Benutzbare Sicherheit: Usability, Safety und Security bei Passwörtern

Christian Reuter, Marc-André Kaufhold, Jonas Klös

Institut für Wirtschaftsinformatik, Universität Siegen

Zusammenfassung

Obwohl Usability und Sicherheit beides relevante Anforderungen für Anwendungssysteme sind, stehen sie in einem Spannungsfeld. Sicherheit kann als Schutz vor Angriffen von außen (Security), aber auch für das sichere Funktionieren (Safety) dieser Anwendungssysteme verstanden werden. Durch die immer größere Vernetzung klassischer Safety-Domänen, wie dem Katastrophenschutz, gewinnen Security-Aspekte dort ebenfalls an Bedeutung. Die Übertragung von kritischen und vertraulichen Informationen auf mobile Endgeräte muss zugleich passwortgeschützt als auch schnell verfügbar sein; zeitintensive Authentifizierungsmechanismen können hier stören. In dieser Studie werden die Nutzung von Passwörtern vor dem Hintergrund der Abwägung von Sicherheit und Usability exploriert und Hypothesen zum Umgang mit Passwörtern aufgestellt, die im Kontext der Digitalisierung in der zivilen Sicherheit sowie mobilen und ubiquitären Geräte im Katastrophenschutz an enormer Bedeutung gewinnen.

1 Einleitung

Im Zuge der steigenden Verbreitung von Computern und Internetzugängen für Menschen auf der ganzen Welt hat die Digitalisierung großen Einfluss auf das Leben und unterdessen auch auf sicherheitskritische Bereiche des Lebens. So werden Gebrauchstauglichkeit und die Sicherheit von Software in immer mehr Bereichen relevant. Der Nutzer verlangt bei sicherheitskritischen Angelegenheiten, wie dem Bezahlen im Internet, betrieblichen Anwendungssystemen oder Kriseninformationssystemen, von einer Software ein hohes Maß an Sicherheit im Sinne von Safety. Dies kann oft bedeuten, dass die Benutzung aufwendiger und die Transaktion für den Anwender komplizierter wird. Nicht nur Sicherheit und Privatsphäre (Reuter et al., 2016), sondern auch Sicherheit und Benutzbarkeit stehen in einem gewissen Spannungsfeld. Dieser Zielkonflikt ist ein interessantes Forschungsgebiet und in vielen sicherheitskritischen Bereichen von enormer Relevanz.

Seit etwa 15 Jahren existiert diese adressierende Forschung an der Schnittstelle der Mensch-Computer-Interaktion und IT-Sicherheit, die häufig unter dem Begriff „Usable Security“ zusammengefasst wird (Garfinkel & Lipford, 2014). Heute gibt es einen Konsens, dass Systeme,

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2017 in
M. Burghardt, R. Wimmer, C. Wolff, C. Womser-Hacker (Hrsg.):
Mensch und Computer 2017 – Workshopband, 10.–13. September 2017, Regensburg.
 https://doi.org/10.18420/muc2017-ws01-0384

die nicht nutzbar sind, unweigerlich Sicherheitsversagen erleiden, wenn sie in der realen Welt eingesetzt werden. Nur durch gleichzeitige Ansprache von Usability- und Sicherheitsbedenken können sichere Systeme entstehen (Garfinkel, 2014).

Diese Arbeit soll einen Aspekt, in dem Usability und Security zusammenkommen, untersuchen und in Form einer empirischen Studie explorieren, wie Menschen mit Passwörtern umgehen. Dazu wird ein Fragebogen entwickelt, der das bisherige Nutzerverhalten im Umgang mit Passwörtern untersucht und eine Selbsteinschätzung der Teilnehmer abfragt, wie diese ihre Passwörter gestalten und in der Praxis einsetzen. Aus den Ergebnissen sollen Hypothesen generiert werden. Abschließend soll die Arbeit Handlungsempfehlungen geben.

2 Sicherheit und Usability bei Passwörtern

Usability und Security scheinen auf den ersten Blick Gegensätze eines Zielkonflikts zu sein (Sahar, 2013), was bedeutet, dass eine Verbesserung des einen unmittelbar zu einer Verschlechterung des anderen führt. Viele Autoren sehen jedoch eine Trendwende dahingehend, dass Usability die Sicherheit auch erhöhen kann (Sahar, 2013). Ein sicheres Computersystem ist für den Benutzer leicht verständlich, weil dadurch Missverständnisse und Fehler vermieden werden, wodurch wiederum die Sicherheit des Systems steigt (Yee, 2002).

Merkfähigkeit und Anzahl von Passwörtern: Adams und Sasse (1999) deuten an, dass ein normaler Anwender sich nur vier oder fünf Zeichen lange Passwörter merken und im Alltag anwenden kann. Verschiedene Studien zeigen jedoch, dass Passwörter mindestens sechzehn Zeichen lang sein sollten, um ein gewisses Maß an Sicherheit zu bieten (Sasse et al., 2001). Eine weitverbreitete Praxis von Anwendern ist das doppelte Verwenden von Passwörtern oder das Aufschreiben von Passwörtern auf Papier (Adams, 1999). Zudem werden gerne Passwörter verwendet, die einem bestimmten Muster folgen, um besser im Gedächtnis zu bleiben (Yan et al., 2004). Dies verursacht hingegen neue Sicherheitsprobleme. Andere Studien haben mit einer Umfrage unter einer halben Millionen Internetnutzern herausgefunden, dass durchschnittlich 25 Passwörter pro Person existieren und jedes dieser Passwörter wiederum für durchschnittlich 6,5 Seiten gleichzeitig verwendet wird (Florencio & Herley, 2007). Einfache Passwörter werden präferiert, da sie leicht zu implementieren und einfach zu merken sind, keine extra Hardware oder Software benötigen, leicht zu administrieren sind und schnell verstanden werden (Renaud & De Angeli, 2004).

Mechanismen des Passwortschutzes: Auf der Suche nach Studien, die diese Probleme lösen, findet man die Versuche, durch striktere Passwortrichtlinien einfache Passwörter zu verhindern und die Anwender besser zu schulen (Shay et al., 2010). Vermehrt werden deshalb in den letzten Jahren Alternativen zur klassischen Passwortauthentifizierung gesucht, wie z.B. biometrische Verfahren. Dabei werden physische Merkmale oder Verhaltenseigenschaften eines Menschen genutzt, um dessen Identität zu bestätigen (Coventry et al., 2003). Ein konkretes Verfahren, welches bereits bei Android Smartphones angewandt wird, könnten sogenannte graphische Passwörter sein, bei denen Muster nachgezeichnet werden müssen (Dunphy et al., 2010). Dabei tendieren Anwender jedoch dazu, symmetrische Figuren oder Bilder als Passwort

zu zeichnen, wodurch sich die theoretisch mögliche Summe der unterschiedlichen Figuren signifikant reduziert und die Sicherheit somit sinkt (Thorpe & van Oorschot, 2004). Auch kann es sinnvoll sein, für verschiedene Apps auf einem Smartphone unterschiedlich hohe Anforderungen an die Sicherheit und Usability zu stellen. Eine Studie aus dem Jahr 2016 empfiehlt unterschiedliche Passwortrichtlinien je nach Einsatzgebiet einer App (Melicher et al., 2016). Außerdem sollten für Passwortfelder immer Funktionen wie automatisierte Wortvorschläge deaktiviert sein (Melicher, 2016). Das Entwickeln und Designen eines gelungenen Authentifikationsmechanismus ist eine komplexe Aufgabe, die nicht durch mehr Sicherheitsabfragen und längere Passwörter gelöst werden kann (Herley, 2014).

Neue Ansätze der Sicherheit und Usability: Der Ansatz, ein Level von Security zu akzeptieren, das nicht perfekt aber „gut genug" ist, findet weniger Anklang (Sandhu, 2003). Smetters und Grinter (2002) stellen eine sehr interessante Frage: „If you put usability first, how much security can you get?" Dies initiiert einen Ansatz für die Entwicklung von Sicherheitssoftware und es ergibt sich die Frage, wie weit die Sicherheit bei gleichbleibender Usability maximiert werden kann. Dieser Ansatz ist dabei eher für gering- bis mittelrisikoreiche Einsatzgebiete von Sicherheitssoftware gedacht, wodurch er für Krisenszenarien nur bedingt geeignet ist. Auch in den öffentlichen Medien ist die Passwortsicherheit immer noch ein aktuelles Thema und der Bedarf an qualitativ hochwertiger Information ist groß (heise online, 2016). Laut einer repräsentativen Umfrage im Auftrag des ITK Branchenverbands Bitkom sind 36% der deutschen Internetnutzer überfordert von der Vielzahl der Kennwörter und Geheimzahlen, die sie sich merken müssen (Bitkom, 2016).

Zusammenfassend kann man festhalten, dass die Sicherheit und Usability von Authentifizierungssoftware und Systemen ein rege beforschtes Gebiet darstellt. In der Vergangenheit wurde versucht, die Sicherheit durch komplexere Passwörter zu verbessern, was jedoch kontraproduktiv sein kann. Ein neues Ziel sollte sein, neue Methoden zu entwickeln, die das klassische Passwort für hoch sicherheitskritische Anwendungen überflüssig macht. Einige gute Ansätze wie grafische Passwörter oder Zwei-Faktor-Authentifizierung existieren bereits. Für geringbis mittelsicherheitskritische Anwendungen kann es hingegen sehr sinnvoll sein, noch ein klassisches, nicht zu komplexes Passwort einzusetzen. Obwohl sie einer gewissen Sensibilität unterliegen, sind sie nicht sicherheitskritisch und es kann keine Gefahr von ihnen ausgehen.

3 Explorative Studie

Diese Arbeit soll in Form einer Umfrage herausfinden*, nach welchem Schema Passörter vergeben und gemerkt werden (Forschungsfrage)*. Persönliche Passwörter und deren Länge sind für viele Menschen verständlicherweise geheime und private Informationen. Auch wenn diese Studie nie das eigentliche Passwort für bestimmte Anwendungen erfragen soll, werden doch gewisse Metadaten erhoben. Viele Menschen geben solche Informationen wahrheitsgemäß nur an vertraute Personen weiter. Deshalb werden nicht möglichst viele Probanden untersucht, aber eine handverlesene Auswahl, die dafür umso ausführlicher, aber höchstens 30 Minuten befragt wird. Um möglichst unverfälschte Ergebnisse zu bekommen, wird den Probanden das genaue Thema der Studie erst im Anschluss an die Befragung offengelegt.

Fragen: Für die Studie wurde ein Fragebogen aus 14 Fragen mit offenem oder geschlossenem Antwortformat entwickelt. Zunächst wurden demographische Daten wie das Alter und das Geschlecht sowie die subjektive Einschätzung der allgemeinen Merkfähigkeit abgefragt. Anschließend wurden elf Fragen zur Merkfähigkeit (Anzahl auswendig wiedergebbarer Passwörter), Erstellung, Verwendung und Einstellung zu Passwörtern gestellt.

Teilnehmer: Das nach dem Schneeballprinzip entstandene Sample umfasst 103 Teilnehmer, wobei der Anteil der Männer mit 59% höher als der der Frauen (41%) ist. Die größte Altersgruppe stellen mit 64% die 18 bis 29-Jährigen dar, gefolgt von 0-18 (11,7%), 30-39 (9,7%), 40-49 (8,7%), 50-59 (4,9%) und einem ohne Angabe (1%) (Abb. 1). Die Teilnehmer wurden (im Schulnotensystem) außerdem nach ihrer allgemeinen, subjektiven Merkfähigkeit befragt. Die meisten Probanden bewerten ihre Merkfähigkeit mit einer Drei (30,1%), die grobe Normalverteilung lag bei einer Durchschnittsnote von 3,09 (Abb. 2). Im Folgenden werden die Ergebnisse als Hypothesen vorgestellt, indem zuerst einige einfache Auswertungen und danach verschiedenste Kreuztabellen ausgewertet werden.

H1: Fast alle Internetnutzer vergessen Passwörter. 92% der Teilnehmer haben bereits ein Passwort vergessen (Abb. 1), wobei es keinen Unterschied zwischen den Geschlechtern gab.

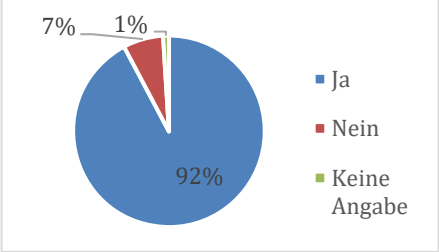

Abb. 1: Haben Sie schon einmal ein Passwort vergessen?

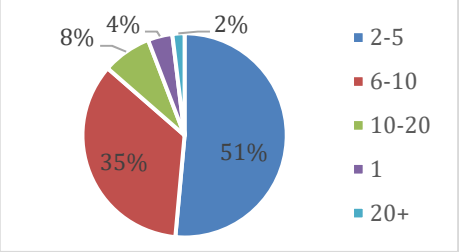

Abb. 2: Wie viele Passwörter können Sie aktuell wiedergeben?

H2: Nur wenige Passwörter können auswendig wiedergegeben werden. Etwa die Hälfte der Befragten kann zwei bis fünf Passwörter auswendig wiedergeben (51,5%). Viele Teilnehmer (35%) können sich sogar bis zu zehn Passwörter merken. Mehr als zehn Passwörter auswendig zu lernen, gelingt hingegen nur einer Minderheit: 10-20 (7,8%), 20+ (1,9%) (Abb. 2). Dabei zeigen weitere Auswertungen, dass die Personen, die über zehn Passwörter auswendig wiedergeben können, meistens mit einer Systematik arbeiten, bei der oft nur ein Buchstabe des Passworts ersetzt wird. Sollte bei diesen Personen die Systematik einem Fremden in die Hand fallen, wären potenziell alle anderen Passwörter kompromittiert.

H3: Persönliche Muster sind beliebteste Passwörter. Auf die offene Frage „Wenn Sie ein Passwort frei wählen dürften, wie würden Sie es erstellen, um es sich noch gut behalten zu können?“ gab es diverse interessante Antworten (Tab. 1). Die meisten Teilnehmer antworteten, dass sie ein persönliches Muster aus bekannten Sachen als Passwort verwenden (35,9%). Exemplarisch für viele der Befragten beschrieb ein Teilnehmer: *„Meine Passwörter ergeben nur für mich einen Sinn, solange ich diese Schematik verwenden kann, kann ich mir meine Passwörter behalten.“* Vermutlich machten viele Personen dazu aus Sicherheitsgründen gar

keine Angaben (28,6%). Am dritthäufigsten wurde eine sehr ähnliche Antwort zu der häufigsten gegeben mit dem Unterschied, dass diese Personen immer angaben, etwas Persönliches als Passwort zu verwenden wie Sachen, Namen oder Geburtsdaten, aber kein besonderes Muster, um die Passwörter abzuändern (12,6%). Die Teilnehmer, die ein Passwort nach einem bestimmten Muster anfertigen, setzen sich dem bereits erwähnten Risiko aus, dass sobald ihre Systematik erkannt wird, alle ihre Passwörter offenliegen. Schweitzer et al. (2009) analysierten heuristische Muster auf der Tastatur und entwickelten ein Wörterbuch, mit dem in ihrer Studie 20% der Passwörter aufgedeckt werden konnte. Die Antworten „mit Sonderzeichen" (7,8%) und „Anfangsbuchstabe eines Satzes" (6,8%) sind als besser zu bewerten. Am sichersten (im Sinne von Security) ist die Antwort, ein völlig zufälliges Passwort zu wählen, welches dann auswendig gelernt wird; ob dies im Sinne von Safety (garantiertes Erinnern im Bedarfsfall) gilt, wäre überlegenswert. Wenige Teilnehmer gaben an, immer das gleiche Passwort zu verwenden (1,9%).

Schema mit persönlichem Muster	35,9%	Völlig zufällig und auswendig lernen	2,9%
Keine Angabe	28,6%	Immer das Gleiche	1,9%
Persönliche Passwörter ohne Muster	12,6%	Aufschreiben	1,9%
Mit Sonderzeichen	7,8%	Muster auf der Tastatur	1,9%
Anfangsbuchstaben eines Satzes	6,8%		

Tab. 1: Antwortkategorien auf die Frage „Wenn Sie ein Passwort frei wählen dürften, wie würden Sie es erstellen, um es sich noch gut behalten zu können?"

H4: Passwörter werden überwiegend doppelt verwendet. Etwa zwei Drittel (66,9%) gaben an, Passwörter doppelt zu verwenden. Dies muss nicht kritisch sein, da einige Passwörter bei unwichtigen Online-Portalen mehrfach eingesetzt werden. Für sicherheitskritische Online-Banking Zugänge werden andere einmalige Passwörter verwendet. Dies ist aus der folgenden beispielhaften offenen Antwort ableitbar: *„Doppelverwendung von Passwörtern (Variation bei Groß- und Kleinschreibung) bei ‚unwichtigen' Zugängen. Eigene Passwörter für Email, Sparkasse und Passwortsafe."* Trotzdem ist dieses Vorgehen nicht optimal, da es in sicherheitskritischen Szenarien bezüglich vertraulicher Informationen enorme Konsequenzen haben kann. Werden Passwörter dort doppelt verwendet und geknackt, gelangen die Daten in unautorisierte Hände.

H5: Passwörter doppelt zu verwenden korreliert mit der Merkfähigkeit. Interessant ist, dass selbst Teilnehmer, die sich eine gute Merkfähigkeit zutrauen, unabhängig vom Alter angaben, Passwörter doppelt zu verwenden. Je höher die Merkfähigkeit ist, desto häufiger werden Passwörter doppelt verwendet. Hier wäre die Kausalität zu prüfen, ob die erhöhte Merkfähigkeit aufgrund der doppelten Verwendung steigt. Für unwichtige Webseiten und Shopping-Konten werden Passwörter offensichtlich gerne doppelt verwendet, für einen Online-Banking Zugang hingegen ein einmaliges komplexes Passwort.

H6: Auch die Verwendung eines einzelnen Passworts führt zum Vergessen. Es ist auffällig, dass selbst Teilnehmer, die nur ein Passwort auswendig wiedergeben können (3,9%), angaben, schon einmal ein Passwort vergessen zu haben. Eine mögliche Erklärung hierfür ist, dass alle Probanden, die schon einmal ein Passwort vergessen haben, nur noch eins besitzen, um künftiges Vergessen zu verhindern. Für die Praxis und die Erhöhung der Sicherheit bedeutet dies, dass es auch immer eine gute und einfache Möglichkeit geben muss, sein Passwort

zurückzusetzen. Dies kann bei hoch sicherheitskritischen Anwendungen (z.B. im Onlinebanking) einen sehr aufwendigen Prozess nach sich ziehen (Zustellung per Post etc.).

H7: Passwörter zu vergessen, ist altersunabhängig. Darüber hinaus wurde ermittelt, dass jede Altersgruppe Passwörter vergisst. 90% der Alterskategorie 30-39, 88,9% der 40-49-Jährigen und 80% der 50-59-Jährigen gaben an, Passwörter schon einmal vergessen zu haben. Bei den 18-29-Jährigen gaben dies 92,4% und bei den unter 18-Jährigen sogar 100% der befragten Personen an. Dies zeigt erneut, wie wichtig ein guter Prozess zum Wiederherstellen von Passwörtern ist. Insgesamt sagten nur 6,8% der Befragten aus, dass sie noch nie ein Passwort vergessen hätten.

H8: Frauen schreiben eher auf Papier. Die Nutzung eines Passwort-Managers oder eines speziellen Programms könnte unabhängig vom Geschlecht auf eine gewisse Technikaffinität bzw. eine Tätigkeit im IT-Bereich zurückzuführen sein. Dennoch ist auffällig, dass 34,4% der befragten Männer und nur 4,8% der teilnehmenden Frauen eine solche Anwendung gebrauchen. Die weiblichen Befragten präferieren die Nutzung von Stift und Papier (47,6%) (Abb. 3), nur 27,9% der befragten Männer notieren Passwörter auf Papier. Insgesamt schreiben jedoch 35,9% ihre Passwörter auf, was noch immer ein beträchtlicher Anteil ist, da diese Methode viele Sicherheitsrisiken beinhaltet. Viele dieser besagten Personen sagten aus, bei der Menge an Passwörtern, die man heutzutage benötigt, keine andere Möglichkeit zu sehen (*„Bei der Vielzahl der Passwörter geht es nicht anders“).*

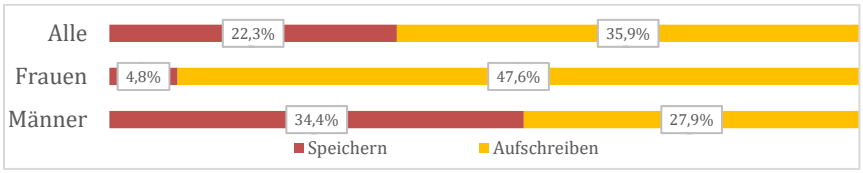

Abb. 3: Passwörter in einem Programm speichern oder aufschreiben?

H9: Männer verwenden eher Sonderzeichen. Bei der Frage nach der Erstellung der Passwörter ist auffällig, dass als zusätzliches Sicherheitsmerkmal für Passwörter nur Männer folgendes angaben: Mit Sonderzeichen (13,1%), völlig zufällig (4,9%), Muster auf der Tastatur (3,3%). Frauen gaben diese Optionen überraschenderweise nicht an. Die anderen Methoden, um Passwörter zu kreieren, kamen etwa gleich häufig bei beiden Geschlechtern vor. Bei der geringen Anzahl an Teilnehmern können diese Auffälligkeiten Zufall sein. Die häufigste Antwort von Frauen war ein Passwort aus persönlichen Mustern bekannter Sachen (47,6%). Zwar verwenden auch 26,2% der Männer diese Methode, jedoch haben 29,5% der männlichen Teilnehmer bei dieser Frage keine Angabe gemacht. Dies verdeutlicht, dass sich Frauen und Männer Passwörter möglicherweise unterschiedlich merken, doch welchen Einfluss dies auf die Passwortsicherheit hat, müsste genauer untersucht werden.

H10: Passwörter werden als wichtig, aber immer hackbar, wahrgenommen. Die letzte offene Frage: „*Was ist Ihre abschließende Meinung zu Passwörtern im Internet?*“ ermöglichte die freie Äußerung der eigenen Meinung. Um dennoch die wesentlichen Inhalte auszuwerten, wurden die einzelnen Aussagen stärker als bei den anderen offenen Fragen zu einer Oberkate-

gorie zusammengefasst. Dabei war die häufigste Antwort „keine Angabe“ (26,2%). Die häufigste aussagekräftige Antwort ist, dass Passwörter notwendig und wichtig sind (21,4%). Auffällig ist jedoch, dass viele Teilnehmer befürchten, dass ihre Computer und Online-Aktivitäten komplett überwacht werden bzw. gehackt werden können und es egal ist, welches Passwort sie verwenden (16,5%). Vielen scheint nach den immer öfter vorkommenden Veröffentlichungen von Überwachung und Passwortdiebstahl dieses Risiko bewusst zu sein, was mit der Vergabe von Passwörtern in Verbindung gebracht wird. Ein Teilnehmer beschrieb: *„Dadurch, dass man heutzutage alles hacken kann, egal wie und wo und es anscheinend an ausreichender IT-Sicherheit mangelt, kann man sich ein Passwort zwar zulegen, aber wohl nur davor, um Freunde, Bekannte oder Personen, die sich normalen Zugriff zu Seiten verschaffen wollen, abzuhalten und sich abzusichern, aber nicht, um sich Profis vom Hals zu schaffen.“* In den offenen Antworten konnte auch der Vermerk auf *„alternative Verfahren der Identifikation“* festgestellt werden, welche nicht explizit in der Befragung angesprochen wurden. Weitere Antworten waren „*Passwörter sind ein notwendiges Übel*“ (13,6%), „*Nutzer sollten zu langen Passwörtern mit technischen Voraussetzungen gezwungen werden*“ (4,9%) und „*Anwender sollten eine Passwortverwaltung nutzen*“ (1,9%).

4 Diskussion und Handlungsempfehlungen

Der Großteil der Teilnehmer macht sich Gedanken über sichere Passwörter, erzeugt manchmal jedoch unbewusst neue Angriffsflächen durch das Verwenden von Mustern und Zeichenfolgen. Ein kleiner Teil reagiert durch die Überforderung mit Resignation und dem Verwenden eines immer gleichen Passworts. Wie andere repräsentative Studien der Bitkom (2016) bereits gezeigt haben, sind viele Personen mit der Passwort-Flut überfordert. In unser Befragung wurde dabei zusätzlich deutlich, dass es möglicherweise einen Unterschied dabei gibt, wie sich Männer und Frauen Passwörter merken. In der neuesten repräsentativen Studie der Bitkom (2016) hat sich die gleiche Tendenz der Teilnehmer gezeigt, für das Online-Bankkonto ein gesondertes Passwort zu verwenden. Dies verdeutlicht, dass besondere Auffälligkeiten unser Stichprobe auch in einer großen Umfrage bewiesen werden können.

Die Studie von Adams und Sasse (1999) konnte ebenfalls bestätigt werden. Das doppelte Verwenden von Passwörtern und das Aufschreiben dieser ist immer noch üblich. Heute lässt sich jedoch ein Trend zu dem Verwenden einer Passwortverwaltungssoftware erkennen. Dies ist wahrscheinlich auf die Notwendigkeit einer noch höheren Anzahl an Passwörtern zurückzuführen. Zusätzlich ist eine solche Passwortsoftware mittlerweile auch viel leichter und einfacher zu erhalten, wie z.B. Browser Add-Ons. Auch werden immer noch gerne Passwörter verwendet, die einem Muster folgen, um besser im Gedächtnis zu bleiben (Yan et al. 2004). Ebenfalls auffällig ist, dass in dieser kleinen Studie wenig von alternativen Methoden der Passwortauthentifizierung wie RFID Chips oder biometrischen Verfahren berichtet wurde. Diese Methoden sind noch wenig im Alltag der Menschen verbreitet.

Als Handlungsempfehlung für Entwickler von Sicherheitsabfragen kann man dem Benutzer beim Erstellen eines Passworts auf die bekannten Schwächen der menschlichen Passwortver-

gabe hinweisen. Zusätzlich sollten die Anforderungen an das Passwort aber auch nicht zu komplex sein, da der Anwender sonst dazu geneigt ist, ein bereits verwendetes Muster oder eine gewohnte Zeichenfolge zu wählen. Da Menschen aller Altersgruppen angaben, Passwörter zu vergessen, sollte der Prozess zum Wiederherstellen eines Passworts gut durchdacht und einfach sein. Darüber hinaus erscheint es sinnvoll, die Passwortverwaltungsprogramme weiter publik zu machen, um zum einen die doppelte Verwendung oder das Aufschreiben von Passwörtern zu vermeiden und zum anderen die Komplexität eines Passworts aufrechtzuerhalten, ohne der Gefahr von Mustern oder Zeichenfolgen zu unterliegen. Im sicherheitskritischen Kontext ist teilweise nur Safety bedeutsam (Notruf am Handy), häufig sind jedoch sowohl Safety als auch Security (z.B. sensible Anwendungen für Hilfsorganisationen) von Relevanz. Demnach sollte der Zugang schnell und einfach, dennoch sicher sein.

5 Fazit

Diese Arbeit hat sich mit dem Spannungsfeld von Usability und Security beschäftigt und anhand einer Umfrage den Umgang und die Verbesserungswürdigkeit von Passwörtern von 103 Teilnehmern untersucht. Hierauf aufbauend konnten zehn Hypothesen aufgestellt werden, die einer quantitativen Überprüfung bedürfen: Demnach vergessen fast alle Internetnutzer ihre Passwörter (H1) und nur wenige Passwörter können auswendig wiedergegeben werden (H2). Persönliche Muster werden gerne als Passwort verwendet (H3), Doppelverwendungen sind üblich (H4), was jedoch nicht von der Merkfähigkeit abhängig ist (H5). Passwörter werden auch vergessen, wenn nur eines für alle Dienste verwendet wird (H6); dies ist altersunabhängig (H7). Um sich Passwörter zu merken, schreiben Frauen häufiger auf Papier (H8). Zur Passwortsicherheit verwenden Männer eher Sonderzeichen (H9). Passwörter werden als wichtig, aber immer als zu entschlüsselnd, wahrgenommen (H10). Die Limitationen dieser Studie liegen darin, dass vergleichsweise wenig Personen teilnahmen. Aufgestellte Hypothesen sollten in zukünftigen Arbeiten überprüft werden. Darüber hinaus wurden in dieser Studie nicht explizit Nutzer sicherheitskritischer Anwendungen untersucht, was in zukünftigen Studien vergleichend erfolgen sollte.

Literaturverzeichnis

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46. doi:10.1145/322796.322806

Bitkom. (2016). Stress mit der Passwort-Flut. https://www.bitkom.org/Presse/Presseinformation/Stress-mit-der-Passwort-Flut.html

Coventry, L., De Angeli, A., & Johnson, G. (2003). Usability and biometric verification at the ATM interface. In *Proc. CHI* (p. 153). New York, New York, USA: ACM Press. doi:10.1145/642611.642639

Dunphy, P., Heiner, A. P., & Asokan, N. (2010). A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

New York, USA: ACM Press. doi:10.1145/1837110.1837114

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the International Conference on World Wide Web* (p. 657). New York, New York, USA: ACM

Garfinkel, S., & Lipford, H. R. (2014). *Usable Secuirty: History, Themes, and Challenges*. Morgan.

heise online. (2016). Wider den Zwang zur Passwort-Änderung. https://www.heise.de/newsticker/meldung/Wider-den-Zwang-zur-Passwort-Aenderung-3176493.html

Herley, C. (2014). More Is Not the Answer. *IEEE Security & Privacy*, *12*(1), 14–19. doi:10.1109/MSP.2013.134

Melicher, W., Mazurek, M. L., Kurilova, D., Segreti, S. M., Kalvani, P., Shay, R., … Cranor, L. F. (2016). Usability and Security of Text Passwords on Mobile Devices. In *Proc. CHI* (pp. 527–539). New York, New York, USA: ACM Press. doi:10.1145/2858036.2858384

Renaud, K., & De Angeli, A. (2004). My password is here! An investigation into visuo-spatial authentication mechanisms. *Interacting with Computers*, *16*(6), 1017–1041.

Reuter, C., Geilen, G., & Gellert, R. (2016). Sicherheit vs. Privatsphäre: Zur Akzeptanz von Überwachung in sozialen Medien im Kontext von Terrorkrisen. In H. C. Mayr & M. Pinzger (Eds.), *Informatik 2016: von Menschen für Menschen*. Klagenfurt: GI-Edition-Lecture Notes in Informatics (LNI). http://subs.emis.de/LNI/Proceedings/Proceedings259/P-259.pdf#page=1760

Sahar, F. (2013). Tradeoffs between Usability and Security. *International Journal of Engineering and Technology*, 434–437. doi:10.7763/IJET.2014.V5.591

Sandhu, R. (2003). Good-enough security. *IEEE Internet Computing*, *7*(1), 66–68. doi:10.1109/MIC.2003.1167341

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the “Weakest Link” — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, *19*(3), 122–131. doi:10.1023/A:1011902718709

Schweitzer, D., Boleng, J., Hughes, C., & Murp, L. (2009). Visualizing keyboard pattern passwords. In *6th International Workshop on Visualization for Cyber Security* (pp. 69–73). Atlantic City, NJ, USA: IEEE. doi:10.1109/VIZSEC.2009.5375544

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., … Cranor, L. F. (2010). Encountering stronger password requirements. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. New York, USA: ACM Press.

Smetters, D. K., & Grinter, R. E. (2002). Moving from the design of usable security technologies to the design of useful secure applications. In *Proceedings of the workshop on New security paradigms (NSPW)* (p. 82). New York, New York, USA: ACM Press. doi:10.1145/844102.844117

Thorpe, J., & van Oorschot, P. C. (2004). Graphical dictionaries and the memorable space of graphical passwords. In *Proceedings of the conference on USENIX Security Symposium - Volume 13* (p. 10). San Diego, CA.

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: empirical results. *IEEE Security & Privacy Magazine*, *2*(5), 25–31. doi:10.1109/MSP.2004.81

Yee, K.-P. (2002). User Interaction Design for Secure Systems. In *ICICS 2002: Information and Communications Security* (pp. 278–290). doi:10.1007/3-540-36159-6_24