

FIF-Konferenz 2020

Stephan Wiefling

Usable Security und Privacy – eine Einführung

Vortrag auf der FIF-Konferenz am 14. November 2020

Transkription: Kai Nothdurft. Überarbeitung: Eberhard Zehendner.

Vielen Dank für die Einleitung und Anmoderation. Ich bin Stephan Wiefling, wissenschaftlicher Mitarbeiter bei der Gruppe für Daten- und Anwendungssicherheit von der Hochschule Bonn-Rhein-Sieg, der Gruppe von Prof. Dr. Luigi Lo Iacono. Wir arbeiten täglich an Usable-Security-und-Privacy-Themen. Das gehört bei uns zum Tagesgeschäft und deswegen freue ich mich natürlich sehr über die Einladung vom FIF, das Thema hier vorstellen zu dürfen.

Wir werden Euch und Ihnen näherbringen, was uns so fasziniert an diesem Thema und wie man das vielleicht später umsetzen kann, eine kleine Einführung in Usable Security und Privacy.

Aber ich gehe jetzt mal davon aus, dass wir vielleicht nicht auf dem gleichen Stand sind, was IT-Sicherheit angeht. Näher betrachtet schauen wir uns Datenschutz und Datensicherheit an und was wollen wir damit erreichen?

Wir wollen Schutzziele erreichen. Das ist das Ziel in der IT-Sicherheit. Wir wollen uns vor allem vor Angreiferinnen und Angreifern schützen. Das können Amateure sein, das können Profis sein, das können aber auch staatliche Akteure sein. Die wollen uns beispielsweise abhören und davor wollen wir uns dann schützen.

Die wichtigsten dieser Schutzziele sind in Abbildung 1 dargestellt: Das sind so Begriffe wie Zurechenbarkeit, Zugriffskontrolle



Abbildung 1: Wichtige Schutzziele der IT-Sicherheit.
© Stephan Wiefling/Peter Leo Gorski (Montage) 2020.

Designed by Freepik

rolle, Vertraulichkeit, Integrität, Verbindlichkeit. Das sind ganz tolle Wörter, die stehen bestimmt auch im Duden drin, aber ich denke mal, für den einen oder anderen werden diese wahrscheinlich schwer zu verstehen sein.

Deswegen gehen wir jetzt ein bisschen näher rein in die Themen, um diese Begriffe ein bisschen genauer zu erklären. Inklusive der Erklärung dieser schwierigen Wörter gehen wir auch auf Beispiele von Auswirkungen ein, die auch im realen Leben vorkommen können.

Vertraulichkeit

Wenn wir beispielsweise auf einem Cloudserver Daten über uns speichern, dann wollen wir natürlich auch sicherstellen, dass diese Daten dann nur für uns zugänglich sind. Die Praxis zeigt leider auch, dass durch Datenschutzverletzungen oder Hacks Datensätze abhandenkommen. Es zeigt leider eindeutig, wie schwierig Datenschutz und Datensicherheit in der Praxis ist.

In Abbildung 2 ist eine große Anzahl an Hacks dargestellt. Die Größe der Kreise gibt an, wie viele Datensätze von Nutzerinnen und Nutzern abhandengekommen sind. Das ist schon eine beeindruckende Grafik, weil ich denke, manche dieser Dienste, die da in der Grafik dargestellt sind, werden wir alle in gewisser Weise mal benutzt haben oder zumindest einige davon.

Das sind schon Milliarden an Datensätzen, die da abhandengekommen sind. Wir dürfen aber nicht vergessen: Mit jedem

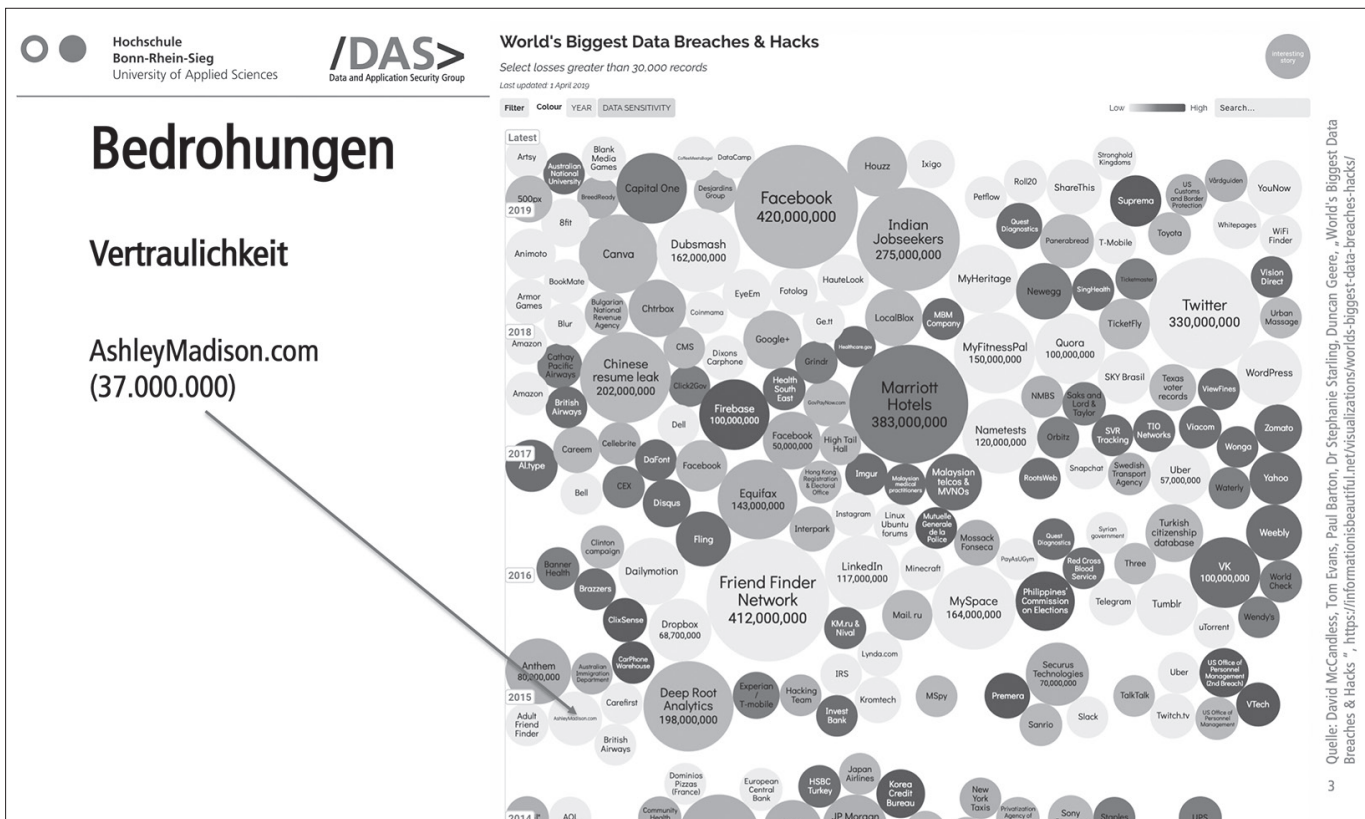


Abbildung 2: Reale Verletzungen von Vertraulichkeit.¹
© Information is Beautiful 2019/Stephan Wiefeling (Bearbeitung)/Peter Leo Gorski (Montage)

einzelnen abhandengekommenen Datensatz sind persönliche Schicksale und Konsequenzen verbunden. Wir nehmen mal als Beispiel die Webseite *Ashley Madison*.

Bei *Ashley Madison* können sich verheiratete Männer und Frauen anmelden, mit dem Ziel, eine Affäre zu suchen. Moralisch wollen wir nicht diskutieren über diese Webseite. Fakt ist aber, dass Datensätze der Kundinnen und Kunden komplett abhandengekommen sind. Wo persönliche Nachrichten dabei waren, Kreditkartendaten, Anschriften der Personen, die Namen, mit wem sie vermutlich eine Affäre aufgebaut haben, und Ähnliches. Und wenn der Datensatz einmal gestohlen wurde, dann haben wir keine Kontrolle mehr darüber. Die Folgen davon sind wirklich gravierend, denn wir hatten es in diesem Beispiel mit einem sehr gravierenden Eingriff in die Privatsphäre zu tun. Das ist dann wirklich kein Spaß mehr, denn, wenn ich jetzt diesen Datensatz habe, könnte ich mit diesem dann Leute erpressen, Identitätsdiebstahl, ...

Im Fall *Ashley Madison* gab es sogar Fälle, die mit dem Tod endeten haben, das ist wirklich harter Stoff. Das wäre jetzt zum Beispiel eine echte Bedrohung mit Folgen, die wir in Bezug auf die Vertraulichkeit hätten.

Verbindlichkeit und Zurechenbarkeit

Bei dieser Webseite sind auch Kreditkartendaten geklaut worden. Es kommt leider in der Praxis sehr häufig vor, dass Online-Dienste unerlaubterweise auch den Sicherheitscode der Kreditkarte (CVC) speichern. Den Code darf man aber nicht speichern,

weil damit eben jede Person valide Transaktionen mit meinem Geld durchführen kann. Wenn man sich also überlegt: *Angreifende* haben die Kreditkartennummer und die Sicherheitsnummer und wenn diese dann noch die Adresse dabei haben, können sie in fremdem Namen einkaufen gehen.

Womit wir beim Punkt Verbindlichkeit und Zurechenbarkeit sind, denn jetzt kann jemand in meinem Namen Produkte bestellen. Das hat dann nicht nur strafrechtliche, sondern auch finanzielle Konsequenzen für mich und ich denke, wo wir jetzt eh alle in den COVID-19-Zeiten leben, da wird vermutlich der Kreditkartenbetrug noch mehr angestiegen sein oder zumindest auf hohem Niveau bleiben. Denn durch Social Distancing ist es vermutlich schwerer, den Geldbeutel zu klauen, weil wir ja in der Regel 1,5 m Abstand halten sollen und wenn sich da einer uns nähert, wirkt das verdächtig.

Integrität und Verfügbarkeit

Eine weitere Bedrohung ist die Integrität, also: *Wie erkenne ich, dass Daten von anderen manipuliert werden?* Das kann beispielsweise eine E-Mail sein. Ich bekomme vielleicht eine E-Mail von meinem Chef oder meiner Chefin mit dem Inhalt: „Sie sind gefeuert.“ Dann will ich natürlich wissen, ob die Mail wirklich von der entsprechenden Person versendet worden ist und da kann Integrität entsprechend helfen.

Es können aber natürlich auch Daten manipuliert werden, die ich herunterlade. Wenn ich Pech habe, habe ich so etwas wie eine Ransomware heruntergeladen. So heißt eine Software, die

ich auf meinen Computer lade und wenn ich die dann ausführe, wird der komplette Festplatteninhalt verschlüsselt und ich werde dann erpresst. Für die Entschlüsselung müsste ich Lösegeld an die Hackerinnen und Hacker zahlen. Das hat natürlich Konsequenzen, wenn das Backup fehlt. Das Blöde ist, dass die Cyberkriminellen auch keinen Halt machen vor kritischen Infrastrukturen, wie das letztens auch bei der Uni-Klinik Düsseldorf passiert ist. Da war eine Ransomware aktiv und dann musste das Krankenhaus komplett von digital auf analog umstellen. In diesem Fall waren wirklich Menschenleben gefährdet: Wir haben eine Pandemie, (*es besteht*) sowieso schon *eine* hohe Belastung für Krankenhäuser und dann kommt jetzt noch die Ransomware dazu. Womit wir auch bei der Verfügbarkeit wären: Die ist dann gefährdet, weil ich vielleicht nicht mehr alle Patientinnen und Patienten bedienen kann.

Wenn wir das Thema Integrität ein bisschen weiter greifen, lässt sich das natürlich auch auf das aktuelle Thema Social Media/Fake News beziehen. Was ist denn noch wahr, was ist falsch? Wenn Akteurinnen und Akteure die Möglichkeit haben, Falschnachrichten oder Desinformation zu verbreiten, dann bedroht das natürlich auch die Integrität von Wahlen beispielsweise.

Zugriffskontrolle und Authentizität

Aus Sicht von Banken ist es wichtig zu wissen, dass sich die legitime Person bei der Online-Bank einloggen möchte. Weil sonst, natürlich, finanzieller Schaden entsteht.

Bei der Authentizität geht es um die Fragen: *Habe ich es mit dem richtigen Kommunikationspartner auf der anderen Seite zu tun? Rede ich also mit meiner Bank oder habe ich aus Versehen eine Phishing-Seite angeklickt?* Und dann ist vielleicht das Geld weg, wenn ich auf der Phishing-Seite meine Online-Bankingdaten angegeben habe. Um Kundinnen und Kunden vor solchen Angriffen zu schützen, gibt es mittlerweile die europäische PSD2-Richtlinie. Da wurde Zwei-Faktor-Authentifizierung verpflichtend für Online-Banking vorgeschrieben, d. h., ich logge mich bei meiner Online-Bank ein und werde dann zusätzlich nach einem weiteren Authentifizierungsfaktor gefragt. Das ist beispielsweise ein Zahlencode, den ich an mein Handy geschickt bekomme. Für erhöhte Sicherheit muss ich den dann noch eingeben.

Der Security-Usability-Tradeoff-Mythos

Tagesschau.de hat auch über die PSD2-Richtlinie berichtet und im zugehörigen Artikel² war ein interessanter Satz dabei. Zitat:

„Überweisungen und Online-Käufe sind künftig etwas komplizierter – aber hoffentlich auch sicherer.“

Dieser Satz spiegelt diese typische Denkweise wieder, die manche offensichtlich im Bereich IT-Sicherheit haben, nämlich: Wenn ich die Sicherheit erhöhe, habe ich automatisch weniger Usability.

Mit diesem Mythos haben renommierte Forscherinnen und Forscher im Usable-Security-Bereich aufgeräumt in ihrem Artikel zum Thema „The Security-Usability Tradeoff Myth“³ im IEEE Security & Privacy Magazine.

Darin geht es um dieses typische Klischee: *Ich habe mehr Sicherheit, bedeutet das, dass ich weniger Usability habe?* Die Autorinnen und Autoren sagen: Nein! Es funktioniert nicht, weil, wenn ich jetzt die Sicherheit komplett hoch setze, aber dann meine Userinnen und User die Sicherheitsmechanismen nicht richtig anwenden können, dann schlägt die Sicherheit fehl.

Wie bei der E-Mail-Verschlüsselung, auch so ein Thema, ...

Wer von Euch, von Ihnen, hat schon mal PGP benutzt? Ich bin richtig dran verzweifelt bei der Konfiguration, leider. Aber das ist auch so ein Beispiel. Ich kann hier sehr viel Sicherheit erreichen, muss aber genau wissen, was ich einstellen muss. PGP lässt sich aber nicht so leicht und intuitiv bedienen und wenn ich einen Button falsch klicke, schlägt die Sicherheit fehl. Das heißt: Weniger Usability bedeutet nicht automatisch mehr Sicherheit und da gibt es genügend Studien, die das auch entsprechend gezeigt haben.

Jetzt gehen wir mal in den umgekehrten Fall rein. *Wenn ich mehr Usability habe, bedeutet das, dass ich weniger Sicherheit habe?* Die Autorinnen und Autoren sagen: Natürlich nicht, weil ich ohne Sicherheitsmechanismen so gut wie keine App bedienen kann. Wenn ich Online-Banking mache, muss ich mich irgendwie noch auf meiner Webseite einloggen. Das heißt, irgendein Sicherheitsfeature muss ich dabei haben, sonst klappt das nicht.

Und es gibt ja genügend Fälle in der Praxis, bei denen wir sehen können, dass das eben nicht funktioniert. Deswegen sind die Forscherinnen und Forscher auf den Konsens gekommen, das Ziel soll am Ende sein, eine *reflektierte Ausgewogenheit* zu schaffen. Denn wenn ich Sicherheitsfunktionen gebrauchstauglich mache, dann nutzen sie meine Nutzerinnen und Nutzer wahrscheinlicher richtig, womit wir insgesamt die Sicherheit erhöhen. Und das ist das Thema, worüber wir eben sprechen: Usable Security. Natürlich gibt es auch Usable Privacy, die sich mehr auf Privatheit bezieht. Es geht aber grundsätzlich darum: Wir haben diese technologischen Faktoren, d. h. Sicherheits- oder Privatheitsfunktionen, und die menschlichen Faktoren und gucken eben, wie Menschen darauf reagieren. Die akademischen Forschungsgebiete sind da ziemlich groß, beispielsweise: Wie authentifiziere ich Personen? Phishing – wie gehe ich dagegen vor? Wie sieht das mit Social Media und der Privatsphäre aus? Email Privacy, wie schütze ich mich vor Massenüberwachung? Wie verbinde ich Geräte usw. Das ist wirklich ein breites Forschungsgebiet. Wir gehen in den näheren Beispielen mehr auf Usable Security ein aus Zeitgründen. Es gibt aber ähnliche Beispiele, die auf Privacy zutreffen.

The Elephant in the Room

Wenn wir jetzt mal aus der IT-Sicherheitsperspektive agieren, stehen wir natürlich auch vor Herausforderungen, denn wir haben ein offensichtliches Problem in der IT-Sicherheit. Das Problem ist nämlich einerseits technisch: IT-Sicherheitsmechanismen sind schwer zu erklären und nicht so leicht zu verstehen. Andererseits ist Security immer eine Nebenaufgabe.

Wir haben beispielsweise einen Cloud-Speicher, bei dem ich meine Daten hochladen möchte, und dann, während ich diese Aufgabe erledigen möchte, kommt irgendein Sicherheitsmechanismus dazwischen. Beispielsweise die Passwortabfrage. Wir haben ja eigentlich ein anderes Ziel und das ist besonders dann schwierig, wenn wir im Stress sind. Jeder von uns hat mal einen schlechten Tag oder ist gerade krank und muss jetzt irgendwie Aufgaben erledigen und dann kann es richtig schwierig werden. Gerade, wenn ich dann in diesen Momenten nicht richtig aufpasse, weil ich vielleicht einen schlechten Tag habe, klicke ich vielleicht aus Versehen auf eine Phishing-Mail und gebe Daten preis, die ich nicht preisgeben wollte, wie Firmendokumente oder Ähnliches. Fehler sind menschlich, das kann schon mal passieren.

Ebenso dürfen wir nicht vergessen: Angreifende sind nun mal Akteure, die unsere Daten haben wollen. Dazu nutzen sie menschliche Eigenschaften aus. Die wollen uns psychologisch dazu bringen, dass wir beispielsweise auf einen Phishing-Link klicken und unsere Logindaten preisgeben. Und da müssen wir versuchen, mit Usable Security die Software widerstandsfähig dagegen zu machen.

Ein paar Beispiele, die noch mit reinkommen: Wir haben beschränkte kognitive Fähigkeiten, wir können uns jetzt nicht hunderte Passwörter merken oder gewöhnen uns vielleicht auch an Dinge, Beispiel Browser-Warnungen: Wenn zu häufig eine Meldung kommt wie „Ihre Webseite ist unsicher“ und wir zum hundertsten Mal gelernt haben, „ok, das ist nicht wichtig, jetzt klicke ich einfach auf ‚Ignorieren‘“, dann klicke ich immer auf „Ignorieren“. Dann habe ich mich schon so daran gewöhnt, dass ich das automatisiert mache und ich nicht mehr drüber nachdenke. Und dann kommt vielleicht eine böse Gegenseite und mogelt uns auch so eine Meldung unter. Wir klicken dann auch instinktiv auf „Ignorieren“ und schwupp – haben die Angreifenden ihr Ziel erreicht.

Deswegen: Software entsprechend widerstandsfähig bauen. Wir dürfen auch nicht vergessen, jeder Mensch ist anders. Jeder hat ein anderes Sicherheitsempfinden, wir empfinden Risiken vielleicht anders, wir haben einen anderen Wissensstand bezüglich IT-Sicherheit und das müssen wir später alles beachten, wenn wir Usable-Security-Sachen behandeln wollen.

Sind die User an allem schuld?

Passend dazu gibt es auch typische Sachen, mit denen wir mal aufräumen wollen.

Beispielsweise in der Firmenkommunikation hat eine bekannte Firma folgenden Satz gebracht: „Users are the weakest link in security“ (Die User sind das schwächste Glied in der IT-Sicherheit). Hier wurde dann auch erwähnt, 63 % der Passwörter, die verwendet wurden, sind schwach oder wurden geklaut. Ja, aber, wenn wir uns das genauer angucken: Sind wir wirklich das schwächste Glied in der IT-Security? Sind wir die Feinde, die das Problem sind?

Vom Britischen BSI-Pendant, dem NCSC (*National Cyber Security Center*), hat Ciaran Martin dieses Thema später in einem Vortrag aufgegriffen:

„Lassen Sie uns ernsthaft versuchen, den Menschen in all dem zu verstehen. Lassen Sie uns aufhören, Unsinn darüber zu reden, dass der Mensch das schwächste Glied in der Cybersicherheit sei. Es ist ein bisschen so, als würde man sagen, das schwächste Glied in einer Sportmannschaft seien alle Spieler.“⁴

Und das trifft es eigentlich gut auf den Punkt. Denn nur wenn wir alle zusammenarbeiten, dann können wir die Sicherheit verbessern, und ich denke, ein Fußballteam mit lauter Egoisten spielt nicht so gut. Dieses Thema hatten schon vor 20 Jahren die Forscherinnen Anne Adams und Angela Sasse in ihrer Publikation „Users are not the enemy“⁵ beschrieben. Dieses Feindbild des „dümmsten anzunehmenden Users“ ist totaler Quatsch und mit diesem Klischee muss aufgeräumt werden. Seitdem gibt es diese Denkweise der Usable Security und Privacy. Dank der Forscherinnen, die das damals in ihrem – etwas zugespitzt formuliert – Brandbrief dargestellt haben. Auch vom NCSC hat Emma W., eine Mitarbeiterin, auch noch mal einen Vortrag⁶ zu diesem Thema gebracht, in dem sie formulierte: „Security must work for people. If security doesn't work for people, it doesn't work.“ (Wenn die Security nicht für Menschen funktioniert, wird sie insgesamt keinen Effekt haben.) Der Titel dieses Vortrags hieß: „People: The Strongest Link“, also Menschen, das stärkste Verbindungsstück. Wir würden das allerdings nochmal ein bisschen genauer formulieren: Empower people to become a strong link, also Menschen befähigen, ein starkes Verbindungsstück zu werden. Und das ist genau, was wir im Bereich der Usable Security und Privacy eben machen. Wir nehmen uns Sicherheitsmechanismen, evaluieren die nach gängigen Usability-Metriken und stellen dann fest, dass sie vielleicht gar keinen Sinn machen, wie die Schranke in Abbildung 3, die alle Personen umfahren.



Abbildung 3: Usability Evaluation von Sicherheitsmechanismen

Wenn man jetzt diese Schranke sieht, bevor sie dann fertig geworden ist und alle drumherum fahren, dann müssen wir uns überlegen: Ok, können wir das vielleicht anders designen? Deswegen: Im Entwicklungsprozess diese Mechanismen testen und schauen, wie Menschen darauf reagieren. Sozusagen *Security and Usability by Design*. Und dann werden die Sicherheitsmaßnahmen effektiver.

Wenn wir uns jetzt nochmal diesen Satz von vorhin anschauen, können wir „Users are the weakest Link in Security“ ganz klar streichen. Weil das Problem, das wir hier haben, nicht die Nutzerinnen und Nutzer sind, sondern die Passwörter, die gewählt worden sind. Die sind schwach, aber vielleicht gab es überhaupt keine Warnmeldung, um zu sagen: Hey, da gibt es ein Datenleck, und jetzt bitte das Passwort ändern. Das ist vielleicht einer der Gründe und deshalb müssen wir hier den Nutzerinnen

und Nutzern helfen, damit sie die Sicherheitsmechanismen richtig anwenden können.

Forschungsbereich Passwörter

Und wo wir schon beim Thema Passwörter sind, gehen wir ein bisschen mehr in den Bereich Personenauthentifizierung rein. Das ist auch der Bereich, in dem ich forsche. Es geht um textbasierte Passwörter.

Klar, Passwörter werden von uns allen benutzt, manche lieben sie, manche hassen sie, aber womit wir uns auf jeden Fall sicher sein können: wir werden sie auf längere Zeit nicht mehr weg bekommen aus dem Netz aus folgenden Gründen: Einerseits aus der Nutzerinnen- und Nutzer-Perspektive: wenn ich so ein Formular sehe, dann weiß ich genau, was zu tun ist. Das können Sie wahrscheinlich Ihrer Oma zeigen oder Ihren Großeltern, ihren Eltern, wem auch immer, die wissen ganz genau, was zu tun ist, wenn sie dieses Formular mit Nutzernamen und Passwort sehen.


Und aus der Entwicklerinnen- und Entwickler-Perspektive ist das auch relativ einfach zu lösen. Wir müssen da nur zwei Zeichenkombinationen prüfen und dann bin ich drin. Und natürlich ein weiterer Vorteil von Passwörtern: unser Gehirn ist nicht hackbar, momentan zumindest noch nicht, und deswegen sind Passwörter erst einmal noch nicht weg zu bekommen. Wir haben aber trotzdem natürlich dieses Sicherheitsproblem: Wenn ich zu lange

Passwörter wähle, kann ich sie mir schwer merken, und wenn ich sie zu kurz wähle, kann ich sie mir leichter merken, sie sind aber auch leichter hackbar. Und in der letzten Zeit sind auch weitere Sicherheitsrisiken dazu gekommen. Das sind Passwörter, die geklaut worden sind, beispielsweise von größeren Internetseiten. Das haben wir am Anfang der Präsentation schon gesehen.

Beispielsweise sind von LinkedIn riesige Datensätze mit E-Mail-Adressen und Passwörtern abhandengekommen. Wenn wir jetzt hacken würden, würden wir einfach diese Datensätze kaufen von irgendwelchen Darknet-Marktplätzen oder wo auch immer her. Dann gehen wir automatisiert diese Nutzernamen-Passwort-Kombinationen durch, können das ja auf einer anderen Webseite mal probieren und dann kommen wir vielleicht in einige Accounts rein. Wir sind halt Menschen und nutzen Passwörter auch gerne mal wieder. Gegen diese Angriffsmethoden müssen wir natürlich vorgehen. Wir müssen schauen: Wie kann ich die Sicherheit von Passwörtern erhöhen, um meine Nutzerinnen und Nutzer zu schützen auf meiner Webseite, dass eben nicht so ein Angriff passieren kann?

Passwortrichtlinien und ihre Probleme

Da gibt es beispielsweise Passwortrichtlinien, so Sachen wie „benutzen Sie ein Passwort mit Groß- und Kleinschreibung, bauen Sie Sonderzeichen ein und machen Sie noch Zahlen rein, viel-




Password Policy

Advice for system owners

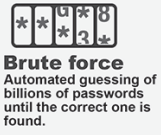
The NCSC is working to reduce organisations' reliance on users having to recall large numbers of complex passwords. The advice below advocates a greater reliance on technical defences and organisational processes, with passwords forming just one part of your wider access control and identity management approach.

How passwords are discovered...


Interception
Passwords can be intercepted as they travel over a network.




Brute force
Automated guessing of billions of passwords until the correct one is found.




Key logging
Installing a keylogger to intercept passwords when they are entered.




Manual guessing
Details such as dates of birth or pet names can be used to guess passwords.




Shoulder surfing
Observing someone typing in their password.




Stealing passwords
Insecurely stored passwords can be stolen, such as ones written on sticky notes and kept near (or on) devices.



Phishing & coercion
Using social engineering techniques to trick people into revealing passwords.



Data breaches
Using the passwords leaked from data breaches to attack other systems.



...and how to improve system security.

Reduce your reliance on passwords

1. Only use passwords where they are needed and appropriate.
2. Consider alternatives to passwords such as SSO, hardware tokens and biometric solutions.
3. Use MFA for all important accounts and internet-facing systems.

Implement technical solutions

1. Throttling or account lockout can defend against brute force attacks.
2. For lockout, allow between 5-10 login attempts before locking out.
3. Consider using security monitoring to defend against brute force attacks.
4. Password blacklisting prevents common passwords being used.

Passwords can only do so much.
 Even when implemented correctly, passwords are limited in helping prevent unauthorised access. If an attacker discovers or guesses the password, they are able to impersonate a user.

Protect all passwords

1. Ensure corporate web apps requiring authentication use HTTPS.
2. Protect any access management systems you manage.
3. Choose services and products that protect passwords using standards such as SHA-256.
4. Protect access to user databases.
5. Prioritise administrators, cloud accounts and remote users.

Help users generate better passwords

1. Be aware of different password generation methods.
2. Use built-in password generators when using password managers.
3. Don't use complexity requirements.
4. Avoid the creation of passwords that are too short.
5. Don't impose artificial capping on password length.

Key messages for staff training

1. Emphasise the risks of re-using passwords across work and home accounts.
2. Help users to choose passwords that are difficult to guess.
3. Help users to prioritise their high value accounts.
4. Consider making your training applicable to users' personal lives.

© Crown Copyright 2018 www.ncsc.gov.uk @ncsc National Cyber Security Centre

Abbildung 4: Password Security Info Sheet des NCSC.⁹ © Crown Copyright NCSC 2018. Lizensiert unter Open Government Licence v3.0 OGL



Sichere Passwörter

BSI-Basistipp

Passwörter für den E-Mail-Account, Soziale Netzwerke oder den Computer sind wie Schlüssel für das eigene Zuhause: Nur ein sicheres Passwort schützt vor ungewollten Gästen und deren Zugriff auf persönliche Daten, Fotos oder Kontoinformationen.

Dabei gilt für den virtuellen Schlüssel, genauso wie für den Haustürschlüssel – je ausgefeilter, umso schwieriger ist es, das Schloss zu knacken.



Weitere Informationen:

<https://www.bsi-fuer-buerger.de/Passwoerter>

Umgang mit Passwörtern

- Passwörter unter Verschluss halten; Passwort-Manager sind eine gute Hilfe
- Passwörter spätestens bei Verdacht auf Missbrauch ändern
- Keine einheitlichen Passwörter für Accounts verwenden
- Voreingestellte Passwörter ändern
- Passwörter nicht an Dritte weitergeben und nicht per E-Mail versenden

Abbildung 5: Ausschnitt aus dem Faktenblatt „Sichere Passwörter“ des BSI⁸ © BSI

leicht noch ein Einhorn-Emoji rein und dann am besten noch das Passwort alle drei Monate ändern“. Das ist so etwas, was man auf Webseiten sehr häufig liest.

Die Praxis zeigt aber: das funktioniert nicht. Wenn man Passwortrichtlinien nämlich mal evaluiert hat in der Wissenschaft, sieht man: Wenn ich Angreifender bin, dann weiß ich ganz genau, wonach ich suchen muss, weil ich ja schon weiß, welche Zeichen im Passwort drin sein müssen. Das heißt: ich spare mir viel Ratezeit. Dazu kann ich mir solche Passwörter nur schwer merken und vor allem lösen sie das Hauptproblem ja gar nicht. Sie verhindern weder Keylogging noch Phishing und wir wissen ja, es ist der effektivste Weg, Menschen mit Ihren Schwächen anzugreifen.

Das heißt: Es ist eine Luftnummer, weshalb man die Passwörter nicht mehr alle drei Monate ändern sollte. Mittlerweile sagt das auch das BSI, nachdem es die amerikanischen und britischen Behördenpendants schon lange empfohlen haben.

In der Praxis, für diesen Fall, was machen wir dann, wenn wir uns Passwörter schwer merken können? Genau, wir schreiben sie auf Post-Its oder malen sie auf die Pinnwand drauf! Und wenn ich dann Pech habe und ein Fernseherteam bei mir reinkommt und dann diese Wand abfilmt, dann haben wir das Problem, dass wir eventuell gehackt werden, wenn Online-Dienste keine weiteren Sicherheitsmaßnahmen einbauen. Nicht zu vergessen: Vergessene Passwörter können auch finanzielle Folgen haben, wie man das bei einem bekannten Autohersteller sehen konnte. Die hatten nämlich einen externen Dienstleister bestellt,

der für die Passwortzurücksetzung zuständig war und dann für jede Rücksetzung Geld verlangte. Blöderweise haben die Mitarbeiterinnen und Mitarbeiter, weil sie alle drei Monate ihr Passwort ändern mussten, sehr oft ihr Passwort vergessen und letzten Endes war das dann teuer. Eine Million Euro Extra-Ausgaben nur durch die Passwortzurücksetzungen.

Wenn Sie und Ihr da noch Interesse dran habt, da noch ein bisschen näher rein zu schauen: Es gibt zu Passwörtern vom NCSC aus Großbritannien noch ein Infosheet, auf welchem man die Empfehlungen für Passwörter nachschauen kann (Abbildung 4). Da steht auch nochmal „blacklist the most common password choices“. D. h., hier ist auch nochmal die Empfehlung, nicht die häufigsten, beliebtesten Passwörter zu wählen für einen Online-dienst.⁷ Beim BSI gibt es auch noch eine ähnliche Broschüre⁸, da dann einfach mal reinschauen (Abbildung 5).

Zwei-Faktor-Authentifizierung als Allheilmittel?

Also, das haben wir abgehakt: Password Policies – keine so gute Idee, um die Sicherheit zu erhöhen. Aber was ist denn jetzt mit Zwei-Faktor-Authentifizierung, werden vielleicht manche jetzt im Podium denken? Klar, es wird natürlich von vielen Online-Diensten angewendet. Ich logge mich mit Nutzernamen und Passwort ein. Dann werde ich nach einem zusätzlichen Authentifizierungsfaktor gefragt, also dieser SMS-Code beispielsweise. Oder ich klicke auf einer App irgendwo drauf. Wenn dieser Beweis erbracht wurde, dann bin ich drin auf der Webseite.

Spätestens seit dem „Bundes-Hack“ – manche erinnern sich vielleicht noch letztes Jahr daran, als von Politikern und Prominenten Konversationen gehackt und öffentlich zugänglich ins Internet gestellt worden sind – da war dann das Echo in der Politik groß, nach dem Motto: „wir brauchen eine Zwei-Faktor-Authentifizierungspflicht!“ Ich weiß gar nicht, ob viele Politiker mittlerweile überhaupt noch wissen, was Zwei-Faktor-Authentifizierung ist. Das Thema ist irgendwie in Vergessenheit geraten. Vielleicht liegt das auch daran, dass das offensichtliche Problem nicht angesprochen wurde: Die Akzeptanz von Zwei-Faktor-Authentifizierung ist recht gering, sofern auf der Website keine sehr sensiblen Daten im Spiel sind, wie z. B. bei Online-Banking. Selbst Google musste zugeben, dass weniger als 10 % der Nutzerinnen und Nutzer bei Google überhaupt Zwei-Faktor-Authentifizierung aktiviert haben. Um die restlichen 90 % der Personen zu schützen, die keine Zwei-Faktor-Authentifizierung aktiviert haben, sollten entsprechende Maßnahmen ergriffen werden.

Risikobasierte Authentifizierung (RBA)

Eine davon wäre risikobasierte Authentifizierung. Die erhöht nämlich die Sicherheit im Vergleich zu Nur-Passwort-Authentifizierung und erhöht gleichzeitig die Usability.

Es funktioniert wie folgt: Ich habe meinen Anmeldenamen und mein Passwort und wenn ich das Login-Formular absende, übermittle ich automatisch zusätzlich Metadaten, die sowieso schon in dem Kontext vorhanden sind, beispielsweise: Welche IP-Adresse habe ich, welches Gerät nutze ich zum Einloggen, welchen Browser? Und basierend darauf wird im Hintergrund ein Risiko berechnet. Basierend auf meinen vorherigen Login-Versuchen, wie wahrscheinlich ich das jetzt bin oder wie hoch das Risiko ist, dass das jetzt ein Hacking-Angriff ist. Das Risiko wird normalerweise in niedrig, mittel und hoch unterteilt.

Wenn wir jetzt mal den Fall für niedriges Risiko anschauen. Ich bin jetzt beim FIFF und logge mich aus Bremen ein, mit einem Gerät, das ich sonst immer benutze. Und wenn das Verhalten

so wie immer ist, komme ich einfach in meine Webseite rein und werde nicht nach zusätzlichen Authentifizierungsfaktoren gefragt.

Und jetzt gehen wir mal an einen Ort, wo ich mich persönlich relativ selten aufhalten würde. Und da ist sich das System nicht mehr ganz so sicher, weil ich mich vorher noch nie aus dem Land eingeloggt habe und ein Gerät benutze, was ich sonst nie benutzt habe, dann ist sich die Website nicht so sicher: Ist das wirklich die richtige Person, die sich hier einloggen möchte? Und dann fragt mich die Website nach einer zusätzlichen Authentifizierung. Das kann beispielsweise eine E-Mail-Adresse sein, die ich dann noch einmal bestätigen muss. Das heißt, ich muss mich nochmal in den E-Mail-Account einloggen und wenn ich diesen Beweis erbracht habe, komme ich auf die Webseite drauf.

Und hier sieht man den Unterschied zur Zwei-Faktor-Authentifizierung im klassischen Sinne: Wir werden nicht immer nach zusätzlicher Authentifizierung gefragt. Diese Technologie wird empfohlen vom NIST, also dem amerikanischen Pendant zum BSI, in den NIST Digital Identity Guidelines¹⁰ – wenn es noch nicht gelesen wurde, einfach mal reinschauen. Da sind sehr viele Usable Security und Privacy Metriken drin, das ist ganz interessant zu lesen.

Große Onlinedienste setzen RBA ein, Facebook, Google, LinkedIn und weitere. Wir wissen auch durch unsere Forschung, dass RBA von Anwendern als gebrauchstauglicher angesehen wird als vergleichbare Zwei-Faktor-Authentifizierungsmethoden und auch die Sicherheit wird vergleichbar wahrgenommen. Darüber hinaus wissen wir, dass RBA in der Praxis sehr selten nach der zusätzlichen Authentifizierung fragt. Selbst dann, wenn mehr als 99,45 % intelligenter Angriffe blockiert werden. Also Angriffe mit Kenntnis zu den Anmeldedaten des Opfers sowie dessen typischem Standort (Stadt, Land), Browser und Gerät. Abbildung 6 zeigt Beispiele von Dialogen, wenn RBA aktiv wird.

Zum Thema RBA haben wir eine Info-Webseite aufgesetzt: risk-basedauthentication.org. Da sind viele Studien dabei, unter an-

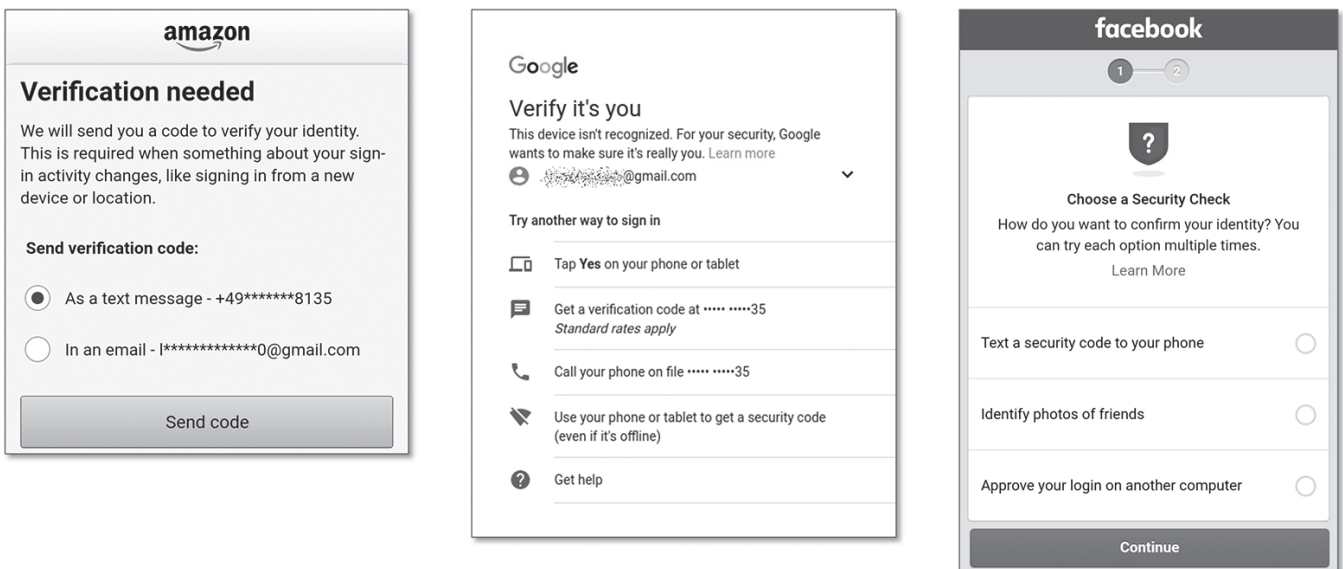
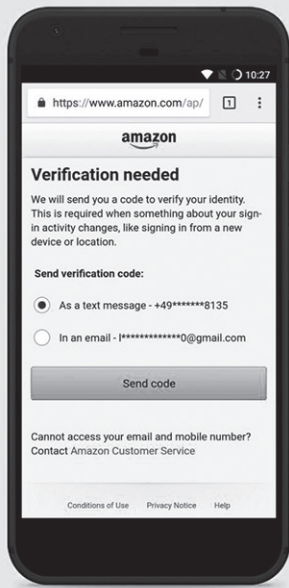


Abbildung 6: Dialoge während risikobasierter Authentifizierung. © Stephan Wiefeling 2019



More Than Just Good Passwords?

A Study on Usability and Security Perceptions of Risk-based Authentication (RBA)

Stephan Wiefeling, Markus Dürmuth, and Luigi Lo Iacono
H-BRS University of Applied Sciences & Ruhr University Bochum

Summary: Popular online services use RBA to protect their users without enforcing Two-factor authentication (2FA). User study shows that RBA is perceived as more usable than 2FA and comparably secure. However, it strongly depends on the use case.

- [Paper](#)
- [Journal Article](#)
- [Overview](#)
- [Talk](#)

Abbildung 7: A Study on Usability and Security Perceptions of Risk-based Authentication (RBA).¹¹ © Stephan Wiefeling 2020

derem auch eine ganz neue Studie (Abbildung 7), in der wir die Usability von RBA genauer untersucht haben.

Der IT-Security-Guru Bruce Schneier hat auch darüber berichtet, das ist ganz lustig gewesen. Er fand es auf jeden Fall „interesting“. Also wenn das kein Grund ist, rein zu schauen, dann weiß ich auch nicht!

Usable Security & Privacy in die Praxis bringen

Aber wir kommen jetzt nochmal generell zu Usable Security und Privacy hin. Irgendjemand muss es ja in die Praxis umsetzen und das sind meistens Entwicklerinnen und Entwickler. Wie können wir diesen Personen helfen, um Usable Security und Privacy in Software einzubauen? Dafür haben wir ein Tool gebaut, die USecureD-Plattform (Abbildung 8).

Da haben wir beispielsweise für alle möglichen Kategorien aufgelistet, was es so gibt an Sachen, die man als Programmiererin und Programmierer gestalten kann. Wenn wir uns beispielsweise Warnmeldungen anschauen wollen, ist da genau aufgelistet, wie der aktuelle Forschungsstand ist und was die Empfehlungen sind: Wie soll ich eine Warnmeldung gestalten, damit das dann auch effektiv zu einem zufriedenstellenden Ergebnis führt, dass Sicherheitsmethoden richtig angewendet werden?

Da gibt es auch eine Übersicht, wo wir uns durchklicken können. Wenn wir z. B. die Warnmeldungen haben, können wir draufgehen und dann werden auch noch andere Kategorien angezeigt, die verwandt sind. Das ist ein ganz gutes Nachschlagtool, um einfach eine Übersicht zu haben: Was ist denn aktuell populär und was ist der aktuelle Stand der Forschung? Einfach mal vorbei schauen lohnt sich an der Stelle.



Abbildung 8: Oberfläche der USecureD-Plattform.¹² © DAS-Group TH Köln 2017

Zusammenfassung

Was sollten wir jetzt von dem Vortrag mitgenommen haben?

Zunächst mal Security ohne Usability geht auf jeden Fall nicht. Ausgewogenheit ist gefragt, der Usability-Security Tradeoff Myth – mehr Sicherheit = weniger Usability – ist Quatsch.

Und ebenso: Empower people to become a strong link in Security, d. h., nur zusammen können wir wirklich stark werden.

Und dann möchten wir noch ein paar Literaturtipps am Ende mitgeben:

- „Usable Security: History, Themes and Challenges“, Simson Garfinkel und Heather Lipford, 2014
- „Security and Usability: Design Secure Systems that People can use“, Lorrie Faith Cranor und Simson Garfinkel, 2005
- Literaturempfehlungen des Arbeitskreises Usable Security & Privacy der German UPA <https://germanupa.de/arbeitskreise/arbeitskreis-usable-security-privacy/unsere-literaturempfehlungen>

Und es gibt noch Konferenzen, auf denen aktuelle Forschungsergebnisse vorgestellt werden.

Da gibt es das Symposium of Usable Privacy and Security (SOUPS)¹³. Da ist auch viel Open Access dabei, d. h., es kostet auch nichts, es ist keine Paywall dazwischen. Das kann ich empfehlen, alle anderen, die auf der Liste sind, auch. Das Privacy Enhanced Technologies Symposium (PoPETs)¹⁴ ist mehr auf Usable Privacy angewandt und mehr auf dem Usability Fokus ist dann die Conference on Human Factors in Computing Systems (CHI)¹⁵.

Es gibt auch noch wissenschaftliche Workshops zum Thema:

Der deutsche Usable Security & Privacy Workshop¹⁶ findet immer auf der „Mensch und Computer“ statt. In Europa gibt es den European Workshop on Usable Security (EuroUSEC)¹⁷, international die USEC¹⁸. Da treffen sich Forscherinnen und Forscher aus dem Fachbereich und tauschen sich aus. Das ist ganz hilfreich, um Kontakte in die Usable-Security-Szene zu bekommen.

Damit sind wir dann auch am Ende vom Vortrag angekommen.

Ich hoffe, dass ich Sie und Euch für das Thema Usable Security und Privacy begeistern konnte. Weitere Infos haben wir auch auf unserer Webseite das.h-brs.de von unserer Gruppe für Daten- und Anwendungssicherheit der Hochschule Bonn-Rhein-Sieg, wo wir die neuesten Ergebnisse zeigen, oder natürlich [risk-basedauthentication.org](http://riskbasedauthentication.org), unsere RBA-Infoseite.

Wenn es jetzt noch Fragen gibt, freue ich mich auf die, die gleich in den entsprechenden Chat kommen, aber ansonsten bin ich auch per E-Mail¹⁹ erreichbar oder Twitter²⁰. Wenn Sie Fragen haben zu dem Thema, sagen Sie einfach Bescheid und ich freue mich da auf eine Rückmeldung und ansonsten vielen Dank fürs Zuhören.

Anmerkungen und Referenzen

- 1 McCandless D, Evans T, Barton P, Starling S, Geere D (2019) *World's Biggest Data Breaches & Hacks. Information is Beautiful*, 1. April 2019. <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- 2 <https://web.archive.org/web/20190913083203/> <https://www.tagesschau.de/wirtschaft/online-banking-zwei-faktor-methode-101.html>
- 3 Sasse MA, Smith M, Herley C, Lipford H, Vaniea K (2016) *Debunking security-usability tradeoff myths. IEEE Security & Privacy* 14(5):33–39. doi:10.1109/MSP.2016.110
- 4 NCSC (2017) *Ciaran Martin's speech to CBI. 13. September 2017.* <https://www.ncsc.gov.uk/speech/ciaran-martins-speech-cbi>
- 5 Adams A, Sasse MA (1999) *Users are not the enemy. CACM* 42(12):40–46. doi:10.1145/322796.322806
- 6 https://www.youtube.com/watch?v=u6x9C7t_41s
- 7 <https://ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach>
- 8 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=1
- 9 https://www.ncsc.gov.uk/files/password_policy_infographic.pdf
- 10 *Tech. Rep. NIST-SP 800-63b 2017*
- 11 <https://riskbasedauthentication.org/usability/perceptions/>
- 12 <https://das.h-brs.de/usecured>
- 13 <https://www.usenix.org/conference/soups2020>
- 14 <https://www.petsymposium.org>
- 15 <https://chi2020.acm.org>
- 16 <https://das.h-brs.de/workshops/>
- 17 <https://eusec20.cs.uchicago.edu/>
- 18 *Workshop on Usable Security and Privacy.* <http://www.usablesecurity.net/USEC/usec21/>
- 19 Stephan.wiefling@h-brs.de
- 20 [@swiefling](https://twitter.com/swiefling)



Stephan Wiefling

Stephan Wiefling ist wissenschaftlicher Mitarbeiter in der Data and Application Security Group der Hochschule Bonn-Rhein-Sieg. Seine Forschungsschwerpunkte liegen in den Bereichen der Authentifizierung und Usability. E-Mail: Stephan.wiefling@h-brs.de. Twitter: [@SWiefling](https://twitter.com/SWiefling)