderung der Passwörter. Gründe hierfür sind Schwierigkeiten, sich die neuen Passwörter merken zu können oder die übertriebene Strenge der Vorgaben. Insgesamt wird einerseits erkannt, dass es eine Notwendigkeit für die Sicherheit ist, andererseits werden jedoch Zweifel an dem Prinzip genannt („Verständlich, doch fühlt sich überflüssig an, da starke PW gegen Hacks schon helfen“) und es als nervend empfunden („Nervig, aber notwenig“).
Neutral. Diese Kategorie beinhaltet die Kodes, die keine direkte Meinung angaben. Kodes wie „notwendig nur im Falle eines Datenmissbrauchs“ oder „Sollte so sein“ geben keine Wertung ab und beschreiben lediglich Tatsachen oder Teilnehmer, die weder positiv noch negativ über den Prozess denken („Keine Meinung“, „Mittel“).
Positiv/Notwendig. Die restlichen Antwort-Kodes beschreiben eine dringende Notwendigkeit des Passwortänderns.

5.3.3 Selektives Kodieren

Im letzten Kodierungsvorgang, dem selektiven Kodieren, wurde mithilfe der entstandenen Gruppen-Kodes versucht, einen oder wenige Kern-Kodes zu ermitteln. Diese Kern-Kodes stellen die Grundlage der daraus resultierenden Theorie des erforschten Themas dar. Bei der Analyse der Daten wurden vier Leitideen deutlich, wie in der Vorstellung der Testpersonen ein ideales Feedback-System aussieht. In den Antworten der Teilnehmer steckten Aufforderungen nach einer Erweiterung des Feedbacks unter anderem durch mehr Informationen zu den Hinweisen, Aufklärung der Nutzer über etwaige Folgen schlechter Passwörter, eine verbesserte, visuelle Darstellung des Feedbacks und eine direkte Hilfestellung für die Ideenfindung von Passwörtern.
Der Vorgang führte insgesamt zu sechs Kern-Kodes. Im Folgenden werden diese vorgestellt und erläutert.

Mehr Informationen

In den Antwort-Kodes aller Fragen, die sich auf das Feedback-System bezogen, konnte im axialen Kodieren festgestellt werden, dass die Hinweise und Warnungen nicht ausreichend erläutert werden. Beispielsweise antwortete eine Teilnehmerin auf die Frage, wie das Feedback ihrer Meinung nach verändert werden müsste:

> „Es müsste genauer sein. Und man muss das Gefühl haben, das Feedback weiß, wovon es spricht.“ [T1]

Oft wurde nicht verstanden, warum die Hinweise gegeben wurden oder warum nicht mehr auf die Verwendung von Sonderzeichen und Ziffern eingegangen wurde. Ein anderer Teilnehmer zum Beispiel antwortete darauf, wie er das Feedback empfunden hat:

> „I was a bit taken aback, because I thought that the password was at least a 3 on a scale of 0-4. Sure, the password wasn't long enough to add permutations, and hence decrease its strength, but I guess using variety provided me a false sense of security“ [T8]

Er erklärt, die geringe Passwortstärke nicht verstanden zu haben, da er eine andere Vorstellung davon hatte, was ein starkes Passwort ausmachte. Die Aussage wurde so interpretiert, dass mehr Informationen über die Hintergründe der Hinweise von Nöten sind, um es für alle Nutzer verständlich und anwendbar zu gestalten. Der Kode „Erweiterung des Feedbacks“ beinhaltet ferner Kommentare von Testpersonen, mehr auf alle Aspekte einzugehen, die Passwörter stark machen. Sie erklären, dass das gegebene Feedback ausschließlich auf die Aneinanderreihung mehrerer Wörter eingeht. Dies sollte erweitert werden durch die Einbindung von Hinweisen zur Länge und der Verwendung verschiedener Zeichenklassen.

Beispiele für Ideenfindung

Ein in diesem Schritt ermitteltes Problem der Nutzer besteht darin, sich Passwörter auszudenken, die gleichzeitig stark und dennoch merkbar sind. Die Kodes, die dieser Kern-Kode zusammenfasst, beschreiben Äußerungen, konkrete Tipps und Beispiele würden die Passworterstellung erleichtern. Das Feedback soll erweitert werden durch beispielhafte Hinweise zu starken Passwörtern, auf welche Weise diese erstellt werden können. Ein Teilnehmer schrieb:

> [Wie müsste man Ihrer Meinung nach das Feedback verbessern, dass es den Nutzern mehr nutzt bzw. dass Nutzer die Ratschläge befolgen?] „The feedback is good in terms of technical detail (use of special characters, length, etc). I would love to see more creative feedback to encourage the use of memorable strong pass phrases as an alternative, however.“ [T25]

Das Feedback ist seiner Meinung nach gut bezüglich der technischen Details wie die Länge und dem Gebrauch von Sonderzeichen. Er würde sich jedoch wünschen, es gäbe mehr kreative Rückmeldungen, die den Nutzer ermutigen, alternativ Passphrasen zu erstellen, die ebenso stark, doch einfacher zu merken sind. Die Passphrase ist ein Beispiel für eine konkrete Idee zur Passwortfindung. Eine weitere Idee wäre laut einer Teilnehmerin, eine Art Formel zur Passworterstellung („Das schwerste ist auf neue Passwort zusammenstellungen zu kommen, [...] vielleicht eine formel, zum beispiel, name von + geburtsjahr + Sonderzeichen, damit man weis was man zusammen setzen muss.“ [T4]), da dies der schwierigste Teil der Passworterstellung sei. Ein weiterer Vorschlag zur Erleichterung stellt ein Passwort-Generator dar. Dieser wurde mehrfach erwähnt und würde die Passworterstellung vollends übernehmen, sodass der Nutzer von der Aufgabe befreit wird, sich eines einfallen lassen zu müssen.

Visuelle Verbesserungen

Einige Teilnehmer bemängelten die Darstellung des Feedbacks. Zum einen wurde einige Male der Wunsch nach einem Passwort-Stärke-Indikator in Form eines Balkens geäußert. Ein Teilnehmer antwortete hierzu:

> [Wie müsste man Ihrer Meinung nach das Feedback verbessern, dass es den Nutzern mehr nutzt bzw. dass Nutzer die Ratschläge befolgen?] „Wie auf verschiedenen Websites -> Balken, der sich je nach stärke verfärbt und länger wird (von rot -> gelb -> grün). Anschauliches Feedback motiviert eher, Texte werden gerne überlesen.“ [T38]

Zum anderen kam heraus, dass die Hinweise nicht sichtbar genug sind und deutlicher gestaltet werden sollten.

Nutzer aufklären
Dieser Kern-Kode ergab sich aus der Frage nach den Verbesserungsvorschlägen, sodass die Ratschläge von den Nutzern befolgt würden. Wird der Nutzer über die Risiken eines schlechten Passwortes aufgeklärt, wirkt dies als der nötige Anreiz, um ein sicheres Passwort zu erstellen. Außerdem soll erläutert werden, was ein starkes oder schwaches Passwort ausmacht. Dies scheint oft nicht bekannt zu sein und führt somit zu falschen Annahmen in Bezug auf die Sicherheit des Passwortes.

Nutzer ermutigen
Dieser Kern-Kode beschreibt den Vorschlag, das Feedback anwendbarer zu machen, in dem man es personalisiert, um dadurch den Nutzer zu ermutigen. Ein Teilnehmer antwortete „De[m] Kunden das Gefühl geben, dass er alles richtig gemacht hat.“. Durch das direkte Ansprechen des Nutzers soll dieser dazu gebracht werden, starke Passwörter zu erstellen.

Änderungen der Passwort-Vorgaben
Wie zu erwarten, bekundeten einige Teilnehmer ihren Missmut gegenüber der strengen und ihrer Meinung nach oft unsinnigen Passwort-Vorgaben. Es sollten unter anderem ganze Sätze erlaubt werden und allgemein bestehende Zeichenbegrenzungen, sowie Zeichenverbote aufgehoben werden. Mehrfach erwähnt wurde ebenfalls die Aufforderung nach einer visuellen Darstellung der Vorgaben. Einerseits ist nicht immer klar, was die Richtlinien genau vorgeben und andererseits eines der größten Hindernisse darin besteht, allen gerecht zu werden. Anhand einer solchen Anzeige wäre es möglich, die Richtlinien nach einander abzuarbeiten. Laut einer Teilnehmerin ist es schwierig ein Passwort zu erstellen, da man die vorherigen zwei bis drei Passwörter nicht verwenden darf, jedoch nicht mehr weiß, welche das waren. Eine Anzeige dieser Passwörter wäre eine große Hilfe. Wiederum ein anderer Teilnehmer meinte, eine Hilfe wäre, die Passwörter nicht so oft ändern zu müssen.

Zusammenfassend lassen sich eindeutige Verbesserungsvorschläge an das System erkennen. Um zu erarbeiten, wie die Ergebnisse auf das System angewendet werden können, werden sie im folgenden Kapitel interpretiert und zu einem Lösungsvorschlag ausgearbeitet. Vorher wird im Folgenden erläutert, wie die Nutzererfahrung bezüglich des vorgegebenen Feedback-Systems ausgefallen ist.

5.4 Ergebnisse der Bewertung der Nutzererfahrung

Die Daten zur Bewertung der Nutzererfahrung wurden mithilfe zweier Strategien erhoben. Zum einen durch den bereits beschriebenen AttrakDiff Fragebogen und zum anderen durch die Frage „Wie haben Sie dieses Feedback empfunden?“ die mit einem freien Text beantwortet werden sollte. Die Ergebnisse fallen allgemein positiv aus und lauten wie folgt.

Zunächst werden die pragmatischen Qualitäten beschrieben. Insgesamt wurde das Feedback-System als eher technisch empfunden (M=4,58 ; SD=1,24). Es wirkt weder angenehm noch unangenehm (M=3,75 ; SD=1,32). Die Teilnehmer sehen es als eher einfach (M=2,98 ; SD=1,54) und eher sympathisch (M=3,40 ; SD=1,17). Weiterhin empfinden sie es als eher direkt (M=4,65 ; SD=1,58), eher einladend (M=4,70 ; SD=1,24), eher gut (M=2,63 ; SD=1,23) und eher übersichtlich (M=5,03 ; SD=1,31). Außerdem befinden sie es für eher motivierend (M=3,23 ; SD=1,29) und eher handhabbar (M=5,25 ; SD=1,28).
Des Weiteren wurden die hedonischen Qualitäten anekdotisch durch ein bis zwei Adjektive bewertet. Das System wirkt eher fachmännisch (M=3,43 ; SD=1,38) und eher praktisch (M=2,80 ; SD=1,20). Die stimulierende Qualität wird als weder originell noch konventionell bewertet (M=3,70 ; SD=1,54). Abbildung 5.11 zeigt eine Tabelle mit den genauen Werten der sieben-

Punkte-Likert-Skala.

SENMANTISCHES DIFFERENZIAL	**Arithmetisches Mittel M**	**Standard-abweichung SD**
menschlich (1) - technisch (7)	4,58	1,24
angenehm (1) - unangenehm (7)	3,75	1,32
einfach (1) - kompliziert (7)	2,98	1,49
sympathisch (1) - unsympathisch (7)	3,40	1,17
umständlich (1) - direkt (7)	4,65	1,85
zurückweisend (1) - einladend (7)	4,70	1,24
gut (1) - schlecht (7)	2,63	1,23
verwirrend (1) - übersichtlich (7)	5,03	1,31
motivierend (1) - entmutigend (7)	3,23	1,29
widerspenstig (1) - handhabbar (7)	5,25	1,28
fachmännisch (1) - laienhaft (7)	3,43	1,38
praktisch (1) - unpraktisch (7)	2,80	1,20
originell (1) - konventionell (7)	3,23	1,54

Tabelle 5.11: Bewertung der Benutzererfahrung bezüglich des im Test verwendeten Feedback-Systems. Es werden das Semantische Differenzial aufgelistet (links) und wie die Teilnehmer das System bewerten mithilfe des arithmetischen Mittels und der Standardabweichung.

Mithilfe der Grounded Theory wurde analysiert, wie die Testpersonen ihre Gedanken zu dem System beschreiben. Drei Teilnehmer haben keine Antwort gegeben. Insgesamt haben 13 von 37 Teilnehmern das System als positiv bewertet durch Antworten wie „gut“, „Sehr gut!“ oder „Gut und interessant“. Sie wurden empfunden als freundlich, einfach zu verstehen und hilfreich. Einmal wurde das Wort „lehrreich“ genannt. Zwei Teilnehmer antworteten, das Feedback sei gut für die Sicherheit. Es gibt das Gefühl, das Hacking Risiko zu verringern. Zusätzlich wurde von einigen Teilnehmern positiv auf die Passwort-Stärke eingegangen („Gibt Gefühl, dass Passwort stark genug ist“, „Zahlen hilfreich, um Entwicklung mitzuverfolgen“, „Gute Angabe der Passwortstärke“). Neutrale Antworten wurden angegeben, wenn beispielsweise die Hinweise nicht beobachtet wurden. Dies war der Fall, wenn das Passwort zu schnell eingetippt wurde, wie diese Teilnehmerin beschreibt:

> „Ich habe es nicht beachtet, da ich schneller getippt habe, als sich das Feedback aktualisieren konnte.“ [T35]

Nur wenige Teilnehmer empfanden das Feedback als negativ. Ein Teilnehmer fand es „ein wenig bevormundend“, ein anderer „nicht so gut“. Erklärungen hierzu wurden nicht gegeben. Eine Teilnehmerin berichtete:

> „[...] Die Warnungen fand ich ein bisschen nervig, weil sie etwas zynisch geschrieben waren (so was wie, „hilft nicht viel, etc.“)“. [T4]

Positiv fand sie jedoch die Angabe der Passwortstärke.
Im anschließenden Kapitel folgt die Interpretation der Ergebnisse.

6 Interpretation und Lösungsansatz

In diesem Kapitel werden die Ergebnisse der Hauptstudie zunächst interpretiert und zu einer Leittheorie zusammengefasst. Anschließend wird diese mit den Ergebnissen der Vorstudie verglichen. Daraus resultierend wird im abschließenden Abschnitt diese Theorie auf das existierende Feedback-System angewandt und ein Lösungsvorschlag präsentiert.

6.1 Auffälligkeiten in den quantitativen Ergebnissen

Wenige Antworten zu den Fragen des quantitativen Teils der Studie lieferten unerwartete Ergebnisse, welche im Folgenden diskutiert werden.

Länge der Passwörter und ihre Elemente. Die Frage nach der Länge der Passwörter in der Arbeit und der im Test erstellten Passwörter lieferte zum Teil eine sehr geringe Zahl als Antwort. Der Grund für die Passwörter mit einer solchen geringen Länge liegt in beiden Fragen nicht vor. Naheliegend sind Datenschutzgründe. Ebenfalls möglich wäre eine fehlende Motivation des Teilnehmers oder der Teilnehmerin, sich die Zeit zu nehmen ein Passwort zu erstellen oder später die Frage konkret zu beantworten. Ein weiterer Grund könnte sein, dass sich die Testpersonen nicht mehr an die tatsächliche Anzahl der Zeichen erinnern konnten und deshalb eine Zahl wie „1“ angaben.
Weiterhin ergab die Frage nach den verwendeten Elemente sowohl im Arbeitspasswort als auch im Testpasswort insgesamt eine sehr hohe Anzahl an unterschiedlichen Zeichenklassen. Fast Dreiviertel der befragten Personen gaben jeweils an, drei bis vier verschiedene Arten von Zeichen (Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen) verwendet zu haben. Von dem fiktiven Fall der Passworterstellung im Arbeitsumfeld haben die meisten Teilnehmer vermutlich die strengen Vorgaben verinnerlicht und im Test angewandt. Des Weiteren können diese Ergebnisse auf die Vorstellung der Teilnehmer zurückzuführen sein, was ein sicheres Passwort ausmacht. Mit dem Gedanken daran, ein starkes Passwort erstellen zu müssen, haben sich die Testpersonen möglicherweise bemüht, möglichst viele verschiedene Zeichenklassen in ihrem Passwort zu verwenden. Die Ergebnisse der Studie haben gezeigt, dass dies der Vorstellung eines sicheren Passwortes der Teilnehmer entspricht.

Ergebnissen der sozialen Erwünschtheit. Unter den Ergebnissen zur sozialen Erwünschtheit lieferten sechs „Ausreisser“. Die Antworten dieser Teilnehmer wurden im Einzelnen betrachtet, um zu erkennen, wo eventuell unehrlich geantwortet wurde. Da diese gesonderte Untersuchung jedoch keine Auffälligkeiten hervorbrachte, wurden die Antworten aller Teilnehmer in die Analyse einbezogen.

6.2 Interpretation der Ergebnisse

Im letzten Schritt der Grounded Theory wurden die Kern-Kodes noch einmal betrachtet und mithilfe der quantitativen Daten interpretiert, um eine grundlegende Theorie zu formulieren. Die resultierende Theorie beinhaltet das Verlangen der Teilnehmer nach mehr Wissen, auf die sie ihre Entscheidungen basieren können. Des Weiteren enthält sie eine greifbarere Darstellung des Feedbacks, sowie eine Entlastung der Nutzer durch konkrete Vorschläge zur Passworterstellung. Diese Aspekte werden im Folgenden näher erläutert.

6.2.1 Mehr Informationen zu Hintergründen der Hinweise und Warnungen

Die Ergebnisse des selektiven Kodierens brachten hervor, dass die Teilnehmer sich mehr Informationen zu den Hinweisen wünschen. Sowohl durch die Frage nach Vorschlägen zur Verbesserung des Feedbacks, als auch die Frage „Wie haben Sie dieses Feedback empfunden“ wurde ersichtlich,

dass ein Hauptproblem des Systems darin liegt, dass es nicht ausreichend Informationen zu den gegebenen Hinweisen liefert. Die Nutzer wenden Hinweise nicht an, wenn sie nicht verstehen, warum ihnen genau diese Hinweise gegeben werden. Es soll das Gefühl vermittelt werden, das Feedback weiß wovon es spricht. Auch Begründungen zur Frage „Was war nicht nachvollziehbar?“ ergaben Erläuterungen wie „Anforderungen scheinen oft etwas zufällig“ [T5]. Dies lässt sich darauf zurückführen, dass die meisten Teilnehmer hauptsächlich mit diesen Richtlinien vertraut sind: Mindestens acht Zeichen, mindestens ein Großbuchstabe, ein Sonderzeichen und eine Ziffer. Dies wird durch die Angaben der Teilnehmer über ihre vorgegebenen Richtlinien deutlich. Dadurch entsteht die Annahme, dass ein Passwort nur dann sicher sein kann, wenn es diese Kriterien entspricht. Wenn nun das Feedback den Hinweis gibt „Sonderzeichen helfen nicht sehr viel.“ ist der Nutzer verwirrt und zweifelt an der Glaubwürdigkeit des Programms.
Durch die eindeutigen Antworten der Teilnehmer wurde schnell klar, dass das Feedback durch Erklärungen erweitert werden muss, sodass sofort klar ist, was es bedeutet und warum es dem Nutzer angezeigt wird. Es darf kein Raum für Zweifel am System gelassen werden, weil man mit den vom System angewandten Strategien zur Passworterstellung nicht vertraut ist. Dies kann zusätzlich dazu führen, das Wissen der Nutzer im Allgemeinen zu erweitern, sodass sie im privaten Gebrauch die Taktiken anwenden, da sie als gut befunden werden. Eine zusätzliche Erweiterung des Feedbacks wurde in Bezug auf die Passwort-Stärke erwünscht, was im nächsten Abschnitt erklärt wird.

6.2.2 Nähere Erläuterung der Passwort-Stärke und dessen bildliche Darstellung

Wie auch bei den Hinweisen, wurde deutlich, dass eine Anzeige der Passwortstärke nicht ausreichend war. Während einige der Teilnehmer die maximale Stärke erreichen wollten und so lange das Passwort änderten, war sie für andere nicht wichtig genug. Dies wird mit der Frage bewiesen, auf was die Teilnehmer bei der Passworterstellung Wert legen. Weniger als die Hälfte der Teilnehmer (45%) bekundeten, vollen Wert auf die Passwort-Stärke zu legen. Drei Personen gaben an, wenig bis gar keinen Wert darauf zu legen. Ein Ansatz, um dies zu ändern, wäre die Erläuterung der Risiken eines Angriffs und die Folgen eines schlechten Passwortes. Wenn die Nutzer wissen, was passieren kann, wenn sie ein zu schwaches Passwort gewählt haben, ändert das eventuell ihre Einstellung in der Hinsicht. Zusätzlich wurde auch genannt, man wolle wissen, was diese angegeben Stärke bedeutete. Um diese Angabe begreiflich zu machen, sollte erklärt werden, was hinter dieser Zahl steckte und was sie ausmachte.
Der zweite Aspekt bezüglich der Passwortstärke ist ihre visuelle Darstellung. Unter den Verbesserungsvorschlägen der Teilnehmer wurde des Öfteren die Darstellung durch einen Balken oder eine farbige Darstellung der Passwort-Stärke genannt. Auch das Ergebnis, dass sich 13 Teilnehmer an einen Balken erinnert haben wollen, der wächst, wenn das Passwort stärker wird, lässt Raum für Interpretation. Die eine Möglichkeit ist, dass die Teilnehmer den Test nicht durchgeführt haben, um Zeit zu sparen und die Fragen dennoch beantwortet haben. Da jedoch die restlichen Antworten dieser Teilnehmer wiederum keine Hinweise dafür geben, führt dies zur Annahme, dass etwas anderes der Grund für diese hohe Anzahl an Falschantworten sein muss. Dies führt zur zweiten Möglichkeit. Da ein Passwort-Stärke-Indikator in Form eines Balkens bei der Erstellung von Passwörtern im Internet sehr oft vorkommt, wie unter anderem Ur et al. in ihrer Arbeit zeigen [32], ist es möglich, dass die Teilnehmer so sehr an diese Anzeige gewöhnt sind, dass das Gedächtnis eine falsche Erinnerung aufgrund von Erfahrung projiziert hat. Dieser Befund und der direkte Wunsch nach einem Passwort-Stärke-Balken führt zu dem Entschluss, das Feedback um einen solchen zu erweitern. Unter anderem Shay et al. [27] lassen keinen Zweifel daran, dass dies die Usability und Nutzererfahrung des Systems verbessern wird. Diese Nutzererfahrung soll mit einer weiteren Hilfe verbessert werden, die im Folgenden dargelegt wird.

6.2.3 Konkrete Beispiele zur Erstellung starker Passwörter

Die Aufgabe der Erstellung neuer Passwörter ist in vieler Hinsicht eine Bürde für die Nutzer. Zum einen brauchen sie eine Grundidee, einen Ansatz, aus dem das Passwort entsteht. Zum anderen müssen sie den meist strengen Vorgaben genügen, die ihnen vorgesetzt werden. Im Anwendungsfall dieser Arbeit kommt hinzu, dass diese Passwörter regelmäßig erneuert werden müssen, was bedeutet, in regelmäßigen Abständen immer wieder neue Ideen zu benötigen. Zusätzlich wird die Aufgabe dadurch erschwert, dass die Nutzer sich diese neuen Passwörter immer wieder neu merken müssen. Darauf wird bei der Passwortvergabe am meisten Wert gelegt. Dass dies für viele Teilnehmer Schwierigkeiten bereitet, zeigen die Ergebnisse der Fragen, wie das Feedback zu verbessern wäre und welche Vorschläge zur Erleichterung der Passworterstellung man hat. Obwohl die quantitativen Ergebnisse zeigen, dass die Teilnehmer insgesamt eher zustimmen, dass ihnen die Passworterstellung leicht fällt, weil sie eine gute Strategie haben, geben sie gleichzeitig an, sie wünschten sich konkrete Beispiele und Tipps zur Erstellung von sicheren Passwörtern. Daraus lässt sich schließen, dass die Teilnehmer allgemein zwar eine gute Strategie zur Passworterstellung haben, diese jedoch nicht unbedingt sichere Passwörter hervorbringt. Auch die Frage nach den verwendeten Elementen des im Test erstellten Passwortes zeigt, dass der Fokus der Teilnehmer auf der Verwendung von verschiedenen Zeichenklassen liegt. Das liegt zum einen wiederum an den vorgegebenen Richtlinien, doch zum anderen an der eingefahrenen Idee, was ein sicheres Passwort ausmacht. Ebenso festigen die Ergebnisse zur Frage nach der angewandten Strategie, dass nicht einmal die Hälfte aller Teilnehmer ein komplett neues Passwort erstellt haben. Der hohe Anteil an Wiederverwendung festigt die Annahme, dass eine fehlende Idee Grund ist für die Erstellung unsicherer Passwörter. Dem soll entgegen gewirkt werden, indem das Feedback-System erweitert wird durch konkrete Beispiele dafür, wie ein sicheres Passwort erstellt werden kann.

Insgesamt lässt sich feststellen, dass das Feedback um drei konkrete Aspekte erweitert werden sollte, um es für jeden Nutzer anwendbar zu machen. Diese drei Aspekte sind die Erweiterung durch mehr Informationen, einen Passwort-Stärke-Indikator in Form eines Balkens und einer Hilfestellung bei der Ideenfindung. Wenn man diese endgültigen Ergebnisse aus der Hauptstudie mit denen aus der Vorstudie vergleicht, lassen sich einige Gemeinsamkeiten erkennen. Diese werden im nächsten Abschnitt näher beschrieben.

6.3 Ergebnisse der Vorstudie als Voraussage der Ergebnisse

Die Hauptergebnisse der Vorstudie zeigen bereits, dass das Feedback mehr Informationen liefern sollte. Die Hinweise allein genügten nicht, um dem Nutzer das Gefühl zu geben, es wäre richtig, sie zu befolgen. Außerdem äußerten die Teilnehmer den Wunsch nach einer direkten Hilfestellung, um ihnen die Aufgabe der Passwortselektion zu erleichtern. Diese Hilfestellung sollte die Ideenfindung übernehmen, da dies eines der Hauptprobleme der Teilnehmer ist. Diese Ergebnisse wurden durch die Hauptstudie bestätigt. Ebenso verhielt es sich mit dem Vorschlag, eine Anzeige der vorgegebenen Richtlinien bereitzustellen. In der Vorstudie wurde diese Idee konkretisiert, indem vorgeschlagen wurde, es sollten die Vorgaben im Laufe der Eingabe abgehakt werden. Zusammenfassend lässt sich erkennen, dass die Vorstudie bereits die Hauptelemente der Verbesserung des Feedback-Systems ergab, welche die Hauptstudie als Ergebnisse hervorbrachte.

6.4 Verbesserung des Feedback-Systems

In diesem Unterpunkt wird dargestellt, wie die Vorschläge zur Verbesserung in Bezug auf das bestehende System realisiert wurden.

6.4.1 Erweiterung durch Information

Den ersten Aspekt bezüglich der Veränderungen des Feedback-Systems stellte eine Erweiterung der Informationen dar. Um dies zu bewerkstelligen, wurden an alle Hinweise und Warnungen des Programms kurze Erläuterungen angehängt. Diese beschrieben so knapp und dennoch so aussagekräftig wie möglich, die Hintergründe des Hinweises. Für den Fall einer Nachfrage nach der vollständigen Begründung des Feedbacks wurde ein Wort-Link erstellt. Dieser ruft auf Druck ein Pop-up-Fenster auf, in dem eine detaillierte und ausführliche Erklärung zu den gegebenen Hinweisen gegeben werden soll. Dies ließ sich mit dem Testablauf vereinen und wird im anschließenden Kapitel näher dargelegt. Die Anzeige des Fensters enthält ein Beispiel, wie eine solche Begründung erläutert werden könnte und wird in Abbildung 6.1 dargestellt.

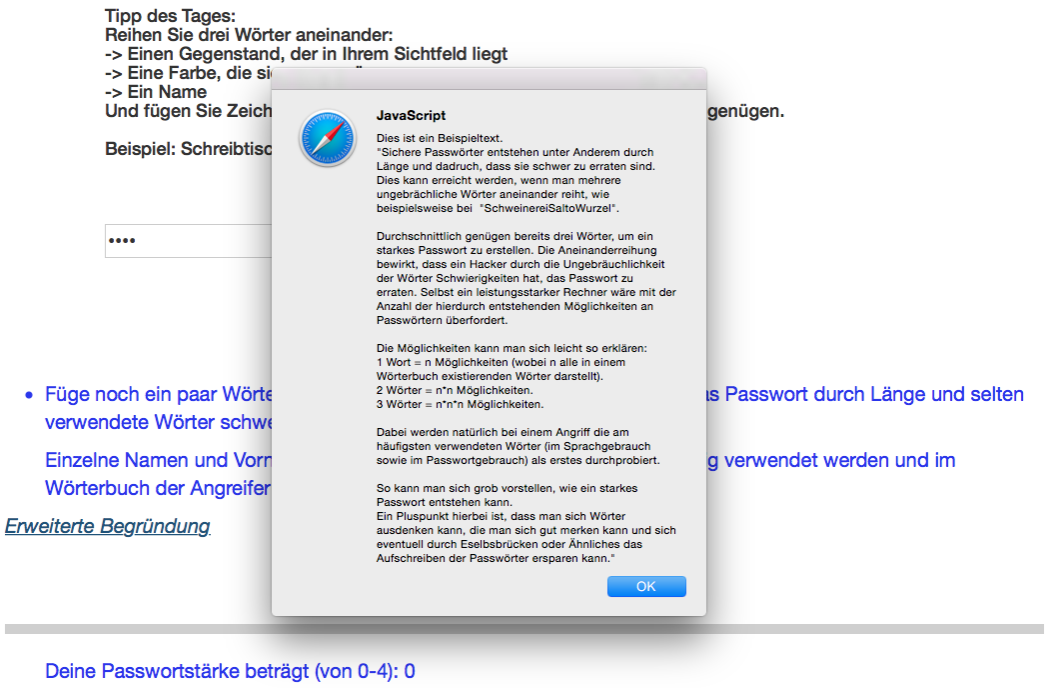

Abbildung 6.1: Hier ist ein Bildschirmphoto zu sehen, das das Pop-Up-Fenster mit einem Beispiel für eine detaillierte Begründung der Hinweise zeigt.

Des Weiteren wurden unter die Angabe der Passwort-Stärke als Zahl die dazugehörigen Bedeutungen gesetzt. Das Programm zxcvbn liefert diese Informationen als Echtzeitfeedback. Es wurde jedoch entschieden, die Anzeige permanent zu gestalten. Zum einen sollte dem Nutzer die Möglichkeit gegeben werden, sich im Vorhinein über die verschiedenen Stärken vertraut zu machen und zu erfahren, was sie besagen. Zum anderen besteht die Möglichkeit, dass diese Informationen andernfalls übersehen werden. Zu viele Anzeigen, die erscheinen und im Laufe der Passworterstellung verschwinden, können zur Folge haben, dass der Nutzer überfordert wird.

6.4.2 Einbau eines Passwortstärke-Indikator

Eine weitere Verbesserung in Verbindung mit der Passwort-Stärke ist der Einbau eines Passwort-Stärke-Indikators in Form eines Balkens. Dieser fällt sich in vier Stufen. Bei Stärke Null bleibt er leer, bei Stärke eins wird das erste Viertel des Balkens rot angezeigt, ab der nächst höheren Stärke wird die Hälfte des Balkens gelb angezeigt, dann orange und letztendlich grün.

Der Balken wurde unterhalb der Hinweise und oberhalb der Stärke-Anzeige als Zahl platziert. Die Entscheidung, die Anzeige der Stärke als Zahl beizubehalten wird einerseits damit begründet,

dass nicht allen Teilnehmern der Hauptstudie ein Balken als Anzeige gefehlt hat. Andererseits wurde von einigen Teilnehmern die Anzeige der Stärke positiv kommentiert. Weiterhin beweisen Ur et al. in einer Studie [32], dass die Kombination aus Text und visueller Darstellung ein wichtiger Faktor für die Zufriedenheit der Nutzer darstellt. Mit dem Erhalt beider Anzeigen wird gesichert, dass der Indikator-Balken nicht nur instinktiv sondern von allen Nutzern sofort verstanden werden kann. Zusätzlich wird verhindert, dass die darunter angezeigten Erläuterungen zur Passwort-Stärke nicht zugeordnet werden können.

6.4.3 Tipp des Tages

Der letzte Aspekt der Studien-Ergebnisse bezieht sich auf eine Hilfestellung zur Ideenfindung für Passwörter, die gleichzeitig sicher und dennoch merkbar sind. Um das zu gewährleisten, wurde der Begründungstext auf der Test-Seite entfernt und mit einem „Tipp des Tages“ ersetzt. Dieser Tipp stellt ein detailliertes Konzept vor, wie ein Passwort erstellt werden kann. Die daraus resultierenden Passwörter weisen stets die Maximalstärke auf. Das Konzept zielt darauf ab, dass das Passwort für den Nutzer gut zu merken ist. Die Idee hinter diesem Tagestipp besteht darin, für jede wiederkehrende Passworterneuerung einen anderen Vorschlag anzeigen zu lassen. Dieser Vorschlag ist freiwillig anzuwenden und soll dem Nutzer den nötigen Anstoß für ein Passwort bringen und die Passwortselektion somit erleichtern und beschleunigen.

Diese Anwendung der Ergebnisse beschränkt sich auf die, im Rahmen dieser Forschungsarbeit, möglichen Anpassungen. Im Folgenden werden Anregungen gegeben, wie die restlichen Ergebnisse dieser Studie von Firmen und Unternehmen verwendet und übernommen werden können.

6.5 Zusätzlicher Verbesserungsvorschlag für Firmen und Unternehmen

Die Äußerungen der Nutzer über die strikten Passwort-Vorgaben in ihrer Arbeit beschreiben einen allgemeinen Missmut. Die Ergebnisse zeigen, dass die Teilnehmer empfehlen würden, die oft unverständlichen Richtlinien zu lockern. Auch ist den Teilnehmern nicht immer klar, welche Vorgaben es gibt. Weiterhin zeigen sowohl die Vorstudie als auch die Hauptstudie, dass eines der hauptsächlichen Hindernisse der schnellen Passworterstellung darin besteht, dass nicht immer klar ist, welche Vorgaben erfüllt wurden und welche fehlen. Dies führt zu teilweise mehrfachen Ablehnung der Eingaben. Ein hierdurch resultierender Lösungsvorschlag wäre eine Anzeige der Richtlinien auf der Nutzeroberfläche, auf der die Passworterneuerung stattfindet. Ein Beispiel hierfür wird unter Anderem bei der Erstellung der „Apple-ID“ oder bei der Erstellung eines „Googlemail“ Accounts verwendet [3] und [13]. Die Abbildungen 6.2 und 6.3 zeigen Bilder dieser beiden Seiten.

Diese Maßnahme würde dazu beitragen, den Mitarbeitern die Passworterstellung zu erleichtern. Das könnte bereits eine Minderung der Frustration bezüglich der regelmäßigen Neuerstellung mindern.

Die oben genannten Veränderungen des Feedback-Systems wurden in einer weiteren Studie getestet. Im nächsten Kapitel werden die Durchführung und die Ergebnisse dieser Studie dargestellt und erläutert.

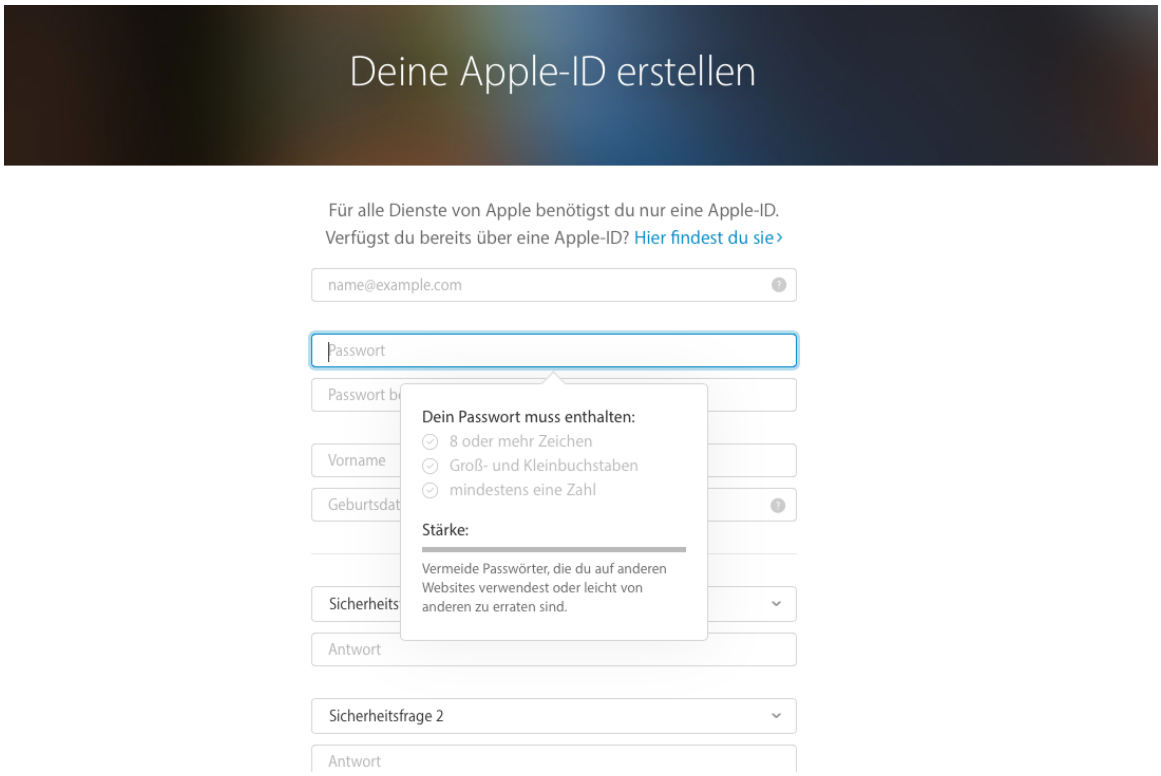

Abbildung 6.2: Bildschirmphoto bei der Erstellung einer Apple-ID

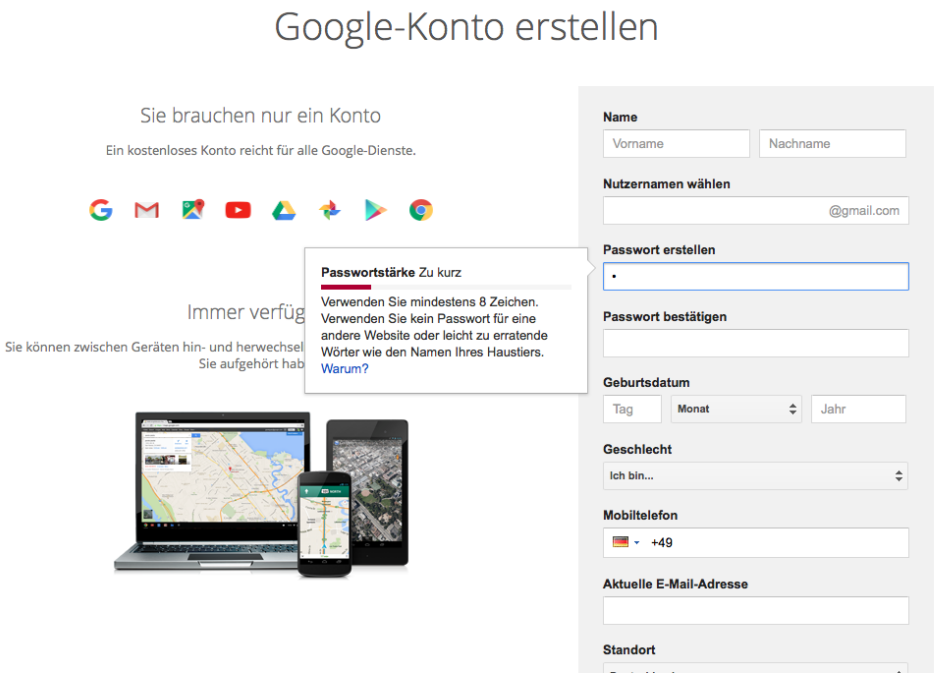

Abbildung 6.3: Bildschirmphoto bei der Erstellung eines Googlemail-Kontos.

7 Testen der Lösung durch anekdotische Befragung

Nach der Implementierung der aus der Hauptstudie resultierenden Verbesserungsvorschläge, wurde eine weitere Befragung durchgeführt. Es sollte herausgefunden werden, inwieweit dieses neue System bei den Nutzern Anklang findet und wie sie es bewerten. In den folgenden Abschnitten wird der Aufbau und die Durchführung dieser Studie beschrieben und anschließend die Ergebnisse präsentiert. Im letzten Abschnitt werden die Erkenntnisse zusammengefasst und ein Vergleich zur Hauptstudie aufgestellt.

7.1 Aufbau und Durchführung der Befragung

Die Testung des verbesserten Systems erfolgte anhand einer anekdotisch aufgezogenen fünf-Personen-Studie. Im Zuge dieser Studie wurde den fünf Personen aus der Vorstudie das neue Programm vorgestellt und erneut befragt. Im Folgenden werden die Gründe für diese Teilnehmerauswahl erläutert und anschließend der Aufbau der HTML-Seite beschrieben. Abschließend folgt die Schilderung des Fragebogens und des Ablaufs der Befragung.

7.1.1 Auswahl der Teilnehmer und Internetseite

Die Ähnlichkeit der Ergebnisse aus Vor- und Hauptstudie liefern die Erkenntnis, dass die fünf Teilnehmer der ersten Studie bereits ausreichen, um das System zu bewerten. Aus diesem Grund wurden diese fünf Personen gebeten, bei einer zweiten Befragung teilzunehmen. Auch hatten diese Fünf die erste Version des Programms ebenfalls getestet, was die Möglichkeit bot, diese zwei Systeme direkt miteinander vergleichen zu lassen. Die Grundlage der Befragung lieferte ein weiteres Mal die erstellte HTML-Seite, die im nächsten Abschnitt beschrieben wird.

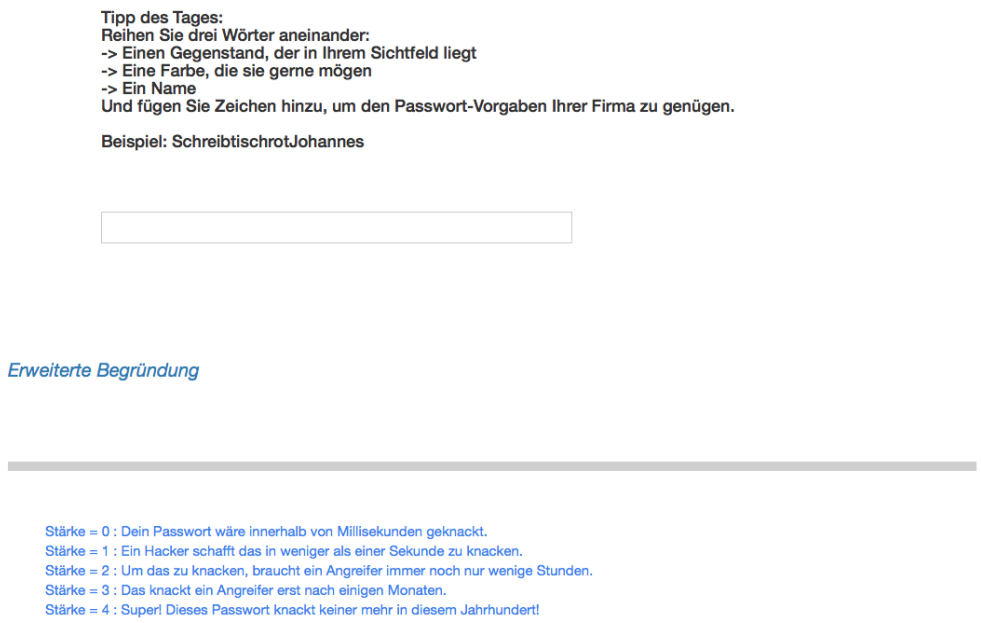

Abbildung 7.1: Bildschirmphoto der neuen, verbesserten Passwort-Testseite vor einer Eingabe.

Die Nutzeroberfläche für die Befragung stellte die verbesserte Testseite aus der Hauptstudie dar (siehe Abbildungen 7.1 und 7.2). Aufgrund der persönlichen Interviews, waren die ergriffenen Maßnahmen für eine Online-Studie nicht mehr notwendig und wurden entfernt. Der Aufbau der

Abbildung 7.2: Bildschirmphoto der neuen, verbesserten Passwort-Testseite, bei Eingabe mit dem zweiten Tipp als Hilfestellung und dem eingefärbten Balken.

Testseite entspricht der Beschreibung des verbesserten Systems. Der „Tipp des Tages“ wurde so implementiert, dass der zugehörige Text nach einem ersten Testdurchlauf geändert wurde und die Teilnehmer gebeten wurden, erneut ein Passwort zu erstellen. Die zwei Tipps lauten wie folgt:

> Tipp 1: „Tipp des Tages: Reihen Sie drei Wörter aneinander.
> -> Einen Gegenstand, der in ihrem Sichtfeld liegt
> -> Eine Farbe, die Sie gerne mögen
> -> Ein Name
> Beispiel: SchreibtischRotJohannes“

> Tipp 2: „Tipp des Tages: Denken Sie Sich einen Satz oder Wörter aus, die ein aktuelles Lebensziel von Ihnen beschreiben und fügen Sie die Symbole, Ziffern, etc. im Inneren des Passwortes ein, um den Passwort-Vorgaben Ihrer Firma zu genügen.
> Beispiel: IchKaufeMir2020EinNeuesAuto!“

Diese Tipps basieren auf einer der Grundideen von zxcvbn. Je länger das Passwort ist, desto stärker wird es. Dies kann durch das Aneinanderreihen von möglichst ungebräuchlichen Wörtern erreicht werden. Ebenso ist bekannt, dass Passphrasen ebenso stark sein können, wie Passwörter aus vier verschiedenen Zeichenklassen bestehend [19].
Der genaue Ablauf der Befragung wird im Folgenden erläutert.

7.1.2 Testablauf und Fragebogen

Die Interviews waren erneut semi-strukturiert und fanden im Rahmen eines persönlichen Gesprächs statt. Sie wurden in zwei Teilen abgehalten. Der erste Teil bestand aus dem eigentlichen Test, welcher zweimal hintereinander durchgeführt wurde. Diesem Verfahren lag der Wechsel des

„Tipp des Tages“ zugrunde. Den Teilnehmern wurde im Vorhinein gesagt, dies sei ein weiteres Feedback-System, das sie testen und mit dem ersten System vergleichen sollten. Sie sollten sich erneut vorstellen, sie seien in der Arbeit und es sei an der Zeit, das Passwort zu erneuern. Sie wurden gebeten, ihr Verhalten und ihre Gedanken während der Testdurchläufe kontinuierlich offen darzulegen und ihre Vorgehensweise zu erläutern. Hierdurch konnte ein Einblick in ihre Handlungen gewährleistet werden.
Nachdem die Teilnehmer das erste Passwort erstellt hatten, wurde der „Tipp des Tages“ verändert. Anschließend wurden die Personen gebeten, sie sollen sich vorstellen, es sei erneut an der Zeit, das Passwort zu ändern und mögen dies tun. Es sollte einerseits getestet werden, ob die Teilnehmer sofort erkennen, dass der Tipp sich verändert hatte. Andererseits diente dieser Schritt der Beurteilung, wie dieses Konzept bei den Nutzern ankommt.
Im anschließenden zweiten Teil der Studie fand das Interview statt. Der grundlegende Fragebogen bestand aus 13 Fragen. Die vollständige Liste der Fragen wird in Appendix C aufgeführt. Als Einstieg wurde zunächst in Erfahrung gebracht, an was sich die Befragten von der ersten Studie erinnern konnten. Dann folgten sechs der Kernfragen aus der Hauptstudie. Dies sollte einen direkten Vergleich der Ergebnisse ermöglichen. Abschließend folgten vier Fragen zu den einzelnen Aspekten des Systems. Es sollte jeweils erkannt werden, ob das Feedback angewendet wurde und inwieweit der neue Link zur näheren Erläuterung der Hinweise Anklang findet. Weiterhin sollte geklärt werden, wie das Konzept des ständig wechselnden Vorschlags zur Passworterstellung von den Nutzern aufgenommen wird. Mithilfe der zwei abschließenden Fragen, sollte ein Vergleich zwischen dem vorherigen und dem aktuellen Feedback-Systems erstellt werden.
Der nächste Abschnitt legt die Ergebnisse der Befragung dar.

7.2 Ergebnisse der Befragung

Insgesamt wurde das System als positiv empfunden, wobei der „Tipp des Tages“ am meisten Zuspruch bekam. Die Teilnehmer würden das System anwenden und erkennen keine grundlegenden Ansätze zur Verbesserung. Im direkten Vergleich mit dem ersten System, würden sie einstimmig das zweite bevorzugen. Die Ergebnisse werden im Folgenden stichprobenartig beschrieben.

7.2.1 Ergebnisse der Kernfragen

Die Frage, wie das Feedback empfunden wurde, ergab eine einstimmige positive Zustimmung. Alle Teilnehmer antworteten „gut“ oder „sehr gut“. Mehrfach wurde erwähnt, dass die Anzeige der Passwort-Stärke eine positive Auswirkung auf der Erstellung des Passwortes habe. Es sei gut zu wissen, wie sicher das Passwort ist, wobei der Passwort-Stärke-Indikator als farbewechselnder Balken eher Zuspruch bekam. Ein Teilnehmer erklärte, die Stärke sei gut zu wissen, doch er habe den Balken eher beachtet, als die Schrift. Eine Teilnehmerin meinte:

> „Passwort ausdenken ist immer so, dass man sich denkt, warum bloß? Und deshalb ist man wohl so fixiert auf Optisches. Deswegen ist der Balken gut, das Geschriebene ist oft zu anstrengend zu lesen.“

Die Hinweise waren insgesamt verständlich. Ein Teilnehmer bemerkte eine Unstimmigkeit des Programms, was zu der Bewertung „Fast immer verständlich“ führte:

> „Wenn das Passwort schon Stärke Zwei hat und man dann eine Wiederholung eintippt, wechselt die Stärke von Vier auf Drei zurück oder von Drei auf Zwei, aber es steht keine Begründung mehr da.“

Des Weiteren bewerteten die Teilnehmer die Hinweise als nachvollziehbar. Drei von ihnen würden das Feedback in der Arbeit willkommen heißen, Vier würden es beachten und alle würden es anwenden. Ein Teilnehmer begründete beispielsweise:

> „Ich würde sonst Gefahr laufen, eines meiner drei Standard-Passwörter zu verwenden, die ja nicht sicher sind. Habe sie gerade getestet. Außerdem ist ein Vorteil der Hinweise vielleicht auch, dass man sich an die Hinweise erinnert und sich dadurch an sein Passwort besser erinnern kann."

Auf die Frage nach Verbesserungen des Feedbacks wurden einerseits Verschönerungen des Layouts genannt. Außerdem kam die Idee, dass das Passwort erkannt werden und darauf gezielt eingegangen werden sollte, an welcher Stelle es noch verbessert werden kann. Ein Teilnehmer schlug eine Art Bonussystem vor, das den Zeitraum wann das Passwort wieder geändert werden müsste, verlängerte, je stärker das Passwort war. Welche Ratschläge gerne gesehen worden wären, ergab lediglich die Anzeige der Passwort-Vorgaben und eines Zeichenzählers. Eine Teilnehmerin äußerte zusätzlich die Idee eines Wiederholungsfeldes, um Tippfehlern vorzubeugen.
Die Ergebnisse bezüglich der einzelnen Aspekte der Hilfestellung wird im nächsten Abschnitt präsentiert.

7.2.2 Resonanz der einzelnen Features und Vergleich mit erster Version

Die Ratschläge und Hinweise wurden insgesamt nur teilweise angewandt. Oft wurden sie übersehen, da der Tipp bereits dazu geführt hatte, dass das Passwort sofort die maximale Stärke erreichte. Es fand jedoch Anklang, wenn das Passwort noch nicht stark genug war.
Die Anzeige der Stärke in Form eines Balkens ist allen Teilnehmern positiv aufgefallen. Die Erläuterung der einzelnen Stärke-Stufen verstärkte das Gefühl der Sicherheit durch die konkrete Angabe der Zeit, die ein Angreifer benötigte, um das Passwort zu knacken. Die Information wurde dadurch „greifbarer".
Der „Tipp des Tages" wurde von allen Teilnehmern verwendet. Insgesamt erhielt jedoch das erste Beispiel mehr Zustimmung, da es als leichter anwendbar empfunden wurde. Allen Testpersonen fiel sofort auf, dass er sich im zweiten Durchlauf geändert hatte und bewerten dies als „gut".
Die erweiterte Begründung in Form eines Links wurde lediglich einmal aufgerufen. Der Teilnehmer tat dies aus Neugier. Er hatte mehr Interesse zu erfahren, was angezeigt werden würde, als an der tatsächlichen Information. Er bekundete jedoch, wenigstens einmal lesen zu wollen, welche zusätzlichen Informationen gegeben werden würden. Zwei Teilnehmern war der Link nicht aufgefallen, da sie nicht dazu kamen, die Hinweise zu beachten. Eine Person erklärte dies wie folgt:

> „Ich bin nicht zu den Hinweisen gekommen, deswegen hätte ich den Link auch nicht geklickt. Wenn mein Passwort im roten Bereich geblieben wäre, hätte ich drauf gedrückt, um zu erfahren, warum das so ist. Aber da mein Passwort sofort die Stärke Vier hatte, gab es für sie keinen Grund."

Mit dem Wissen, dass es einen solchen Link gibt, gaben vier der Befragten an, sie würden einmal nachlesen, was die erweiterte Begründung darstellte, zur Befriedigung der Neugier. Einer sah kein Interesse darin, da ihn ausschließlich die Stärke des Passwortes interessierte. Die Hintergründe, wie es dazu kam, waren für ihn nicht ausschlaggebend.

Verglichen mit der ersten getesteten Version des Programms, schnitt diese Zweite deutlich besser ab. Die Frage „Versuchen Sie Sich zu erinnern: Wie vergleichen Sie das Feedback-System vom letzten Mal mit dem Heutigen?" ergab Folgendes. Es wurde erkannt, dass im zweiten Test das Feedback detaillierter war. Die Begründungen hinter den Hinweisen waren eine Verbesserung. Sie waren kurz und prägnant und konnten auf Dauer bewirken, dass man verinnerlicht, was ein starkes Passwort ausmacht und es in Zukunft von Haus aus anwendet.
Als ein weiterer Zusatz wurde der Passwort-Balken genannt. Gemeinsam mit den Erklärungen sei das eine „signifikante Steigerung [...] für das Sicherheitsdenken". Insgesamt wurde im zweiten

Interview das Feedback als „deutlicher und verständlicher“ bewertet.
Alle Teilnehmer würden das zweite System bevorzugen.
Als Nächstes werden diese Ergebnisse mit denen aus der Hauptstudie verglichen und ein Fazit daraus gezogen.

7.3 Diskussion der Ergebnisse

Die Resultate der letzten Studie zeigen eine deutliche Verbesserung bezüglich der Zufriedenheit mit dem vorgegebenen Feedback-System auf. Die wenigen Verbesserungsvorschläge, die noch genannt wurden, wenden sich nicht mehr an das System selbst. Es kann demnach festgestellt werden, dass die Verbesserung erfolgreich durchgeführt wurde. Die Lösungsansätze zeigten eine ausreichende Befriedigung der Wünsche der Nutzer. Dies wird im Folgenden näher erläutert.

Mehr Informationen zu Hinweisen und Warnungen Das Verlangen nach mehr Informationen wurde durch die Erweiterung der bereits vorhandenen Sätze bewerkstelligt. Der zusätzliche Link zu einer näheren Begründung stellt sicher, dass alle eventuellen Fragen beantwortet werden können, falls dies erwünscht ist. Er vereint die Neugier der Nutzer mit der Vorgabe, ihn nicht mit zu viel Informationen zu überfordern.

Nähere Erläuterungen zur Passwortstärke und visuelle Darstellung Eine gute Resonanz des Passwort-Stärke-Indikators wurde bereits ausgiebig erforscht [32] und war demnach zu erwarten. Die zusätzlich Erläuterungen, was die Passwort-Stärke bei einem Angriff ausmacht, verstärkt das Gefühl der Sicherheit und bewirkt, dass die Passwort-Stärke nicht mehr missverstanden wird.

Konkrete Beispiele zur Passworterstellung Der Lösungsansatz, die Ideenfindung zur Passworterstellung mithilfe eines „Tipp des Tages“ zu erleichtern fand großen Anklang. Jeder der Befragten äußerte sich positiv darüber und hat ihn sofort verwendet. Er hilft den Nutzern, schnell ein sicheres Passwort zu erstellen. Statt diesem Lösungsvorschlag hätte hier ein Passwortgenerator implementiert werden können. Dieser hätte den Nutzern die Aufgabe des Passworterstellens vollständig abgenommen. Die Ergebnisse deuten jedoch auf ausreichende Zufriedenheit bei den Nutzern hin.

Die Studie arbeitet den vorgestellten Lösungsvorschlag als einen insgesamt guten Ansatzpunkt heraus, um die Nutzer bei der Passwortselektion zu unterstützen. Er stellt jedoch lediglich ein Bruchteil der Möglichkeiten dar, wie die Ergebnisse der Hauptstudie implementiert werden könnten. Des Weiteren gibt es noch weitere Aspekte der Verbesserung, die den Rahmen dieser Forschungsarbeit überschreiten würden. Im nächsten und abschließenden Teil der Arbeit folgt die Zusammenfassung der Erkenntnisse und der Ausblick auf daraus resultierenden Forschungsansätze.

8 Zusammenfassung und Ausblick

In diesem Abschnitt wird die Arbeit zunächst im Ganzen zusammengefasst und die Ergebnisse in den Gesamtzusammenhang eingeordnet. Abschließend wird ein Ausblick auf zukünftige Arbeiten und Forschungsansätze gegeben.

Zusammenfassend bestätigt diese Studie, dass die Nutzer grundsätzlich starke Passwörter erstellen möchten. Dies scheitert jedoch teilweise an einer falschen Vorstellung davon, woraus diese Stärke hervorgeht und an den zu strengen Vorgaben, die von Sicherheits-Administratoren auferlegt werden. Um Diesem entgegenzuwirken und den Usern zur Hilfe zu kommen, wurde ein bestehendes Feedback-System für den Nutzer angepasst und verbessert. Die Anliegen der Anwender wurden erkannt und das Feedback dementsprechend erweitert. Es werden nun alle Warnungen und Hinweise kurz und knapp erläutert und somit ihre Hintergründe dargestellt. Die visuelle Darstellung wurde durch einen "Passwort-Meter" ergänzt, welcher dynamisch die Stärke des Passwortes anzeigt. Schließlich wurde der Wunsch der Nutzer nach konkreten Vorschlägen zur Passworterstellung durch das Konzept erfüllt, bei jeder Passworterneuerung ein neues Beispiel zur Ideenfindung für ein starkes Passwort vorzuschlagen. Eine anekdotisch aufgezogene abschließende Studie zeigt, dass das neue Programm die Bedürfnisse der Anwender erfüllt.
Es wurde gezeigt, dass es wichtig ist, den Nutzer bei der Passwortwahl zu unterstützen. Hierfür genügt selbst eine grundlegende Hilfestellung, um ein Gefühl der Unterstützung hervorzurufen und dadurch die schwere Aufgabe der Passworterstellung zu erleichtern.

Dass ein solches Feedback die Usability erhöht, beweisen bereits Shay et al. [27] und wurde in dieser Arbeit nicht weiter erforscht. Die Arbeit baut darauf auf und bestätigt die Vermutung von Ur et al. [31], dass man durch gezieltes Feedback den Usern helfen kann, zu verstehen, was ein tatsächlich starkes Passwort ausmacht. Ebenso wird Adams und Sasses Ansatz [1] bestätigt, es müsse auf den Nutzer eingegangen werden, um ihren Missmut diesbezüglich zu mindern. In weiteren Studien kann nun getestet werden, wie weit dieser Missmut und die Frustration der Anwender tatsächlich sinkt. Ein weiterer Ansatz für fortführende Arbeiten wäre eine Untersuchung der auf Basis des Feedback-Systems erzeugten Passwörter hinsichtlich ihrer Stärke. Es wäre wichtig und ebenso interessant zu erfahren, ob dieses System nicht nur eine Hilfestellung für die Nutzer darstellt, sondern gleichzeitig eine Verbesserung der Sicherheit bewirkt. Auch ob die Hilfe in der Praxis so viel Anwendung findet, wie erwartet, bleibt eine zu beantwortende Frage.

Insgesamt ist eines der wichtigsten Erkenntnisse dieser Arbeit, dass die Unternehmen beziehungsweise Organisationen nicht viel unternehmen müssten, um ihren Mitarbeitern das Arbeitsleben zu erleichtern und gleichzeitig die Sicherheit zu gewährleisten. Das vorgeschlagene Programm bietet einen allgemeinen Anhaltspunkt, auf dem für verschiedene Anwendungsbereiche aufgebaut werden kann. Um das Programm weiter zu optimieren, könnte der beschriebene Vorschlag aufgenommen und zusätzlich eine Anzeige ihrer Richtlinien implementiert werden. Das Beste für die Mitarbeiter wäre jedoch, die regelmäßige Passworterneuerung aus der Welt zu schaffen. Dies unterstützt eine Arbeit von Zhang et al. [37], in welcher die Autoren nahelegen, die Nutzer lieber zu einem einzigen sehr starken Passwort zu bewegen oder auf ganz andere Alternativen wie Biometrik oder ähnliches umzusteigen. Dies sei eine bei weitem effektivere Weise seine Daten zu schützen. Bis das jedoch geschieht, sollten sich die Sicherheits-Verantwortlichen zumindest ein Beispiel nehmen an System-Anbietern wie unter Anderem Google [13] und Apple [3], die ähnliche, jedoch weitaus beschränkte Programme bei der Passworterstellung zur Verfügung stellen. Sie stellen jedoch einen ersten Schritt dar, mit dem auf die Nutzer zugegangen wird. Dieser Schritt sollte unbedingt fortgeführt und erweitert werden, da auf absehbare Zeit die Passwörter auch zukünftig den Alltag begleiten werden und diese gerade vor dem Hintergrund der ständig wachsenden Bedrohung durch Hacker-Angriffe weiter an Bedeutung gewinnen.

Appendix A

FRAGELISTE ZUR VORSTUDIE

I. DEMOGRAFISCHE ANGABEN

1. Geschlecht:
2. Alter:
3. Beschäftigungsbereich:

II. EINLEITENDE FRAGEN

2.1 Wie oft müssen Sie in der Arbeit das Passwort ändern?

2.2 Wie haben Sie dieses Feedback empfunden?

2.3 Fällt es Ihnen leicht, ein neues Passwort zu erstellen und warum/warum nicht?

2.4 Gibt es in Ihrer Arbeit Richtlinien für die Erstellung des neuen Passwortes? Wenn ja, welche sind das?

2.5 Stellen diese Richtlinien ein Hindernis für Sie dar oder wie bewerten Sie sie?

2.6 Wie lange brauchen Sie durchschnittlich für die Erstellung des neuen Passwortes? Begründung.

2.7 Brauchen Sie manchmal mehrere Versuche? Wenn ja, wie viele?

2.8 Woran scheitert es, dass das Passwort nicht akzeptiert wird?

2.9 Gibt es eine Art Feedback, warum das Passwort nicht akzeptiert wurde? Wenn ja, in welcher Form?

2.10 Gibt es sonst bei der Erstellung irgend eine Art von Feedback zum eingegebenen Passwort?

2.11 Könnten Sie Sich vorstellen, dass Ihnen ein paar Tipps bei der Erstellung des Passwortes helfen könnten, weniger Fehlversuche zu haben? Begründung.

2.12 Wie empfinden Sie die Prozedur des regelmäßigen Passwort-Änderns? Begründung.

DURCHFÜHRUNG DES TESTS

III. FRAGEN ZUR DURCHFÜHRUNG DES TESTS

3.1 Welche Art von Passwort haben Sie erstellt? (Anzahl Zeichen, Anzahl Charakter-Klassen), Begründung.

3.2 Wie ist es Ihnen bei der Passworterstellung ergangen? Wie würden Sue es im Vergleich zu Erfahrung in der Arbeit beschreiben?

3.3 Wie haben Sie das Feedback empfunden?

3.4 Waren die Hinweise verständlich/nachvollziehbar?

3.5 War das Feedback hilfreich? Begründung.

3.6 Wie viele Versuche hatten Sie, bevor Sie auf „Enter" geklickt haben? Wenn mehr als 1: Was haben Sie geändert und warum?

3.7 Welche Art von Hinweisen hätten Sie gerne gesehen?

IV. ABSCHLIEßENDE FRAGEN

4.1 Wie war es für Sie, dieses Interview mit Test durchzuführen?

4.2 Gibt es irgendwelche Fragen/Anmerkungen?

4.3 Würden Sie bei einer Folgestudie teilnehmen?

Appendix B

FRAGEBOGEN ZUR HAUPTSTUDIE

I. DEMOGRAFISCHE ANGABEN

1. Bitte geben Sie als erstes Ihre Prolific-UserID hier ein:

2. Geschlecht: o weiblich
   o männlich

3. Alter:

4. Beschäftigungsbereich:
   - o Agentur, Werbung, Marketing & PR
   - o Automobilbranche
   - o Banken
   - o Baugewerbe/-industrie
   - o Bildungswesen
   - o Elektrotechnik, Feinmechanik & Optik
   - o Energie- und Wasserversorgung
   - o Fahrzeugbau/-zulieferer
   - o Finanzdienstleister
   - o Freizeit, Touristik, Kultur & Sport
   - o Gesundheit & Soziale Dienste
   - o Gross- und Einzelhandel
   - o Hotel und Gastronomie
   - o Immobilien
   - o IT- & Internetbranche

o Luft- und Raumfahrt

o Maschinen- und Anlagebau

o Medien

o Medizintechnik

o Öffentlicher Dienst & Verbände

o Personaldienstleister

o Telekommunikation

o Unternehmensberatung

o Wirtschaftsprüfung, Recht

o Versicherungen

o Wissenschaft & Forschung

II. FRAGEN ZUR TESTDURCHFÜHRUNG

2.1 AN WAS KÖNNEN SIE SICH ERINNERN - WAS FÜR EIN FEEDBACK HABEN SIE ERHALTEN?

o Balken, der wächst, wenn Passwort stärker wird.

o Passwortstärke als Zahl

o Tipps in Form von Sätzen

o Warnungen in Form von Sätzen

2.2 WIE HABEN SIE DIESES FEEDBACK EMPFUNDEN?

2.3 WAREN DIE HINWEISE VERSTÄNDLICH?

(Haben Sie verstanden, was die Hinweise bedeuten und wie Sie es anwenden können?)

Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

Die Hinweise waren…	o	o	o	o	o
	unverständlich	nicht immer verständlich	neutral	fast immer verständlich	verständlich

2.4 WAS WAR NICHT VERSTÄNDLICH?

2.5 WAREN DIE HINWEISE NACHVOLLZIEHBAR?

(Haben Sie verstanden, warum Ihnen diese Hinweise gegeben wurden?)

Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

Die Hinweise waren…	o	o	o	o	o
	nicht	nicht immer nachvollziehbar	neutral	fast immer nachvollziehbar	nachvollziehbar

2.6 WAS WAR NICHT NACHVOLLZIEHBAR?

2.7 STELLEN SIE SICH VOR, DAS NÄCHSTE MAL, WENN SIE IN DER ARBEIT DAS PASSWORT ÄNDERN MÜSSEN, BEKOMMEN SIE SO EIN FEEDBACK WIE IN DIESER STUDIE. WIE WÜRDEN SIE DARAUF REAGIEREN?

Kreuzen Sie die Sätze an, die auf Sie zutreffen.

o Ich würde es willkommen heißen.

o Ich würde das Feedback anwenden.

o Ich würde das Feedback nicht beachten.

o Ich würde das Feedback nicht anwenden.

o Ich würde das Feedback beachten.

o Sonstiges:

2.8 BEGRÜNDEN SIE IHRE ANTWORT.

2.9 WIE MÜSSTE MAN IHRER MEINUNG NACH DAS FEEDBACK VERBESSERN, DASS ES DEN NUTZERN MEHR NUTZT BZW. DASS NUTZER DIE RATSCHLÄGE BEFOLGEN?

2.10 WELCHE VORSCHLÄGE HÄTTEN SIE, UM IHNEN DIE PASSWORTNEUERSTELLUNG ZU ERLEICHTERN?

2.11 AUF WAS LEGEN SIE AM MEISTEN WERT BEI DER ERSTELLUNG EINES NEUEN PASSWORTES?

1 = keinen Wert, 5 = sehr viel Wert

Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	1	2	3	4	5
Passwortstärke	o	o	o	o	o
Erfüllung der Kriterien	o	o	o	o	o
Erinnerbarkeit	o	o	o	o	o
Dass sie sich von Ihren anderen und vorherigen Passwörtern unterscheiden	o	o	o	o	o

III. FRAGEN ZUM PASSWORT

3.1 WELCHE ELEMENTE HABEN SIE IN IHREM PASSWORT VERWENDET?

Bitte wählen Sie alle zutreffenden Antworten aus:

o Großbuchstaben

o Kleinbuchstaben

o Sonderzeichen

o Ziffern

o Muster auf der Tastatur

o Datum

o Buchstabe durch Ziffern oder Sonderzeichen ersetzt

o Vorname

o Nachname

o Spitzname

o ein Wort

o mehrere Wörter

o Zahlenfolge

o Buchstabenfolge

3.2 WIE VIELE ZEICHEN HATTE IHR PASSWORT?
Bitte geben Sie Ihre Antwort hier ein:

3.3 WELCHE ELEMENTE VERWENDEN SIE IN DER ARBEIT IN IHREM PASSWORT?
Bitte wählen Sie alle zutreffenden Antworten aus:

o Großbuchstaben

o Kleinbuchstaben

o Sonderzeichen

o Ziffern

o Muster auf der Tastatur

o Datum

o Buchstabe durch Ziffern oder Sonderzeichen ersetzt

o Vorname

o Nachname

o Spitzname

o ein Wort

o mehrere Wörter

o Zahlenfolge

o Buchstabenfolge

3.4 WIE VIELE ZEICHEN HATTE IHR PASSWORT?
Bitte geben Sie Ihre Antwort hier ein:

3.5 WARUM UNTERSCHEIDEN SICH DIE PASSWÖRTER VON HEUTE UND AUS DER ARBEIT IN IHREN ELEMENTEN UND/ODER DER LÄNGE?

(WARUM HABEN SIE ANDERE ELEMENTE GEWÄHLT UND/ODER EIN LÄNGERES BZW. KÜRZERES PASSWORT GEWÄHLT?)

3.5 WELCHE STRATEGIEN HABEN SIE ANGEWANDT, UM DAS HEUTIGE PASSWORT ZU ERSTELLEN?

Bitte wählen Sie alle zutreffenden Antworten aus:

o Ich habe eines meiner Passwörter verwendet.

o Ich habe einer meiner Passwörter modifiziert.

o Ich habe ein komplett neues Passwort erstellt.

o Das Passwort basiert auf den Anfangsbuchstaben jeden Wortes aus einem Satz, den ich mir gut merken kann.

o Das Passwort basiert auf einem Namen/Wort und ich habe Ziffern/Symbole hinten und/oder vorne angehängt.

o Das Passwort basiert auf einem Namen/Wort, in dem ich bestimmte Buchstaben durch Ziffern/Symbole ersetzt habe.

o Das Passwort basiert auf einem Namen/Wort, in dem ich manche Buchstaben weggelassen habe.

o Das Passwort basiert auf einem Namen/Wort, das aus einer anderen Sprache als Deutsch stammt.

o Das Passwort basiert auf einer Adresse.

o Das Passwort basiert auf einer Telefonnummer.

o Das Passwort basiert auf einem Geburtsdatum.

o Sonstiges: ☐

3.6. WIE SICHER SIND SIE SICH, DASS SIE IHR PASSWORT IN EIN PAAR TAGEN ERNEUT EINGEBEN KÖNNTEN?

1 = gar nicht sicher, 5 = sehr sicher

Bitte wählen Sie nur eine der folgenden Antworten aus:

o 1

o 2

o 3

o 4

o 5

IV. BEWERTUNG DER USEREXPERIENCE

4.1 WIE HABEN SIE DIE PASSWORTERSTELLUNG MIT FEEDBACK EMPFUNDEN?
Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	1	2	3	4	5	6	7	
menschlich	○	○	○	○	○	○	○	technisch
angenehm	○	○	○	○	○	○	○	unangenehm
originell	○	○	○	○	○	○	○	konventionell
einfach	○	○	○	○	○	○	○	kompliziert
fachmännisch	○	○	○	○	○	○	○	laienhaft
praktisch	○	○	○	○	○	○	○	unpraktisch
sympathisch	○	○	○	○	○	○	○	unsympathisch
umständlich	○	○	○	○	○	○	○	direkt
zurückweisend	○	○	○	○	○	○	○	einladend
gut	○	○	○	○	○	○	○	schlecht
verwirrend	○	○	○	○	○	○	○	übersichtlich
motivierend	○	○	○	○	○	○	○	entmutigend
widerspenstig	○	○	○	○	○	○	○	handhabbar

V. ALLGEMEINE FRAGEN

5.1 DIESE STUDIE BAUT DARAUF, DASS SIE JEDE FRAGE KORREKT LESEN UND EHRLICH BEANTWORTEN. DIE UNTENSTEHENDE FRAGE DIENT DEM ZWECK, ZU TESTEN, OB SIE SICH DIE ZEIT NEHMEN, ALLES ZU LESEN. WENN SIE ALSO ALLES GELESEN HABEN, BEANTWORTEN SIE DIESE FRAGE MIT (3).

Wie häufig gehen Sie ins Kino? (1= nie, 5 = jeden Tag)

Bitte wählen Sie nur eine der folgenden Antworten aus:

o 1

o 2

o 3

o 4

o 5

5.2 WELCHE RICHTLINIEN GIBT ES BEI IHNEN IN DER ARBEIT FÜR DIE ERSTELLUNG DES NEUEN PASSWORTES?

Bitte wählen Sie alle zutreffenden Antworten aus:

o Mindestanzahl Zeichen

o Mindestanzahl Großbuchstaben

o Mindestanzahl Kleinbuchstaben

o Mindestanzahl Sonderzeichen

o Mindestanzahl Ziffern

o Darf keine Ähnlichkeit zu vorherigen Passwörtern haben

o Darf bestimmte Wörter nicht enthalten

o Darf keine Wörter enthalten

o Darf nur eine bestimmte Maximallänge haben

o Ich bin mir nicht sicher

o Sonstiges: [ ]

5.3 BITTE BEWERTEN SIE DIE AUSSAGEN, SO WIE SIE AUF SIE ZUTREFFEN.
Ihnen fällt es leicht/nicht leicht, ein neues Passwort zu erstellen, weil…

	Ich stimme nicht zu.	Ich stimme eher nicht zu.	Ich stimme teilweise zu, teilweise nicht zu.	Ich stimme eher zu.	Ich stimme zu.
Mir fällt es leicht, ein neues Passwort zu erstellen, weil ich eine gute Strategie habe.	○	○	○	○	○
Mir fällt es leicht, ein neues Passwort zu erstellen, weil ich meine eigenen Passwörter wiederverwende.	○	○	○	○	○
Mir fällt es leicht, ein neues Passwort zu erstellen, weil ich sehr kreativ bin.	○	○	○	○	○
Mir fällt es nicht leicht, ein neues Passwort zu erstellen, weil ich nicht sehr kreativ bin.	○	○	○	○	○
Mir fällt es nicht leicht, ein neues Passwort zu erstellen, weil ich mir Passwörter schwer merken kann.	○	○	○	○	○
Mir fällt es nicht leicht, ein neues Passwort zu erstellen, weil ich keine gute Strategie habe.	○	○	○	○	○

5.4 WAS IST IHRE STRATEGIE ZUR PASSWORTERSTELLUNG?
Bitte wählen Sie alle zutreffenden Antworten aus:

o Ich setze das Passwort aus bestimmten Wörtern zusammen.

o Ich nehme die Anfangsbuchstaben eines Satzes, den ich mir gut merken kann.

o Ich habe ein Passwort, das ich immer wieder abändere und erweitere.

o Ich verwende ein Passwort eines anderen Accounts.

o Ich habe keine Strategie.

o Sonstiges: ☐

5.5 HABEN SIE EINE STRATEGIE, SICH DIE PASSWÖRTER ZU MERKEN?

Bitte wählen Sie alle zutreffenden Antworten aus:

o Passwort-Manager

o Notizblätter oder Ähnliches

o Textfile (digitales "Notizblatt")

o Eselsbrücken

o Keine

o Sonstiges: [ ]

5.6 BENUTZEN SIE EIN PASSWORT FÜR MEHR ALS NUR EINEN ZWECK?

Bitte wählen Sie nur eine der folgenden Antworten aus:

o Ja

o Nein

5.7 WIE VIELE PASSWÖRTER HABEN SIE? UND ANHAND WELCHER KRITERIEN ENTSCHEIDEN SIE, WELCHES PASSWORT SIE BENUTZEN?

5.8 WIE BEWERTEN SIE DIE NOTWENDIGKEIT, REGELMÄßIG PASSWÖRTER ZU ÄNDERN?

5.9 WERDEN SIE IN DER ARBEIT IN IRGENDEINER WEISE BEI DER PASSWORTERSTELLUNG UNTERSTÜTZT?

Bitte wählen Sie alle zutreffenden Antworten aus:

o Hilfestellung vor der Eingabe des Passwortes

o Hilfestellung während der Eingabe des Passwortes

o Hilfestellung nach der Eingabe des Passwortes

o Keine Hilfestellung

o Sonstiges: [ ]

5.10 BITTE ERKLÄREN SIE, IN WELCHER WEISE SIE BEI DER PASSWORTEINGABE UNTERSTÜTZ WERDEN.

5.11 WIE OFT AM TAG GEBEN SIE DIESES PASSWORT EIN?
Bitte wählen Sie nur eine der folgenden Antworten aus:

o 1-2 mal

o 2-4 mal

o 4-6 mal

o 6-8 mal

o Häufiger

o Weiß ich nicht.

5.12 WIE REGELMÄßIG MÜSSEN SIE IN DER ARBEIT IHR PASSWORT ÄNDERN?
Bitte wählen Sie nur eine der folgenden Antworten aus:

o 3-4 Wochen

o 6-8 Wochen

o 2-4 Monate

o 3-6 Monate

o Häufiger

o Seltener

o Nie

VI. FRAGEN ZUR PERSON

6.1 DIE UNTENSTEHENDE LISTE ZEIGT EINE REIHE VON AUSSAGEN AUF, DIE SICH AUF DIE PERSÖNLICHEN CHARAKTEREIGENSCHAFTEN BEZIEHEN.

Bitte lesen Sie jeden Satz sorgfältig durch und entscheiden Sie, ob dieser auf Sie zutrifft (Ja) oder nicht zutrifft (nein).

Bitte wählen Sie die zutreffende Antwort für jeden Punkt aus:

	Ja	Nein
Manchmal werfe ich Müll einfach in die Landschaft oder auf die Straße.	○	○
Eigene Fehler gebe ich stets offen zu und ertrage gelassen etwaige Konsequenzen.	○	○
Im Straßenverkehr nehme ich stets Rücksicht auf die anderen Verkehrsteilnehmer.	○	○
Ich habe schon einmal Drogen (Tabletten, Haschisch oder "ähnliches") konsumiert.	○	○
Ich akzeptiere alle anderen Meinungen, auch wenn sie mit meiner eigenen nicht übereinstimmen.	○	○
Meine Wut oder schlechte Laune lasse ich hin und wieder an unschuldigen oder schwächeren Leuten aus.	○	○
Ich habe schon einmal jemanden ausgenutzt oder übers Ohr gehauen.	○	○
In einem Gespräch lasse ich den anderen stets ausreden und höre ihm aufmerksam zu.	○	○
Ich zögere niemals, jemandem in einer Notlage beizustehen.	○	○
Wenn ich etwas versprochen habe,		

halte es ohne Wenn und Aber.	○	○
Ich lästere gelegentlich über andere hinter deren Rücken.	○	○
Ich würde niemals auf Kosten der Allgemeinheit leben.	○	○
Ich bleibe immer freundlich und zuvorkommend anderen Leuten gegenüber, auch wenn ich selbst gestresst bin.	○	○
Im Streit bleibe ich stets sachlich und objektiv.	○	○
Ich habe schon einmal geliehene Sachen nicht zurück gegeben.	○	○
Ich ernähre mich stets gesund.	○	○
Manchmal helfe ich nur, wenn ich eine Gegenleistung erwarte.	○	○

Appendix C

FRAGELISTE ZUR ABSCHLIEßENDEN STUDIE

1. An was erinnern sie sich von der letzten Studie?

2. Wie haben Sie das Feedback empfunden? -> Genaue Erklärung

3. Waren die Hinweise verständlich?

Die Hinweise waren…

- o unverständlich
- o nicht immer verständlich
- o neutral
- o fast immer verständlich
- o verständlich

Begründung:

4. Waren die Hinweise nachvollziehbar?

Die Hinweise waren…

- o nachvollziehbar
- o nicht immer nachvollziehbar
- o neutral
- o fast immer nachvollziehbar
- o nachvollziehbar

Begründung:

5. Stellen Sie Sich vor, das nächste Mal, wenn Sie in der Arbeit Ihr Passwort ändern müssen, bekommen Sie so ein Feedback. Wie würden Sie darauf reagieren?

- o ich würde es Willkommen heißen
- o Ich würde es anwenden
- o Ich würde es beachten
- o Ich würde es nicht beachten
- o Ich würde es nicht anwenden

Begründung:

Literaturverzeichnis

[1] Anne Adams und Martina Angela Sasse. „Users are not the enemy“. In: *Communications of the ACM* 42.12 (1999), S. 40–46.

[2] Anne Adams, Martina Angela Sasse und Peter Lunt. „Making passwords secure and usable“. In: *People and Computers XII*. Springer, 1997, S. 1–19.

[4] Imperva Application Defense Center. „Consumer password worst practices“. In: *Imperva (White Paper)* 1.1.2 (2010), S. 1.

[5] Rainer Banse und Bertram Gawronski. „Die Skala Motivation zu vorurteilsfreiem Verhalten: Psychometrische Eigenschaften und Validität“. In: *Diagnostica* 49.1 (2003), S. 4–13.

[6] Joseph Bonneau u. a. „Passwords and the evolution of imperfect authentication“. In: *Communications of the ACM* 58.7 (2015), S. 78–87.

[7] Juliet M Corbin und Anselm Strauss. „Grounded theory research: Procedures, canons, and evaluative criteria“. In: *Qualitative sociology* 13.1 (1990), S. 3–21.

[8] Anupam Das u. a. „The Tangled Web of Password Reuse.“ In: *NDSS*. Bd. 14. 2014, S. 23–26.

[9] Serge Egelman und Eyal Peer. „The Myth of the Average User“. In: NSPW'15. 2015.

[10] Dinei Florencio und Cormac Herley. „A large-scale study of web password habits“. In: *Proceedings of the 16th international conference on World Wide Web*. IW3C2 WWW 2007. 2007, S. 657–666.

[11] Dinei Florêncio, Cormac Herley und Baris Coskun. „Do strong web passwords accomplish anything?“ In: *HotSec* 7 (2007), S. 6.

[12] Dinei Florêncio, Cormac Herley und Paul C Van Oorschot. „Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts“. In: *23rd USENIX Security Symposium (USENIX Security 14)*. 2014, S. 575–590.

[14] Marc Hassenzahl, Michael Burmester und Franz Koller. „AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität“. In: *Mensch & Computer 2003*. Springer, 2003, S. 187–196.

[15] Eiji Hayashi und Jason Hong. „A diary study of password usage in daily life“. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2011, S. 2627–2630.

[16] Peter Hoonakker, Nis Bornoe und Pascale Carayon. „Password authentication from a human factors perspective: Results of a survey among end-users“. In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. Bd. 53. 6. SAGE Publications. 2009, S. 459–463.

[17] Philip G. Inglesant und M Angela Sasse. „The true cost of unusable password policies: password use in the wild“. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2010, S. 383–392.

[19] Mark Keith, Benjamin Shao und Paul John Steinbart. „The usability of passphrases for authentication: An empirical field study“. In: *International journal of human-computer studies* 65.1 (2007), S. 17–28.

[21] Saranga Komanduri u. a. „Of passwords and people: measuring the effect of password-composition policies“. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2011, S. 2595–2604.

[23] Ijlal Loutfi und Audun Jøsang. „Passwords are not always stronger on the other side of the fence“. In: USEC'15. 2015.

[26] Stuart Schechter, Cormac Herley und Michael Mitzenmacher. „Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks“. In: *Proceedings of the 5th USENIX conference on Hot topics in security*. USENIX Association. 2010, S. 1–8.

[27] Richard Shay u. a. „A Spoonful of Sugar?: The Impact of Guidance and Feedback on Password-Creation Behavior“. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM. 2015, S. 2903–2912.

[28] Richard Shay u. a. „Can long passwords be secure and usable?“ In: *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM. 2014, S. 2927–2936.

[29] Richard Shay u. a. „Encountering stronger password requirements: user attitudes and behaviors“. In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM. 2010, S. 2.

[30] Elizabeth Stobert und Robert Biddle. „The password life cycle: user behaviour in managing passwords“. In: *Symposium On Usable Privacy and Security (SOUPS 2014)*. 2014, S. 243–255.

[31] Blase Ur u. a. „Do Users' Perceptions of Password Security Match Reality?“ In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 2016.

[32] Blase Ur u. a. „How does your password measure up? the effect of strength meters on password creation“. In: *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*. 2012, S. 65–80.

[34] Matt Weir u. a. „Testing metrics for password creation policies by attacking large sets of revealed passwords“. In: *Proceedings of the 17th ACM conference on Computer and communications security*. ACM. 2010, S. 162–175.

[35] Dan Lowe Wheeler. „zxcvbn: Low-budget password strength estimation“. In: *Proc. USENIX Security*. 2016.

[37] Yinqian Zhang, Fabian Monrose und Michael K. Reiter. „The security of modern password expiration: An algorithmic framework and empirical analysis“. In: *Proceedings of the 17th ACM conference on Computer and communications security*. ACM. 2010, S. 176–186.

[38] Moshe Zviran und William J. Haga. „Cognitive passwords: The key to easy access control“. In: *Computers & Security* 9.8 (1990), S. 723–736.

Weblinks

[3] Apple. Eingesehen am 25.10.2016. URL: https://appleid.apple.com/account#!&page=create.

[13] Google. Eingesehen am 25.10.2016. URL: https://accounts.google.com.

[18] Kaspersky. Eingesehen am 01.10.2016. URL: https://password.kaspersky.com.

[20] Ben Kennish. Eingesehen am 20.07.2016. URL: https://www.bennish.net/password-strength-checker/.

[22] Limesurvey. Eingesehen am 03.08.2016. URL: https://www.limesurvey.org/de/#.

[24] Jakob Nielsen. *Why You Only Need to Test With 5 Users*. Eingesehen am 15.07.2016. URL: https://www.nngroup.com/articles.

[25] Prolific. Eingesehen am 15.08.2016. URL: https://www.prolific.ac.

[33] Ashlee Vance. *If Your Password Is "123456", Just Make It HackMe*. Eingesehen am 01.11.2016. URL: http://www.nytimes.com/2010/01/21/technology/21password.html.

[36] XKCD. *Password Strength*. Eingesehen am 20.9.2016. URL: https://xkcd.com/936/.

Inhalt der beigelegten CD

Die CD beinhaltet folgende Ordner:

- Diagramme-Bilder: Hier sind alle in der Arbeit verwendeten Diagramme und Bilder gespeichert.
- Grounded Theory: Beinhaltet die Tabellen der einzelnen Kodierungsvorgänge
- Vorstudie: Enthält die Frageliste der Vorstudie
- Hauptstudie: Enthält den Fragebogen der Hauptstudie und die Ergebnisse als xls-Datei SPSS-Datei und Excel-Datei.
- Nachstudie: Enthält die Frageliste der abschließenden Studie und die zusammengetragenen Ergebnisse
- Paper: Enthält die verwendeten Quellen als PDF.
- websiteBA: Hier sind alle Dateien enthalten, welche die Webseite der Studien bilden. Dieser Ordner enthält eine kurze Erläuterung zu den vorhandenen Dateien.
- Caroline Olsienkiewicz - Bachelorarbeit: Enthält die Latex-Rohdatei der Arbeit.