123456

Eine Hommage an das Passwort

Biarna Diegmüller

Inhaltsverzeichnis

Gehen wir davon aus, dass ich eine verantwortungsvolle Internet-Nutzerin bin. Gehen wir davon aus, dass ich für jeden einzelnen meiner Online-Accounts ein anderes Passwort erstellt und bei „möchten Sie dieses Passwort abspeichern“ niemals „Ja“ geklickt habe:

Mein Wecker klingelt. Ich schalte ihn aus und tippe die PIN für mein Smartphone ein. Dann fange ich an, durch die Feeds meiner sozialen Medien zu scrollen. Nun muss ich mich auf Facebook, Instagram und Pinterest jeweils mit einem anderen Passwort anmelden. Das sind bereits vier Verifizierungen vor dem Frühstück. Nach dem Frühstück kurz unter die Dusche, in dieser Zeit habe ich bereits um die 20 Mal mein Handy entsperrt. Um meine Backup-Wecker auszustellen, WhatsApp Nachrichten zu beantworten oder um einfach kurz das Wetter zu checken. Um 9 Uhr muss ich bei der Arbeit sein. Dort entsperre ich zuerst den Bürolaptop, dann muss ich mich in das hauseigene Programm einloggen. Um den Dienstplan zu checken, benötige ich für den Google-Kalender ebenfalls ein Passwort. Auch auf dem i-Pad muss ich mich zuerst in das Programm einloggen, allerdings mit einem anderen Account und deshalb auch mit einem anderen Passwort. Auf dem Weg zurück nach Hause gehe ich noch schnell einkaufen. Für den Einkauf zahle ich mit Karte und tippe meine PIN in das EC-Gerät ein. Zu Hause angekommen, setze ich mich an den Laptop und gelange mit Hilfe meines Passwortes auf meinen Desktop. Beim schnellen Konto-Check muss ich mich über die 3-Phasen Authentifizierung einloggen. Das heißt ich gebe zuerst mein Passwort ein, muss meine Identität dann aber mit einer weiteren PIN bestätigen und bekomme schließlich eine TAN per SMS zugeschickt. Erst dann bekomme ich Zugriff auf mein Konto. Apple hat mal mitgezählt, wie oft wir im Durchschnitt unser Handy entsperren: 2016 lag die Zahl bei rund 80 Mal am Tag. „Junkies“ dagegen entsperren ihr Smartphone

wohl um die 130 Mal am Tag.[1] Wenn ich davon ausgehe, dass die Zahl seit 2016 etwas angestiegen ist, habe ich wohl am frühen Abend mein Handy um die 60 Mal entsperrt. Immer dieselbe PIN, aber nichts desto trotz. Während ich nun am Laptop sitze, checke ich noch einmal diverse Mails. Dafür logge ich mich bei drei verschiedenen Mail-Anbietern ein, natürlich mit drei verschiedenen Passwörtern. Dann muss ich noch Hundefutter bestellen. Auch für die Webseite des Hundefutterherstellers benötige ich mein Passwort, allerdings kann ich per Lastschrift zahlen, sonst wäre auch hier wieder das Passwort für meine Bank fällig gewesen. Schließlich lasse ich mich auf die Couch fallen. Bevor ich jedoch einen Film schauen kann, muss ich mich zuerst in Netflix einloggen. Der Fernseher hat Probleme, sich mit dem Internet zu verbinden, deshalb muss ich auch dort den 16-stelligen Schlüssel des WLAN-Routers eingeben. Finde ich meinen Wunschfilm nicht bei Netflix, wechsele ich zu Amazon Prime; auch hier ist ein Passwort erforderlich.

Dieser nahezu perfekte Passwortmarathon entspricht selbstverständlich nicht der Wirklichkeit. Keine vergessenen und zurückgesetzten, keine sich wiederholenden Passwörter und keine kleinen Zettel unter der Schreibtischplatte, auf welchen handschriftlich sämtliche Passwörter notiert sind. Am Ende des Tages hätte ich mir mindestens um die 20 verschiedene Passwörter merken müssen. Die Realität sieht deshalb anders aus. Unser Passwortverhalten ist riskant und wir gehen leichtsinnig mit unseren Daten um. Denn das System Passwort ist logisch und perfekt, der Mensch aber ist es nicht. 123456 war im Jahr 2018 das am häufigsten verwendete Passwort der Welt. Wie das Hasso-Plattner Institut ermittelte,[2] folgten auf die bereits genannte Zahlenreihe „hochkomplexe" Passwörter wie „1234" oder „passwort". Obwohl wir es alle besser wissen müssten. Immer wieder werden wir ermahnt, ein möglichst langes Passwort zu benutzen. Mindestens 8 Zeichen sollte es haben, dabei nicht nur aus Buchstaben, sondern möglichst auch aus Ziffern und Sonderzeichen bestehen. Selten befolgen wir diese Ratschläge.

Der Grund ist offensichtlich: die schiere Fülle an Passwörtern, die wir gezwungen sind, in unserem Online-Leben zu erstellen und uns dann ein Leben lang zu merken, ist eine Zumutung. Das Vergessen von Zahlenreihen ist menschlich. Die Aussage, wir würden unsere Daten wider besseres Wissen nicht gut genug schützen, ist zwar richtig, aber sie unterschlägt eine wichtige Komponente, nämlich den Menschen in seiner Menschlichkeit. Bei mindestens 78 Online-Accounts pro Person[3] übersteigt die Anforderung, für jeden dieser Accounts ein sicheres Passwort zu erstellen, die Kapazitäten des Menschen bei weitem. In den USA kommt ein Mensch sogar auf bis zu 150 Online Konten. Die Softwarefirma Dashlane geht davon aus, „dass sich die Gesamtzahl der Konten, die Passwörter benötigen, in den nächsten fünf Jahren verdoppeln wird.".[4] Das System „Passwort" ist demnach nicht dem Menschen und seinem Können angepasst. Es ist alles andere als menschenfreundlich. Gerade aus diesem Grund ist es besonders interessant zu

beobachten, wie der Mensch als Individuum das Passwort nach seinem Können generiert und es sich zu Nutze macht. Der Mythos „Passwort“ wird immer wieder in Erzählungen behandelt und findet sich in der Unterhaltungsindustrie, wie beispielsweise in Filmen, wieder. Eine der bekanntesten Geschichten, in welchen das Passwort eine bedeutende Rolle spielt, ist „Ali Baba und die 40 Räuber“. Wie so oft entscheidet die Antwort auf die Frage nach dem Passwort über Leben und Tod. Im Film ist die „Passwortszene“, also die Suche nach dem richtigen Passwort, nicht selten entscheidend für den Ausgang des Filmes. Das, was seinen Mythos ausmacht, ist seine Exklusivität. Um relevant zu sein, muss das Passwort ein Geheimnis bleiben. Und möglicherweise ist es eines der letzten echten Geheimnisse, die wir im Internet haben. Auch deshalb sind Passwörter oft etwas zutiefst Persönliches. Um sie uns merken zu können, müssen wir uns mit ihnen identifizieren. Ob wir den Lieblingsfußballverein verwenden oder den Namen eines geliebten Menschen und dessen Geburtsdatum, das Passwort verrät viel über unseren Charakter und offenbart Dinge, die uns besonders wichtig sind, sowie unsere Wünsche und Begehren. Deshalb spielt auch die Suche nach unserer Identität, die sich im Passwort offenbart, eine Rolle. Gleichzeitig gilt es, diese Identität durch das Passwort zu schützen. Letztendlich ist die Beziehung zwischen dem Passwort und dem Menschen eine Hassliebe. Das Passwort des digitalen Zeitalters ist omnipräsent. Die schiere Fülle an Passworteingaben am Tag macht das Passwort zu einem Werkzeug, ohne das es kaum denkbar ist, am täglichen Leben teilzuhaben. Zum anderen ist es uns unmöglich, dieses Werkzeug sicher und verantwortungsvoll zu gebrauchen. Jeder kennt das Gefühl, wenn ein Passwort unwiderruflich aus dem Gedächtnis gelöscht ist. Doch gibt es überhaupt eine Alternative zum Passwort oder sollten wir uns auf das zurück besinnen, was das Passwort für den Menschen ausmacht? Ist das Passwort ohne den Menschen nur eine Abfolge von zufälligen Buchstaben, Ziffern und Zeichen? Die wahre Bedeutung des Passwortes scheint der Mensch ihm zu geben auf die Art und Weise, wie er es nutzt. Fragen wir uns also, wo wir den Menschen im Passwort finden können.

Anmerkung:

Im Folgenden werde ich vor allem auf das nach meiner Definition klassische Passwort eingehen. Das Passwort ist demnach selbstgeneriert und kann aus Zahlen, Zeichen, Buchstaben etc. bestehen. Die PIN (Persönliche Identifikationsnummer) wie man sie beispielsweise für die Zahlung mit Bankkarte verwendet, nehme ich heraus. PINs sind oft vorgegeben, bestehen nur aus Ziffern und sind demnach nicht persönlich genug, um sie in die nachfolgende Recherche mit einzubeziehen.

Kapitel 1: Der Mythos Passwort

K 1 :

D M

P w

„Sesam öffne dich“,

so sind die entscheidenden Worte des Märchens „Ali Baba und die 40 Räuber“. In dem Märchen entdeckt der Hauptcharakter Ali Baba die Höhle einer Räuberbande. Die Höhle ist bis zur Decke gefüllt mit Schätzen. Sie lässt sich jedoch nur mit den Worten „Sesam öffne dich“ betreten. Durch Zufall erfährt Ali Baba das geheime Passwort und gelangt in die Höhle. Während er sich nur mit einem kleinen Sack voll Gold davonstiehlt, möchte sein habgieriger Bruder, nachdem er ihm das Passwort entlockt hat, gleich den ganzen Goldschatz mitnehmen. In seiner Habgier vergisst er das Passwort und sitzt in der Höhle gefangen. Die Räuber entdecken ihn bei ihrer Rückkehr und er findet in der Räuberhöhle den Tod.[5] Das Märchen ist in Europa eines der bekanntesten aus der Sammlung „1001 Nacht“[6] und meiner Meinung nach eines der bekanntesten analogen Form des Systems „Passwort“.

Nicht selten endet die Suche nach dem Passwort derart dramatisch und ist entscheidend über Leben und Tod wie in diesem Märchen. Auch im Film nimmt die sogenannte „Passwortszene“ meist einen der spannendsten Momente des Filmes ein und ist ungewöhnlich zeitintensiv im Gegensatz zum Rest des Filmes. Auch offenbart das darin herausgefundene Passwort oft eine Menge untergründiges über den Film und dessen Charaktere, wie beispielsweise deren innigste Wünsche oder Begehren.

So auch in der Serie „Sherlock“ in der Folge „A scandal in Belgravia“[7]. In der gesamten Folge spielt die Suche nach dem Passwort des Handys von Irene Adler, einer Domina, die mit den Geheimnissen ihrer Kunden handelt, eine wichtige Rolle. “This is your heart and you should never let it rule your head”, sagt Sherlock Holmes und entsperrt das Telefon. Der Pin: SHER. Damit ergeben sich auf dem Display die Worte “I AM SHERLOCKED”. Dem Zuschauer offenbart sich damit die Information, dass die berechnende und kluge Miss Adler Gefühle für Sherlock Holmes entwickelt hat. In „Harry Potter und die Kammer des Schreckens“ verschafft sich Professor McGonagall mit den Worten “Sherbet Lemon” Zutritt in das Büro des Schuldirektors Professor Dumbledors. Dadurch offenbart sich seine Vorliebe für Zitronenbrausebonbons.[8] In anderen Filmen entscheidet das Passwort über Leben und Tod, wie in der Szene des ersten Jurassic Park Films, in welcher die Wissenschaftler versuchenm das System neu zu starten. Mit den Worten “Ah ah ah, you didn’t say the magic word”, verweigert Programmierer Dennis Nedry ihnen den Zutritt. Die Hauptdarsteller*innen müssen sich daraufhin den gefährlichen Raptoren aussetzen und dies bedeutet für einige unwiederbringlich den Tod.[9]

Im Film sowie auch in Erzählungen entscheidet das Wissen oder Nichtwissen des Passwortes stets über die Wendung des Filmes und ist nicht selten dessen Höhepunkt. In „Jurassic Park“ stirbt als eine Konsequenz auf das Nicht-Erraten des Passwortes in einer der spektakulärsten Szenen des Filmes die Hälfte seiner Hauptdarsteller*innen, weil sie sich den fleischfressenden Dinosauriern aussetzen müssen.[10] Hätte Ali Babas Bruder sich an das Passwort erinnert, wäre er wohl als reicher und vor allem lebendiger Mann zu seiner Frau zurückgekehrt.[11] Irene Adlers Lebensversicherung, die Geheimnisse, welche in dem Handy versteckt waren, wären nicht aufgedeckt worden und sie hätte nicht untertauchen müssen. Wir hätten allerdings auch nie erfahren, dass sie und Sherlock sich zueinander hingezogen fühlen, was wiederum die ganze Sicht auf Sherlock Holmes für den Rest der Serie ändert.[12] Und letztendlich hätte Harry, wenn McGonagall das Passwort für den Eingang des Büros vergessen hätte, wohl an zumindest dieser Stelle nicht das Gespräch mit Dumbledore haben können. Dort erfährt Harry über die heilende Wirkung von Phoenixtränen, die ihm später im Film das Leben retten sollen.[13]

Ob groß inszeniert oder nur am Rande erwähnt, die Passwortszene kann immer in genau zwei Richtungen gehen: entweder wird der Zutritt verwehrt oder gestattet. Und die Richtung, die eingeschlagen wird, ist meistens für den Ausgang der Handlung und für die Spannung der Erzählung von besonderer Bedeutung. So entwickelt sich ein Mythos um das Passwort, welches über allem zu stehen scheint. Das Passwort ist in der Erzählung entweder Offenbarung oder Rettung.
Dieser Mythos führt dazu, dass auch wir das Passwort als Element des Geheimen und Exklusiven gebrauchen. So gibt es den Eintritt in den Club X in Wien nur nach Nennung eines bestimmten Passwortes.[14] Früher gelangte man in den Club

mit einem Schlüssel, welcher nur an von Clubbesitzer Martin Ho ausgewählte Personen übergeben wurde.[15] Heute wird der Eintritt auch per Passwort gewährt. Dieses wechselt täglich und wird über Facebook weitergegeben. Ein striktes Fotoverbot herrscht ebenfalls. Der Club gilt damit als geheimster und exklusivster Club Wiens[16]. Im Club X bewegt man sich eher in elitären Kreisen.[17] Auch der Frannz Club in Berlin verwendet ein Passwort, um den Besucher*innen freien Eintritt bis Mitternacht zu gewähren. Allerdings wird dieses öffentlich auf der Facebook Seite des Clubs bekannt gegeben und ist somit für alle sichtbar und deshalb nicht ganz so exklusiv.[18] Passwörter geben einem das Gefühl über ein geheimes Wissen zu verfügen und Teil von etwas Besonderem zu sein.

Exklusiv und vor allem intim wird es, wenn man das sogenannte Safeword auch als eine Art Passwort versteht. Das Safeword wird vor allem in der BDSM-Szene verwendet und dient der Kommunikation während des Sexspiels. Der passive Part soll damit klar kommunizieren können, wenn die eigenen Grenzen überschritten werden.[19] Das Safeword ist nun erstmal kein geheimes Wort und deshalb kein Passwort in dem Sinne. Dennoch öffnet es Türen, nämlich den Weg raus aus der Situation. Dem Safeword schwingt dabei selbstverständlich eine gewisse Erotik und Verruchtheit mit. Das Safeword wird zwischen den beiden Personen, die es vereinbart haben, zum Schlüssel sicherer Kommunikation. Und gerade dadurch, dass es selten nötig sein sollte und damit kaum ausgesprochen wird, bleibt das Safeword auch sexy und geheim.

(...) das Passwort gibt das Gefühl über ein geheimes Wissen zu verfügen und Teil von etwas Besonderem zu sein.

Auch in der Geschichte spielte das Passwort schon immer eine entscheidende Rolle. Besonders in der Militärsprache, beispielsweise als Parole. Diese Parole diente als Kennwort und war nur dem Kommandeur einer Einheit bekannt. Näherte sich ein Truppenteil dem anderen, verlangte der Wachtposten die Parole. So wurde verhindert, dass sich der Feind

unbehelligt in das Lager begeben konnte. Zusätzlich war allen Soldaten einer Truppe die „Losung“ bekannt. Ein Doppelwort, das der gegenseitigen Erkennung diente.[20] Wären die Kennworte an die feindlichen Truppen geraten, hätte dies über das Schicksal vieler Leben und den Ausgang von Kriegen entscheiden können. Der Mythos des Passwortes liegt selbstverständlich auch in seiner Entschlüsselung. Die Spannung liegt vor allem in der Suche nach der richtigen Lösung. 1939 gelang es polnischen Mathematikern, den Code der Chiffriermaschine Enigma zu entschlüsseln. Mit Hilfe der Enigma kommunizierte damals die Wehrmacht. Die Entschlüsselung der Gespräche deutscher Truppen verkürzte damals wohl den Zweiten Weltkrieg um mehrere Jahre.[21]

In allen genannten Beispielen ist das Passwort von höchster Bedeutung und bestimmt oft schwerwiegend über den Ausgang einer Situation und nicht selten über den Ausgang einer Geschichte. Daneben liegt sein Mythos in seiner Exklusivität, einem Wissen, über welches nicht jeder verfügt. Nur wer zu einem ausgewählten Kreis zählt oder in der Lage ist, den Code zu entschlüsseln, kann sich Zutritt zu bedeutenden Informationen und zu besonderen Orten verschaffen.

Dabei liegen der Mythos und der Reiz in dem, was das Passwort ist und im Idealfall immer bleiben sollte.
Ein Geheimnis.

Kapitel 2:
Das
Passwort als
Geheimnis

K 2 :
D P w
a G

Das Passwort ist allgegenwärtig. Es spielt besonders für unsere Sicherheit im Netz eine bedeutende Rolle. Dennoch tendieren wir dazu, es als beiläufig und lästig zu bezeichnen und werden ihm damit nicht gerecht. Im folgenden Kapitel möchte ich deshalb auf die Bedeutung des Passwortes und im Besonderen auf das Passwort als Geheimnis eingehen.

Der Duden beschreibt das „Passwort“ folgendermaßen:

„nur Eingeweihten bekannte, aus Buchstaben, Ziffern oder Sonderzeichen bestehende Zeichenfolge, die den Gebrauch einer Sache, den Zugang zu ihr ermöglicht und sie gegen den Missbrauch durch Außenstehende schützen soll“[22]

Beginnen wir mit der ersten Zeile. „Nur Eingeweihten bekannte“ Dort wird deutlich, was das Passwort vor allem ist. Ein Geheimnis. Ohne die Geheimhaltung wird das Passwort redundant. In erster Linie schützt das Passwort etwas, welches nicht für jeden zugänglich sein soll. Dazu muss es geheim bleiben. Schließlich steht das Passwort auch in direktem Zusammenhang mit der Kryptographie. „(...) aus Buchstaben, Ziffern oder Sonderzeichen bestehende Zeichenfolge (...)“. Denn das, was im besten Falle ein Passwort zusätzlich sicher und geheimnisvoll macht, ist seine Verschlüsselung. Dabei wird die eigentliche Botschaft durch andere Zeichen ersetzt und damit nicht sofort lesbar gemacht. Dies ist selbstverständlich nur der Fall, wenn wir beispielsweise eine Passphrase verwenden, also den Inhalt unseres Passwortes tatsächlich verschlüsseln. Aber auch nur dann ist ein Passwort tatsächlich sicher. Der Unterschied zur Kryptographie ist, dass das Passwort nicht entschlüsselt werden muss, um von Angreifer*innen verwendet zu werden. Die Botschaft hinter dem Passwort ist unwichtig, solange der richtige Code eingetippt wird. Das Passwort muss deshalb unter allen Umständen geheim bleiben. Man könnte sagen, ein Geheimnis zu sein ist die Daseinsberechtigung des Passwortes.

Auf das Digitale bezogen sind dies vor allem unsere Daten, also ein Stück unserer Persönlichkeit, „(...) die den Gebrauch einer Sache, den Zugang zu ihr ermöglicht und sie gegen den Missbrauch durch Außenstehende schützen soll“. Mit der hier erwähnten Sache sind also unsere intimsten Daten

gemeint. Nicht nur unsere Namen und unser Geburtsdatum – diese Daten sind heute nur selten geheim zu halten – sondern auch unser Nutzerverhalten und wie und wo wir uns im Netz bewegen. Mit dem Passwort beschützen wir also eigentlich unsere Identität, das,was wir sind, wie wir uns verhalten. Während wir auf unseren Social Media Accounts erstaunlich viel über uns preisgeben, sollte von unserem Passwort im Idealfall niemand erfahren. Nicht nur geben wir durch Selbstdarstellung immer mehr von uns Preis. Das focaultsche Modell des Panoptikums, einem Gefängnis, in dem man sich zu jeder Zeit beobachtet fühlen muss, ist längst Realität geworden.[23]

Der gläserne Mensch

So leben wir in Zeiten, in denen der Mensch gläsern geworden ist. Jeder will am besten in Echtzeit alle unsere intimsten Daten von uns haben, und dadurch weiß das Internet und jene, welche für unsere Daten viel Geld bezahlen, fast alles über uns und meistens auch schon Dinge, die wir nicht einmal über uns selbst wissen.[24] Gleichzeitig geben wir bereits in unseren sozialen Medien eine Menge über uns Preis. Das Passwort jedoch, ob „Schalke2000“ oder „Purzel<3“, scheint unser allerletztes richtiges Geheimnis zu sein. Online-Dienste speichern Passwörter grundsätzlich verschlüsselt ab. Dies entspricht dem europäischen Datenschutzrecht.[25] Während also die Dinge, die durch das Passwort geschützt werden sollen, sehr oft bereits in alle Welt verkauft wurden, ist das Passwort selbst das, was geheim ist und geheim bleiben soll. Hier wird wieder der Mythos, die Heiligkeit des Passwortes bedeu-

„Niemand will uns ausspionieren (...) Wir sind es, die unsere Geheimnisse preisgeben.“

tend, ganz nach dem Grundsatz: „Niemand darf es erfahren!“ Dabei spielt für die „Großen“, die unsere Daten wollen, das Passwort gar keine Rolle.“ Niemand will uns ausspionieren“, schreibt Martin Zeyn für den Deutschlandfunk, „Wir sind es, die unsere Geheimnisse preisgeben.“ Die Informationen, die das Passwort schützt, haben wir sowieso schon verkauft, durch unterschriebene Datenschutzerklärungen und beiläufig gesetzte Haken in den AGBs.[26] Die Daten, die wir mit dem Passwort schützen, sind deshalb kein Geheimnis mehr. Selten haben wir die Wahl, diese tatsächlich geheim zu halten. Es ist kaum mehr möglich, uns für Privatsphäre zu entschei-

den, ohne deutliche Abstriche in unserem sozialen Leben zu machen. Der Gedanke, Facebook, Amazon und Co nicht mehr nutzen zu können, ist für die meisten Menschen unvorstellbar. Das Passwort ist damit als Illusion seiner eigentlichen Schutzfunktion beraubt und existiert im Grunde nur noch für sich selbst. Das Passwort ist sein eigenes Geheimnis.

Das Passwort als Objekt der Macht

Damit kann das Geheimnis kann auch als ein Objekt der Macht gesehen werden, eine Selbstermächtigung:

„Wir bestimmen, wer wir sind, weil wir es sind, die das Bild von uns bestimmen“,

so Martin Zeyn.[27] Durch den sorglosen Umgang mit unseren Daten verzichten wir nur zu häufig auf diese Macht. Uns obliegt die Macht, zu entscheiden, was wir über uns preisgeben möchten und was nicht, und diese Macht haben wir in vielen Bereichen des Digitalen bereits abgegeben. Denn Geheimnisse sind Macht und das Passwort als Geheimnis und Wächter von Geheimnissen wird damit zu einem Symbol der Macht. Winzig klein ist sein Ermessensspielraum eigentlich. Besonders, wenn wir ein unsicheres Passwort wählen. Metaphorisch könnte es der Schlüssel sein, der in unseren Händen liegt. Wir durften uns zwar nicht aussuchen, welches Schloss in die Tür kommt, wir durften aber den Schlüssel wählen. Außer unserer Vermieterin oder unserem Vermieter hat niemand denselben Schlüssel. Die Geheimnisse, die hinter der verschlossenen Tür liegen, sind längst offenbart und das Schloss damit eigentlich nutzlos. Dennoch ergibt diese Situation ein anderes Machtverhältnis, als wenn wir uns vorstellen, dass die Tür einfach immer offen steht. Jeder darf rein, sich nehmen was er möchte und wieder gehen. Solange wir den Schlüssel haben, dürfen wir auch abschließen. Solange wir Macht über unser Passwort haben, gehört uns auch unsere Identität. In dem Moment, wo wir uns aktiv dazu entscheiden, die Tür offen stehen zu lassen, haben wir bereits aufgegeben. Der Schlüssel sowie das Passwort geben uns das Recht an dem, was uns gehört. Heute hat das Haus, in dem wir sitzen, zwar eine Tür und auch einen Schlüssel; die Wände aber sind aus Glas, denn das, was sich im Inneren befindet, ist zum großen Teil kein Geheimnis mehr. Das, was das Passwort noch in der Lage ist, zu schützen ist unsere Identität, die beispielsweise durch biometrische Erkennungsmethoden permanent in Gefahr ist, gestohlen zu werden.

Kapitel 3:
Das Passwort
als Teil
unserer
Identität

K 3 :
DPw
aTuI

Mit dem Passwort bestätigen wir erst einmal unsere Identität. Dort, wo wir ein Passwort eingeben müssen, wirkt es wie ein Ausweisdokument. Es bestätigt, dass wir der rechtmäßige Nutzer sind, vorausgesetzt wir haben unser Passwort geheim gehalten.

Das Konzept der Identifikation gibt es auch in der Tierwelt. Wie eine „Art der biometrischen Ausweiskontrolle“ erkennt das Zebra seine Herde an den Streifen auf ihren Hinterteilen. Männliche Glühwürmchen wiederum blinken während der Paarungszeit ein ganz bestimmtes Signal, das Weibchen antwortet. Und auch hier gibt es die Identitätsfälschung: Einige Leuchtkäferweibchen beherrschen die Leuchtsignale der anderen Glühwürmchenarten und locken so die falschen Männchen an.[28] Auch in der Menschenwelt werden biometrische Ausweismethoden schon lange genutzt. Fingerabdruck und Face-ID haben sich längst etabliert, doch auch unser Personalausweis bestätigt die Identität seines Besitzers. Wirklich geheim ist an dieser Identitätskontrolle jedoch nichts mehr. Möglicherweise einzigartig, aber definitiv nicht unfälschbar und von uns selbst beeinflussbar schon gar nicht. Das Passwort gibt uns eine gewisse Macht, weil wir die freie Wahl haben. Es bestätigt nicht nur unsere Identität, wir müssen uns auch mit ihm identifizieren, und zwar bewusst. Nicht selten verwenden wir für wichtige Accounts auch persönlichere Passwörter. „123456“ wird wohl kaum das Passwort zum Online-Banking sein…hoffentlich!

der Fan

der Familientyp

der Phantast

der Kryptiker

Die Passworttypen

Wie britische Psycholog*innen schon 2001 herausfanden, lassen sich User anhand von Passwörtern in vier Gruppen aufteilen. Diese vier Gruppen bestehen aus dem „Fan-Typ" der in seinen Passwörtern die Namen von Fußballspieler*innen oder Stars verwendet. Wie beispielsweise „Schalke04". Zu diesem Passworttypen gehört knapp ein Drittel der Befragten. Etwa die Hälfte der Nutzer*innen verwendet den Namen eines geliebten Menschen, das eigene Geburtsdatum oder den Namen des Haustieres als Passwort und gehört damit zum „Familien-Typ". Zu der Gruppe der „Phantasten" zählen in etwa 11 Prozent der Befragten. Diese lassen das eigene Wunschdenken in die Passwortkreation mit einfließen und erstellen deshalb Passwörter, die oft auch von sexuellen Wünschen oder Vorlieben durchzogen sind.[29] Das vierthäufigste Passwort 2018 war demnach „ficken"[30], wie das Hasso-Plattner Institut in Potsdam herausgefunden hat. Nur ein sehr kleiner Teil denkt sich wirklich sichere Passwörter aus, diese Gruppe Internet Nutzer wird dann als „Kryptiker" bezeichnet.[31] In dem Artikel aus der Computerwoche von 2001, aus welchem diese Informationen stammen, werden die „Kryptiker" als „Sicherheitsfanatiker" bezeichnet. Dieses Bild wird sich bis heute ins Jahr 2020 geändert haben. Wer ein sicheres Passwort erstellt, wird längst nicht mehr als IT-Nerd abgestempelt, sondern der Schutz unserer Daten ist uns nur zu sehr bewusst und die Verwendung von schlechten Passwörtern eher unangenehm und peinlich. Den „Kryptiker" würde man wohl heute eher als die verantwortungsvolle Internet-Nutzer*in bezeichnen.

Ich würde deshalb die Internet Nutzer*innen in drei weitere Kategorien einteilen. Nach Gesprächen mit Freunden, Familienmitgliedern und Bekannten sowie nach meiner Recherche im Internet ergeben sich meiner Meinung nach diese drei Passworttypen:

1. Der „Ich habe nichts zu verbergen"-Typ

Dieser Typ Passwortnutzer ist meist mit dem Internet aufgewachsen. Er bewegt sich sicher im Netz und ist in den meisten sozialen Medien aktiv. Er gibt relativ viel im Netz über sich preis, da er aber ein braver Bürger ist, gibt er die Daten, die er hat, bereitwillig heraus. Schließlich hat er ja „nichts zu verbergen". Vielleicht fehlt es ihm an Wissen oder er sieht die Herausgabe seiner Daten als faires Zahlungsmittel für die Nutzung seiner zahlreichen kostenlosen Online-Dienste an. Fakt ist, er ist nicht sonderlich kritisch in seinem Online-Nutzerverhalten. Für sein Handy verwendet er deshalb auch eher PINs wie „1234" oder „6969". Als Kind der Generation Y hat er eine Vielzahl von Accounts über das ganze Internet verteilt. Meist verwendet er dasselbe Passwort. An die Grundregeln „8 Zeichen, Zahlen, Sonderzeichen" hält er sich, daraus ergeben sich dann aber eher Passwörter wir „$tuttgart1994" oder „HoppelRIP<3". Muss er das Passwort ändern, wird aus dem vorhandenen Passwort eine Variation generiert. Für scheinbar unwichtige Accounts nimmt er Passwörter wie „123456" oder „passwort1, passwort2, passwort3".

2. Der „Ich traue dem Hokuspokus nicht“-Typ

Dieser Typ findet sich meist am ganz anderen Generationenende wieder und war möglicherweise sogar schon in Rente, als er seinen ersten E-Mail Account erstellte. Er hat eine gesunde Skepsis gegenüber all dem „Technikkram“, weiß aber den Luxus und die Vorzüge des Digitalen zu schätzen. Er hat schon von Internet-Sicherheit gehört, und vor allem auf Grund seiner Skepsis möchte er sich verantwortungsvoll in den neuen Medien bewegen. Doch ihm fehlt das Know-How, um diese Sicherheit auch umzusetzen. Begrenzt er die Anzahl seiner Online-Accounts auch auf ein Minimum, so verwendet er doch dort einfache Passwörter, die er sich merken kann. Beispielsweise eine Kombination aus den Namen und Geburtsdaten seiner Kinder und Enkel. Vielleicht gelingt es ihm jedes Mal, ein anderes Passwort zu verwenden, doch um sich diese alle merken zu können, kommt es früher oder später zu Passwortvariationen. Wird ihm von einer Webseite einmal ein sicheres Passwort vorgegeben, verwendet er es zwar, kann es sich allerdings nicht merken. Und so landet ein kleiner gelber Zettel in der obersten Schublade des Schreibtisches, auf dem alle Passwörter notiert sind.

3. Der „Ich fühle mich nicht sicher, aber weiß nicht, was ich ändern kann“-Typ

Wer sich ansatzweise mit IT-Sicherheit beschäftigt hat und sich Gedanken über den Umgang mit seinen Daten macht, wird sich wohl zu diesem Typ zählen. Er ist wie der erste Typ Passwortbenutzer auf relativ vielen Accounts angemeldet, gibt aber nur halb so viel über sich preis. Er versucht, sichere Passwörter zu verwenden, gibt aber bei der Hälfte seiner Accounts auf und verwendet für weniger geheime Daten die gleichen Passwörter. Den Passwortmanager hat er ausprobiert, da er aber erst einmal bei der kostenlosen Version geblieben ist, kann er nicht für jeden seiner Accounts das Passwort abspeichern. Er versucht, verantwortungsvoll mit seinen Passwörtern umzugehen, gibt aber nach erneuter Zurücksetzung eines Passwortes oft nach und verwendet auch hier dasselbe Passwort für mehrere Accounts. Er weiß, dass jeder Dinge zu verbergen hat und dass Privatsphäre ein hohes Gut ist. Dennoch verzweifelt er immer wieder an den Vorgaben für ein sicheres Passwort. Waren seine Passwörter mit 8 Zeichen vor 3 Jahren noch sicher, müsste sich die Anzahl der Zeichen für eine höhere Sicherheit nun verdoppeln. Er hat biometrische Erkennungsmethoden ausprobiert, nur um wenige Wochen später in einem Blogartikel zu lesen, dass diese spielend leicht zu replizieren sind. Der Wille bei diesem Typ Passwortnutzer ist da, an der Umsetzung scheitert er jedoch immer wieder.

Mit diesen drei Typen Passwortbenutzern kann sich, denke ich, jeder auf die eine oder andere Art und Weise identifizieren. Selbst, wenn du eigentlich Typ eins bist, aber gerade versuchst, dein Internetverhalten zu verbessern. Oder du dich schon zu Typ drei zählen würdest, aber weißt, dass du dich manchmal so unvorsichtig wie Typ eins verhältst. Die bereits beschriebenen Passworttypen von 2001 würde ich deshalb nicht aus dem Ring werfen. Noch immer kann sich der eine oder andere mit einem dieser Typen identifizieren. Der Grund ist offensichtlich: der Bezug zu etwas, das uns wichtig ist, sei es der Lieblingsfußballverein oder der Name des Kanarienvogels, ist uns zum einen leichter zu merken, zum anderen erscheint mir der Schutz der Privatsphäre mit etwas Persönlichem nur sinnvoll. Außerdem bedeutet dies nicht, dass wir keine persönlichen Informationen in unseren Passwörtern verwenden dürfen, wir müssen sie nur besser verschlüsseln. Beispielsweise durch die Erstellung von Passphrasen, doch dazu später mehr.

Wir müssen uns mit dem Passwort identifizieren können

(...) auch, weil wir etwas uns wichtiges im Netz mit etwas schützen wollen, dass uns auch in der realen Welt von großer Bedeutung ist.

Ich würde mich persönlich vollkommen zu dem Familientyp zählen. Ob es der Name meines Partners oder der Name meines Haustieres ist. Etwas weniger wichtiges als Passwort zu nehmen erschien mir in diesem Fall schon fast unangemessen. Wir müssen uns mit dem Passwort identifizieren können, um es uns einerseits besser merken zu können, andererseits auch, weil wir etwas uns wichtiges im Netz mit etwas schützen wollen, dass uns auch in der realen Welt von großer Bedeutung ist. So schützte ich meinen Laptop nicht mit „123456“, sondern mit dem Vornamen meines Partners, mit dem Jahr, in dem wir uns kennen lernten und einem Herz, bestehend aus „<“ und „3“. Unser Passwort gibt damit einen Einblick in unsere Identität. Auch geht aus der Studie nicht hervor, ob wir in unseren durchschnittlich 75 Online-Konten nicht auch verschiedene Online-Identitäten verwenden. Vielleicht sind wir bei Facebook eher der Familienmensch und für das Online-Konto

unserer Krankenkasse werden wir zum Kryptiker. Dazu lässt sich feststellen, dass die Theorie der multiplen Persönlichkeiten, insbesondere in Bezug auf unsere Online-Identität, besonders interessant ist und dass Identität im Grunde nur ein Repertoire von Rollen ist, besonders im Cyberspace.[32]

Vielleicht offenbart die Passwortgruppe das wieder, was uns im Leben tatsächlich wichtig ist. Vielleicht aber nur einen winzigen Teil unseres Lebens. Sei es der Lieblingsfußballverein oder der Wunsch, im Bett ein echter „Hengst" zu sein. Wie unsere Identität im echten Leben sind wir aber niemals nur Schalke Fan oder nur Familienmensch.

Unsere Passwortidentität im Cyberspace ist genauso multipel und fluid wie unsere Identität im realen Leben.[33]

Das Passwort und die Gesellschaft

Während dein Passwort viel über deine Identität aussagen kann, so lassen sich auch gesellschaftliche Strömungen in Passwörtern ausmachen. Die Online-Sicherheitsfirma Splash Data veröffentlicht jedes Jahr eine Liste der „schlimmsten Passwörter". Im Jahr 2018 war auf Platz 23 das Passwort „donald" zu finden.[34] Im Jahr 2019 wiederum wurde der US-Präsident auf Grund des GOT Finales vom 23. Platz gestoßen. „dragon" landete im letzten Jahr auf Platz 23.[35] Welche Passwörter eine Gesellschaft wählt, gibt Einblicke darin, wie sie denkt. Die Beispiele „dragon" und „donald" spiegeln vor allem wider was in der Welt in den Jahren 2018 und 2019 gerade passierte. Dass die erfolgreiche Präsidentschaftswahl eines patriarchalischen selbstverliebten Geschäftsmannes so präsent zu sein scheint wie das Serienfinale einer der erfolgreichsten Serien unserer Zeit, regt zum Nachdenken an.

Die Experten der Softwarefirma Dashlane untersuchten 2017 die Daten einer Studie der Virginia Tech University, in welcher 61 Millionen Passwörter analysiert wurden, und entdeckten verschiedene Schemata in der Passworterstellung. So ist zum Beispiel die Verwendung der Themen Liebe und Hass oder die Verwendung von vulgärer Sprache sehr beliebt. Auch leidenschaftliche Phrasen wurden besonders häufig verwendet. So waren die 10 beliebtesten Passwörter dieser Kategorie: iloveyou, f*ckyou, a**hole, f*ckoff, iloveme, trustno1, beautiful, ihateyou, bullsh*t, lovelove.[36]

iloveyou

trustno1

f*ckyou

beautiful

a**hole

ihateyou

f*ckoff

bullsh*t

iloveme

lovelove

Schnittstelle zwischen Mensch und Maschine

Dass der Mensch sich mit seinem Passwort identifizieren muss, macht das Passwort menschlicher. Das Passwort, wie wir es heute verwenden, ist extrem menschenunfreundlich. Es soll möglichst lang sein, am besten keine Wörter beinhalten und wir sollen für jeden Account ein anderes verwenden. Für das menschliche Gehirn alleine ist dies nicht zu bewältigen. Das Passwort, wie wir es uns angeeignet haben, wie wir uns mit ihm identifizieren und es mit unserer Persönlichkeit versehen, ist deshalb menschlicher geworden. Vielleicht liegt genau hier die Schnittstelle zwischen Mensch und Maschine. Maschinen haben keine eigene Identität. Das, was wir in sie hinein projizieren, verleiht ihnen Charakter. So machen wir das technische System „Passwort“ zu etwas Persönlichem, zu etwas das uns nahe ist und uns am Herzen liegt, anstatt nur eine zufällige Abfolge von Zeichen zu sein.

Wir haben gelernt, dass das Konstrukt „Identität“ untrennbar mit dem Passwort verbunden ist. Das Passwort schützt unsere Privatsphäre online und damit auch unsere Identität, und wir stecken einen Teil unserer Identität in das Passwort. Damit wird das Passwort menschlicher. Doch auch wenn das System „Passwort“ von Menschen erschaffen ist und wir unsere Menschlichkeit in es hinein projiziert haben, hat es mittlerweile wenig damit zu tun, wie der Mensch funktioniert und sich an den Menschen nur wenig angepasst.

Das Passwort, wie wir es heute verwenden, ist extrem menschenunfreundlich

Kapitel 4: Das Passwort Paradox

K 4 :

D P

w P x

„Neutral, objektiv und präzise, das sind Computer. Beeinflussbar, ineffizient, unbeherrscht, das ist der Mensch.“[37]

– Martin Zeyn

Wir gehen unvorsichtig mit unseren Daten um und auch unser Umgang mit Passwörtern ist nicht gerade verantwortlich. Oft verwenden wir für mehrere Accounts dasselbe Passwort, wir nehmen die Namen und Daten von geliebten Menschen oder Tieren und von Sachen die uns wichtig sind, in unser Passwort auf. Selten sind diese Informationen, die wir in unseren Passwörtern verwenden, anderen Menschen ein Geheimnis. Verwendest du zum Beispiel den Namen deines Partners und das Jahr, in dem ihr zusammen kamt, lässt sich dies spielend leicht von jedem in deinem Bekanntenkreis erraten, und je nachdem wie viel du auf sozialen Medien preisgibst, auch von jedem Fremden. Die Schuld für dieses Verhalten liegt zum Teil natürlich bei uns. Wie in unserem gesamten Onlineverhalten, gehen wir im Augenblick eher unvorsichtig mit unseren Daten um. Wollen wir mehr Sicherheit, müssen wir alle unser Passwortverhalten überdenken. Ähnlich wie überall im Internet verfallen wir bei der Passwortgenerierung jedoch in eine Art Schockstarre.

In unserem Umgang mit den „neuen Medien“ ist dies kein neuer Zustand. Gerhard Banse beschreibt in „Informationsgesellschaft und Kultur“ als Effekt auf die Online-Welt „die Möglichkeit inhaltlicher Beliebigkeit und haltloser Orientierungslosigkeit.“[38] Die Hilflosigkeit gegenüber dem richtigen Umgang mit der Sicherheit im Internet ist ein Thema, welches alle Generationen betrifft. Laut einer Statistik von 2017 nutzen 44 Prozent der jungen US-Amerikaner*innen zwischen 18 und 34 Jahren für alle oder die meisten ihrer Online-Accounts

dasselbe Passwort. Nur 15 Prozent der über 55-jährigen zeigen ein ähnlich leichtsinniges Passwortverhalten. So geben auch 42 Prozent der unter 35 jährigen an, zumindest schon einmal Opfer von Hacking geworden zu sein.[39] Dies macht deutlich, dass der fahrlässige Umgang mit unserer IT-Sicherheit keineswegs ein Problem der älteren Generation ist. Es scheint vielmehr, als dass die Skepsis jener, die ohne das Internet aufgewachsen sind, sie auf unbekanntem Gelände vorsichtiger werden lässt. Während für uns, die jüngere Generation, die Grenzen zwischen Digitalem und Realem mehr und mehr verschwimmen, wir die Sicherheit im Netz aber viel weniger ernst nehmen als in der Realität. Das viel benutzte Argument „Ich habe ja nichts zu verstecken" sollte gründlich hinterfragt werden,

schließlich lässt du deine Wohnungstür selten offen stehen, wenn du das Haus verlässt.

Am Ende benutzen wir dann seufzend und wohlwissend überall dasselbe Passwort, um wenigstens den Prozess der Passwortzurücksetzung zu umgehen. Dies offenbart eine paradoxe Beziehung zum Passwort. Zum einen ist Datenschutz so wichtig wie nie zuvor. Niemals haben wir so viel Zeit im Internet verbracht wie heute. Unser Leben verlagert sich mehr und mehr in die digitale Welt. Doch je sicherer Datenschutz wird, desto mehr Passwörter benötigen wir. Je mehr Passwörter wir bekommen, desto weniger sicherer werden sie, weil wir uns wirklich sichere Passwörter nicht merken können. Jedenfalls nicht 100 verschiedene Passwörter für 100 verschiedene Online Accounts. Möglicherweise haben wir aber auch einfach zu wenig Übung mit dem Werkzeug „Passwort". Gerhard Banse erklärt die Veränderungen, die sich im Zuge neuer technischer Lösungen ergeben, als umso schwerwiegender, je weiter die zwei Systeme, die alte und die neue technische Lösung voneinander entfernt sind. Dafür spiele außerdem die Zeit für die Gewöhnung an die neue Lösung und die Übung mit ihr eine bedeutende Rolle.[40] Als „alte Lösung" könnten wir hier beispielsweise das System von Schloss und Schlüssel nehmen. Im Gegensatz zu diesem System der Sicherung des Heims oder des Besitzes, hat die Menschheit mit dem System „Passwort" möglicherweise zu wenig Umgang gehabt. Das Digitale jedoch bewegt sich in einem unglaublichen Tempo voran und lässt uns kaum Zeit, mit gewissen Dingen vertraut zu werden. Die Ergebnisse sind erneut Hilflosigkeit und Frustration.

Aus der Beziehung Mensch-Passwort entsteht deshalb geradezu eine Hassliebe. Wir wollen und wir müssen das Passwort sicher gebrauchen, wir können es aber nicht. Es ist uns in seiner jetzigen Fülle und Form schlichtweg unmöglich. Auch möchten wir mit ihm unsere Identität und unser Leben schüt-

~~123456~~

~~12345678~~

~~123456789~~

~~12345~~

~~qwerty~~

~~iloveyou~~

~~password~~

~~111111~~

~~1234567~~

~~123123~~

zen. So sehr wie sich unser Leben ins Internet verlagert hat, lässt sich sagen, dass mit dem Knacken eines Passwortes ein Teil unseres Lebens verlorengehen kann. So versuchen wir, wie bereits beschrieben, das Passwort an uns anzupassen und es mit Menschlichkeit zu versehen, damit wir es nutzen können. Wir alle kennen die Verzweiflung, wenn ein Passwort verloren gegangen ist und wir uns daraufhin ein neues ausdenken müssen. Noch eins. Wir unterwerfen uns damit geradezu dem System „Passwort“ und müssen uns fragen, wer beherrscht hier wen? Doch der Computer und das Internet sind von Menschen erschaffen, möglicherweise sollten wir uns die Kontrolle zurückholen und aufhören, uns anzupassen. Das, was das Passwort fehlbar macht, ist der Mensch. Computer sind, was Passwörter angeht, selten fehlerhaft und vergessen nie. Ohne den Menschen gibt es jedoch keine Passwörter. Das Passwort ist damit ein gutes Beispiel für die Kontrolle des Digitalen über uns. Anstatt das Passwort für den Menschen nutzbar zu machen, passen wir uns ihm an und versuchen, es zu nutzen. Und scheitern daran kläglich. In unserer Beziehung mit dem Passwort offenbart sich deshalb ein Paradox. Wir sind von ihm abhängig, es ist uns aber unmöglich, es sicher zu gebrauchen. Abstrus ist diese Beziehung auch deshalb, weil wir als Menschen das System „Passwort“ erschaffen haben und es deshalb auch an unsere Menschlichkeit anpassen könnten. Rosa Riera, zuständig für Employer Branding und Social Innovation bei Siemens AG, beschreibt in ihrem Artikel über die digitale Transformation die Beziehung zwischen Mensch und Technologie folgendermaßen:

„Es geht (...) im digitalen Zeitalter nicht primär um Technologie, sondern darum, wie wir diese digitale Welt für uns gestalten wollen. Wir sind ohnehin nicht mehr in der Lage, mit Maschinen zu konkurrieren. Es wird daher Zeit, dass wir uns auf unsere „Kernkompetenz“ als Mensch besinnen und uns in Zukunft darauf spezialisieren.“[42]

Zu dieser Aussage gehört meiner Meinung auch, dass wir die Maschinen und damit auch das Passwort für uns Menschen benutzerfreundlicher gestalten. Es ist nicht Mensch gegen Maschine, sondern Maschine für den Menschen. Technologien sind entwickelt worden, um uns in unserem Alltag zur Seite zu stehen, Maschinen müssen deshalb nicht menschlicher, aber menschenfreundlicher werden. Dies könnte meiner Meinung der einzige logische Schritt sein, um das Überleben des Passwortes zu sichern und damit auch ein Stück unserer Unabhängigkeit. Die Anpassung an die menschlichen Bedürfnisse. Matthias Meifert schrieb für „Manager-Magazin“ den kategorischen Imperativ Immanuel Kants folgendermaßen um:

„Digitalisiere nur das, was Du auch digitalisiert haben möchtest.
Digitalisiere so, wie Du auch digitalisiert werden möchtest.
Digitalisiere, um dem Menschen zu dienen.“ [43]

Technik und Digitale Transformation sollten nicht da sein um ihrer eigener Erhaltung wegen, sondern sie sind menschengemacht und müssen deshalb für den Menschen anwendbar sein. Dazu müssen wir untersuchen, an welchen Stellen bestimmte digitale Hinterlassenschaften für uns noch brauchbar sein könnten. Eine derartige Analyse könnte zu dem Ende des Passwortes führen. Längst scheint es Alternativen zu geben, die das Passwort an Sicherheit und Benutzerfreundlichkeit übertreffen. Deshalb müssen wir uns die Frage stellen:

Brauchen wir das Passwort überhaupt, oder ist es ein überholtes Werkzeug, dessen wir uns längst hätten entledigen sollen?

Kapitel 5: Das Ende des Passwortes (?)

K5:D

EdP

w(?

Die Softwarefirma XignSys wirbt auf ihrer Webseite gegen das Passwort. Als Gründe nennt sie 5 Punkte:[44]

1. Passwörter sind oft leicht zu knacken, weil wir zu einfache Passwörter erstellen. Dabei liegt die Schuld nicht bei uns, wir müssen uns schlichtweg zu viele Passwörter merken, um diese auch noch komplex zu gestalten

2. Sobald einmal das Passwort geknackt wurde, haben die Angreifer*innen meist Zugang zu weiteren Konten, zu Zahlungsinformationen und persönlichen Informationen. Besonders, wenn überall dasselbe Passwort verwendet oder der Email Account angegriffen wurde.

3. Gegen Hackingmethoden wie Phishing, Malware oder Social Engineering kann meist das beste Passwort nichts ausrichten. Zum Beispiel wird man beim Phishing auf gefälschte Websites weitergeleitet, auf welchen man dann ganz freiwillig und ahnungslos seine Login Daten eingibt.

4. „Passwörter fressen Zeit und Geld“. Passwörter abzusichern, durch Software wie beispielsweise Passwort-Manager kostet oft zusätzliches Geld. Passwörter neu zu beantragen ist nicht schwer, aber oft lästig.

5. Je digitaler unsere Welt wird und je mehr unser Privates in das Digitale gleitet, desto wichtiger wird es, dass wir sichere Authentifizierungsmethoden haben.

Hier kommt XignSys dann auf ihr eigenes Produkt zu sprechen, ein Multifaktorauthentifikationssystem. Die Multifaktorauthentifizierung findet beispielsweise auch schon am Bankautomaten statt. Dort müssen wir uns sowohl mit unserer Bankkarte ausweisen als auch unsere PIN eingeben. XignSys spricht auch über biometrische Erkennungsmethoden wie Face-ID und den Fingerabdruck, als sichere Authentifizierungsmethoden.

Dabei spricht einiges gegen die Multifaktorauthentifizierung wie auch gegen biometrische Erkennungsmethoden. Für Webseitenbetreiber*innen, die mit sensiblen und vertraulichen Daten hantieren, wie beispielsweise dein Online-Banking Account oder der Account deiner Krankenkasse, ist es sinnvoll, das doppelte Login-Verfahren einzusetzen. Für alle Accounts erscheint dies wenig sinnvoll, es ist meist einfach zu kompliziert: Du brauchst meist dennoch ein Passwort, musst aber zum Beispiel auch dein Handy jederzeit in Reichweite haben, um eine SMS-Tan zugesendet zu bekommen. Und für Dienste, auf denen wir ständig eingeloggt sind wie die meisten der Apps auf unserem Handy, spielt die Authentifizierung quasi keine Rolle. Ein sicheres Authentifizierungsverfahren zu benutzen ist nur von Vorteil, wenn wir uns auch regelmäßig ausloggen. Dies gilt im Grunde auch für sichere Passwörter, biometrische Erkennungsmethoden und jede andere Authentifizierungsmethode. Auch das biometrische Erkennungsverfahren hat seine Tücken. James L. Wayman, international anerkannter Bio-

metrie-Experte, erklärt biometrische Erkennungsmethoden folgendermaßen: „Unter Biometrie versteht man die automatische Erkennung von menschlichen Individuen, und zwar aufgrund ihrer physischen Kennzeichen und Verhaltensmerkmale.“[45] Als Vorteil der Biometrie, nennt er die physische Verbindung, die zwischen Technik und Person hergestellt wird. Wir werden anhand unserer individuellen Merkmale identifiziert und können deshalb niemals zweimal im System vorkommen.[46] Anders als beim Passwort. Dort ist es spielend einfach, als eine Person mehrere verschiedene Accounts zu erstellen und damit auch mehrere Identitäten zu faken. Das Einzige was meist dafür benötigt wird, sind unterschiedliche E-Mail Adressen. Aber auch Wayman nennt die Grenzen der biometrischen Erkennungsmethoden: Augenverletzungen oder beispielweise zwei rechte Daumen sind Probleme für das System.[47] Außerdem sei auch hier ein hundertprozentiger Schutz nie gewährleistet.

Auch große Datenbanken die unsere biometrischen Daten speichern, können sich vor Sicherheitslücken nicht schützen.[48]

Die Auswirkungen wären dann umso fataler, wenn diese Daten in die falschen Hände oder an die Öffentlichkeit geraten. Denn in diesem Fall wird die Einzigartigkeit eines jeden, mit welcher biometrische Erkennungsmethoden arbeiten, zu einem Problem. Im Falle eines geklauten Passwortes können wir dieses ändern, das Muster unserer Iris oder die Rillen auf unserer Fingerspitze jedoch nicht. Sollten deine biometrischen Daten also einmal gestohlen worden sein, wirst du sie ein Leben lang nicht mehr als Authentifizierungsmethode verwenden können.[49] Außerdem wurde in jenem Fall quasi deine Identität gestohlen und könnte auch gegen dich verwendet werden. Stell dir nur einmal vor, dein persönlicher Fingerabdruck gerät in kriminelle Hände. Gerade dieser kann bereits mit Hilfe eines Fotos rekonstruiert werden. Hacker Jan Krissler, Mitglied des CCC (Chaos Computer Clubs), hatte bereits 2014 den Fingerabdruck von Politikerin Ursula von der Leyen mit Hilfe eines Fotos kopiert. Entscheidend ist für die Hacker nur noch die Qualität des Fotos als auch die Entfernung zum Finger.[50] Beim Iris-Scan reicht meistens schon ein einfacheres Porträtfoto. 2017 zeigte der CCC in einem Video, wie der Iris-Scanner des Samsung Galaxy S8 ganz einfach ausgetrickst werden konnte. Dazu wurde ein Foto des Auges aufgenommen, vergrößert, auf einfachem Papier ausgedruckt und eine Kontaktlinse auf das gedruckte Auge platziert „damit das echter aussieht“. Das Handy erkannte das Auge und entsperrte sich.[51]

Biometrische Erkennungsmethoden sind also mit Vorsicht zu behandeln. Keine Datenbank kann garantieren, dass deine

Daten bei ihnen zu 100% sicher sind. Dies gilt auch für Passwörter, doch sind unsere biometrischen Daten weitaus sensibler als ein Passwort, das wir im Notfall einfach zurücksetzen können. In jedem Fall eignet sich die Biometrie höchstens als zusätzliches Werkzeug in der Zwei-Faktor Authentifizierung. Die biometrische Erkennungsmethode ist zwar bequem, aber nicht sicher. Deine Biometrie ist deine Identität. Ob du diese Daten der Welt offenbaren willst, und im Internet musst du immer damit rechnen, dass jemand deine Daten klauen könnte, ist letztendlich immer deine Entscheidung. Ich würde mich in jedem Fall dagegen entscheiden und habe mich auch schon beim Herausgeben meines Fingerabdruckes für den neuen Personalausweis unwohl gefühlt.

Ein sicheres Authentifizierungsverfahren zu benutzen ist nur von Vorteil, wenn wir uns auch regelmäßig ausloggen

Zusätzlich zu der biometrischen Erkennungsmethode nennt die Sicherheitsfirma „BullGuard“ noch drei weitere Authentifizierungsmethoden der Zukunft:[52]

1. ***Zero Login***
   Beim Zero Login erkennt das Login-Programm einzigartige Verhaltensmuster wie beispielsweise Tippmuster, der Druck auf den Bildschirm bei Touch-Geräten oder deinen Standort. Du bekommst somit automatisch Zugriff zu deinem Account, ohne dich aktiv einloggen zu müssen. Nach einer weiteren Authentifizierung wird nur gefragt, wenn es teilweise nicht zu Übereinstimmungen kommt.

2. ***Mikrochip Implantate***
   Diese Idee gibt es schon seit längerem. Mit Hilfe von einem unter die Haut implantierten Chip können Türen geöffnet und Geräte entsperrt werden.

3. ***Brain Password***
   Das Brain-Password ist das gespeicherte digitale Muster deiner Gehirnaktivität, während du auf bestimmte Reize reagierst. Wie die Organisation futurity.org berichtet,[53] werden der Person dabei drei Bilder gezeigt, je nachdem, wie das Gehirn reagiert, ergibt sich dabei ein individuelles Muster, welches wie ein Passwort funktionieren kann. Obwohl diese Methode in seiner Entwicklung noch in der Anfangsphase ist, gilt es als besonders sicher, da Gehirnströme nicht replizierbar sind.

Der Vorteil dieser Erkennungsmethoden ist im Besonderen, dass sie schwieriger zu replizieren und zu fälschen sind als einfache Passwörter. Dennoch haben sie alle eine entscheidende Schwachstelle: Wie auch bei biometrischen Erkennungsmethoden gibt man gefährlich viel über sich Preis und es gibt keine Hundertprozentige Garantie dafür, wie sicher deine Daten in den jeweiligen Datenbanken aufgehoben sind.

Authentifizieren bedeutet immer auch Identifizieren, und so ist auch das Passwort mit Identifikation und Identität untrennbar verbunden. Wie auch mit der Frage, wie wir unsere Identität am besten schützen können. Weder das Passwort alleine noch neue Methoden versprechen ausreichend Sicherheit. Zum Teil erscheinen die neuen Erkennungsmethoden als eine noch größere Gefahr für unsere Person. Ein Ende des Passwortes sehe ich deshalb in naher Zukunft nicht. Vielmehr muss das Passwort für uns besser zu benutzen sein. War es am Anfang seiner digitalen Nutzung noch ein gutes Werkzeug, um sich in seinen wenigen Accounts zu authentifizieren, so ist es bei den hunderten von Online-Accounts, die wir heute besitzen, schwierig geworden, das Passwort in seiner Urform zu gebrauchen. Das Passwort bleibt, wir müssen aber unseren Umgang mit ihm ändern. Gleichzeitig muss es für uns besser zu gebrauchen sein, denn die Anforderungen, die das Passwort an den Menschen stellt, sind zu hoch.

Kapitel 6: But for now...

K 6 : B f n ...

Im Augenblick erscheint ein Ende des Passwortes also nicht in Sicht.

Es gibt Alternativen, in jeglicher Hinsicht besser und sicherer als das gute alte Passwort ist jedoch keine von ihnen. Auch wenn sich dies möglicherweise in naher Zukunft bereits ändern wird, unsere Daten sind hier und jetzt in Gefahr. Wir alle brauchen sofort Unterstützung in unserem Passwortverhalten. Deshalb hier eine einige Tipps, die jeder spielend leicht befolgen kann, also keine Ausreden mehr!

1. Verwende einen Passwort-Manager

Der Passwort Manager ist ein Programm, das du auf deinem Rechner speicherst. Es merkt sich alle deine Passwörter, übernimmt oft die Passwörter, die dein Browser meist sowieso schon von dir kennt, und wenn du willst kreiert der Passwort Manager ein besonders langes kryptisches Passwort für dich und speichert es ab. So schaffst du es, für jeden Account ein anderes Passwort zu verwenden, ohne dir alle merken zu müssen. Für den Passwort Manager benötigst du im Prinzip nur ein einziges Passwort, nämlich das für deinen Passwort-Safe.[54] Allerdings solltest du dich immer aus dem Safe ausloggen, wenn du deinen Rechner schließt. Der Passwort Manager kostet dich unter Umständen etwas, allerdings sind auch viele gratis verfügbar, haben dann allerdings Einschränkungen wie beispielsweise die Anzahl der Passwörter, die gespeichert werden können. Ich selbst verwende zum Beispiel Dashlane: *www.dashlane.com*

2. Je länger, desto sicherer

Die Empfehlung, ein möglichst langes Passwort zu verwenden, gibt es nicht ohne Grund. Bei der sogenannten „Brute Force“ Methode versuchen die Angreifer*innen, sich durch wahlloses Durchprobieren Zugang zu deinem Account zu verschaffen. Das Durchprobieren erledigt selbstverständlich ein Computer, der binnen kürzester Zeit mögliche Passwortkombinationen abfragt.[55] Besteht ein Passwort aus sechs Kleinbuchstaben, gibt es um die 309 Millionen Kombinationen. Ein moderner Rechner errät ein solches Passwort innerhalb

von 7 Sekunden, benötigt allerdings für ein Passwort mit zwölf Kleinbuchstaben um die 66 Jahre.[56] Je länger und komplexer ein Passwort also ist, desto höher die Anzahl der Versuche. Auch deshalb macht eine Kombination aus Groß-und Kleinbuchstaben, Sonderzeichen und Zahlen Sinn.[57] In erster Linie reicht aber bereits die Länge für die Sicherheit des Passwortes aus. Je länger das Passwort, desto mehr Rechenleistung wird benötigt.[58] Ist der Zeit-und Kostenaufwand für das Herausfinden des Schlüssels zu hoch, wird es schlicht und einfach ineffizient.[59]

3. Verwende eine Passphrase

Um ein gutes und sicheres Passwort zu generieren, solltest du keine Wörter in deinem Passwort verwenden, die auch im Wörterbuch zu finden sind. Diese Wörter werden oft in wahrscheinlichen Wortkombinationen verwendet, womit das Passwort mit Hilfe der Brute-Force Methode leichter herauszufinden ist. Am einfachsten ist es, dein Passwort mit Hilfe eines Satzes zu generieren. Dabei verwendest du jeweils nur den ersten Buchstaben eines jeden Wortes, und schon hast du eine zufällige Abfolge von Buchstaben und wenn möglich auch Ziffern und Zeichen.[60] Zum Beispiel:

„Mein Vorsatz für das neue Jahr 2020 ist, nur noch sichere Passwörter zu verwenden“

daraus ergibt sich die Passphrase:

M V f

d n J 2

0i, — nn

s P z v

So lässt sich schnell ein Passwort generieren, welches sowohl die geforderte Anzahl an Zeichen enthält, als auch Groß- und Kleinschreibung, Ziffern, Sonder-und auch Leerzeichen. Leicht zu erratende und populäre Passphrasen sollte man allerdings hier vermeiden. Ein bekannter Satz wie „Fuchs du hast die Gans gestohlen, gib sie wieder her", also „FdhdGg, gswh" ist zu vorhersehbar und kann mit verschiedenen Methoden nur zu leicht erraten werden.[61] Hacker lernen schließlich auch dazu, und Computer haben immer höhere Rechenleistungen. Auch deshalb steigt die empfohlene Zeichenanzahl immer weiter an.

4. Achte darauf, wo du dich mit deinem Passwort einloggst

In deinem eigenen WLAN bist du, vor allem wenn du die bereits genannten Tipps befolgst, relativ sicher. Anders sieht es dagegen aus, wenn du dich in einem offenen WLAN mit deinen Daten einloggst. In einem offenen WLAN ist meist nichts verschlüsselt und deine Daten können recht einfach mitgelesen werden. Ich würde dir deshalb davon abraten, dich im WLAN des Flughafens in den Account deiner Bank einzuloggen. Achte besonders hier darauf, was du preisgeben möchtest. Dein Passwort sollte es in aller Regel nicht sein. Generell solltest du deinem Gerät verbieten, sich automatisch in bereits bekannte WLAN-Netzwerke einzuwählen.[62] An unbekannten Geräten, wie beispielsweise deinem Rechner am Arbeitsplatz, ein wichtiges Passwort einzugeben, birgt ebenfalls Risiken. Zu leicht könnte es passieren, dass der Browser deine Login-Daten speichert. Falls sich dies nicht vermeiden lässt, solltest du zumindest deine Browser-Daten löschen und dich nach jeder Sitzung ordentlich ausloggen.[63]

5. Zwei-Faktor-Authentifizierung

Wird die zwei-Faktor-Authentifizierung angeboten, solltest du sie nutzen. Zumindest für einige deiner wichtigsten Accounts wie beispielsweise dein Online-Banking. Dabei loggst du dich mit einem Passwort ein und musst dich daraufhin nochmals authentifizieren. Häufig geschieht dies über einen Code, den du per SMS auf dein Handy geschickt bekommst. Meist findet man diese Authentifizierungsmethode bereits bei Banken oder anderen Anbietern, die mit besonders sensiblen und wertvollen Daten hantieren, aber auch auf Facebook kann man sich bereits über den SMS-Code zusätzlich einloggen.[64]

6. Achte auf Virenschutz und Sicherheits-Updates

Nicht nur auf deinem Laptop, auch auf deinem Smartphone solltest du auf deinen Virenschutz achten. Das Smartphone ist, was deine Daten und auch deine Passwörter angeht, besonders angreifbar. Es enthält oft die privatesten Dinge aus unserem Leben, ist aber nur durch eine einfache PIN geschützt. In diverse Apps ist man ununterbrochen eingeloggt und selten ist eine Virenschutz-Software installiert. Außerdem solltest du Betriebssysteme und Apps immer auf den neuesten Stand bringen.[65] Updates beseitigen oft Sicherheitslücken im System, durch die deine Daten angreifbar werden.[66]

7. Logg dich aus!

Ja, es ist ein notwendiges Übel, aber ein sicheres Passwort ist nur von Vorteil, wenn die Tür, die es verschließt, auch geschlossen ist. Ja, es ist praktisch, in deinen Apps am Handy dauerhaft eingeloggt zu sein und dieses Verhalten wird sich – bis es eine einfachere Login-Methode gibt – auch nicht ändern, aber dann versehe zumindest dein Handy mit einem starken Schlüssel und reduziere die Apps, in die du dauerhaft eingeloggt bist, auf ein Minimum.

Ändern solltest du dein Passwort übrigens nur, wenn es bereits einen Angriff gab oder die konkrete Gefahr darauf besteht. Studien zufolge macht eine Passwort-Änderung nur Sinn, wenn man ein komplett neues Passwort verwendet. In der Praxis geschieht dies allerdings eher selten, außerdem wird das Passwort simpler, wenn man bereits von vornherein weiß, dass es bald wieder geändert werden muss.[67] Folgst du bereits diesen sechs Tipps für ein verantwortungsvolles Passwortverhalten, bist du auf einem guten Weg, dich und deine Daten sehr gut zu schützen. Dann kostet es Angreifer*innen schlicht und einfach zu viel Zeit und Geld, deine Passwörter herauszufinden. Dort draußen warten außerdem noch viel leichtere Opfer als du. Beispielsweise Kanye West, der 2018 bei seinem Besuch im Weißen Haus mit dem Code „000000“ sein Smartphone entsperrte.[68]

Nachwort

Nachdem ich meine Suche nach dem Menschen im Passwort beendet habe, lässt sich sagen, dass das Passwort und der Mensch so eng verbunden sind wie nie zuvor. Es ist zu einem Werkzeug geworden, welches wir tagtäglich benutzen und welches wir brauchen. Für die Sicherheit im Netz spielt es eine bedeutende Rolle, ob Alternativen die Lösung sein können, ist fraglich. Im Laufe meiner Recherche ist deutlich geworden, dass das Passwort nicht gegen den Menschen arbeitet und kein Übel sein muss, dem wir uns nicht entledigen können. Vielmehr sollten wir, nachdem feststeht dass jetzt und heute noch nicht das Ende des Passwortes gekommen ist, wieder lernen, es wert zu schätzen. Wir haben das Passwort für uns erschaffen und wir müssen es so optimieren, dass es für uns nutzbar wird. Das Passwort stellt wieder einmal die Schnittstelle zwischen der Technik und dem Menschen dar. Der Mensch projiziert seine Menschlichkeit in das Passwort. Und so ist das Passwort ein wunderbares Beispiel für die Fähigkeit des Menschen, sich nicht von scheinbar seelenlosen Dingen kontrollieren zu lassen, sondern seine Menschlichkeit auf sie zu übertragen und ihnen aufgrund der Benutzung durch ihn, Leben einzuhauchen.

Vorwort

01 bigFM Staff: So oft entsperren wir am Tag unsere Handys (24.04.2016), bigFM, https://www.bigfm.de/topic/12232/entsperren-tag-handys (Stand: 13.01.2020)

02 John Hall: SplashData's Top 100 Worst Passwords of 2018 (13.12.2018), TeamsID, https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/ (Stand: 28.01.2020)

03 Georgina Bott: Haben wir ein Passwortproblem? (04.05.2017), marconomy, https://www.marconomy.de/digital/articles/605153/ (Stand: 19.01.2020)

04 Ebd.

Kapitel 1: Der Mythos Passwort

05 o.V.: Die Geschichte von Ali Baba und den vierzig Räubern (o.J.), Labbé, http://www.labbe.de/lesekorb/index.asp?themakatid=11&themaid=92&titelid=720 (Stand: 06.01.2020)

06 o.V.: Ali Baba (03.12.2019), KLEXIKON, https://klexikon.zum.de/wiki/Ali_Baba (Stand: 06.01.2020)

07 Sue Vertue & Paul McGuigan: Sherlock Holmes "A Scandal in Belgravia" (01.01.2012), Staffel Nr.2, Folge Nr.1, BBC, UK

08 David Heyman & Chris Columbus: Harry Potter und die Kammer des Schreckens (2002), Warner Bros. GmbH, USA/UK/Deutschland

09 Kathleen Kennedy,Gerald R. Molen & Steven Spielberg: Jurassic Park (1993), Amblin Entertainment & Universal Studios, USA

10 Ebd.

11 o.V.: Die Geschichte von Ali Baba und den vierzig Räubern (o.J.), Labbé, http://www.labbe.de/lesekorb/index.asp?themakatid=11&themaid=92&titelid=720 (Stand: 06.01.2020)

12 Sue Vertue & Paul McGuigan: Sherlock Holmes "A Scandal in Belgravia" (01.01.2012), Staffel Nr.2, Folge Nr.1, BBC, UK

13 David Heyman & Chris Columbus: Harry Potter und die Kammer des Schreckens (2002), Warner Bros. GmbH, USA/UK/Deutschland

14 Rafaela Khodai: Diese Wiener Clubs sind streng geheim (17.01.2018), ichreise, https://ichreise.at/oesterreich/diese-wiener-clubs-sind-streng-geheim/ (Stand: 08.01.2020)

15 Alexandra Stani: Der Schlüssel zur Nacht – Undercover im Club X (06.02.2017), dasBiber, https://www.dasbiber.at/content/der-schluessel-zur-nacht-undercover-im-club-x (Stand: 08.01.2020)

16 Rafaela Khodai: Diese Wiener Clubs sind streng geheim (17.01.2018), ichreise, https://ichreise.at/oesterreich/diese-wiener-clubs-sind-streng-geheim/ (Stand: 08.01.2020)

17 Alexandra Stani: Der Schlüssel zur Nacht – Undercover im Club X (06.02.2017), dasBiber, https://www.dasbiber.at/content/der-schluessel-zur-nacht-undercover-im-club-x (Stand: 08.01.2020)

18 o.V.: Frannz Club (09.07.2016), Facebook, https://www.facebook.com/frannz/posts/10153887629672893/ (Stand: 08.01.2020)

19 Liv: Sag besser „Käsekuchen" anstatt „Nein"! — Über das Safeword im BDSM (19.04.2018), ohja, https://www.ohja.de/safeword-bdsm/ (Stand: 08.01.2020)

20 o.V.: Parole (Militär) (22.12.2014), Wikipedia, https://de.wikipedia.org/wiki/Parole_(Milit%C3%A4r) (Stand: 22.01.2020)

21 Monika Piotrowska: Triumph der Mathematik (10.11.2007), Welt, https://www.welt.de/welt_print/article1349440/Triumph-der-Mathematik.html (Stand: 22.01.2020)

Kapitel 2: Das Passwort als Geheimnis

22 o.V.: Passwort (o.J.), Duden, https://www.duden.de/rechtschreibung/Passwort (Stand: 08.01.2020)

23 Kurt Marti: Das panoptische System totaler Überwachung (07.10.2013), hpd-humanistischer Pressedienst, https://hpd.de/node/16887 (Stand: 28.01.2020)

24 Hendrik Ankenbrand & Britta Beeger: Der gläserne Mensch (09.06.2013), FAZ, https://www.faz.net/aktuell/wirtschaft/internet-der-glaeserne-mensch-12214568.html (Stand:08.01.2020)

25 Paul Gäbler: Datenschützer sehen durch Passwort-Herausgabe Grundwerte in Gefahr (16.12.2019), Der Tagesspiegel, https://

www.tagesspiegel.de/politik/umfassende-ueberwachungsrechte-fuer-den-staat-datenschuetzer-sehen-durch-passwort-herausgabe-grundwerte-in-gefahr/25339980.html (Stand: 27.01.2020)
26 Martin Zeyn: Niemand hat nichts zu verbergen (04.08.2019), Deutschlandfunk, https://www.deutschlandfunk.de/soziale-medien-niemand-hat-nichts-zu-verbergen.1184.de.html?dram:article_id=454749 (Stand: 08.01.2020)
27 Ebd.

Kapitel 3: Das Passwort als Teil unserer Identität

28 Veronika Straass: Die Biometrie der Tiere, in: Identität im digitalen Zeitalter, hrsg. v. Bundesdruckerei GmbH, Hoffmann und Campe GmbH, Berlin, 2004, S.40-43, S.41
29 o.V.: Passwörter verraten den Charakter (04.07.2001), Computerwoche, https://www.computerwoche.de/a/passwoerter-verraten-den-charakter,521854 (Stand: 23.01.2020)
30 Jörn Brien: „ficken" ist zurück: Die 10 meistgenutzten Passwörter 2018 (18.12.2018), t3n – digital pioneers, https://t3n.de/news/beliebteste-passwoerter-2018-1133707/ (Stand: 23.01.2020)
31 o.V.: Passwörter verraten den Charakter (04.07.2001), Computerwoche, https://www.computerwoche.de/a/passwoerter-verraten-den-charakter,521854 (Stand: 23.01.2020)
32 Sherry Turkle: Leben im Netz, Reinbek, Hamburg, 1995, S.289 zitiert nach: Gerhard Banse: Identität in der realen Welt und im Cyberspace – Chancen und Gefahren, in: Informationsgesellschaft und Kultur – Internet-globale Kommunikation-Identität, hrsg. v. Andrzej Kiepas & Urszula Zydek-Bednarczuk, trafo Verlag, Berlin, 2006, S. 53-66, S.54
33 Jayne Gackenbach: Psychology and the Internet, Academic Press, California/London, 1998, S.40-41
34 Splash data: The Top 50 Worst Passwords of 2018 (o.J.), TeamsID, https://www.teamsid.com/100-worst-passwords-top-50/ (Stand: 10.01.2020)

35 Splash data: The Top 50 Worst Passwords of 2019 (o.J.), TeamsID, https://www.teamsid.com/1-50-worst-passwords-2019/ (Stand: 10.01.2020)
36 Peter Schmitz: 61 Millionen Passwörter und beunruhigende Muster (11.06.2018), Security Insider, https://www.security-insider.de/61-millionen-passwoerter-und-beunruhigende-muster-a-719383/ (Stand: 27.01.2020)

Kapitel 4: Das Passwort Paradox

37 Martin Zeyn: Niemand hat nichts zu verbergen (04.08.2019), Deutschlandfunk, https://www.deutschlandfunk.de/soziale-medien-niemand-hat-nichts-zu-verbergen.1184.de.html?dram:article_id=454749 (Stand: 08.01.2020)
38 Gerhard Banse: Identität in der realen Welt und im Cyberspace – Chancen und Gefahren, in: Informationsgesellschaft und Kultur – Internet-globale Kommunikation-Identität, hrsg. v. Andrzej Kiepas & Urszula Zydek-Bednarczuk, trafo Verlag, Berlin, 2006, S. 53-66, S.59
39 Felix Richter: Young Americans Are Careless With Their Online Passwords (18.10.2017), statista, https://www.statista.com/chart/11525/americans-using-the-same-online-password/ (Stand: 22.01.2020)
40 Gerhard Banse: Identität in der realen Welt und im Cyberspace – Chancen und Gefahren, in: Informationsgesellschaft und Kultur – Internet-globale Kommunikation-Identität, hrsg. v. Andrzej Kiepas & Urszula Zydek-Bednarczuk, trafo Verlag, Berlin, 2006, S. 53-66, S.64
41 Splash data: The Top 50 Worst Passwords of 2019 (o.J.), TeamsID, https://www.teamsid.com/1-50-worst-passwords-2019/ (Stand: 10.01.2020)
42 Rosa Riera: Warum uns die Digitalisierung menschlicher macht (21.03.2018), Zukunft der Arbeit, https://www.zukunftderarbeit.de/2018/03/21/warum-uns-die-digitalisierung-menschlicher-macht/ (Stand: 27.01.2020)
43 Matthias Meifert: Es geht um die Freiheit, stupid! (08.06.2019),

Manager Magazin, https://www.manager-magazin.de/digitales/it/digitalisierung-macht-die-digitale-transformation-unfrei-a-1271471-3.html (Stand: 27.01.2020)
44 Markus Hertlein: Wir schaffen das Passwort ab - mit Sicherheit! (o.J.), XignSys, https://weltpassworttag.de/#xignsys, (Stand: 10.01.2020)
45 James L. Wayman & Marc Pitzke: Zwei rechte Daumen, in: Identität im digitalen Zeitalter, hrsg. v. Bundesdruckerei GmbH, Hoffmann und Campe GmbH, Berlin, 2004, S.58-61, S.59
46 Ebd. S.60
47 Ebd.
48 Ebd. S.61
49 Alexandra Bröhm: Ein Passwort kann man ändern, die eigene Iris nicht (01.09.2016), Süddeutsche Zeitung, https://www.sueddeutsche.de/digital/biometrische-systeme-ein-passwort-kann-man-aendern-die-eigene-iris-nicht-1.3144344 (Stand: 16.01.2020)
50 Ali Vahid Roodsari: Fingerabdruck-Scan kann mit Fotos geknackt werden (01.02.2017), Süddeutsche Zeitung, https://www.sueddeutsche.de/wissen/biometrie-sicher-unsicher-1.3357627 (Stand: 16.01.2020)
51 Jan Krissler: Die Sendung mit dem Chaos - Iris-Scanner im Samsung Galaxy S8 (23.05.2017), CCC, Web, https://media.ccc.de/v/biometrie-s8-iris-fun#t=79 (Stand: 16.01.20209
52 Steve Bell: The future of passwords, would you like a microchip in your hand? (09.05.2019), BullGuard https://www.bullguard.com/blog/2019/05/the-future-of-passwords,-would-you-like-a-microchip-in-your-hand?lang=en-IN (Stand: 04.02.2020)
53 Cory Nealon-Buffalo: 'Brain password' uses Leo DiCaprio to unlock your phone (07.06.2018), FUTURITY, https://www.futurity.org/unlocking-phone-brain-password-1778612/ (Stand: 17.01.2020)

Kapitel 6: But for now...

54 Peter Schmitz: Nur ein langes Passwozzrt ist ein gutes Passwort (03.05.2018), Security Insider, https://www.security-insider.de/nur-ein-langes-passwort-ist-ein-gutes-passwort-a-710589/ (Stand: 13.01.2020)
55 Stefan Luber & Peter Schmitz: Was ist ein Brute-Force-Angriff? (17.01.2018), Security Insider, https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/ (Stand: 13.01.2020)
56 Peter Schmitz: Nur ein langes Passwort ist ein gutes Passwort (03.05.2018), Security Insider, https://www.security-insider.de/nur-ein-langes-passwort-ist-ein-gutes-passwort-a-710589/ (Stand: 13.01.2020)
57 Stefan Luber & Peter Schmitz: Was ist ein Brute-Force-Angriff? (17.01.2018), Security Insider, https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/ (Stand: 13.01.2020)
58 Marvin Strathmann: Das sind die fünf größten Passwort-Mythen (04.05.2017), Süddeutsche Zeitung, https://www.sueddeutsche.de/digital/it-sicherheit-das-sind-die-fuenf-groessten-passwort-mythen-1.3489400 (Stand: 14.01.2020)
59 Stefan Luber & Peter Schmitz: Was ist ein Brute-Force-Angriff? (17.01.2018), Security Insider, https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/ (Stand: 13.01.2020)
60 Peter Schmitz: Nur ein langes Passwort ist ein gutes Passwort (03.05.2018), Security Insider, https://www.security-insider.de/nur-ein-langes-passwort-ist-ein-gutes-passwort-a-710589/ (Stand: 14.01.2020)
61 Marvin Strathmann: Das sind die fünf größten Passwort-Mythen (04.05.2017), Süddeutsche Zeitung, https://www.sueddeutsche.de/digital/it-sicherheit-das-sind-die-fuenf-groessten-passwort-mythen-1.3489400 (Stand: 14.01.2020)
62 Jörg Breithut: So schützen Sie sich beim Surfen im offenen WLAN (11.02.2018), Spiegel Netzwelt, https://www.spiegel.de/netzwelt/web/wlan-hotspots-sicher-verwenden-einfache-tipps-fuer-nutzer-a-1192526.html (Stand: 14.01.2020)
63 o.V.: Das unknackbare Password: Wie der Computer zur Enigma wird (05.07.2018), Gothaer Maklerblog, https://gothaer-maklerblog.

de/internet-security-passwort/ (Stand: 14.01.2020)

64 Facebook: Was ist die zweistufige Authentifizierung und wie funktioniert sie auf Facebook? (o.J.), Facebook, https://www.facebook.com/help/148233965247823 (Stand: 14.01.2020)

65 Peter Schmitz: Nur ein langes Passwort ist ein gutes Passwort (03.05.2018), Security Insider, https://www.security-insider.de/nur-ein-langes-passwort-ist-ein-gutes-passwort-a-710589/ (Stand: 14.01.2020)

66 Jamal Fischer: Android-Nutzer sollten auf Updates checken: BSI warnt vor kritischen Sicherheitslücken (08.07.2019), CHIP, https://www.chip.de/news/Android-Nutzer-sollten-sofort-updaten-BSI-warnt-vor-kritischen-Sicherheitsluecken_170773093.html (Stand: 14.01.2020)

67 Simon Hurtz: Warum es falsch ist, Passwörter regelmäßig zu ändern (20.01.2017), Süddeutsche Zeitung, https://www.sueddeutsche.de/digital/it-sicherheit-warum-es-falsch-ist-passwoerter-regelmaessig-zu-aendern-1.3106648 (Stand: 14.01.2020)

68 Peter Schmitz: Die größten Passwort-Sünder 2018 (04.01.2019), Security Insider, https://www.security-insider.de/die-groessten-passwort-suender-2018-a-785803/ (Stand: 23.01.2020)

Literaturverzeichnis

Hendrik Ankenbrand & Britta Beeger: Der gläserne Mensch (09.06.2013), FAZ, https://www.faz.net/aktuell/wirtschaft/internet-der-glaeserne-mensch-12214568.html (Stand: 08.01.2020)

Gerhard Banse: Identität in der realen Welt und im Cyberspace – Chancen und Gefahren, in: Informationsgesellschaft und Kultur – Internet-globale Kommunikation-Identität, hrsg. v. Andrzej Kiepas & Urszula Zydek-Bednarczuk, trafo Verlag, Berlin, 2006, S. 53-66

Steve Bell: The future of passwords, would you like a microchip in your hand? (09.05.2019), BullGuard https://www.bullguard.com/blog/2019/05/the-future-of-passwords,-would-you-like-a-microchip-in-your-hand?lang=en-IN (Stand: 04.02.2020)

bigFM Staff: So oft entsperren wir am Tag unsere Handys (24.04.2016), bigFM, https://www.bigfm.de/topic/12232/entsperren-tag-handys (Stand: 13.01.2020)

Georgina Bott: Haben wir ein Passwortproblem? (04.05.2017), marconomy, https://www.marconomy.de/digital/articles/605153/ (Stand: 19.01.2020)

Jörg Breithut: So schützen Sie sich beim Surfen im offenen WLAN (11.02.2018), Spiegel Netzwelt, https://www.spiegel.de/netzwelt/web/wlan-hotspots-sicher-verwenden-einfache-tipps-fuer-nutzer-a-1192526.html (Stand: 14.01.2020)

Jörn Brien: „ficken" ist zurück: Die 10 meistgenutzten Passwörter 2018 (18.12.2018), t3n – digital pioneers, https://t3n.de/news/beliebteste-passwoerter-2018-1133707/ (Stand: 23.01.2020)

Alexandra Bröhm: Ein Passwort kann man ändern, die eigene Iris nicht (01.09.2016), Süddeutsche Zeitung, https://www.sueddeutsche.de/digital/biometrische-systeme-ein-passwort-kann-man-aendern-die-eigene-iris-nicht-1.3144344 (Stand: 16.01.2020)

Facebook: Was ist die zweistufige Authentifizierung und wie funktioniert sie auf Facebook? (o.J.), Facebook, https://www.facebook.com/help/148233965247823 (Stand: 14.01.2020)

Jayne Gackenbach: Psychology and the Internet, Academic Press, California/London, 1998

Paul Gäbler: Datenschützer sehen durch Passwort-Herausgabe Grund-

werte in Gefahr (16.12.2019), Der Tagesspiegel, https://www.tagesspiegel.de/politik/umfassende-ueberwachungsrechte-fuer-den-staat-datenschuetzer-sehen-durch-passwort-herausgabe-grundwerte-in-gefahr/25339980.html (Stand: 27.01.2020)

John Hall: SplashData's Top 100 Worst Passwords of 2018 (13.12.2018), TeamsID, https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/ (Stand: 28.01.2020)

Markus Hertlein: Wir schaffen das Passwort ab - mit Sicherheit! (o.J.), XignSys, https://weltpassworttag.de/#xignsys, (Stand: 10.01.2020)

David Heyman & Chris Columbus: Harry Potter und die Kammer des Schreckens (2002), Warner Bros. GmbH, USA/UK/Deutschland

Kathleen Kennedy, Gerald R. Molen & Steven Spielberg: Jurassic Park (1993), Amblin Entertainment & Universal Studios, USA

Rafaela Khodai: Diese Wiener Clubs sind streng geheim (17.01.2018), ichreise, https://ichreise.at/oesterreich/diese-wiener-clubs-sind-streng-geheim/ (Stand: 08.01.2020)

Jan Krissler: Die Sendung mit dem Chaos - Iris-Scanner im Samsung Galaxy S8 (23.05.2017), CCC, Web, https://media.ccc.de/v/biometrie-s8-iris-fun#t=79 (Stand: 16.01.2020)

Liv: Sag besser „Käsekuchen" anstatt „Nein"! — Über das Safeword im BDSM (19.04.2018), ohja, https://www.ohja.de/safeword-bdsm/ (Stand: 08.01.2020)

Stefan Luber & Peter Schmitz: Was ist ein Brute-Force-Angriff? (17.01.2018), Security Insider, https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/ (Stand: 13.01.2020)

Kurt Marti: Das panoptische System totaler Überwachung (07.10.2013), hpd-humanistischer Pressedienst, https://hpd.de/node/16887 (Stand: 28.01.2020)

Matthias Meifert: Es geht um die Freiheit, stupid! (08.06.2019), Manager Magazin, https://www.manager-magazin.de/digitales/it/digitalisierung-macht-die-digitale-transformation-unfrei-a-1271471-3.html (Stand: 27.01.2020)

Cory Nealon-Buffalo: "Brain password" uses Leo DiCaprio to unlock your phone (07.06.2018), FUTURITY, https://www.futurity.org/unlocking-phone-brain-password-1778612/ (Stand: 17.01.2020)

Monika Piotrowska: Triumph der Mathematik (10.11.2007), Welt, https://www.welt.de/welt_print/article1349440/Triumph-der-Mathematik.html (Stand: 22.01.2020)

Felix Richter: Young Americans Are Careless With Their Online Passwords (18.10.2017), statista, https://www.statista.com/chart/11525/americans-using-the-same-online-password/ (Stand: 22.01.2020)

Rosa Riera: Warum uns die Digitalisierung menschlicher macht (21.03.2018), Zukunft der Arbeit, https://www.zukunftderarbeit.de/2018/03/21/warum-uns-die-digitalisierung-menschlicher-macht/ (Stand: 27.01.2020)

Ali Vahid Roodsari: Fingerabdruck-Scan kann mit Fotos geknackt werden (01.02.2017), Süddeutsche Zeitung, https://www.sueddeutsche.de/wissen/biometrie-sicher-unsicher-1.3357627 (Stand: 16.01.2020)

Peter Schmitz: 61 Millionen Passwörter und beunruhigende Muster (11.06.2018), Security Insider, https://www.security-insider.de/61-

millionen-passwoerter-und-beunruhigende-muster-a-719383/ (Stand: 27.01.2020)

Peter Schmitz: Nur ein langes Passwort ist ein gutes Passwort (03.05.2018), Security Insider, https://www.security-insider.de/nur-ein-langes-passwort-ist-ein-gutes-passwort-a-710589/ (Stand: 13.01.2020)

Splash data: The Top 50 Worst Passwords of 2018 (o.J.), TeamsID, https://www.teamsid.com/100-worst-passwords-top-50/ (Stand: 10.01.2020)

Alexandra Stani: Der Schlüssel zur Nacht – Undercover im Club X (06.02.2017), dasBiber, https://www.dasbiber.at/content/der-schluessel-zur-nacht-undercover-im-club-x (Stand: 08.01.2020)

Veronika Straass: Die Biometrie der Tiere, in: Identität im digitalen Zeitalter, hrsg. v. Bundesdruckerei GmbH, Hoffmann und Campe GmbH, Berlin, 2004, S.40-43

Marvin Strathmann: Das sind die fünf größten Passwort-Mythen (04.05.2017), Süddeutsche Zeitung, https://www.sueddeutsche.de/digital/it-sicherheit-das-sind-die-fuenf-groessten-passwort-mythen-1.3489400 (Stand: 14.01.2020)

Sherry Turkle: Leben im Netz, Reinbek, Hamburg, 1995, S.289 zitiert nach: Gerhard Banse: Identität in der realen Welt und im Cyberspace – Chancen und Gefahren, in: Informationsgesellschaft und Kultur – Internet-globale Kommunikation-Identität, hrsg. v. Andrzej Kiepas & Urszula Zydek-Bednarczuk, trafo Verlag, Berlin, 2006, S. 53-66

Sue Vertue & Paul McGuigan: Sherlock Holmes "A Scandal in Belgravia" (01.01.2012), Staffel Nr.2, Folge Nr.1, BBC, UK
James L. Wayman & Marc Pitzke: Zwei rechte Daumen, in: Identität im digitalen Zeitalter, hrsg. v. Bundesdruckerei GmbH, Hoffmann und Campe GmbH, Berlin, 2004, S.58-61

Martin Zeyn: Niemand hat nichts zu verbergen (04.08.2019), Deutschlandfunk, https://www.deutschlandfunk.de/soziale-medien-niemand-hat-nichts-zu-verbergen.1184.de.html?dram:article_id=454749 (Stand: 08.01.2020)

o.V.: Passwort (o.J.), Duden, https://www.duden.de/rechtschreibung/Passwort (Stand: 08.01.2020)

o.V.: Passwörter verraten den Charakter (04.07.2001), Computerwoche, https://www.computerwoche.de/a/passwoerter-verraten-den-charakter,521854 (Stand: 23.01.2020)

o.V.: Das unknackbare Passwort: Wie der Computer zur Enigma wird (05.07.2018), Gothaer Maklerblog, https://gothaer-maklerblog.de/internet-security-passwort/ (Stand: 14.01.2020)

o.V.: Parole (Militär) (22.12.2014), Wikipedia, https://de.wikipedia.org/wiki/Parole_(Milit%C3%A4r) (Stand: 22.01.2020

o.V.: Ali Baba (03.12.2019), KLEXIKON, https://klexikon.zum.de/wiki/Ali_Baba (Stand: 06.01.2020)

o.V.: Die Geschichte von Ali Baba und den vierzig Räubern (o.J.), Labbé, http://www.labbe.de/lesekorb/index.asp?themakatid=11&themaid=92&titelid=720 (Stand: 06.01.2020)

o.V.: Frannz Club (09.07.2016), Facebook, https://www.facebook.com/frannz/posts/10153887629672893/ (Stand: 08.01.2020)

Impressum

Bachelorarbeit von:
Biarna Diegmüller
Bachelor integriertes Design
Wintersemester 2019/2020
Hochschule für Künste Bremen

Prüferinnen:
Prof. Dr. Annette Geiger
Prof. Andrea Rauschenbusch

Gestaltung & Text:
Biarna Diegmüller
bdiegmueller@hfk-bremen.de

Schrift:
Mr Eaves San OT

Druck:
STÜRKEN Print Productions, 2020

Papier:
Munken Polar weiß 120g/m²