Sicherheit, Privatsphäre und Datenschutz

Grundlagen | Ein Modul des CUMILA-Projekt | www.cumila.eu

Impressum

Dieses Dokument ist Teil des Projektes “CUMILA - Curriculum guide of media and information literacy for adults”.
Name des Modules: "Sicherheit, Privatsphäre und Datenschutz"
KA204-45D50F70
Mehr Informationen unter https://www.cumila.eu

Herausgeber / Kooperationspartner:
Medienkompetenz Team e.V.
Sophienstr. 120
76135 Karlsruhe – DE

Akademie für Politische Bildung und demokratiefördernde Maßnahmen
Hauptplatz 23
4020 Linz – AT

CIDET - Centre for the innovation and development of education and technology, S.L
Carrer Pintor Ribera 18
Entresuelo, local 3
12004 Castellón - ES

Über dieses Modul:
Verantwortliche Organisation **CIDET**
Grafik & Layout Ann-Kathrin Giuriato

Autoren:
Roger Esteller Curto, Daniel Nübling, Helmut Moritz

Co-funded by the
Erasmus+ Programme
of the European Union

Inhaltsverzeichnis

1. Digitale Identität

Unsere Identität ist unverwechselbar. Im realen Leben können wir unsere Identität anhand des Fingerabdrucks oder über den Personalausweis nachweisen. Heutzutage besitzt aber jeder auch eine digitale Identität, über welche es uns möglich ist, uns im Internet zu erkennen zu geben. Das kann beispielsweise über eine digitale Unterschrift, ein E-Mail-Konto oder ein Social-Media-Konto erfolgen. Und selbst wer sich stets bemüht, keine Spuren im Internet zu hinterlassen, wird nicht verhindern können, dass persönliche Informationen seiner Person über Umwege im Netz landen. Zum Beispiel wenn andere Personen die eigenen persönlichen Informationen wie Namen, Videos, Fotos oder andere persönliche Daten im Internet veröffentlichen. Somit kann jemand sogar über eine digitale Identität verfügen, ohne dass er sich darüber bewusst ist.

In diesem Kapitel wollen wir den Fragen nachgehen, inwieweit wir Personen in der digitalen Welt identifizieren können? Wie entstehen digitale Identitäten aufgrund von persönlichen Informationen die wir im Internet hinterlassen (ob bewusst oder unbewusst)? welche Risiken sind damit verbunden und welchen Wert besitzen sie? Dies soll dabei helfen, mit persönlichen Daten vorsichtiger umzugehen und diese vor ungewollten Zugriffen zu schützen.

Digitale Identität		
Er/Sie versteht die Bedeutung einer digitalen Identität. Insbesondere im Umgang mit Daten und beim Erstellen oder Teilen von Inhalten im Internet. Er/Sie kennt die Risiken im Umgang mit anderen digitalen Identitäten.		
Wissen	**Fertigkeiten**	**Kompetenz**
Er/Sie kann • die Risiken im Umgang mit digitalen Identitäten benennen • die Notwendigkeit, seine eigene digitale Identität zu schützen, erkennen • die vorhandenen Methoden zur Verifizierung einer Identität benennen	Er/Sie ist in der Lage • die eigene digitale Identität zu verwalten und für die eigenen Zwecke zu nutzen. • einzelne Methoden zur Identitätsbestimmung zu benennen und einzusetzen	Er/Sie ist in der Lage • eine digitale Identität zu erstellen und zu pflegen. • die digitalen Identitäten anderer Personen zu identifizieren und zu verifizieren

1.1 Unser zweites “Ich”

Sherry Turkle, Psychologin und Soziologin und Professorin am MIT, versucht in ihrem Buch "Second Self: Computers and the Human Spirit" den Einfluss, den das Internet auf den Menschen und die Gesellschaft hat, zu verstehen. Technische Geräte wie Computer und Mobiltelefone sind nicht einfach nur Werkzeuge, die uns mit anderen Menschen verbinden. Durch die Daten die wir von uns preisgeben und die Art wie wir diese nach außen hin darstellen, erschaffen wir auch eine Projektion unseres Selbst in der digitalen Welt und formen auf diese Weise unser Identitätsgefühl von einem zweiten Ich.

Die Studien von Turkle und anderen Forschern zeigen uns die Komplexität der Beziehung zwischen Mensch und Maschine. Es beginnt schon damit, dass wir im Internet die Rolle des einfachen, passiven Lesers verlassen und zu einem aktiven Teilnehmer werden, der sein Auftreten und seine Wirkung selbst gestaltet.

Das Erschaffen einer eigenen Identität beginnt bereits, wenn wir ein Konto erstellen und mit anderen interagieren (z.B. per E-Mail). Sie wird weiter gefestigt, sobald wir damit beginnen, eigene Informationen zu veröffentlichen (z.B. über den eigenen Weblog) und uns aktiv in Gemeinschaften einzubringen (z.B. In Foren oder sozialen Netzwerken). Das schöne Bild von unserem letzten Urlaub oder unserem Haustier, der zitierte Satz unseres Lieblingsautoren - jede dieser Informationen fließt in unsere digitale Identität ein.

Auch durch die Beteiligung andere Menschen wird unsere eigene Identität geformt. Das Bild von uns im öffentlichen Fotoalbum unseres Bekannten auf dem wir markiert sind, Kommentare von Freunden auf unseren Social Media-Profilen, die Veröffentlichung unserer Leistungen auf der Webseite des Sportvereins: Wir mögen Kontrolle darüber haben, welche Informationen wir über uns selbst veröffentlichen, aber wir haben nur eine eingeschränkte Kontrolle darüber welche Informationen andere Menschen über uns preisgeben.

Durch diese Unkontrollierbarkeit ist ein gesundes Maß an Vorsicht geboten, aber gleichzeitig eröffnen sich eine Menge an Möglichkeiten.

Im Internet ist es heute einfacher als je zuvor, neue Identitäten zu erschaffen.

Über unser "digitales Ich" bauen wir eine neue (digitale) Identität auf, die sich von unserer ersten (der realen) durchaus unterscheiden kann. Menschen können sich online sogar mehr als eine Identität erstellen, und diese müssen nicht zwangsläufig mit der realen Identität in Verbindung stehen. Das ist nicht unbedingt falsch oder verboten, sondern bietet uns vielmehr Freiheiten, das zu tun, was wir möchten und unsere persönliche Entwicklung davon profitieren zu lassen.

Ob Spieler-Account in einem Onlinespiel, das Profil auf einem Datingportal, der anonyme Account in einem Online-Forum - all das sind Identitäten, die mir Möglichkeiten im Internet eröffnen, und zu denen ich auch nicht direkt persönliche Informationen preisgeben muss.

Das Internet ermöglicht es uns, neue Identitäten zu schaffen, die vielleicht mehr unserer Denkweise entsprechen, mutiger sind, besser aussehen, als unser wahres Selbst.

AVATAR
Der erste Schritt zu unserer individuellen Repräsentation im Internet ist bereits der Avatar den wir als Profilbild nutzen. Als Avatar wird das Symbol oder das Bild bezeichnet, welches wir in der digitalen Welt nutzen; also z.B. das klassische Profilbild bei einem Online Service . Dieses Bild vermitteln anderen Personen einen ersten Eindruck von uns und sagt bereits einiges über uns aus.

1.2 Identitäten aufbauen

Durch unsere Aktionen im Internet nähren wir unsere Online-Identitäten. Gerade in sozialen Netzwerken ist dies gut zu beobachten. Die Fotos welche wir online stellen, die Beiträge die wir verfassen, teilen oder kommentieren, Gruppen denen wir beitreten: all dies sind Informationen die unsere Identität schärfen.
Soziale Netzwerke bauen zudem darauf auf, dass wir uns mit anderen Personen vernetzen. Wenn wir einen Beitrag öffentlich kommentieren, können andere Profile dies sehen und darauf antworten. Somit treten wir in Kontakt mit anderen Identitäten. Wir haben die Möglichkeit die Aktivitäten anderer Profile zu verfolgen und zu kommentieren. Hierdurch bauen sich Netzwerke mit Personen gleichen Interesses auf.
Erfolgt ein reger Austausch über die sozialen Netzwerke mit einzelnen Online-Profilen, sind wir anhand der uns vorliegenden Information geneigt, eine eigene Vorstellung der dahinter stehende Person zu erschaffen. Je intensiver der Austausch, desto mehr erleben wir die Identität der Person, mit der wir kommunizieren, als real und befreundet. Auf dem sozialen Netzwerk Facebook werden alle Identitäten, mit denen wir uns verbunden haben, “Freunde” genannt. Die Verknüpfung zu einem anderen Account entsteht über eine “Freundschaftsanfrage”, die akzeptiert werden muss. Das Netzwerk Instagram verwendet ein anderes Konzept. Hier ist als Grundeinstellung alles öffentlich und wir können anderen Profilen folgen. Statt Freunden sprechen wir hier von “Followern” (also den “Folgenden”) - was weitaus zutreffender ist. Denn wahrscheinlich werden wir die Personen hinter unseren neuen Online-Bekanntschaften nie von Angesicht zu Angesicht treffen. Die Verbindung zwischen unseren Identitäten basiert nur auf einem gemeinsamen Interesse.

Mit jemandem im realen Leben befreundet zu sein, unterscheidet sich stark von einer Freundschaft im Internet. Im Internet finden wir Freunde vorwiegend nach konkreten Interessen. Wir müssen die Namen unserer befreundeten Profilen nicht einmal kennen. Der Austausch erfolgt meist ausschließlich online über das entsprechende Netzwerk. Das Internet erlaubt uns in Kontakt zu sein, zu teilen, zu entdecken, zu lernen, etwas zu erschaffen und zu genießen. Und das ohne einen persönlichen Kontakt. Wir entscheiden was wir wann teilen. Die Verbindung ist ausschließlich das gemeinsame Interesse

Aber auch die Verknüpfung mit anderen Profilen ist Teil unserer eigenen Identität. Mit wem wir kommunizieren, welchen Profilen wir folgen und in welchen Kreisen wir uns bewegen, sagt wiederum einiges über uns selbst aus. Aufgrund der vielen Informationen über uns ist es möglich, ein konkretes Profil über unsere Identität zu erstellen. Diese Informationen werden von den Anbietern der entsprechenden Plattformen genutzt. Die Haupteinnahmequelle der großen sozialen Netzwerke wie Facebook ist der Verkauf von Werbung. Gerade weil unsere Identitäten mit so vielen Informationen angereichert sind, kann unsere Identität einer konkreten Zielgruppe zugewiesen werden. Wir sind viel in der Natur unterwegs und kommentieren viel auf den Profilseiten des Wandervereins? Wir veröffentlichen viele Bilder mit uns und unserer Familie? Somit könnten wir demnächst Werbung für Kinderrucksäcke oder Familienurlaube auf dem Bauernhof angezeigt bekommen.

Identitäten werden aber nicht nur auf sozialen Netzwerken gebildet. Überall dort, wo wir einen Account besitzen, können wir davon ausgehen, dass unsere Aktivitäten gespeichert werden. je aktiver wir den entsprechenden Service nutzen, umso umfangreicher wird unser Profil. Schon mal über die Treffsicherheit der vorgeschlagenen Produkte des Onlineshops gewundert? Oder über passende Werbeeinblendungen bei Google? Letztlich basieren die Entscheidungen des jeweiligen Systems, uns diese Informationen anzuzeigen, auf Daten, die durch unser Verhalten gesammelt wurden.

1.3 Vertrauen (in Identitäten)

Die Möglichkeit, sich im Internet eine eigene neue digitale Identität aufzubauen, bietet viele Chancen. Im Schutz der Anonymität fällt es manchen leichter, sich anderen gegenüber zu öffnen und Hilfe und Rat zu suchen. Whistleblower oder politisch Verfolgte können ihr Wissen mit geringerer Gefahr teilen.

Die Anonymität birgt aber auch Risiken. Wenn niemand meine wahre Identität kennt, muss ich die Konsequenzen meines Handelns nicht fürchten. Hemmungen fallen und der Ton in Foren und sozialen Netzwerken wird rauer. Diskussionen werden zu Streitereien, in denen einzelne Teilnehmer persönlich beleidigt werden.

Betrüger legen falsche Identitäten an und versuchen, Kontakt aufzunehmen, Informationen zu erhalten oder mich zum "Gefällt mir" und "Teilen" von Produkten und Informationen zu bewegen. Wenn wir die Person nicht aus unserem "realen Leben" kennen und damit sicherstellen können, dass sie hinter dem entsprechenden Profil oder der E-Mail steckt, bleibt immer ein Restrisiko, dass unser Gegenüber nicht der ist, der er vorgibt zu sein.

Wenn ich eine Kontaktanfrage von einem Profil mit dem Namen einer mir bekannten Person bekomme: Wie kann ich sicher sein, dass hinter dem Profil auch wirklich die mir bekannte Person steckt? Letztlich ist dies eine reine Vertrauensfrage. Ist es mir möglich das Profil der Person einzusehen und finde ich dort ausreichend Fotos und sonstige Informationen, die die Identität der Person bestätigen? Mit welchen anderen Profilen ist die Person ansonsten noch online verbunden? All diese Informationen helfen mir, die Identität des Profils zu bestätigen.

Vertrauensvolle Verbindungen werden durch die Verknüpfung von Identitäten geschaffen. Der beliebte Satz "deine Freunde sind auch meine Freunde" kommt gerade in sozialen Netzwerken zum tragen. Wenn ein Profil bereits mit anderen mir befreundeten Profilen vernetzt ist, steigt die Wahrscheinlichkeit, dass es sich hierbei auch um die Person handelt, für die das Profil steht. Die Identität wird durch die Gemeinschaft sichergestellt.

Die vermeintliche Vertrautheit zu einer Identität birgt die Gefahr, dass wir nachlässig werden und eventuell unreflektiert handeln. Bei der Menge an Informationen die wir heute in das Internet stellen, ist die Tatsache, dass andere Menschen etwas Persönliches über uns wissen, kein Identitätsnachweis. Zudem wurden Konten auf sozialen Netzwerken bereits des öfteren von Dritten übernommen. Auch gibt es Fälle, in denen fremde Personen Online-Profile von anderen Menschen angelegt, und sich als diese ausgegeben haben. Derjenige muss hierfür kein IT-Experte sein. Dazu braucht es lediglich eine E-Mail-Adresse. Und auch diese können ohne Weiteres erstellt oder gar missbraucht werden. Mit einer gestohlenen E-Mail-Adresse und einigen weiteren Informationen lässt sich recht einfach eine echt wirkende E-Mail erstellen, über die versucht werden kann, an weitere persönliche Informationen oder gar an Geld zu gelangen. Sogenannte Phishing-E-Mails sehen auf den ersten Blick aus als kämen sie von der eigenen Bank oder dem Onlineshop, bei dem wir erst kürzlich bestellt haben. In Wirklichkeit wurde sie aber von einem Betrüger erstellt, der nur darauf abzielt, uns auf eine gefälschte Webseite zu leiten, auf der wir dann unsere Kunden- oder

Kontodaten eingeben sollen.
“Traue niemandem” mag sich in diesem Zusammenhang übertrieben anhören, aber ein gesundes Maß an Skepsis sollten wir uns grundsätzlich bei all unseren Aktivitäten in der digitalen Welt bewahren.

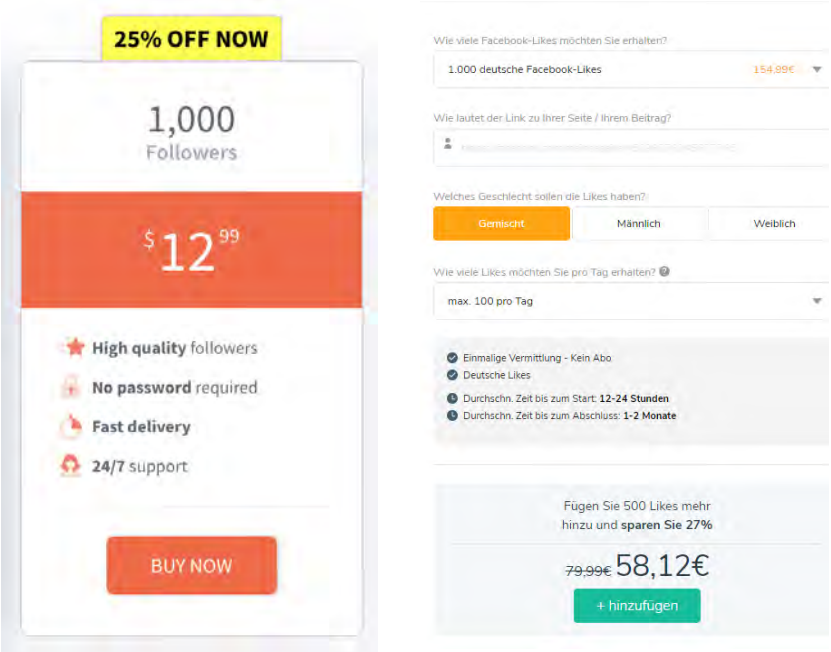
1.4 Gefälschte Identitäten

Für die Anlage einer E-Mail-Adresse oder eines Profils auf einem sozialen Netzwerk gibt es kaum Regeln. Es findet auch keine Identitätsüberprüfung statt. Somit ist es möglich E-Mail-Adressen oder Accounts auf Webseiten auch unter falschem Namen anzulegen. Die großen Netzwerke bemühen sich falsche Profile (Fake-Profile) zu entfernen, sobald diese als solche erkannt werden. Entsprechend der Nutzungsbedingungen von Facebook sind diese auch nicht zulässig. Bis es aber zu einer Entfernung kommt sind diese jedoch einige Zeit online und aktiv.

Alleine Facebook löscht seit 2019 im Quartal durchschnittlich 1,5 Milliarden Fake-Accounts.[1] Die gefälschten Identitäten werden zu unterschiedlichen Zwecken eingesetzt - meist mit betrügerischen Absichten. So werden gefälschte Gewinnspiele veröffentlicht, Links zu betrügerischen Webseiten geteilt oder versucht über die Profile Kontakte zu knüpfen, um an persönliche Daten heranzukommen.

Im größeren Stil werden auch nicht einzelne Profile angelegt, sondern gleich ein ganzes Netz aus hunderten oder mehr gefälschten Identitäten. Die falschen Profile werden dann dazu eingesetzt, um andere Profile, Seiten oder Themen zu unterstützen.

Sie haben ein Restaurant und wollen mehr positive Bewertungen auf einem Bewertungsportal? Dann kaufen sie sich diese eben ein. Sie wollen mehr “Likes” oder “Followers” auf ihrem Profil in einem sozialen Netzwerk? Dann bezahlen sie einfach für zusätzliche Klicks. Es gibt Webseiten auf denen Hunderte oder Tausende von Konten gekauft werden können. Und auch wenn diese Möglichkeit verlockend klingt, so ist davon abzuraten. Die großen Anbieter sind sehr bemüht solche gekauften Meinungen zu erkennen und dagegen vorzugehen.



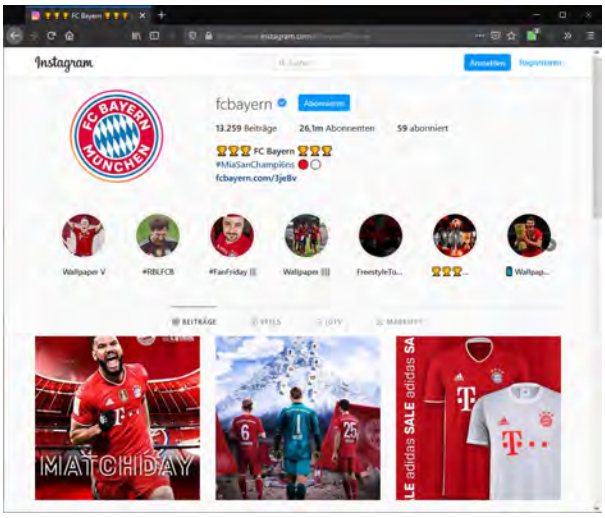
Links: Für knapp 13$ erhalten Sie 1.000 Instagram-Follower.
Rechts: Für 1.000 deutsche Facebook-Likes bezahlt man bereits über 150€. 100 werden für 19,99€ angeboten.

Gefälschte Profile werden auch für politische Zwecke eingesetzt. Mit ihnen ist es möglich, bestimmte Meinungen und Nachrichten in die Öffentlichkeit zu bringen. Je mehr ein Thema diskutiert, geteilt und kommentiert wird, desto mehr Menschen werden erreicht. Informationen mit viel Interaktion werden von den automatisierten Systemen der Netzwerke (die "Algorithmen") als wichtig und "wertiger" identifiziert. Somit werden diese entsprechend bevorzugt behandelt und eher in die Kanäle andere Nutzer platziert. So können gezielt Versuche zur Beeinflussung der öffentlichen Meinung unternommen werden, in dem bestimmte Themen über eine längere Zeit verstärkt geteilt und kommentiert werden. Dabei werden die Fake-Profile automatisiert über Programmierung gesteuert und verwaltet. Es braucht keine realen Personen, die hier aktiv werden.

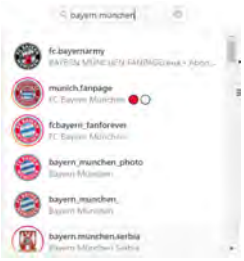
Wie aber können wir gefälschte Identitäten von echten unterscheiden? Das ist leider kaum möglich, denn eine hundertprozentige Sicherheit gibt es hierbei nicht. Selbst das bekannte Profil eines Freundes, der uns plötzlich seltsame Nachrichten schickt, könnte ja manipuliert worden sein. Es bleibt uns auch hier nur ein gesundes Maß an Skepsis und ein Gefühl dafür zu entwickeln, wie vertrauenswürdig eine Nachricht oder ein bestimmtes Profil ist.

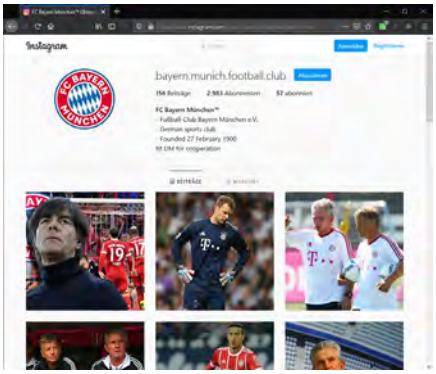
Wichtige Personen wie Politiker, Künstler oder Marken und Unternehmen haben bei den großen sozialen Medien die Möglichkeit, ihr Profil zu verifizieren. Ein verifiziertes Profil wird meist mit einem blauen Häkchen gekennzeichnet. Dieses zeigt an, dass das entsprechende Profil seitens des Netzwerk Anbieters die Identität des Besitzers verifiziert hat. Das bedeutet nicht, dass ein solches Profil vor Missbrauch sicher ist, es zeigt uns aber zumindest an, dass es sich bei dem Profil um eine reale Identität des Profils Besitzers handelt.

Facebook schätzt, dass gefälschte Konten im 3. Quartal 2020 etwa 5 % der weltweiten monatlich aktiven Nutzer auf Facebook ausmachten. 1,5 Milliarden Konten wurden in Q2 2020 auf 1,3 Milliarden in Q3 2020 zurückgeführt[30]



Der offizielle Instagram-Account des Fussballvereins "Bayern München".
Er hat ein blaues Häkchen und 26 Millionen Abonnenten. (Quelle: Screenshot Instagram.com, 10.04.2021)





Links: Wer nach "Bayern München" sucht, findet weitere Profile.
Rechts: Unter anderem findet sich hier das Profil "bayern.munich.football.club". Dieses Profil hat kein blaues Häkchen und auch nur knapp 3000 Follower. Das muss kein Fake-Profil sein, aber es ist nicht das offizielle Profil des Fussballclubs. Vermutlich ist dies ein Profil, das von einem Fan angelegt wurde
(Quelle: Screenshot Instagram.com, 10.04.2021)

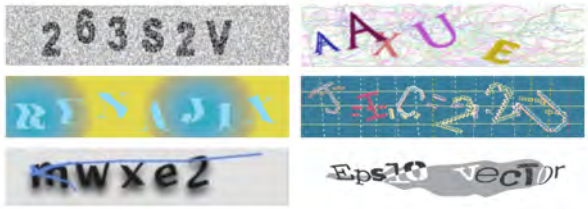
1.5 Möglichkeiten der Identitätsbestätigung

Da wir uns in der Regel anonym durch das Internet bewegen, brauchen wir Möglichkeiten, um uns online authentifizieren können. Es gibt verschiedene Methoden zur Überprüfung einer Identität im digitalen Raum. Einige dieser Lösungen stellen lediglich sicher, dass es sich um eine reale Person handelt, andere wiederum identifizieren die Person anhand von weiteren persönlichen Merkmalen, wie z.B. der Telefonnummer.
Unternehmen nutzen diese Art einer Identitätsbestätigung auch, um den Zugriff auf unsere Konten und Profile zu schützen. Sie kommen spätestens dann zum Einsatz, wenn eine verdächtige Anmeldung festgestellt wurde. Zum Beispiel wenn unser Anmeldeverhalten von unserem bisherigen Verhalten abweicht.

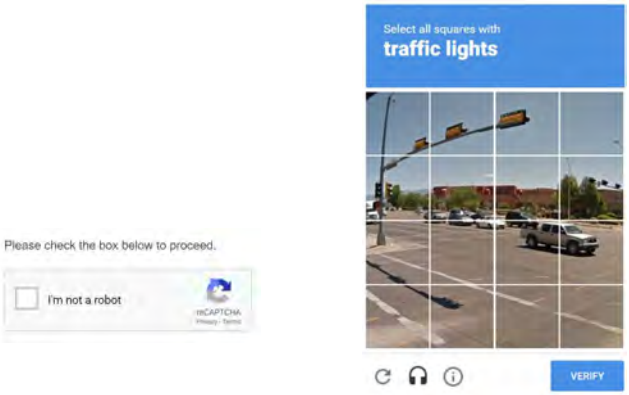
1.5.1 Captcha

Captchas sollen sicherstellen, dass es sich bei dem Besucher einer Webseite um einen Menschen handelt, und die Webseite nicht gerade automatisiert von einem Programm verarbeitet wird.
Ursprünglich wurden Captchas als Reihe von Zahlen und Buchstaben dargestellt, wobei die Darstellung verzerrt oder mit Effekten belegt ist. Die Aufgabe des Webseiten Besuchers ist es nun, die Zeichenfolge als Bestätigung in ein Eingabefeld einzugeben. Da es für automatisierte Prozesse schwierig ist, die Symbole richtig zu identifizieren, ist das Captcha eine gute Möglichkeit einen automatisierten, nichtmenschlichen Zugriff zu vermeiden.
Heute existieren unterschiedliche Arten von Captchas. Es gibt Rechen- und Verständnisaufgaben, oder auch Bilderreihen mit der Aufgabe, einzelne Bilder auszuwählen, auf denen ein bestimmter Gegenstand abgebildet ist. All dies sind Aufgaben, die nur von Menschen gelöst werden können, da zur Lösung ein grundsätzliches Verständnis der Aufgabe notwendig ist.
Captchas können zwar sehr lästig sein, aber es ist eine Möglichkeit, Missbrauch und Fehlbedienung von Webseiten und Online-Anwendungen zu vermeiden.
Captchas verhindern jedoch nur den automatisierten Missbrauch. Ein menschlicher Betrüger ist weiterhin in der Lage ein Konto unter falschen Namen zu erstellen und sich für eine andere Person ausgeben.

CAPTCHA steht für “Completely Automated Public Turing test to tell Computers and Humans Apart”.
Der Turing-Test wurde 1950 von Alan Turing begründet. Der Test prüft die Fähigkeit einer Maschine, intelligentes Verhalten zu zeigen, das dem eines Menschen gleichwertig ununterscheidbar ist. Der Testablauf wurde von Turing folgendermaßen skizziert: Wir unterhalten uns mit Tastatur und Bildschirm mit zwei Gesprächspartnern, die wir nicht sehen können. Einer der Gesprächspartner ist ein Mensch, der andere ein Computer. Wenn wir selbst nach intensiver Befragung nicht sicher sagen können, welcher Interviewpartner Mensch und welcher die Maschine ist, hat diese den Test bestanden und es wird ihr ein dem Menschen ununterscheidbares Denkvermögen zugesprochen.



Dies ist ein typisches Captcha. Durch zusätzliche Bildstörungen und Verzerrungen soll eine automatisierte Bilderkennung verhindert werden und sichergestellt werden, dass nur Menschen die Zeichen lesen können



Links: Eine einfache Methode zur Identifizierung durch einen separaten Mausklick
Rechts: Eine weitere Captcha-Methode; Identifizierung von Elementen in einem Foto (Ampel)

1.5.2 E-Mail-Konto

Unser E-Mail-Konto ist unser digitaler Briefkasten. Die dazugehörige E-Mail-Adresse ist einmalig. Damit wird unsere E-Mail-Adresse zu einem wichtigen Element, um uns online zu identifizieren.

Bei der Erstellung eines neuen Kontos auf einer Webseite werden wir in fast allen Fällen nach einer bereits bestehenden E-Mail-Adresse gefragt. In der Regel erhalten wir nach erfolgreicher Registrierung eine Bestätigungs-E-Mail an unsere Adresse mit einem Link, den wir anklicken müssen. Damit prüft der Anbieter, ob wir auch tatsächlich Besitzer dieser E-Mail-Adresse sind, bzw. ob wir darauf Zugriff haben.

Und haben wir uns einmal bei dem Anbieter registriert, erfolgt die Anmeldung zukünftig meist über eine Kombination aus E-Mail-Adresse und einem individuellen Passwort. Und selbst wenn die Anmeldung auch über einen selbstgewählten Benutzernamen möglich ist, so dient die E-Mail-Adresse als Identifikationsmittel zwischen uns und dem Anbieter und vor allem auch für wichtige Funktionen wie dem Zurücksetzen des eigenen Passworts, sollten wir es einmal vergessen haben.

1.5.3 Telefonnummer oder Kreditkarte

Neben einer E-Mail-Adresse werden von Online Anbietern auch gerne die Telefonnummer oder die Kreditkartennummer abgefragt. Eine E-Mail-Adresse kann auch anonym erstellt und schnell wieder gelöscht werden. Telefonnummern und Kreditkarten sind in der Europäischen Union jedoch immer mit einer Person verknüpft.
Online-Dienste, die nach diesen Informationen verlangen, wollen damit sicherzustellen, dass es sich bei dem Nutzenden um eine reale Person handelt. Grundsätzlich sollte die Herausgabe dieser Daten immer erst nach reiflicher Überlegung erfolgen. Kenne ich das Unternehmen, welches nach dieser Information fragt? Bin ich sicher, dass meine Daten bei dem Anbieter sicher sind und nicht an Dritte weitergeben werden? Wer sich unsicher ist, sollte sich zunächst die Datenschutzbedingungen des Anbieters durchlesen.
Gerade Telefonnummern werden gerne als zusätzliche Komponente bei der Überprüfung der Identität über eine Zwei-Faktor-Authentifizierung genutzt.

1.5.4 Zwei-Faktor-Authentifizierung

Lange Zeit verwendeten Websites ausschließlich Benutzernamen und Kennwort, um sicherzustellen, dass wir legitimiert sind den entsprechenden Service zu verwenden. Sobald jemand an unsere Login-Daten gelangte, hat er in diesem Fall uneingeschränkten Zugriff auf unser Konto. Die Zwei-Faktor-Authentifizierung (2FA) fügt einem Konto eine weitere Sicherheitsebene hinzu.

Sie beschreibt einen Identitätsnachweis mittels einer Kombination von zwei unterschiedlichen Faktoren. Neben der Kombination aus Benutzernamen und Kennwort wird z.B. noch eine SMS mit einem PIN an eine hinterlegte Mobilfunknummer gesendet. Damit erfolgt eine doppelte Prüfung der Identität.

Seit 2019 ist der Einsatz einer Zwei-Faktor-Authentifizierung für die Nutzung von Zahlungsdiensten über eine EU-Richtlinie vorgeschrieben. Aber sie wird zunehmend auch von Anbietern anderer Dienste als zusätzlicher, optionaler Sicherheitsmechanismus angeboten.

Es ist theoretisch auch möglich die Authentifizierung auf mehr als nur zwei Faktoren auszuweiten. Dann wird von einer Multi-Faktor-Authentifizierung gesprochen. Je mehr Faktoren überprüft werden, umso sicherer ist einerseits der Identitätsnachweis, aber andererseits wird der Anmeldeprozess umfangreicher und länger.

Um Betrugsversuche zu vermeiden, verlangen Anbieter unter Umständen eine weitere Authentifizierung, wenn sie verdächtige Anmeldeversuche feststellen. Sollten wir normalerweise ausschließlich auf unser Online-Konto von zuhause aus zugreifen und dann plötzlich einmal aus dem Ausland, weil wir im Urlaub sind, dann erkennt das System unter Umständen einen verdächtigen Anmeldeversuch und verlangt von uns eine zusätzliche Verifizierung, z. B. in der Form unseres Geburtsdatums, einer Sicherheitsfrage oder einer anderen Information, die wir im Account hinterlegt haben. Zusätzliche Schritte in der Authentifizierung sollten daher nicht als lästige Abfragen angesehen werden, denn sie dienen der Sicherheit unserer Daten.

Die Zwei-Faktor-Authentifizierung ist für viele Dienste obligatorisch. Einer davon ist die Kreditkartenzahlung über das Internet. In der EU ist es zwingend erforderlich, dass der Händler sicherstellt, dass es sich bei der Nutzung der Kreditkarte um eine legitime Nutzung handelt. Dies ist über einen zusätzlichen Schritt in der Authentifizierung, wie der Übermittlung einer PIN auf das Mobilfunktelefon des Kunden, möglich

1.5.5 Digitale Zertifikate (E-Identity)

Bei einem digitalen Zertifikat handelt es sich um einen elektronischen Echtheitsnachweis, der von einer Zertifizierungsstelle ausgestellt wurde. In der IT werden digitale Zertifikate dort eingesetzt, wo die Identität eines Kommunikationspartners oder einer Quelle eindeutig festgestellt werden muss - beispielsweise bei der Verschlüsselung von E-Mails. Die gleiche Technologie wird bei elektronischen Identitätsnachweisen in der virtuellen Welt eingesetzt. [2]

Es gibt staatliche und privatwirtschaftliche Lösungen für elektronische Identitätsverfahren. In der Privatwirtschaft sind es in der Regel Banken oder IT-Unternehmen, die uns eine digitale ID bereitstellen, mit der wir uns online, z.B. beim Online-Banking, ausweisen können.

Im staatlichen Bereich geht es vor allem um die Digitalisierung von Verwaltungsvorgängen. Zukünftig wird es nicht mehr notwendig sein, persönlich zum Schalter zu gehen und dort unsere Unterschrift zu leisten. Vielmehr werden wir Behördengänge online abwickeln können. Als Identitätsnachweis dient der digitale Personalausweis. Genauso wie wir uns heute mit dem Reisepass oder dem Personalausweis beim Grenzübertritt oder beim Gang zur Bank ausweisen, können wir das über unsere digitale ID auch online.

Die Initiative der Europäischen Union zur Vereinheitlichung der nationalen IDs ist in der Verordnung 910/2014 verankert.

Digitale IDs können die Verwendung von Benutzernamen und Passwörtern bei Vorgängen, die unsere Identifikation erfordern, überflüssig machen. Unsere Identität wird über die elektronische ID verifiziert. Auch ist es nicht mehr notwendig auf Papier zu unterschreiben. Über die Verifizierung unsere digitalen ID können wir unser Unterschrift elektronisch einreichen.

Tastatur, die einen Kartenleser enthält. Die Karte enthält einen Chip, der unsere digitale ID speichert

1.5.6 Biometrische Daten

Neben den bereits beschriebenen personenbezogenen Daten gewinnt auch vermehrt die Erhebung und Verwendung von biometrische Daten an Bedeutung. Laut dem Portal datenschutz.org beschreiben biometrische Daten "per Definition personenbeziehbare oder personenbezogene Informationen zu physischen, physiologischen oder verhaltens typischen Eigenschaften einer identifizierbaren Person." Dazu gehören körperliche Merkmale, die eindeutig einer Person zugeordnet werden können, also beispielsweise die Geometrie des Gesichts, der Augenhintergrund, die Klangfarbe der Stimme, ein Zahnabdruck, aber auch die Handschrift.

Neben der eindeutigen Zuordnung zu einer Person können biometrische Daten auch dafür verwendet werden, eine Authentifizierung durchzuführen. Am weitesten verbreitet ist hierbei sicherlich die Entsperrung eines Smartphones per Fingerabdruck. Aber auch klassische Computer verfügen bereits teilweise über Fingerabdrucks-Scanner. Geforscht wird auf diesem Gebiet auch an neueren Techniken wie der Abdruck des Fingerknöchels oder auch der Zungenspitze. Das mag sich zunächst befremdlich anhören - wenn wir uns aber vorstellen, wie schwierig es ist, in böswilliger Absicht an den Abdruck der Zungenspitze eines anderen Menschen zu gelangen, spielt natürlich der Aspekt der Sicherheit hier eine große Rolle.

Die DSGVO stuft biometrische Daten wie die DNA, die Gesichtsgeometrie oder auch den Fingerabdruck als besondere Kategorien personenbezogener Daten ein. Daher dürfen diese nur in Ausnahmefällen oder per Einwilligung verarbeitet werden. Gewisse biometrische Daten wie die Gesichtsgeometrie dürfen sogar nur unter bestimmten Voraussetzungen erhoben werden, beispielsweise durch die Polizei, und müssen effektiv gegen unbefugten Zugriff geschützt werden.[3]

2. Herausforderungen der digitalen Welt

Die digitale Welt bietet enorme Vorteile und Annehmlichkeiten. Doch auch im Internet begegnen uns Risiken. Diese sind vielfältig und sind auch in ihrer Gefahrenstufe unterschiedlich zu bewerten. Letztlich stellen sie aber immer einen Angriff auf unsere Privatsphäre und unsere Daten dar. Die Gefahren reichen von der ungewollten Offenlegung unserer Daten bis zur Löschung und Zerstörung.

Es ist wichtig die Gefahren und deren Auswirkungen zu kennen. Denn verstehen wir die zugrundeliegenden Mechanismen, sind die meisten Risiken vermeidbar oder wir können sie über entsprechende Verhaltensweisen zumindest minimieren.

Grundlegende Tipps zum Schutz unserer Daten:

- Anpassen der Verhaltensweise im Umgang mit digitalen Medien - ein gesundes Maß an Vorsicht und Skepsis ist angebracht, insbesondere im Umgang mit Nachrichten von Unbekannten oder E-Mail-Anhängen
- Nutzung sicherer Passwörter und einer 2-Faktor-Authentifizierung
- Einsatz einer Antivirensoftware und einer Software-Firewall
- Aktualisierung aller wichtigen Programme - insbesondere des Betriebssystems und des Internetbrowsers
- Überprüfung der Datenschutzeinstellungen der genutzten Onlineangebote - insbesondere in den sozialen Netzwerken.
- Regelmäßige Datensicherung

Herausforderungen im Internet		
Er/sie kennt Risiken, die unsere Privatsphäre und die Sicherheit unserer Daten beeinträchtigen können und kennt Strategien diese Risiken zu minimieren.		
Wissen	**Fertigkeiten**	**Kompetenz**
Er/Sie kann • die gängigen Risiken im Internet benennen und kennt Möglichkeiten diese zu minimieren. • die möglichen Auswirkungen von wissentlich oder unwissentlich veröffentlichten Daten im Internet beschreiben	Er/Sie ist in der Lage • die gängigen Risiken zu verstehen und entsprechende Schutzmaßnahmen durchzuführen • Gefahren zu erkennen und entsprechend zu handeln. • den Wert der eigenen Daten einzuschätzen	Er/Sie ist in der Lage • Maßnahmen zu ergreifen, um die Sicherheit der eigenen Daten und Privatsphäre im Internet zu erhöhen • Strategien zum Schutz der Privatsphäre und der eigenen Daten zu entwickeln. • selbstbestimmt mit den eigenen Daten umzugehen

2.1 Risiken im Internet

2.1.1 Von Datensammlern

Unsere Daten sind wertvoll. Und letztlich wollen sehr viele Anbieter und Services an unsere Daten. Es wird versucht an unsere E-Mail-Adresse und sonstigen Kontaktdaten zu kommen, damit uns im harmlosesten Falle Werbung zugeschickt werden kann. Schlimmstenfalls versucht jemand in böswilliger Absicht an unsere Daten zu kommen, um sich Zugriff auf unsere Konten zu verschaffen.

Wie kommen Dritte aber an unsere Daten? Dies muss nicht zwingend über Schadsoftware erfolgen. Gerade in den sozialen Netzwerken wird versucht uns zu einer Aktion zu verleiten. Wenn wir liken und kommentieren zeigen wir, das unser Profil aktiv ist und sich dahinter eine reale Person verbirgt.

Gerade auf Facebook finden sich zudem viele gefälschten Gewinnspiele, die nur darauf abzielen, an unsere E-Mail-Adresse zu kommen. Diese werden dann seitens der Betreiber gewinnbringend an Werbepartner verkauft. Das führt zunächst zu einem höheren Aufkommen an Werbemails und sogar zu Werbeanrufen. Gefährlich wird es, wenn unsere Daten bewusst dazu eingesetzt werden, um an weitere Informationen zu kommen (z.B. über Phishing). Die Webseite Mimikama listet alleine für das Jahr 2020 über 150 solcher identifizierter “Fake-Gewinnspiele” auf.[4]

Ansonsten sind alle Informationen, die wir öffentlich im Internet hinterlassen, auch öffentlich zugänglich: Kommentare in Online-Foren, auf öffentlichen Facebook-Seiten oder auch Informationen auf unserer eigenen Webseite. All diese Informationen können erfasst und analysiert werden. Welche Auswirkungen dies langfristig haben kann, können wir nicht absehen. Es ist nicht die eine kleine Information über uns, die problematisch ist, sondern die Anhäufung von vielen Informationen, die miteinander verknüpft und in Relation gestellt werden können.

Sogenannte Datenbroker sammeln verschiedenste Informationen, um unsere Daten anschließend an andere Unternehmen weiterzuverkaufen. Diese Unternehmen werben damit, dass sie über 250 Merkmale zu einer Person besitzen.

Neben Informationen zu unserer Person, inklusive Informationen zum Familienstand, Bildungsniveau, Einkaufsgewohnheiten und vielem mehr, werden hier auch Merkmale wie z.B. “konsumfreudig” hinterlegt. Das Unternehmen “AZ Direct” der Bertelsmann-Gruppe besitzt, nach eigenen Angaben, Profildaten von über 70 Millionen Personen und 41 Millionen Haushalten. Es betrifft also uns alle.[5]

Einen kompletten Schutz gegen Datensammler gibt es nicht. Wir können lediglich mit unseren Daten sensibler umgehen. Wir sollten immer nur die Daten von uns preisgeben, die in dem entsprechenden Anwendungsfall benötigt werden. [6]

2.1.2 SPAM & Phishing

SPAM - Wer kennt sie nicht, die unliebsamen E-Mails, die immer wieder im Postfach landen: Werbung von uninteressanten Produkten, dubiose Geschäftsangebote oder sonstige unerwünschte E-Mails. Ende 2019 lag der Anteil dieser unverlangten, massenhaft verschickten Werbe-E-Mails bei 57% des gesamten E-Mail-Verkehrs weltweit. Und selbst die besten Spam-Filter schaffen es nicht immer alle unerwünschten Spam-E-Mails herauszufiltern.[7]

Woher kommt die Bezeichnung "SPAM"?
Spam ist zunächst ein Markenname für Dosenfleisch. In dem nur dreiminütigen Sketch der britischen Komikergruppe Monthy Python aus dem Jahre 1970 fällt das Wort Spam über 130 mal. Das Wort wird zunehmend in das Gespräch eingebaut und so häufig genannt, dass eine vernünftige Konversation nahezu unmöglich wird. Dieses Überschwemmen des Gespräches mit dem Wort Spam ist die Parallele zu den unerwünschten E-Mails, die täglich massenhaft ungefragt verschickt werden und unser digitales Postfach verstopfen.

Die Versender solcher E-Mails werden Spammer genannt. Sie gelangen auf unterschiedliche Arten an unsere E-Mail-Adressen. Hier einmal an einem Gewinnspiel teilgenommen, dort die eigene E-Mail-Adresse hinterlegt und der Verwendung durch den Werbepartner unbemerkt zugestimmt und schon landet unsere E-Mail-Adresse in einer Adressdatenbank, die dann wiederum verkauft wird. Aber auch automatisierte Programme, die das Internet systematisch nach E-Mail-Adressen durchsuchen, werden eingesetzt.

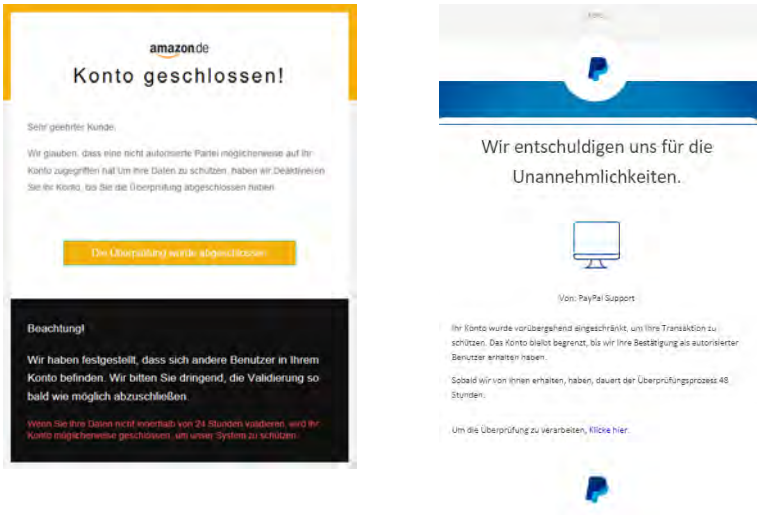
Spam ist nervig, aber welche Gefahren gehen von diesen E-Mails aus?

Kommerzielle Werbe-E-Mails werben für Produkte und Dienste, an denen wir kein Interesse haben. Diese Art der Werbung mag unser Postfach zumüllen, ist aber in der Regel ungefährlich. Trotzdem sollte vermieden werden, Anhänge oder Links in diesen E-Mails zu öffnen. Ein Link auf eine Webseite kann z.B. eine Kennung mit übermitteln, über die uns der Spammer identifizieren kann. In diesem Fall bestätigen wir, dass es sich bei unserer Adresse um eine reale, sich in Nutzung befindende E-Mail-Adresse handelt.

Auch landen Fälle des sogenannten **Vorschussbetrugs** in unserem E-Mail-Postfach. Hierbei wird versucht uns unter Vorspiegelung falscher Tatsachen zu bestimmten Aktionen zu verleiten: Der reiche Unternehmer, der im Sterben liegt, und sein Vermögen verschenken möchte; die Bank, die nach dem Erben eines reichen verstorbenen Unternehmer sucht, und die Erbschaft in Millionenhöhe anbietet. All das sind Varianten dieser Betrugsmasche, die es bereits seit Ende der 80er Jahre gibt. Die bekannteste Variante ist die sogenannte "Nigeria-Connection". Afrikanische Geschäftsleuten versprechen große Summen, wenn wir behilflich sind, riesige Dollarbeträge außer Landes zu schaffen. Wer auf solche E-Mails reagiert, wird in einem der nächsten Schritte gebeten zunächst eine Gebühr für anfallende Kosten zu bezahlen.[8]

Spam wird auch zur Verbreitung von **Schadsoftware** verwendet. Viren, Trojaner und andere Schadsoftware werden in vermeintlich harmlosen Anhängen versteckt. Öffnen wir den Anhang der E-Mail wird die Schadsoftware auf unserem Computer installiert.
Daher sollten grundsätzlich keine Anhänge in E-Mails von unbekannten Absendern geöffnet werden. Und auch bei bekannten Absendern ist ein gesundes Maß an Vorsicht angebracht. Es kann nie ausgeschlossen werden, dass ein anderes E-Mail-Postfach kompromittiert wurde und für den Versand von Spam missbraucht wird.

Ebenso gefährlich ist das sogenannte **Phishing**. Der Begriff ist an das englische Wort "fishing", Angeln, angelehnt. Hierbei versuchen die Betrüger unsere Passwörter und Zugangsdaten "abzufischen". Der Köder ist zunächst eine möglichst echt wirkende E-Mail, die in ihrer Gestaltung und ihrem Design einer echten E-Mail des jeweiligen Unternehmens nachempfunden wurde. Unsere Bank teilt uns darin mit, dass neue Sicherheitsregeln erfordern nochmals unsere Daten zur Autorisation zu übermitteln. Oder ein Online-Shop informiert uns über eine routinemäßige Sicherheitskontrolle, die wir binnen 48 Stunden durchzuführen haben. All diese E-Mails verlinken auf eine gefälschte Webseite und die von uns angegebenen Daten landen so direkt beim Betrüger. Dieser ist daraufhin in der Lage, unser Konto zu plündern oder unsere Identität zu stehlen. Auch kann diese Methode dazu genutzt werden, um Schadsoftware auf unseren Rechner zu bringen.[9]



LINK: Dies ist keine echte E-Mail von Amazon, sondern eine Spam-Mail. Wer auf die Schaltfläche klickt, wird auf eine gefälschte Webseite weitergeleitet, auf der wir aufgefordert werden unsere Benutzernamen und Passwort einzugeben.
RECHTS: Gefälschte E-Mail des Zahlungsdienstleisters Paypal.
(Quelle: Verbraucherzentral.de (https://twitter.com/vznrw_phishing)

Wie kann ich mich schützen?

Der wichtigste Schritt zum Schutz vor Spam ist ein umsichtiges Verhalten im Umgang mit den eigenen Daten und speziell der eigenen E-Mail-Adresse. Bereits bei der Wahl der eigenen E-Mail-Adresse ist darauf zu achten, keine vollständigen Namen zu offenbaren. Auch hat es sich bewährt, eine zweite unabhängige E-Mail-Adresse für Rechtsgeschäfte im Internet einzurichten.
Aus technischer Sicht gehören Virenschutzprogramme, Anti-Spam-Filter sowie regelmäßig durchgeführte Updates des Betriebssystems und der verwendeten Software zu den wichtigsten Maßnahmen.
Spam stellt ein Eindringen in die Privatsphäre dar und ist rechtswidrig. Verbraucher haben einen Anspruch auf Löschung der personenbezogenen Daten und können auch eine Unterlassungserklärung von dem Versender einer Werbe-E-Mail einfordern. Gerade Phishing-Mails können einen Straftatbestand darstellen. Entsprechend kann auch eine Strafanzeige in Erwägung gezogen werden.

In Deutschland können sich betroffene Verbraucher beim eco-Verband beschweren.[10] In Österreich kann eine Beschwerde bei dem zuständigen Fernmeldebüro eingereicht werden, sofern der Versender aus Österreich stammt.[11]

Ansonsten kann leider nur unter den Bestimmungen des Herkunftslandes des Spam vorgegangen werden. In vielen Fällen wird jedoch die wahre Identität und das Herkunftsland des Spammers nicht feststellbar sein. Daher bleibt eine Beschwerde in vielen Fällen leider ohne Auswirkung.

Woran erkenne ich eine Spam- & Phishing-E-Mail?

Spammer setzen häufig falsche Betreffzeilen wie "Re: Ihre Anmeldung" oder "Klassentreffen" und gefälschte Absender-Adressen ein. Sie geben sich als Freunde, Arbeitskollegen oder seriöse Unternehmen aus, um beim Empfänger einen persönlichen Bezug herzustellen und ihn dazu zu veranlassen, die Mail zu öffnen.

Bei folgenden Merkmalen sollten wir misstrauisch werden und die E-Mail einer genauen Überprüfung unterziehen: [12]

- **Den Absender der E-Mail überprüfen.** Auch wenn als Absender der Name meiner Bank oder eines mir bekannten Unternehmens angezeigt wird, empfiehlt sich ein zweiter Blick auf die Angaben. Oft werden ähnlich klingende Mail Adressen verwendet. Auch gilt es die Domäne der E-Mail-Adresse genau zu betrachten (also der Teil hinter dem @-Zeichen). Statt dem kundendienst@meinehausbank.com schreibt vielleicht meinehausbank123@hotmail.com. In jedem E-Mail-Programm gibt es die Möglichkeit, sich die Details zu einem Absender anzeigen zu lassen. Schnell stellt sich heraus, dass die E-Mail von dem Kundenservice eines Onlinehändlers in Wahrheit über die E-Mail-Adresse “infomail01@acshfg.ru” verschickt wurde, welche definitiv nicht zu dem Unter-

nehmen gehört.

- **In der E-Mail enthaltende Links prüfen.** Die meisten E-Mail-Programme zeigen die Adressen der Webseiten, die sich hinter einem Link verbergen, bereits an, wenn man mit der Maus darüber fährt. Dadurch kann ebenfalls erkannt werden, ob der Link auch wirklich auf die Webseite verweist, auf die im Text hingewiesen wird. Ganz wichtig: Nicht auf den Link klicken, sondern nur einen Moment mit dem Mauszeiger darüber fahren. Dadurch kann der hinterlegte Link angezeigt und überprüft werden.
- **Grammatik- und Rechtschreibfehler.** Spam E-Mails werden oft nicht in unserer Landessprache verfasst und stattdessen mit automatischen Übersetzungsdiensten übersetzt. Dadurch kommt es auch immer wieder zu Fehler im Zeichensatz. Im Text befinden sich auch häufig Sonderzeichen oder kyrillische Buchstaben.
- **Fehlender Name.** Grundsätzlich werden wir in E-Mails mit unserem Namen angesprochen. Banken, Online-Shops und andere Online-Dienste verwenden selten allgemeine Formulierungen wie "Sehr geehrter Kunde". Aber darauf verlassen sollten wir uns nicht, da es durchaus sein kann, dass die Betrüger bereits unseren Namen kennen und uns auch direkt mit Vor- und Nachnamen anschreiben.
- **Unerwartete E-Mail.** Eine E-Mail erreicht uns völlig unerwartet? Und unsere Bank hat uns bis dahin noch nie E-Mails zukommen lassen? Auch das kann ein Merkmal einer betrügerischen E-Mail sein.
- **Aufforderung zum Öffnen einer Datei.** Bei E-Mails mit einem Dateianhang gilt es grundsätzlich misstrauisch zu sein. Besonders, wenn uns der Absender uns dazu auffordert die Datei zu öffnen oder alternativ einen Link zum Download bereitstellt.
- **Dringender Handlungsbedarf.** Oft wird uns eine Frist gesetzt, in der wir handeln müssen, da sonst unser Account gesperrt wird oder ähnliches. Das soll uns unter Druck setzen, und uns dazu bringen, schnell zu agieren. Vorsicht!

Der Schaden durch Spam und speziell Phishing-Angriffen kann durchaus hoch sein. Wer jedoch ein wenig achtsam bleibt und nicht jeder E-Mail uneingeschränkt vertraut, kann sich vor dieser Art von Betrug schützen.

2.1.3 Viren, Trojaner und sonstige Schadsoftware

Arten von Schadsoftware

Schadsoftware (auch Malware genannt) steht ganz oben auf der Liste der Bedrohungen aus dem Internet. Auch wenn die Anzahl der neu registrierten Schadprogramme im Frühjahr 2020 deutlich abgenommen hat, existieren immer noch über 6 Millionen Schadprogramm-Varianten. Es ist also weiterhin Vorsicht angebracht.[13]
Umgangssprachlich bezeichnen wir alle Arten von Schadsoftware als "Virus". Computerviren sind allerdings nur eine Art von Schadsoftware. Daneben gibt es viele andere Varianten wie z.B. Trojaner, Würmer oder Ransomware. Kompliziert wird es zudem, da sich nicht jedes schädliche Programm eindeutig einer bestimmten Klasse von Schadsoftware zuweisen lässt. Gemeinsam haben aber all diese Varianten, dass es sich hierbei um Computerprogramme handelt, die dazu entwickelt wurden unerwünschte und gegebenenfalls schädliche Funktionen auf den Endgeräten der Betroffenen auszuführen.

Die Grafik zeigt die Anzahl der Schadprogramm-Varianten, die in den letzten zwölf Monaten neu registriert wurden (in Mio.) (Quelle: Statista.de)

Computerviren & Würmer

Ein Computervirus ist ein Programm, das dem Computer Schaden zufügt, indem er wichtige Systemdateien beschädigt, Ressourcen verschwendet oder gar Dateien löscht. Wie ein echter Virus können sich einzelne Programme selbstständig vervielfältigen und auf andere Computer kopieren. Entgegen dem biologischen Virus entsteht der Computervirus allerdings nicht "einfach so". Computerviren werden von Menschen programmiert und greifen mit Absicht Computer und ganze Netzwerke an.

Wer sich einen Virus einfängt war nicht vorsichtig genug. Computerviren können sich auf unterschiedliche Art verbreiten. Bei den häufigsten Wegen, wie sich unsere digitale Infrastruktur mit einem Virus infizieren kann, spielen wir selber immer eine entscheidende Rolle.

- **E-Mails -** diese sind eines der beliebtesten Verbreitungsmittel für Computerviren weltweit. Am häufigsten werden Viren über E-Mail-Anhänge verbreitet. Hinter einer harmlos erscheinenden Datei mit harmlos erscheinendem Namen steckt in Wirklichkeit das Virusprogramm, das wir durch Öffnen des Anhangs ausführen. Aber auch eine E-Mail selbst kann bereits Schadsoftware in sich tragen.
- **Instant Messaging** - Auch über Messaging Dienste wie Skype, WhatsApp und Co. können Viren verbreitet werden. In diesem Falle wird der Virus über Chat-Nachrichten, die einen infizierten Link enthalten, verbreitet.
- **Software-Downloads** - Auch Software oder Apps können Viren enthalten. Die vermeintlich kostenlose Software enthält einen Virus, der bei der Installation einfach mitinstalliert wird. Ebenso gibt es gefälschte Antiviren-Programme. Über Werbeeinblendung auf Webseiten wird uns versucht glaubhaft zu machen, dass auf unserem Computer ein Virus gefunden wurde. Gleichzeitig wird uns die entsprechende „Antivirensoftware" angeboten. Doch anstatt den Computer von Viren zu befreien, infiziert das Programm unseren Computer.
- **Fehlende Software-Updates** - Immer wieder werden Sicherheitslücken bei gängigen Softwareprodukten entdeckt. Um diese zu schließen veröffentlichen die Hersteller regelmäßig Updates. Wer seine Software nicht aktuell hält läuft Gefahr, dass über diese Schwachstellen Schadsoftware auf den heimischen Rechner eingeschleust wird.

Während der herkömmliche Computervirus darauf angewiesen ist, dass Nutzer eine infizierte Datei weitergeben, kann sich ein Computerwurm selbst vervielfältigen, nachdem das entsprechende Programm einmal ausgeführt wurde. Computerwürmer verbreiten sich aktiv über Netzwerke ohne fremde Dateien zu infizieren.

Die Auswirkungen von Schadsoftware ist unterschiedlich.

- Der Virus “Stoned” zeigt nur willkürlich die Meldung „Your computer is stoned. Legalize marihuana!“ auf dem Bildschirm an, zerstört aber keine Dateien.
- Der “Ika-Tako-Virus” tarnt sich als Musikdatei. Sobald die Datei abgespielt wird, ersetzt der Virus alle Bilddateien auf dem befallenen Computer mit Bildern von Tintenfischen.
- Die Schadsoftware “Loveletter” (auch bekannt als ILOVEYOU-Virus) verbreitete sich im Jahr 2000 per E-Mail und befiel innerhalb von 24 Stunden 45 Millionen Rechner. Wer den Anhang des vermeintlichen Liebesbriefes öffnete, aktivierte den Virus, der daraufhin automatisch alle Dateien mit bestimmten Dateiendungen löschte. [14]
- 2003 infizierte “Sobig-F” insgesamt 2 Millionen Computer. Er befiel das Windows Betriebssystem und versendete von dem infizierten Rechner automatisch E-Mails an beliebige Empfänger. So verursachte die Schadsoftware eine Millionen E-Mails pro 24 Stunden. Durch die Masse der versendeten E-Mails wurden viele Computer in Mitleidenschaft gezogen. In Washington D.C. war der Datenverkehr aufgrund des Virus für kurze Zeit nicht möglich. Air Canada musste sogar aufgrund von Sobig.F einige Flüge streichen. Der Schaden wurde auf über 37 Milliarden US-Dollar beziffert.[15]
- 2004 infizierte “MyDoom” ebenfalls 2 Millionen Computer. Auch dieser Wurm versendete sich selbst von infizierten Computern an alle Kontakte, die er auf dem entsprechenden Rechner fand. Durch den massiven Mailversand verlangsamte er das gesamte Internet hierdurch um etwa 10%.
- Der Computerwurm “Linux.Wifatch” wurde 2014 entdeckt. Er infiziert Internet-Router ohne die Zustimmung des Benutzers. Doch anstatt Sie zu schädigen, fungiert er als eine Art Sicherheitsdienst. Er zerstört keine Dateien, sondern verändert die Konfiguration, entfernt Malware und sichert die Router gegen weitere Infektionen ab. Ein gutartiger Virus, sozusagen[16]

Trojaner

Wer kennt es nicht: Das trojanische Pferd. Ein hölzernes Pferd als Geschenk, in dem sich jedoch die feindlichen Krieger versteckten. Das gleiche Prinzip gilt bei der trojanischen Software. Hinter der harmlosen legitimen Software verbirgt sich in Wirklichkeit eine Schadsoftware. Im Glauben wir würden eine bestimmte Anwendung installieren, bringen wir so die eigentliche Schadsoftware auf unseren Computer.

Spyware

Eine Spyware (Spy = Spion) ist eine Anwendung, die im Verborgenen auf unserem Rechner läuft und unser Verhalten ausspioniert. Im harmlosesten Falle wird bloß unser Surfverhalten beobachtet. Kritischer sind Programme, die unsere Tastatureingaben mitprotokollieren (sog. Keylogger). Damit können Passwörter, Kreditkartenangaben und andere persönliche Daten abgegriffen werden. Die Schadsoftware sendet diese dann an den jeweiligen Programmierer der Spyware.

Ransomware

Diese Art von Schadprogrammen verschlüsselt Daten auf dem befallenen System und fordert von dem Opfer Lösegeld - wobei die Zahlung der geforderten Summe nicht unbedingt zur Entschlüsselung der Daten führt. Angriffsziel sind oft Unternehmen, Fabriken oder öffentliche Behörden. Hierbei werden teilweise immer wieder gesamte Netzwerke befallen. Ransomware gilt nach wie vor als eine der größten Bedrohungen. 30% der deutschen Unternehmen geben an, bereits einmal von einem Ransomware-Angriff betroffen gewesen zu sein. [17]

Adware

Diese äußerst lästige Art von Schadsoftware überflutet ihre Opfer mit unerwünschter Werbung. Sie wird oft als Teil von kostenloser Software mitinstalliert. Die Schadsoftware setzt sich in dem Betriebssystem fest und zeigt auch dann Werbung an, wenn die entsprechende Anwendung nicht geöffnet ist.

Web-basierte Schadsoftware - Drive-by-Downloads

Ein “Drive-by-Download” beschreibt ein unbeabsichtigtes und unbewusstes Herunterladen von Schadsoftware auf den Rechner. Internetseiten sind heutzutage selten rein statisch. Meist werden mit der eigentlichen Webseite auch Programmcodes übermittelt. Über diese ist es möglich Schadsoftware auf den Computer zu übertragen. Dies ist vorwiegend über Sicherheitslücken in unserem Browser oder in von uns benutzten Browser-Plugins möglich. Unser Browser ist hier das Sicherheitsrisiko. Deswegen ist es ratsam seinen Browser regelmäßig zu aktualisieren und damit bekannt gewordene Sicherheitslücken zu schließen. [18]

Wie schütze ich mich vor Schadsoftware?

Eine der wichtigsten Schutzvorkehrungen ist der Einsatz einer Antivirus-Software. Einmal installiert, hilft die Software eventuelle Schadsoftware aufzuspüren. Dabei ist wichtig zu verstehen, dass ein Antivirusprogramm immer nur vor den aktuell bekannten Computerviren schützen kann. Die Software muss regelmäßig aktualisiert werden.

Weitere Vorkehrung, wie die Absicherung des heimischen Netzwerkes, die regelmäßige Aktualisierung des Betriebssystems und der installierten Software sowie der Einsatz einer Software-Firewall sind ebenfalls wichtige Bestandteile des eigenen Schutzkonzeptes.

Auch wenn uns die genannten Hilfsprogramme schützen, dürfen wir dabei nicht vergessen, dass diese nur die letzte Verteidigungslinie darstellen. Der eigentliche Schutz vor Computerviren beginnt bereits mit unserem eigenen Verhalten. Mit einem gewissen Maß an Vorsicht können wir uns bereits gut vor dem Befall von Schadsoftware schützen.

Firewall (Brandschutzwand, Brandmauer)
Eine Software-Firewall ist ein Programm, das den Datenverkehr des eigenen Computers überwacht und filtert. Sie verhindert Zugriffe von außen und ist ein Schutz vor Angriffen von Würmern. Sie wird vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) als Schutzmaßnahme für die Internetnutzung empfohlen.

- **Vorsicht bei E-Mails von unbekannten Absendern** - Warum sollte uns eine fremde Person eine E-Mail schreiben? Woher hat die Person unsere Adresse?
- **Vorsicht bei E-Mail-Anhängen** - Wir sollten keinen E-Mail-Anhang öffnen, bei dem wir uns nicht 100% sicher sind, worum es sich handelt. Selbst die E-Mail eines uns bekannten Unternehmens mit einer angehängten Rechnung kann gefälscht sein. Wenn wir keine Rechnung erwarten, ist es sinnvoll sich die E-Mail zunächst genauer anzuschauen, und im Zweifelsfall zunächst bei dem Absender telefonisch nachfragen.
- **Nicht jeden Link öffnen** - Dies gilt vor allem für Nachrichten die uns über die sozialen Netzwerke erreichen. Wir sollten grundsätzlich skeptisch sein, wenn wir eine Nachricht ohne Kontext geschickt bekommen oder aufgefordert werden einen Link zu klicken.
- **Keine Hysterie** - Wir sind gerade auf einer Webseite und werden plötzlich mit einer Nachricht überrascht, unser Computer wäre nicht sicher oder bereits von Schadsoftware befallen? Zunächst die Ruhe behalten. Im Zweifelsfall den Rechner erst einmal ausschalten und nach einem Neustart den Computer über das Antivirusprogramm überprüfen lassen.
- **Vorsicht bei Software-Downloads** - Es gibt gute freie und kostenlose Software. Trotzdem sollten wir uns vor einem Download vergewissern, dass die Software ohne Gefahr verwendet werden kann und die Webseite, von der wir die Software herunterladen wollen, auch vertrauenswürdig ist. Hier gilt: Im Zweifelsfall auf den Download verzichten.

2.1.4 Berechtigungen von Apps und Software

Sobald wir eine Software auf unserem Computer installieren, erhält diese Zugriff auf unseren Computer und den darauf befindlichen Daten. Handelt es sich bei der installierten Software um Schadsoftware, so ist es durchaus möglich, dass die Anwendung im Hintergrund Informationen über uns sammelt und diese ohne unser Wissen weiterleitet. Es muss sich aber nicht immer um Schadsoftware handeln. Auch das Betriebssystem Windows sammelt Daten über die Nutzenden. Das aber nicht im Geheimen, sondern mit unserer Einwilligung. Die entsprechenden Einstellungen sind in der Systemsteuerung und in den Datenschutzeinstellungen zu finden. [19]

Auf unserem Smartphone oder Tablet benötigen Apps bestimmte Berechtigungen, um ordnungsgemäß funktionieren zu können. Eine App zur Bildbearbeitung benötigt Zugriff auf unsere Fotos, die Navigations-App auf unseren Standort und der Online-Messenger eine Verbindung in das Internet. Welchen Zugriff die einzelne App benötigt wird bei der Installation (Android) oder dem ersten Start (Apple) angezeigt. Zudem finden sich die entsprechenden Informationen bereits in der Beschreibung der App in den jeweiligen App-Stores.

Welche Berechtigungen haben meine bereits installierten Apps?
Bei Apples iPhone oder iPad findet sich die Informationen in den Einstellungen unter dem Menüpunkt "Datenschutz". Dort sind unter den einzelnen Datenkategorien (z.B. Kalender, Erinnerungen, etc.) alle Apps aufgelistet, die einen Zugriff angefordert haben. Dieser kann für jede einzelne Apps aktiviert und deaktiviert werden. Bei Smartphones mit dem Android-Betriebssystem finden sich die Informationen unter "Apps & Benachrichtigungen" in den Einstellungen. Hier können die Berechtigungen und Benachrichtigungen für die einzelnen Apps aufgerufen und geändert werden. Bei neueren Android-Versionen findet sich dort auch der "Berechtigungsmanager". Hier werden alle Apps nach den jeweiligen Berechtigungen aufgelistet. [31]

Tipp
Ein Überblick über die zustimmungspflichtigen Berechtigungen auf einem Android-Gerät findet sich hier: https://mobilsicher.de/checkliste/app-zugriffsrechte-entschluesselt-android

Doch wer achtet schon genau darauf welche Berechtigungen eine App einfordert? Sind wir uns darüber bewusst, wozu wir unser Einverständnis geben, wenn uns eine App zu einer Einwilligung auffordert? Warum benötigt die Wetter-App Zugriff auf unsere Kontakte? Warum muss ein soziales Netzwerk neben unserem Adressbuch auch auf unsere Kamera zugreifen? Und weshalb möchte das neue Smartphone-Spiel bitteschön Zugriff auf unser Mikrofon haben? Sollten wir entsprechenden Anfragen nicht skeptisch werden?

Natürlich brauchen Apps Zugriff auf bestimmte Informationen auf unserem Smartphone. Und nicht immer können wir überblicken ob die angefragte Berechtigung auch wirklich notwendig ist. Trotzdem sollten wir einzelne Berechtigungen kritisch hinterfragen. Gerade bei dem Zugriff auf unsere Dateien, Kalender, Kontakte oder auf die Informationen zu unserer körperlichen Aktivität und den Körpersensoren, sollten wir genauer hinsehen.

2018 stieß die New York Times bei einer Recherche auf die Software-Komponente "Alphonso" welche in zahlreichen Apps, sowohl in dem Google Play Store wie auch in dem Apple Store, verwendet wurde. Bekommt die entsprechende App Zugriff auf das Mikrofon, so belauscht die Software uns, indem sie regelmäßig alle Umgebungsge-

räusche aufzeichnet. Das Ziel ist hierbei Fernsehwerbung und -sendungen zu identifizieren um entsprechend Werbung auf dem Smartphone anzuzeigen. Dabei werden zwangsläufig auch normale Gespräche aufgezeichnet. Erschreckend ist, dass zum Zeitpunkt, als dies bekannt wurde, allein im Google Play Store bereits an die 1.000 Apps und Spiele angeboten wurden, die Alphonso integriert hatten.[20]

Noch erschreckender ist aber das Ergebnis einer Studie, die 2019 seitens des International Computer Science Institute veröffentlicht wurde. Demnach ist es Apps auf einem Android-Smartphone möglich bestimmte Informationen abzurufen, ohne das sie über die entsprechenden Berechtigungen verfügen. Zum Zeitpunkt der Studie wurden über 1.000 Android-Apps identifiziert, die das System auf diese Weise übergingen. Google versprach zwar das Problem mit dem nächsten Android-Version (welche gegen Ende 2019 veröffentlicht wurde) zu beseitigen, doch zeigt dies, dass wir uns nicht immer auf die Technik verlassen können. Gerade im Software-Bereich finden sich immer wieder Schwachstellen, die dann von Dritten ausgenutzt werden. [21]

Auch wenn es mühsam ist, sollten wir die erteilten Berechtigungen von Apps überprüfen und ihnen diese gegebenenfalls entziehen. Das kann zwar dazu führen, dass bestimmte Funktionen der App nicht mehr verfügbar sind, allerdings lässt sich somit auch feststellen, welche Berechtigungen auch wirklich zwingend notwendig sind. Verlangt eine App zu viele Berechtigungen oder erscheinen uns die angeforderten Berechtigungen zu weitreichend, dann sollten wir uns genau überlegen, ob wir die entsprechende App wirklich benötigen und ob wir uns nicht lieber nochmals nach besseren Alternativen umschauen.

2.1.5 Mikro Zahlungen und Mikro Transaktionen

Unter Mikrozahlungen werden Zahlungen von Kleinbeträgen verstanden. Das können Beträge von einem Cent bis zu fünf Euro sein, wobei es keine einheitliche Grenze gibt.

Hinter dem Prinzip steckt der Verkauf von Abonnements oder kleinerer Einzelelemente. Wir bezahlen für die Freischaltung eines Artikels auf der Webseite des Online-Magazins oder besitzen direkt ein Abonnement der Online-Ausgabe unserer Tageszeitung. Wir kaufen uns digital ein einzelnes Musikstück oder bezahlen monatlich für die Musik-Flatrate eines Streaming-Anbieters. Selbst Apps oder Spiele können im Rahmen eines monatlichen Abonnements angeboten werden. Zudem bieten Computerspiele häufig die Möglichkeit optische Ausstattungsmerkmale einer Spielfigur gegen Bezahlung zu erwerben. Auch können Kleinstbeträge dafür aufgebracht werden, besondere Gegenstände, neue Episoden und sonstige Vorteile in Spielen zu erwerben, die der Spieler auf normalem Weise nicht erhalten kann.

Weit verbreitet ist das Prinzip der Mikro Zahlungen bei vermeintlich kostenlosen Smartphone-Spielen. Diese Spiele sind in der Regel darauf ausgelegt, dass sie über Wochen und Monate hinweg spielbar sind. Um im Spiel voranzukommen muss der Spieler über einen längeren Zeitraum bestimmte Ressourcen sammeln. Ohne den Einsatz von echtem Geld kommt der Spieler nur schwer oder extrem langsam voran. Das Spiel bietet kleine Vorteile oder die hilfreichen Ressourcen gegen Kleinstbeträge im eigenen Shop an. Durch entsprechende Rabatte und Werbung wird der Spieler

dazu animiert, den kleinen Betrag von wenigen Euro zu investieren. Oft wird nicht direkt mit echtem Geld bezahlt, sondern ein Umweg über eine eigene Währung, die nur in dem jeweiligen Spiel existiert (In-Game-Währung), angeboten. Es werden nicht direkt die kostenpflichtigen Ergänzungen gekauft, sondern zunächst eine bestimmte Anzahl an Spiele-Währung, die dann wiederum im Spiele-Shop ausgegeben wird. Ein Beispiel hierfür sind Poké-Münzen für „Pokemon Go" oder Juwelen für „Clash Royale". Der Umweg über die In-Game-Währung verschleiert die echten Kosten. Auch verwenden viele dieser Spiele Mechanismen aus dem Bereich des Glücksspiels, um den Spieler enger an das Spiel zu binden und eine gewisse Abhängigkeit herzustellen. Für die Anbieter sind Mikro-Transaktionen ein lukratives Geschäft. Verkauft wird ein virtueller Gegenstand, dessen Herstellung meist ohne großen Produktionsaufwand möglich ist. Er muss nur einmal hergestellt werden und kann unendlich oft kopiert werden.

Die Gefahr hierbei ist: Schnell verlieren wir die Kontrolle über die vielen kleineren Beträge und Abos. Und all die Kleinstbeträge können sich in Summe durchaus zu größeren Beträgen verdichten

Im Jahr 2019 belief sich der Umsatz durch In-App-Käufe allein in Deutschland auf rund 1,2 Milliarden Euro.[32]
99 Prozent der marktführenden Spiele-Apps sind zunächst gratis spielbar (Free-to-Play, zu deutsch "kostenlos spielbar"). Kosten fallen an, um etwa weitere „Leben" zu erwerben, den Spielfortschritt zu beschleunigen oder die eigene Spielfigur einzukleiden. Fast jeder zweite Euro, der in Deutschland für Computer- und Videospiele ausgegeben wird, entfällt auf diese Free-to-Play-Angebote.[33] Zu den bekanntesten Titeln mit den weltweit höchsten Einnahmen 2019 zählen Spiele wie beispielsweise Fortnite (Platz1, 1,8 Milliarden $ Umsatz), Candy Crush Sage (Platz 5, 1,5 Milliarden $ Umsatz) sowie Pokemon Go (Platz 6, 1,4 Milliarden $ Umsatz)[34]

2.1.6 Datendiebstahl

Wer seine Daten zuhause auf dem eigenen Rechner speichert, ist auch selbst für ihre Sicherheit verantwortlich. Die Absicherung des eigenen Computers vor unerlaubtem Zugriff ist durch entsprechende Vorkehrungsmaßnahmen möglich. Die Wahrscheinlichkeit, ob ein Einbrecher sich Zugang zu unserer Wohnung verschafft und unseren Computer samt Festplatte entwendet, können wir gut einschätzen.
Es gibt aber auch Informationen über uns, die nicht in unserer direkten Verantwortung liegen. Hierzu zählen all unsere persönlichen Informationen die wir bei unzähligen Onlinediensten hinterlegt haben. Dazu gehören unter anderem unsere E-Mails, unsere Dateien und Fotos beim Cloud-Anbieter oder der Benutzeraccount in dem beliebten Onlineshop. In einigen Fällen können diese Daten nicht einmal von uns selbst verwaltet werden; wie die Finanzdaten, die unsere Bank oder das Finanzamt über uns speichert.
Für den Schutz dieser Daten sind die entsprechenden Unternehmen und Institutionen verantwortlich. Wir können auch zur Sicherheit beitragen, in dem wir unseren Account schützen (z.B. durch die Wahl eines sicheren Passworts), aber die Verantwortung über die technische Sicherheit obliegt dem Anbieter.Auch bei größeren Unternehmen kann es zu Datenpannen oder Datendiebstählen kommen, bei denen Daten entweder öffentlich zugänglich gemacht oder von Dritten gestohlen werden.

Einige Beispiele von größeren Vorfällen in der Vergangenheit:

Während des US-Wahlkampfs 2006 gelangten 20.000 interne E-Mails der demokratischen Präsidentschaftskandidatin Hillary Clinton an die Öffentlichkeit. Dieser Hack des Clinton-E-Mail-Servers während des US-Wahlkampfes erregte viel Aufsehen. Die E-Mails stammten aus der Zeit, als Hillary Clinton US-Außenministerin war und enthielten Gesprächsprotokolle, die sie nach den Regularien zum Umgang mit geheimen Informationen nicht mehr hätte besitzen dürfen.

2011 gab es eine Datenpanne bei Sony: Angreifer erbeuteten Informationen von mehr als 75 Millionen Nutzern des Onlinedienstes Playstation Network. Gestohlen wurden Adressen, Passwörter und teilweise auch Kreditkartennummern. Sony schaltete daraufhin den Onlinedienst für ganze 23 Tage aus.

Am 3. Oktober 2013 gab das Unternehmen Adobe bekannt, dass Eindringlinge die verschlüsselten Zugangsdaten und Kreditkartendaten von rund drei Millionen Nutzern erbeuten konnten. Kurze Zeit später wurde bekannt, dass auch eine zweite Datenbank mit Benutzernamen, Passwörtern und Passwort-Hinweisen betroffen war. Diese enthielt 153 Millionen Datensätze. Die erbeuteten Login-Daten tauchten im Netz als Download auf.

Im Mai 2014 meldete eBay, dass Unbekannte einen Großteil der Kundendatenbank der Online-Plattform kopiert hatten. Die Angreifer gelangen über gehackte Mitarbeiter-Zugänge ins Firmennetz und an die Kundendatenbank. Betroffen waren 145 Millionen Kundendatensätze mit Name, E-Mail-Adresse, Postadresse, Telefonnummer,

Geburtsdatum sowie dem verschlüsselten Passwort.

2014 wurden in mehreren Wellen private Fotos von überwiegend weiblichen Prominenten veröffentlicht, die allesamt aus dem Apple-Dienst iCloud entwendet wurden. Es handelte sich um private Bilder, die in den privaten iCloud-Accounts der Betroffenen gespeichert waren. Die Bilder wurden online gegen Geld verkauft.

Rekordverdächtig war Ende 2014 der Angriff auf Yahoo, bei dem Daten von 500 Millionen Nutzern abgegriffen wurden. Yahoo hatte allerdings erst 2016 darüber informiert.

Wenige Monate später musste Yahoo noch einen viel größeren Datendiebstahl eingestehen: Bereits 2013 wurden die Daten von drei Milliarden Accounts entwendet.

Im Januar 2019 wurden private Daten deutscher Politiker und Prominenter veröffentlicht. Die Daten stammten aus verschiedenen Quellen. Neben zum Teil öffentlich einsehbaren Quellen, wurden auch Daten aus gehackten E-Mail- und Social-Media-Accounts sowie Cloud-Diensten entwendet. Veröffentlicht wurden private E-Mail-Adressen und Handynummern der Betroffenen, ebenso wie Bankdaten und Privatadressen. In mehreren Fällen wurden sogar private Chats mit Familienangehörigen veröffentlicht.

All diese Beispiele zeigen, dass kein Unternehmen vor einem Diebstahl geschützt ist. Und die Zahl der Angriffe auf Unternehmen und öffentliche Einrichtungen steigt.[22] Allein in Deutschland verursachte Cyberkriminalität im Jahr 2019 Kosten in Höhe von ungefähr 87,7 Millionen Euro.[23]
Kommt es zum Ernstfall, bleiben uns als Geschädigte meist nur die Änderung unseres Passworts oder die Sperrung von Bankkonten und Kreditkarten (wenn diese ebenfalls betroffen sind). Wir können nur präventiv Vorsorge treffen, in dem wir die Menge der persönlichen informationen die wir preisgeben auf ein Minimum beschränken.

Social Engineering & Social Hacking
Social Engineering bezeichnet die emotionale Manipulation von Personen zum Hervorrufen bestimmter Verhaltensweisen. Eng damit verbunden ist das Social Hacking. Hier versucht ein Angreifer eine Person so zu beeinflussen oder zu täuschen, dass Kontrolle über deren Computersystem erlangt werden kann. Über den direkten, sozialen Kontakt wird hierbei der Versuch unternommen an Informationen zu gelangen. Die Täter täuschen Identitäten vor und erarbeiten sich das Vertrauen ihrer Opfer, um darüber schließlich an die gewünschten Informationen zu gelangen. Häufig ist das Social Hacking der erste Schritt eines Datendiebstahls. Da technische Systeme meist gut geschützt sind, machen sich die Angreifer den Menschen als schwächstes Glied in der Datenschutzkette zu eigen. Der Angreifer könnte zum Beispiel unter einem Vorwand einen Mitarbeiter eines Unternehmens anrufen, sich als Techniker ausgeben und vertraulichen Zugangsdaten erfragen. Um den Anruf glaubhafter zu machen, hat sich der Angreifer im Vorfeld gut über das Unternehmen informiert oder eventuell bereits über eine andere Social Hacking Aktion bestimmte Internas erfahren, die er nun einsetzt. Berichtet der Angreifer z.B. über ein derzeit im Unternehmen laufendes Projekt, wird der Anruf für den Betroffenen glaubhafter.

2.1.7 Datenverlust

Wir sind für unsere Daten verantwortlich. Dies gilt vor allem für den heimischen Computer. Eine Festplatte kann kaputt gehen. Eine externe Festplatte hat eine maximale Lebensdauer von 10 Jahren. Eine eingebaute, interne Festplatte in der Regel nur eine Lebensdauer zwischen 5 und 10 Jahren. Und auch die Lebensdauer eines USB Sticks ist begrenzt. Diese wird mit maximal 30 Jahren angegeben. Aber auf diese Werte sollten wir uns nicht verlassen. Gerade neuere SSD-Festplatten sowie USB-Sticks haben eine begrenzte Anzahl von Schreibzyklen. Das bedeutet, je häufiger sie benutzt werden, desto kürzer ist die Lebensdauer.

Regelmäßige Backups der eigenen Daten sind extrem wichtig. Und wir sollten uns über das Thema Gedanken machen bevor es zum ersten Datenverlust kommt. Jeder, der einmal seine Festplatte mit den Urlaubsbildern der letzten Jahre verloren hat, weiß wie sich das anfühlt. Leider machen wir uns immer erst über das Thema Datensicherung Gedanken wenn es bereits zu spät ist. Zwar ist es mit ein wenig Glück noch möglich zerstörte Daten auf einer Festplatte zu retten, doch ist eine solche Wiederherstellung recht teuer und ein Erfolg kann nicht garantiert werden. Daher hilft nur ein funktionierendes Backup-Konzept.

Auch unsere Daten in der Cloud sind nicht vor Verlust geschützt, wie der Vorfall im Straßburger Rechenzentrum des Unternehmens OVH im März 2021 zeigte. Durch einen Großbrand wurde ein fünfstöckiges Rechenzentrum mit Platz für rund 12.000 Server völlig zerstört. Insgesamt 3,6 Millionen Websites verschwanden dadurch aus dem Netz. Wer kein zusätzliches Backup seiner Daten angelegt hat, verlor seine Daten unwiderruflich. Ein solcher Großbrand ist natürlich eher die unglückliche Ausnahme, zeigt aber wie schnell es zu einem Datenverlust kommen kann.

Wir sind für unsere Daten verantwortlich. Und über die Sicherheit unserer Daten müssen wir uns Gedanken machen, bevor es zu einem Datenverlust kommt. Ansonsten wird uns eine alte Weisheit aus dem IT-Bereich zugerufen werden:
Kein Backup? Kein Mitleid!

2.2 Unsere Daten im Netz

Bei allen unseren Aktivitäten hinterlassen wir Spuren. Wenn wir im Internet surfen, erzeugen wir einen digitalen Fußabdruck. Selbst beim Aufruf einer einfachen Website, tauscht unser Browser Informationen mit der von uns besuchten Website aus: Informationen über unsere IP-Adresse, dem von uns verwendeten Browser, ob wir ein Tablet oder einen Computer nutzen, von welcher Marke dieser ist, und vieles mehr. Diese Informationen mögen uns auf den ersten Blick nicht wichtig erscheinen, aber sie liefern genügend Material, um erste Rückschlüsse auf unsere Person zu ziehen. Werden über sogenannte Cookies Informationen über mehrere von uns besuchten Webseiten hinweg gesammelt, können diese Daten dazu genutzt werden, ein konkreteres Bild von uns zu zeichnen.

"Was habe ich zu verbergen?" ist meist die erste Reaktion auf diese Tatsache. Und sicherlich sind einzelne Informationen für sich genommen nicht entscheidend. Aber wenn viele Informationen über einen längeren Zeitraum gesammelt und mit verschiedenen Datenquellen verknüpft werden, erhält man schnell ein komplexes Bild einer Person. Dies reicht von den Vorlieben bis hin zu ihren politischen Ansichten. Wenn diese Informationen verwendet werden, um Werbung anzuzeigen, die auf unsere individuellen Bedürfnisse zugeschnitten ist, mag uns das nicht stören. Aber was ist, wenn diese Daten genutzt werden, um unsere Person zu bewerten, beispielsweise um unsere Kreditwürdigkeit einzustufen? Selbst wenn die vorliegenden Informationen über uns nicht korrekt sein sollten: Sind wir erst einmal automatisch in eine Schublade gesteckt worden, kommen wir dort nur schwer wieder heraus. Die Frage die wir uns stellen sollten ist demnach eher: “Was offenbare ich über mich?”

Malte Spitz, deutscher Politiker und Aktivist bei "netzpolitik.org", wagte im Jahr 2009 ein Experiment: Er verschaffte sich Zugang zu den Daten seines Mobilfunkanbieters. Im Zeitraum von August 2009 bis Februar 2010 gab sein Handy mehr als 35.000 Mal Informationen preis. Jede davon ist für sich genommen unbedeutend und harmlos. In Zusammenarbeit mit der Zeitung "Die Zeit" wurden die Daten jedoch mit öffentlich im Netz verfügbaren Informationen (z.B. Nachrichten auf Twitter, Blogbeiträge etc.) angereichert. So entstand ein klares Bild der Person Malte Spitz: Gewohnheiten und Vorlieben werden plötzlich deutlich und lassen Rückschlüsse auf seine Person und sein Privatleben zu. [24]

Dieses Beispiel zeigt, was Daten über uns verraten und was mit der Analyse von Daten möglich ist. Und je mehr Daten über uns gesammelt werden, desto genauer und detaillierter wird das Profil, das ohne unser Wissen über uns erstellt werden kann.

Längst gibt es Angebote, die uns bewusst eine Gegenleistung für die Übermittlung unserer Daten anbieten. Krankenkassen bieten beispielsweise Tarife an, in denen wir einen Bonus erhalten können, wenn wir regelmäßig unsere Gesundheitsdaten übermitteln und damit z.B. nachweisen können, dass wir uns in einem bestimmten Umfang bewegt haben. Daten sind zu einem wichtigen Rohstoff geworden. Durch die Sammlung von Daten und das Verknüpfen von verschiedenen Datenquellen, lassen sich neue Erkenntnisse gewinnen. Welche Nutzungsmodelle existieren für unsere Daten? Können Daten auch gegen uns verwendet werden? Nur wenn wir die Mechanismen

und Auswirkungen von solchen Datenauswertungen kennen, ist es uns überhaupt möglich Risiken zu erkennen und eigenverantwortlich und selbstbestimmt mit unseren Daten umzugehen.

2.2.1 Der Wert unserer Daten

Warum sollte jemand an meinen Daten interessiert sein?
Zunächst einmal benötigen bestimmte Stellen bestimmte Informationen aus unterschiedlichen Gründen. Ein Einzelhändler braucht meine Adresse, um mir Waren schicken zu können. Bei meinem Sportverein hinterlasse ich meine Telefonnummer, damit ich in dringenden Fällen erreicht werden kann.
Es gibt aber auch Daten, die automatisch über mich gesammelt werden: Meine Bank kennt die Bewegungen auf meinem Konto, mein Mobilfunkanbieter speichert die Rufnummern, die ich anrufe und die mich anrufen, sowie die Gesprächsdauer und auch meine Standortdaten. In die meisten dieser Verarbeitungen habe ich eingewilligt, als ich einen Vertrag mit dem jeweiligen Anbieter abgeschlossen habe. Was mit den Daten geschieht, ist uns in der Regel nicht bekannt. Die Verarbeitung meiner Daten muss auch nicht immer zu meinem Nachteil sein. Ich beschwere mich vielleicht nicht bei meinem Lieblings-Onlineshop, wenn dieser mir auf Basis meiner bisherigen Einkäufe und des Vergleichs mit anderen Kunden passende Artikel vorschlägt.
Je mehr Daten ein Unternehmen über mich gesammelt hat, desto konkreter lassen sich Rückschlüsse auf meine Person ziehen und desto wertvoller sind diese Daten. Dieser Wert wird meist deutlich, wenn ein Unternehmen verkauft wird oder an die Börse geht. Facebook hat bei der Übernahme von WhatsApp umgerechnet 55 US-Dollar pro Nutzer bezahlt. Bei Instagram waren es nur knapp 20 US-Dollar. Beide Dienste sind kostenlose nutzbar.
Und auch Google verdient 34 Dollar pro Nutzer und Quartal.[25] Und das, obwohl wir für die Nutzung von Googles Diensten nichts bezahlen. Wie funktioniert das?
Die Antwort liegt in der Werbung. Im Jahr 2019 machte Facebook allein mit Werbung 69,66 Milliarden Dollar Umsatz.[26] Google sogar von über 130 Milliarden.[27] Das liegt vor allem an den Daten, die über uns gesammelt werden. Je mehr Daten wir über uns preisgeben, desto konkreter können sich Unternehmen ein Bild von uns machen. Dies wiederum ermöglicht es ihnen, auf uns zugeschnittene Werbung zu verkaufen. Sie sind ein Unternehmen und wollen Werbung in der Zielgruppe der alleinstehenden jungen Frauen zwischen 25 und 29 Jahren mit einem bestimmten Durchschnittseinkommen schalten? Kein Problem!
Es geht aber nicht immer nur um Werbung. Navigationsgeräte übermitteln ihre Position an die Zentrale, die dann die Stauwahrscheinlichkeit vorhersagt und die entsprechende Warnung auf unserem Display anzeigt. Betreiber von Internetanwendungen beobachten das Nutzerverhalten und wissen so, wann die Dienste von vielen Menschen genutzt werden. Entsprechend können diese Daten genutzt werden, um zu Spitzenzeiten mehr Rechenkapazität bereitzustellen. All dies basiert auf den beobachteten Nutzerdaten.
Für uns ist es schwierig, den einzelnen Daten einen konkreten Wert zuzuordnen. Was ist das Bewegungsprofil wert, das mein Smartphone automatisch erstellt? Welchen

Tipp
Wieviel sind unsere Daten Wert? Die Webseite der Financial Times zeigt es auf (in englischer Sprache) https://ig.ft.com/how-much-is-your-personal-data-worth/

Wert hat es, zu wissen, mit wem ich in den letzten Monaten regelmäßig E-Mail-Kontakt hatte? Der Wert von Daten ist nicht universell und sehr abstrakt. Er ist stark von der Qualität und dem Zweck und anderen Umständen abhängig. Daten sind daher eher wie Rohstoffe. Wir müssen uns im Klaren darüber sein, dass unsere Daten für andere wertvoll sein können.

Bereits 2013 zeigte eine Studie, dass es möglich ist, anhand von leicht zugänglichen Informationen wie Facebook-Likes Rückschlüsse auf hochsensible persönliche Eigenschaften einer Person zu ziehen. Sei es die sexuelle Orientierung, die ethnische Zugehörigkeit, religiöse und politische Ansichten, Alter, Geschlecht und andere Persönlichkeitsmerkmale. Die Forscher waren in der Lage, psychodemografische Profile auf Basis von Facebook-Likes zu erstellen. Das Modell konnte in 88% der Fälle korrekt zwischen homosexuellen und heterosexuellen Männern und in 85% der Fälle zwischen Demokraten und Republikanern unterscheiden.

Wieviel sind unsere Daten Wert? Die Webseite der Financial Times veranschaulicht das an einem eigenen Konfigurator.
Quelle: https://ig.ft.com/how-much-is-your-personal-data-worth/ (englische Sprache)

2.2.2 Nichts ist umsonst - wir tauschen Leistung gegen Daten

Zu Beginn der Popularisierung des Internets in unseren Haushalten nutzten wir das Internet, um die Nachrichten und Zeitschriften zu lesen. Wir konnten Informationen erhalten, ohne zu bezahlen, anstatt zum Kiosk zu gehen und eine Zeitung zu kaufen. Seitdem sind die gedruckten Zeitungen immer weniger geworden, was das traditionelle Geschäftsmodell in Gefahr brachte. Es war zwar schön, kostenlos Informationen online zu bekommen, aber es war kein nachhaltiges Geschäftsmodell für die Medienunternehmen.

Wir wachsen mit dem Internet auf und haben uns daran gewöhnt, Dinge kostenlos zu bekommen, und dann dachten wir, dass es so sein sollte. Nichts könnte weiter von der Realität entfernt sein, und jetzt sehen wir uns damit konfrontiert, wie Medienunternehmen zum Erhalt der Qualität verlangen, dass wir einige Abschnitte der Website abonnieren, oder sie begrenzen die Menge der Seiten, auf die wir online zugreifen können.

Auch Wikipedia bittet darum zu Spenden - wahrscheinlich kennen Sie ein Banner, das einmal im Jahr während einiger Tage auf Wikipedia erscheint:

Eine Bitte um Spenden auf der Webseite www.wikipedia.org

Sofern wir es als Internetnutzer möchten, auch weiterhin jederzeit zu qualitativ hochwertige Nachrichten Zugang zu haben, müssen wir uns von der weithin existierenden Haltung verabschieden, dass Nachrichten im Internet kostenlos sein müssen. Verlagen bleiben sonst nur die Möglichkeiten, sich in finanzielle Abhängigkeiten zu begeben - dies widerspricht aber dem Grundsatz des "unabhängigen Journalismus", oder die Qualität des Angebots zu reduzieren. Aktuell beobachtet man beispielsweise, dass Nachrichtenportale vermehrt Nutzer mit aktivierten AdBlockern aussperren - dies sind Zusatzprogramme, die Werbeanzeigen unterdrücken. Denn wie sollen die Redaktionen ihre Arbeit finanzieren, wenn selbst die Einnahmequelle der Werbung wegfällt? Es ist zu erwarten, dass wir in naher Zukunft nur noch einen Bruchteil der Nachrichten frei werden lesen können, und für alle weiteren Beiträge mindestens ein Login bei deaktiviertem Werbeblocker, oder aber ein Abo erforderlich sein werden. Die freie Presse ist die vierte Gewalt in einer Demokratie - wir sollten uns fragen, was uns diese wert ist, und wie viel wirtschaftlichen Druck wir dieser wichtigen Instanz aufschultern wollen

2.2.3 Metadaten

Metadaten enthalten zusätzliche Informationen über Merkmale von Daten. So gehören zu den Metadaten eines Buches der Name des Autors, die ISBN-Nummer sowie Erscheinungsjahr und Auflage. Das sind Informationen die dem Buch als Objekt zuzuordnen sind aber nicht den Inhalt des Buches beschreiben. Im Digitalen bleiben uns Metadaten meist verborgen. Sind sind zum Beispiel in den Dateien versteckt. So enthält die Datei eines digitalen Fotos neben Angaben zur Kamera mit der es aufgenommen wurde, sämtliche technischen Einstellung der Aufnahme (z.B. Angaben zur Brennweite, ISO, Belichtungszeit) sowie Angaben zum Zeitpunkt und Ort der Aufnahme (wenn bei der Aufnahme ein GPS-Signal vorhanden war). All diese Informationen werden automatisch in der Bilddatei gespeichert. Wenn wir telefonieren erfährt unser Telefonanbieter unter anderem unseren Standort und den Standort unserer Gesprächspartners wie auch die Dauer des Gesprächs. Und auch wenn wir bloß eine Webseite aufrufen, werden Informationen über uns über unseren Browser übermittelt. [28]

Unter Metadaten im Kontext unserer Daten im Internet verstehen wir die Bestands- und Verkehrsdaten eines Nutzers.

- Bestandsdaten: Dies sind die Daten, die ein Telefon- oder Internetanbieter, teilweise dauerhaft, über seine Nutzer speichert. Dies können sein: Adresse, Kontodaten, IP-Adressen, Passwörter, Telefonnummern sowie alles, was zur Erbringung der Leistung erforderlich ist.
- Verkehrsdaten: Dies sind Daten die anfallen, wenn ein Dienst genutzt wird, und normalerweise nach einem bestimmten Zeitraum wieder gelöscht werden müssen. Dazu gehören beispielsweise mit wem ich mich per Telefon oder Internet verbunden habe, welchen Browser ich verwendet habe oder zu welcher Uhrzeit dies stattgefunden hat.

Und gerade die Verkehrsdaten sagen mehr über uns, als wir vielleicht vermuten - im speziellen der verwendet Browser mit der Konfiguration und dem Standort, den wir auf Basis unserer IP automatisch mit übertragen. Im schlimmsten Fall kann eine Webseite beispielsweise erkennen, dass wir das letzte Sicherheitsupdate noch nicht durchgeführt haben und gerade eine Schwachstelle offenbaren. Letztendlich ist es sogar recht wahrscheinlich, dass wir alleine mit unserem Browser so viele Informationen übertragen, dass wir bereits eindeutig identifizierbar sind.
Getestet werden kann dies mit dem Test “Cover Your Tracks” der “Electronic Frontier Foundation”. Dieser überprüft die vom Browser übertragenen Metadaten und ermittelt, ob es sich hierbei um eine tendenziell einmalige Kombination handelt. Interpretiert werden beispielsweise die übermittelte Zeitzone, die installierten Browser-Plugins, die Bildschirmgröße, die installierten Schriftarten, die eingestellte Sprache, das Betriebssystem, der verfügbare Speicherplatz, JavaScript-Unterstützung - und das sind nur einige der Parameter. Das ernüchternde Resultat: Bereits die Metadaten unseres Browsers reichen aus, um uns eindeutig wiederzuerkennen.

2.2.4 Cookies

Seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) im Jahre 2018 müssen Webseiten ihre Besucher über die verwendeten Cookies und deren Zwecke informieren, zu denen diese vom Webseitenbetreiber eingesetzt werden. Daher kamen die meisten Internetnutzer sicherlich schon mit dem Begriff "Cookies" in Kontakt, dabei wissen vermutlich nur die wenigsten, um was es sich hierbei handelt und welchen Zweck diese haben.

Im Speicher des Browsers können von Webseiten Cookies abgelegt werden. Die Abbildung zeigt den Applikationsbereich des Google Chrome Browsers nach einem einmaligen Besuch der Google Startseite.

Cookies sind kleine Textdateien, die von Webseiten im Browser des Besuchers gespeichert werden. Die grundlegendste Verwendung von Cookies ist die Nachverfolgung unserer Aktivitäten innerhalb der gerade aufgerufenen Webseite. Für den Betreiber der Webseite sind dies wertvolle Informationen. Diese zielen nicht darauf ab, unsere Interessen zu sammeln und weiterzugeben, sondern vielmehr möchte der Webseitenbesitzer wissen, welche Seiten seines Onlineangebots am häufigsten besucht werden, wann Besuchende wiederkehren, wie viele Minuten auf der Webseite verbracht werden oder welches die letzte Seite war, die wir besucht haben. Hierbei handelt es sich in der Regel um statistische Informationen, die keine tieferen persönlichen Informationen ermitteln. Viele Cookies sind somit harmlos und eine Unterstützung für den Webseitenbetreiber, sein Angebot nutzerfreundlicher gestalten zu können.

Es gibt auch "technisch notwendige" Cookies, die beispielsweise dazu verwendet werden, um in einem Online-Shop den Bestellvorgang durchzuführen. Hierbei merkt sich die Webseite über den Cookie temporär den Benutzer und die Produkte im Warenkorb um zu einem späteren Zeitpunkt darauf zurückgreifen zu können. Auch Informationen, wie beispielsweise die eingestellte Sprache oder andere vorgenommene Grundeinstellungen können über den Cookie gespeichert werden.

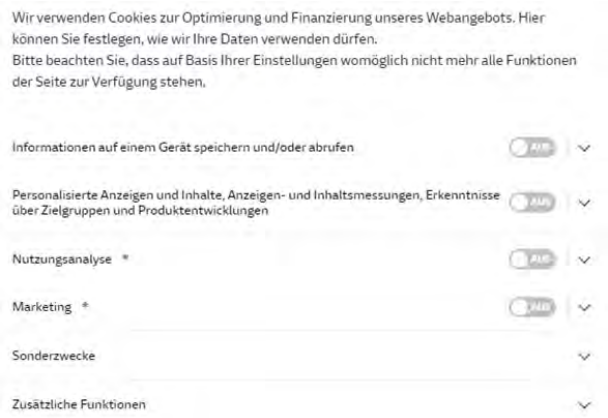
Letztlich werden Cookies aber auch dazu verwendet um unser Surfverhalten nachzuverfolgen.

So können unsere Suchanfragen in Suchmaschinen oder Onlineshops gespeichert werden. Suchen wir nach einem Hotel in Paris oder nach einem neuen Kühlschrank, werden wir feststellen, dass wir plötzlich auch auf anderen Webseiten Werbeanzeigen angezeigt bekommen, die sich auf dies Informationen beziehen. Hierbei handelt es sich um Cookies mit dem Verwendungszweck der so genannten "Personalisierten Anzeigen und Inhalte".

Cookies ermöglichen es also, uns anhand des Browsers und den darüber verfügbaren Informationen zu identifizieren - genauer gesagt: Unsere bisherigen Aktionen zu erkennen.

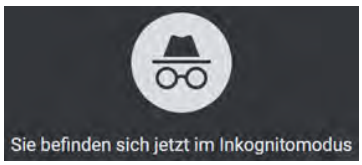
Ob wir Nachrichten lesen, Produkte kaufen oder nach Informationen suchen, soweit Webseiten Cookies auf unserem Gerät speichern, können dieses Informationen - unsere Zustimmung vorausgesetzt - an so genannte Werbenetzwerke (Ad-Networks) weitergereicht werden. Diese Netzwerke bieten, basierend auf unseren Daten, Werbetreibenden die Möglichkeit uns gezielt personalisierte Inhalte und Werbung anzeigen zu können.

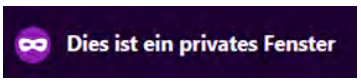
Die meisten aller Webseiten im Internet nutzen Cookies. Seit der Einführung der DSGVO müssen uns alle Webseiten über die Verwendung von Cookies informieren und unsere Einwilligung zur Verarbeitung unserer Daten einholen. Daher werden wir auf Webseiten zunächst nach unserer Zustimmung zur Verwendung von Cookies gefragt. Die Webseitenbetreiber kommen war somit ihrer Verpflichtung nach, für uns ist es aber weiterhin nicht immer ersichtlich welche Daten von uns beim Besuch der Webseite erhoben werden und was mit ihnen geschieht. Wer sich einmal die Mühe gemacht hat, bei einem sogenannten Cookie-Banner sich die Details anzeigen zu lassen, wird feststellen, dass eine spezifische Freigabe unserer Informationen durchaus möglich ist. Allerdings ist die Handhabung meist kompliziert. Daher klicken viele die entsprechenden Meldungen weg und akzeptieren somit in der Regel den Einsatz der Cookies. Aber wissen wir hierbei eigentlich zu was wir zugestimmt haben?



Cookie-Informationen auf einem Nachrichtenportal (sz.de - Screenshot vom 30.3.21). Die DSGVO verlangt, dass über die Verwendungszwecke von Cookies transparent informiert wird.

Wenn wir darauf bedacht sind, die Menge an übermittelten Informationen zu reduzieren, ist ein möglicher Schritt der sogenannte Privat- oder Inkognito-Modus unserer Browsers.





Links: Inkognito-Symbol in Google Chrome
Rechts: Privates Fenster in Firefox

Google Chrome und Firefox bieten eine sehr einfache Möglichkeit, ein Inkognito-Fenster bzw. ein privates Fenster zu öffnen. In diesem Modus werden alle Cookies und im Browser gespeicherten Daten entfernt, sobald wir das Fenster schließen. Jedoch bedeutet dies nicht, dass wir völlig anonym surfen: Jede Information, die wir über eine Webseite übermitteln (E-Mail Adresse, Kreditkartendaten, usw.) oder in einem authentifizierten Kontext besuchen kann trotzdem potenziell mit unserer Person in Verbindung gebracht werden. Inkognito bedeutet in diesem Zusammenhang lediglich, dass alle Informationen, die der Browser über uns preisgeben kann, beim Schließen automatisch gelöscht werden.

Ein Beispiel: Sie wollen Ihren Lebensgefährten mit einer Reise überraschen und suchen hierfür über das Internet ein Hotel. Wenn Sie dies über ein privates Fenster machen, bleibt Ihre Buchung zwar gültig - denn hierbei haben Sie sich authentifiziert und beispielsweise Kreditkartendaten übertragen - jedoch kann Ihr Suchverlauf nicht mehr nachvollzogen werden:

Die Spuren zur Suche sind verwischt, und die Überraschung wird zumindest auf diesem Wege nicht verraten.

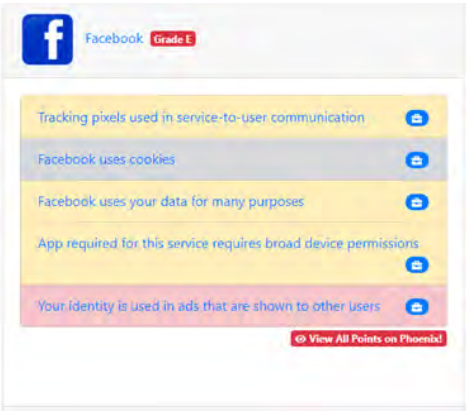
2.2.5 Nutzungsbedingungen - Informierte Einwilligung?

Beim Anlegen eines Benutzerkontos, bei der Installation eines Programms oder einer App erscheint ein langer Text, den wir akzeptieren sollen, um das Programm nutzen zu können. Das sind je nach Rechtslage des Programms die Nutzungsbedingungen oder die Allgemeinen Geschäftsbedingungen. Rein rechtlich sind diese Dokumente von hoher Bedeutung, denn sie regeln die zur Verfügung gestellten Leistungen sowie die Rechte und Pflichten zwischen Anbieter und Konsument. Laut Statista dauert das Lesen der Nutzungsbedingungen prominenter Internetanwendungen bis zu 27 Minuten - ob sie dabei auch verstanden werden können und wir daraufhin eine fundierte Entscheidung treffen können, ist hierbei nicht eingerechnet. Zudem bleibt uns letztlich auch keine Wahl den Nutzungsbedingungen zuzustimmen, wenn wir die Software nutzen wollen. Generell fordert der Gesetzgeber, dass die Formulierung der Bedingungen klar und verständlich sein müssen. Aber wissen wir eigentlich, wozu wir unser Einverständnis geben? Wer hat jemals die Nutzungsbedingungen einer Software oder App gelesen?

Als Aprilscherz schrieb die Firma Gamestation am 1. April 2010 in ihre AGB: ***"Indem Sie am ersten Tag des vierten Monats des Jahres 2010 Anno Domini eine Bestellung über diese Website aufgeben, erklären Sie sich damit einverstanden, uns eine nicht übertragbare Option zu gewähren, Ihre unsterbliche Seele für jetzt und für immer zu beanspruchen. Sollten wir diese Option ausüben wollen, erklären Sie sich damit einverstanden, Ihre unsterbliche Seele und jeden Anspruch, den Sie darauf haben, innerhalb von 5 (fünf) Arbeitstagen nach Erhalt einer schriftlichen Benachrichtigung von gamestation.de oder einem seiner ordnungsgemäß autorisierten Untergebenen aufzugeben."*** Hierdurch besitzt Gamestation theoretisch nun die Seelen von 7.500 Kunden. Amazon nutzte bei der Einführung seiner neuen Spiele-Engine Lumberyard deren AGB zu Marketingzwecken. In der US-Version der AGBs verwies das Unternehmen darauf, dass bestimmte Nutzungsbeschränkungen im Falle einer Zombieapokalypse entfallen. Der Abschnitt versteckte sich gegen Ende der über 50 Seiten umfassenden Nutzungsbedingungen des Amazon Webservices (AWS).

Angenommene Lesedauer prominenter Nutzungsbedingungen:
Quelle: https://de.statista.com/infografik/21430/lesedauer-der-nutzungsbedingungen-ausgewaehlter-internetunternehmen/

Natürlich gibt es auch viele positive Beispiele, in denen Nutzungsbedingungen verständlich beschrieben sind - auch wenn sie sehr lang sein mögen. Es gibt aber auch viele Anwendungen, bei denen es über die Nutzungsbedingungen nur schwer ersichtlich ist, was in dem Vertrag zwischen Betreiber und uns, dem Konsumenten, eigentlich rechtlich gültig vereinbart wird. Initiativen wie "Terms of Service; Didn´t Read" versuchen die Nutzungsbedingungen verständlich zu erklären, so dass Nutzer schnell eine Übersicht bekommen, zu was sie gerade zustimmen oder eventuell bereits in der Vergangenheit zugestimmt haben.



Bewertung der Nutzungsbedingungen auf "Terms of Service; Didn´t Read" am Beispiel von Facebook. Quelle: https://tosdr.org/en/service/182 (zuletzt besucht am 30.3.21)

Leider gibt es keine einfache Lösung für das Problem der unverständlichen Nutzungsbedingungen - außer einer aufwändigen Auseinandersetzung mit dem geschrieben Werk. Wenn wir die App oder den Dienst nutzen wollen, müssen wir den Nutzungsbedingungen zwingend zustimmen. Daher akzeptieren die meisten Nutzer ohne genauere Kenntnis darüber, zu was sie gerade ihre Einwilligung gegeben haben. Wir können zumindest am Ende darauf vertrauen, dass Gesetzgeber und Aufsichtsbehörden uns Verbraucher vor missbräuchlichen Bedingungen schützen.

Darüber hinaus gibt es diese weiteren Empfehlungen zum Umgang mit Nutzungsbedingungen:

- Wir sollten nach Möglichkeit nur Apps und Diensten, von denen wir wissen, dass sie eine hohe Nutzerzahl haben, vertrauen. Dies ist kein umfänglicher Schutz vor unangemessenen Nutzungsbedingungen, aber zumindest ist es bei großen Unternehmen und Dienstleistern wahrscheinlicher, dass diese regelmäßig von Aufsichtsbehörden kontrolliert werden.
- Kostenlose Dienste oder Programme werden vermutlich tatsächlich nichts kosten, aber sofern es sich nicht um öffentlich bereitgestellte Anwendungen handelt, wird sich der Dienst auf einem anderen Wege monetarisieren, möglicherweise über Werbung oder Weitergabe unserer Daten. Hier ist Vorsicht angebracht.
- Im Verdachtsfall kann eine schnelle Suche im Internet durchgeführt werden. Hören wir beispielsweise davon, dass zu Facebook hochgeladene Bilder automatisch das Eigentum von Facebook werden, können wir dies relativ einfach

herausfinden. Beispiel: Suchen Sie nach "Facebook use of images property" und Sie erhalten die entsprechende Information darüber, dass dies tatsächlich der Fall ist.

Ein sehr kritisches Beispiel für die Ausnutzung der Unwissenheit um Nutzungsbedingungen wurde Anfang 2018 durch die New York Times veröffentlicht. Dabei ging es um die Software "Alphonso". Diese Software lauschte Nutzer aus, indem sie über das Mikrofon des Smartphones Informationen darüber sammelte, welche Werbespots im Umfeld zu hören waren. Zum Zeitpunkt des Berichts war die Software bereits in rund 1000 Smartphone-Apps integriert (darunter allein 250 Spiele). Und natürlich war "Alphonso" in der Lage, mehr als nur Werbespots zu belauschen. [29] Der Geschäftsführer des Unternehmens war der Meinung, dass die Überwachung durch Alphonso zulässig sei, weil die Nutzer die Nutzungsbedingungen wissentlich akzeptiert hätten.

2.2.6 Social-Credit-Systeme

In der Volksrepublik China wird derzeit ein nationales Social-Credit-System aufgebaut, das ursprünglich bereits im Jahre 2020 landesweit eingeführt werden sollte. Kern des Projekts ist ein punktebasiertes Bewertungssystem, das Bewohnern einen Punktewert zuweist. Das System zielt darauf ab, die Bürger zu systemkonformen und vorbildlichen Verhalten zu erziehen. Wer sich richtig verhält, sich an Regeln hält, bekommt Punkte gutgeschrieben. Schlechtes Verhalten - aus Sicht der Regierung - wiederum wird mit einem Punktabzug bestraft. Mit einer höheren Bewertung schalten die Bürger bestimmte Vorteile frei wie beispielsweise Zugang zu besseren Schulen oder Arbeitsplätzen, besserer Gesundheitsversorgung oder auch Vergünstigungen im öffentlichen Nahverkehr.

Ein solches System ist jedoch nur durch ein umfangreiches Monitoring und die Zusammenführung verschiedener Datenquellen möglich. Zu diesem Zweck hat die Chinesische Regierung Lizenzen an acht große Unternehmen vergeben, darunter Big Player wie die Plattform Alibaba.com und Tencent (das chinesische Facebook). Wichtige Bewertungsfaktoren sind derzeit die Kredithistorie und das Konsumverhalten (online und offline) sowie Aktivitäten und Regelverstöße in sozialen Medien. Ebenso eine Rolle spielen das eigene Vorstrafenregister und das Verhalten im Straßenverkehr.

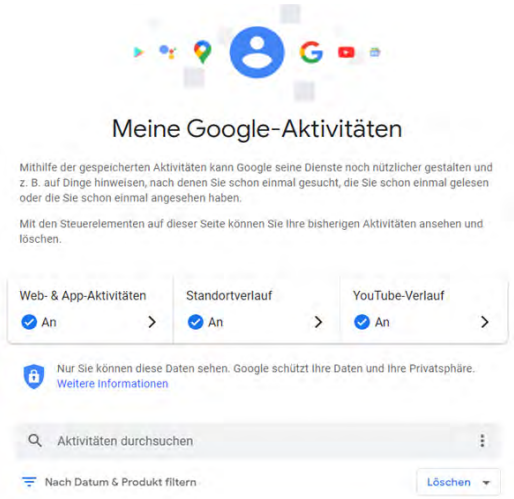
Seit 2017 werden einzelne Pilotprojekte in verschiedenen Städten durchgeführt und auch wenn noch kein konkreter Termin für die landesweite Einführung feststeht, ist dies nur eine Frage der Zeit.

2.2.7 Beispiele Google & Facebook - Was sie über uns wissen

Beispiel Google

Im Zusammenhang mit Google wir meist der Begriff der “Datenkrake” verwendet. In der Tat speichert Google sehr viele Informationen über uns. Unsere Suchanfragen, Interessen, Standorte, welche Webseiten wir besucht haben und welche Youtube-Videos wir uns angesehen haben werden zumindest bei der Nutzung eines aktiven Google-Account gespeichert. Um einen Eindruck davon zu gewinnen welche Informationen Google von uns gespeichert hat, genügt es, im eigenen Google-Account einen Blick in den Bereich “My Google Activity” zu werfen. Viele Informationen werden von Google zur Verbesserung der Funktionen und zur Lösung von Nutzerproblemen gesammelt und analysiert. Das Unternehmen generiert aber nach wie vor einen großen Teil seines Umsatzes mit Werbeflächen und der Möglichkeit für Werbetreibende, personalisierte Werbung platzieren zu können.
Ein Blick in das eigenen Google Konto lohnt sich also...

Google Activity - Ich weiß, wonach Du letzten Sommer gesucht haben...
Nach welchen Stichworten habe ich gesucht? Welche Videos habe ich mir auf YouTube angesehen? Die Aktivitätsübersicht bietet einen Überblick. Hier kann die Speicherung von Aktivitäten teilweise verhindert werden und einzelne Aktivitäten können gelöscht werden. Wir können sogar nach einer bestimmten Aktivität aus der Vergangenheit suchen.



https://myactivity.google.com/myactivity

Einstellung für Werbung - Wie wird Werbung über Google personalisiert?
Hier können wir uns einen Einblick in die personenbezogenen Informationen, die Google über uns gesammelt hat, verschaffen. Diese Informationen generiert Google nicht nur über die eigenen Services, sondern ist als Teil eines größeren Werbenetzwerkes auch Empfänger von Informationen, die auf anderen Webseiten angegeben oder ermittelt wurden.

https://adssettings.google.com/authenticated

Google Standortverlauf: Dies sind die Orte, die ich besucht habe

Ein Android-Smartphone kann den Standort des Geräts ermitteln und an Google senden, sofern die Funktion nicht in den Geräteeinstellungen deaktiviert ist. Die Ansicht zeigt die gemeldeten Standorte auf einer Karte und mit einer Zeitleiste an.
https://www.google.com/maps/timeline

Google-Berechtigungen - Wer hat Zugriff auf mein Konto?

Viele Tools und Dienste können mit Google verknüpft werden und erhalten dadurch Zugriff auf individuelle Profilinformationen und Google-Funktionen. Unter diesem Menü können wir überprüfen, welche Tools aktuell Zugriff auf unser Google-Konto haben und bei welchen Diensten wir uns mit meinem Google-Konto angemeldet habe.
https://myaccount.google.com/permissions

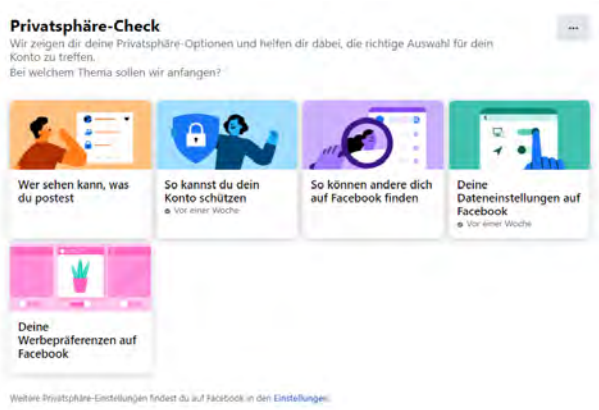
Beispiel Facebook: Einstellung der Privatsphäre

Facebook steht im Umgang mit den Daten seiner Nutzerinnen und Nutzern seit Jahren in Kritik. Das Unternehmen erscheint stets bemüht an dieser Stelle nachzubessern, und stellte seinen Nutzern in den vergangen Jahren vermehrt Datenschutzeinstellungen zur Verfügung. Da Facebook aber seinen Umsatz ausschließlich über den Verkauf von Werbeanzeigen generiert, ist davon auszugehen, dass das Unternehmen weiterhin die Daten seiner Anwenderinnen und Anwendern nutzt. Trotzdem sollte jeder Einzelne zumindest einmal die Einstellungen zu Datenschutz und Privatsphäre durchgehen.

Facebook bietet umfassende Konfigurationsmöglichkeiten in den Kontoeinstellungen, bietet aber auch die Möglichkeit, eine schnelle Überprüfung unserer Datenschutzeinstellungen vorzunehmen.

Der Privatsphären-Check findet sich unter.

https://www.facebook.com/privacy/checkup



Optionen auf https://www.facebook.com/privacy/checkup

Der Privatsphären-Check bietet und folgende Optionen:

- "Wer sehen kann, was du postest": Normalerweise sind der Name, der Wohnort, das Studium oder die Arbeit öffentlich, damit andere Personen nach uns suchen können. Andere Daten, wie die Handynummer oder das Geburtsdatum, sollten privat sein.
- "So kannst du dein Konto schützen": Dies sind die Möglichkeiten das Passwort zu ändern, oder zu entscheiden, wie Facebook uns benachrichtigen soll, wenn sich jemand an einem Ort, der Facebook nicht bekannt ist, bei unserem Konto anmeldet.
- "So können andere dich auf Facebook finden": Hier können wir den Personenkreis eingrenzen, der uns Freundschaftsanfragen senden kann. Und auch wenn unsere Mobiltelefonnummer oder E-Mail nicht sichtbar sind, können wir hier einstellen, ob andere Personen uns anhand dieser Daten suchen können.
- "Deine Dateneinstellungen auf Facebook": Hier werden Apps und Webseiten angezeigt, über die wir uns mit unserem Facebookaccount angemeldet haben. Entsprechende Verbindungen können hier auch wieder entfernt werden. Zudem kann hier die automatische Gesichterkennung aktiviert und deaktiviert

werden, mit der wir Facebook erlauben können, uns auf Fotos und in Videos zu erkennen.
- "Deine Werbepräferenzen auf Facebook": An dieser Stelle können wir festlegen, anhand welcher Profilinformationen Werbetreibende uns erreichen können. Auch können wir festlegen, wer unsere Aktionen auf Werbeanzeigen sehen kann.

Eine vollständige Liste aller Einstellungsmöglichkeiten findet sich in den Konto-Einstellungen: https://www.facebook.com/settings
Hier empfehlen wir, sich einmal Zeit zu nehmen und sich in Ruhe einmal durch alle Menüpunkte durch zu arbeiten. Es finden sich unter anderem folgende wichtige Einstellungsmöglichkeiten:

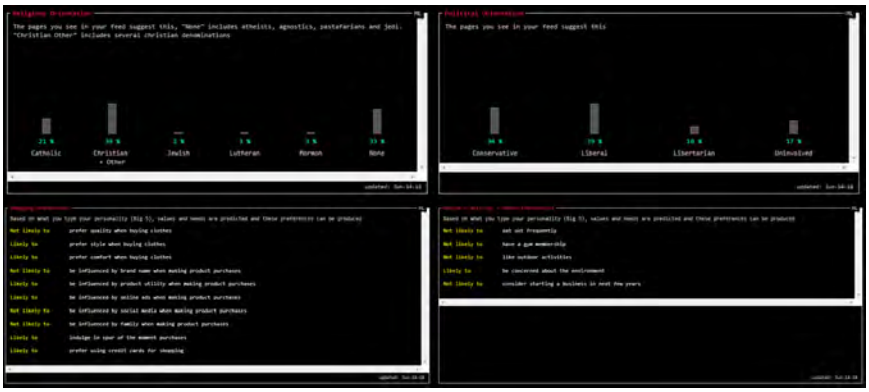
- Wer soll Zugriff auf mein Konto nach meinem Tod bekommen?
- Wer darf Nachrichten an meine Pinnwand schreiben? Wer darf mich markieren? Und möchte ich Beiträge, auf denen ich markiert bin, erst freigeben? All das findet sich in den Einstellung zu Profil und Markierungen (https://www.facebook.com/settings?tab=timeline)

Und wer einmal sehen möchte, welche Daten Facebook gesammelt hat, kann dies in dem Bereich "Zugriff auf deine Informationen" einsehen. (https://www.facebook.com/your_information/). Dort finden sich alle Beiträge, Fotos, Kommentare und sonstige Informationen, die über das eigene Profil seitens Facebook gespeichert wurde. Ganz interessant sind in diesem Zusammenhang der Bereich "Werbeanzeigen und Unternehmen". Hier finden wir Informationen zu Werbetreibenden, mit denen wir verknüpft wurden - sei es, weil wir eine Anzeige des entsprechenden Unternehmens geklickt haben oder die Unternehmen eine Liste mit Kontaktinformationen mit Facebook geteilt haben, die auch unsere Daten enthielt. Ein Blick in diese Liste lohnt sich.

2.2.9 Beispiel "Cambridge Analytica": Erstellung von Persönlichkeitsbildern

Cambridge Analytica war ein amerikanisches Unternehmen, das Insolvenz anmelden musste, nachdem bekannt wurde, dass es viele Millionen Facebook-Konten und deren Profilinformationen dazu verwendet hatte, Persönlichkeitsprofile zu erstellen und diese zur Platzierung von Wahlkampfwerbung zu verkaufen. Dies gilt als einer der bisher größten Datenschutzverstöße überhaupt. Cambridge Analytica nutzte einen Persönlichkeitstest, der auf der Grundlage von einigen wenigen Fragen bereits ein sehr genaues Bild der Interessen eines Nutzers ermitteln kann, insbesondere der politischen Interessen, und wie diese wiederum beeinflusst werden können. Diese Fragen wurden im typischen Stil von Facebook-Umfragen in einer App von den Nutzern beantwortet. Durch die Zustimmung der Nutzungsbedingungen erlaubten die Facebook-User dem Unternehmen auch Zugriff auf die Freundeslisten der Facebook-Profile. Somit war es Cambridge Analytica möglich nicht nur ein Profil der Nutzenden der Anwendung zu erstellen, sondern auch von ähnlichen Nutzern, die die App gar nicht verwendeten. Auf diese Weise entstand am Ende eine Datensammlung von über achtzig Millionen Datensätzen. Als Folge musste Facebook-Gründer Mark Zuckerberg vor dem US-Kongress Rede und Antwort stehen und die Reputation seines Unternehmens bekam einen wahrnehmbaren Dämpfer.

Generell sollten wir als Nutzer sehr vorsichtig sein, wenn uns auf werbefinanzierten Internetseiten und -portalen Umfragen begegnen. Denn beispielsweise wird durch das “Fünf-Faktoren-Modell”, bei dem es sich um ein Modell der Persönlichkeitspsychologie handelt, beschrieben, dass durch die Faktoren “Aufgeschlossenheit”, “Perfektionismus”, “Geselligkeit”, “Empathie” und “Labilität” bereits ein recht genaues Persönlichkeitsbild entworfen werden kann. Das Modell ist auch als “OCEAN-Modell” bekannt und war die Basis für den von Cambridge Analytica entwickelten Persönlichkeitstest. Dies sollten Besucher von Internetseiten im Hinterkopf behalten, wenn sie das nächste Mal auf einem Portal gefragt werden, welche Meinung sie zu einem Thema haben. Schnell ist hier eine Antwort gegeben, und genau so schnell ist damit beispielsweise das persönliche Maß an Empathie eingeordnet.



Simulation einer Datenverarbeitung von Cambridge Analytica: Es wird eine Vermutung über Ihre Religion, Persönlichkeit, Stimmung, Aktivität und politische Ausrichtung angestellt.

2.2.10 Beispiel "Strava"; Risiken bei öffentlichen Daten

Strava ist ein soziales Netzwerk, das von Läufern, Radfahrern und anderen Sporttreibenden verwendet wird. Über eine App können die sportlichen Aktivitäten aufgezeichnet und mit anderen geteilt werden. Gespeichert werden die zurückgelegten Strecken über GPS mit Distanz, Zeit und weiteren Details. Die App kann in Kombination mit weiteren Fitnessgeräten wie Garmin, Fitbit oder Jawbone genutzt werden, um die eigene Leistung zu überprüfen, und mit anderen Nutzenden zu vergleichen.
Im Januar 2018 veröffentlichte Strava eine sogenannten "Heatmap". Die Idee war, die in Strava aufgezeichneten Strecken anonymisiert auf einer Karte darzustellen. Als Basis dienten Daten aus Aktivitäten, die zwischen 2015 und September 2017 aufgezeichnet wurden. Laut eigenen Angaben waren das über eine Milliarde Aktivitäten, die 27 Milliarden Kilometer an gelaufenen, gejoggen oder geschwommenen Strecken abdeckten.
Durch das Übereinanderlegen der einzelnen Aktivitäten wurden Strecken, die öfters gelaufen wurden, heller dargestellt als weniger beliebte Strecken. Somit gab die Heatmap einen Einblick in die beliebtesten Strecken der Welt. Soweit so gut…
Leider führte dieses Vorhaben zu einem Sicherheitsrisiko für die in Syrien und Irak stationierten US-Einsatzkräfte. Der Strava Dienst ist auch sehr beliebt bei Angehörigen des US-Militärs. Das führte dazu, dass beliebte Laufrouten um US-Militärbasen sichtbar wurden und somit gerade in dünn besiedelten Regionen auch die Grundrisse der Basen. Auch wenn die Lage von Militärstützpunkten allgemein bekannt ist, zeigt die Heatmap, welcher der Stützpunkte am meisten genutzt wird und welche Routen die Soldaten nehmen.

Ausführlicher Bericht der BCC: https://www.bbc.com/news/technology-42853072
Original Twitter-Post: https://twitter.com/Nrg8000/status/957318498102865920

Dies zeigt, dass auch ohne böse Absicht Informationen an die Öffentlichkeit gelangen können, bzw. wie sich anhand unbedenklicher Informationen (anonymisierte Strava-Routen) plötzlich Rückschlüsse auf andere Informationen (Standort von Militärbasen und Versorgungsrouten) ziehen lassen.
Strava bietet in den Datenschutzeinstellungen die Möglichkeit, die Datenerfassung für die Heatmap explizit abzulehnen - auch für Aktivitäten, die nicht als privat markiert sind. Aber wer hätte schon im Vorfeld einen solchen Nebeneffekt einer netten Idee wie einer Heatmap für beliebte Sportstrecken voraussagen können.

3. Meine Daten, meine Rechte

3.1. Wem gehören meine Daten?

Zweifelsohne gehören unsere persönlichen Daten zunächst uns selbst. Und wir haben das Recht über die Verwendung und Veröffentlichung dieser Daten zu bestimmen. Aber gehören all meine Daten wirklich mir persönlich? Wir gehen immer davon aus, dass alle Informationen über mich mir gehören. Aber stimmt das? Was ist mit meiner Telefonnummer oder meiner E-Mail-Adresse? Sind diese wirklich mein Eigentum oder bleiben sie im Besitz des Anbieters, der mir diese Kennungen nur zur Verfügung stellt und mir nur Nutzungsrecht gewährt? Gehören die Nutzungsdaten, die ich z.B. bei der Internetrecherche hinterlasse, mir persönlich oder dem Anbieter, der sie sammelt? Diese Frage ist nicht einfach zu beantworten. Das Problem: Nach geltendem Recht kann Eigentum nur an körperlichen Gegenständen bestehen, Daten zählen leider nicht als geistiges Eigentum.

Auf der anderen Seite stellen Daten ein wertvolles Gut dar. Die Geschäftsmodelle vieler großer Internetunternehmen basieren auf Angeboten die sich durch die Daten der Nutzer finanzieren. Somit ist die Frage nach einem möglichen „Eigentum an Daten“ durchaus berechtigt. Wem gehören unsere Daten und wer darf diese nutzen?

Bei personenbezogenen Daten die eindeutig einer Person zuzuordnen sind, mag die Antwort noch recht einfach sein: Diese Daten dürfen nur aufgrund einer rechtlichen Grundlage verarbeitet werden. Wir haben zumindest ein Recht darauf zu erfahren, welcher Anbieter welche unserer Informationen gespeichert hat und wofür sie ver-

Meine Daten, meine Rechte		
Er/Sie kennt seine Rechte in Bezug auf seine personenbezogenen Daten und kann diese Rechte ausüben.		
Wissen	**Fertigkeiten**	**Kompetenz**
Er/Sie • kann die Grundprinzipien der europäischen Datenschutzgrundverordnung (DSGVO) benennen • kennt die eigenen Rechte die aus der DSGVO hervor gehen. • kennt die Grenzen der DSGVO und die Risiken der Datenverarbeitung außerhalb der EU	Er/Sie ist in der Lage • von seinen durch die DSGVO eingeräumten Rechte Gebrauch zu machen.	Er/Sie ist in der Lage • die datenschutzrechtlichen Risiken der Nutzung eines bestimmten Anbieters zu bestimmen.

wendet werden. Dieses Recht wurde im Rahmen der europäischen Datenschutzgrundverordnung (DSGVO) verankert.

Aber was, wenn unsere Daten anonymisiert werden? Solche Daten besitzen einen erheblichen wirtschaftlichen Wert. Sie sind die Grundlage für verschiedenste Wirtschaftszweige und werden sogar gehandelt. Selbst wenn es in Zukunft eine klare Regelung in Bezug auf das Eigentum an Daten geben sollte, stellt sich die Frage wie ein solches "Dateneigentum" in der Praxis umgesetzt und nachgewiesen werden kann.

Wer eine DVD bei einem Händler kauft, kann sie so lange nutzen, wie es die Lebensdauer des Datenträgers erlaubt. Wer aber z. B. über Amazon eine digitale Kopie kauft, kann den Film nur in Kombination mit seinem Amazon-Konto streamen. Und auch nur so lange, wie Amazon den Film in seiner Bibliothek führt. In den USA sind diesbezüglich bereits mehrere Klagen eingereicht worden.

3.2 Die europäische Datenschutzgrundverordnung (DSGVO)

3.2.1. Einführung

Das Recht auf den Schutz der eigenen personenbezogenen Daten ist bereits in der EU-Grundrechtecharta verankert. Im Mai 2018 trat zudem die europäische Datenschutzgrundverordnung (DSGVO) in Kraft. Ziel der Verordnung ist der Schutz der "Grundrechte und Grundfreiheiten natürlicher Personen", insbesondere deren Recht auf den Schutz personenbezogener Daten (DSGVO Art.1). Sie enthält Regeln und Vorschriften für die Verarbeitung von personenbezogenen Daten. Unter anderem verpflichtet sie Unternehmen und öffentliche Stellen, die betroffenen Personen über die beabsichtigte Verarbeitung von Daten zum Zeitpunkt der Datenerhebung zu informieren.

Welche Daten sind von der DSGVO betroffen?

Laut der DSGVO sind personenbezogene Daten alle Informationen, die sich direkt oder indirekt auf eine Person beziehen. Dazu gehören neben unserem Namen, unseren Login oder unserer E-Mail-Adresse auch Informationen wie Kundennummern, Online-Kennungen, Standortdaten und dergleichen. Letztlich also alle Daten, die in irgendeiner Form Rückschlüsse auf unsere Person zulassen. (DSGVO Art. 4 lit.1)
Unternehmen und öffentliche Stellen dürfen diese Daten nur unter bestimmten Bedingungen speichern und verarbeiten. So dürfen personenbezogene Daten nur für einen bestimmten, eindeutigen und rechtmäßigen Zweck erhoben und nur für diesen verwendet werden. Unternehmen sind zudem verpflichtet, nur die Daten zu erheben, die für den entsprechenden Zweck wirklich benötigt werden (Stichwort "Datenminimierung"). (DSGVO Art. 5 lit.1)
Natürlich muss ich bei einem Online-Versandhandel immer noch meinen Namen und meine komplette Adresse angeben, denn das Unternehmen muss mir die bestellte Ware ja auch zusenden können. Beim Abonnieren eines Newsletters hingegen darf lediglich die E-Mail-Adresse verpflichtend sein, denn nur diese wird wirklich für den Versand des Newsletters benötigt.
Der Anbieter muss meine personenbezogenen Daten auch löschen, sobald der eigentliche Zweck nicht mehr gegeben ist. Das bedeutet aber nicht, dass meine Daten sofort gelöscht werden. Oft greifen hier staatliche Gesetze. In Deutschland müssen Unternehmen Abrechnungsdaten bis zu 10 Jahre aufbewahren, in Spanien 5 Jahre. Nur weil ich also mein Konto bei meinem Online-Versandhändler lösche, bleiben bestimmte weiterhin gespeichert, weil das Unternehmen dazu gesetzlich verpflichtet ist.

3.2.2 Unsere Rechte

Informationspflicht bei Datenerhebung (Art.13 DSGVO)

Die DSGVO versucht, die Verarbeitung unserer Daten für Anwender transparent zu machen. Sobald ein Unternehmen oder eine öffentliche Stelle Daten von uns speichern will, müssen wir zum Zeitpunkt der Erhebung darüber informiert werden, was konkret mit diesen Daten geschieht.
Gemäß der Informationspflicht müssen uns die folgenden Fragen beantwortet werden:

- Wer will unsere Daten speichern und verarbeiten?
- Zu welchem Zweck sollen unsere Daten verarbeitet werden?
- Was ist die Rechtsgrundlage der Speicherung unserer Daten?
- Welche Empfänger erhalten Zugriff auf unsere Informationen?
- Werden unsere Daten in Drittländer außerhalb der EU übertragen?
- Wie lange werden unsere Daten gespeichert?
- Wenn die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für den Abschluss eines Vertrags erforderlich ist: Welche Folgen hätte es für uns, wenn wir die Daten nicht bereitstellen?

Darüber hinaus sind wir bei der Datenerhebung auf weitere Rechte hinzuweisen, wie das Auskunftsrecht, das Widerrufsrecht und das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde.
Die DSGVO sieht keine Einschränkungen für Branchen oder Anwendungsfälle vor. Aus diesem Grund werden wir seit der Einführung der Verordnung zunehmend mit Datenschutzhinweisen und Informationen zur Speicherung unserer Daten konfrontiert.

Recht auf Information (Art.15 DSGVO)

Wir haben das Recht zu erfahren, welche Daten Unternehmen von uns zu welchem Zweck gespeichert haben, und wer Zugriff auf diese Daten hat. Dies können wir auch schriftlich verlangen. Unternehmen sind verpflichtet, uns darüber Auskunft zu erteilen.
Da die Beantwortung dieser Anfragen für die betroffenen Unternehmen mit Aufwand verbunden ist, kann es mehrere Wochen dauern, bis eine solche Anfrage beantwortet wird. Große Anbieter im digitalen Bereich haben begonnen, die entsprechenden Informationen online zur Verfügung zu stellen.

Recht auf Berichtigung und Löschung (Art. 16 + 17 DSGVO)

Sollten über uns gespeicherte Informationen nicht korrekt sein, haben wir selbstverständlich das Recht, die Korrektur der Daten zu verlangen. Wenn wir umziehen, ändert sich sich beispielsweise unsere Adresse.
Außerdem beinhaltet die DSGVO das "Recht auf Vergessenwerden", d. h. das Recht, unsere Daten löschen zu lassen. Wenn wir die Löschung unserer Daten verlangen, ist

der für die Verarbeitung Verantwortliche verpflichtet, diesem Verlangen unverzüglich nachzukommen. Allerdings gibt es hier einige Einschränkungen. Zunächst einmal muss sichergestellt sein, dass der Zweck, zu dem die Daten erhoben wurden, weggefallen ist. Außerdem kann der Datenverantwortliche z. B. gesetzlichen Verpflichtungen unterliegen, die eine Speicherung der Daten erforderlich machen. Wir werden also wahrscheinlich nicht überall unsere Daten einfach löschen können, aber wir können zumindest Auskunft darüber erhalten, welche Daten aus welchem Grund bei der jeweiligen verantwortlichen Stelle gespeichert sind.
Weitere Rechte:

Recht auf Einschränkung (Art. 18 GDPR).

Wenn wir den Verdacht haben, dass die Verarbeitung unserer Daten unrechtmäßig erfolgt oder im Verhältnis zum ursprünglichen Zweck unverhältnismäßig ist, können wir eine Beschwerde einreichen und die Verarbeitung unserer personenbezogenen Daten einschränken lassen.

Recht auf Datenübertragbarkeit (Art. 20)

Die europäische Datenschutzgrundverordnung gibt uns das Recht, die über uns gespeicherten Daten in einem "strukturierten, gängigen und maschinenlesbaren Format" anzufordern. Die Idee dahinter ist, die Portabilität von Daten zu gewährleisten, d.h. die Möglichkeit, personenbezogene Daten direkt von einem Verantwortlichen zu einem anderen Verantwortlichen zu übertragen. Dies könnte beispielsweise den Wechsel von einem sozialen Netzwerk zu einem anderen erleichtern. Allerdings wird dieses Recht durch die Einschränkung "soweit technisch machbar" abgeschwächt. Aber selbst wenn ein nahtloser Datentransfer zwischen verschiedenen Diensten in absehbarer Zeit nicht möglich sein wird, erlaubt uns das Recht auf Datenportabilität zumindest, die über uns gespeicherten Daten in ein Format zu erhalten, das wir weiterverarbeiten können.

Widerspruchsrecht (Art. 21)

Wie bereits erwähnt muss eine Verarbeitung unserer personenbezogenen Daten immer eine gesetzliche Grundlage haben. Wenn wir eine Versicherung abschließen müssen unsere Daten aus vertraglichen Gründen verarbeitet werden. Angaben zu unserer Steuererklärung machen wir aufgrund gesetzlicher Vorgaben.
Oft geben wir aber auch freiwillig Informationen preis. Dann beruht die Verarbeitung unserer Daten meist auf einer Einwilligung, die wir dem jeweiligen Anbieter gegeben haben. Dies ist insbesondere im Bereich der Direktwerbung der Fall. Hier haben wir das Recht zu widersprechen.

Handelt es sich um Werbung, muss der Anbieter den Widerspruch sofort akzeptieren und die Verarbeitung unserer Daten einstellen. In anderen Fällen können wir aufgefordert werden, die Gründe darzulegen, warum wir von der ursprünglichen Einwilligung in die Verarbeitung nun Abstand nehmen. Kommt der Anbieter unserer

Aufforderung nicht nach, haben wir letztendlich immer noch die Möglichkeit, eine Beschwerde bei einer Aufsichtsbehörde einzureichen.

Beschwerde bei der Aufsichtsbehörde

In jedem Land, in dem die Datenschutzgrundverordnung Gültigkeit hat, existiert eine oder mehrere Datenschutzaufsichtsbehörden. In Deutschland hat sogar jedes Bundesland einen eigenen Datenschutzbeauftragten sowie eine Aufsichtsbehörde. Unternehmen sind verpflichtet, datenschutzrechtliche Vorfälle an die Aufsichtsbehörden zu melden. Als Privatperson können wir uns mit Beschwerden ebenso an die Behörden wenden.

Aufgrund von Verstößen gegen die DSGVO können die nationalen Aufsichtsbehörden hohe Geldstrafen verlangen. Die bisher höchste Strafe in Höhe von 50 Millionen Euro ging an Google (Stand Ende 2020). Aber auch andere Unternehmen mussten bereits hohe Bußgelder entrichten: H&M zahlte 35,2 Mio. € und TIM Telecom 27,8 Mio. €.
Die Gründe sind unterschiedlich: Google wurde wegen mangelnder Information und Datenverarbeitung ohne Einwilligung der Verbraucher belangt. Im Fall von H&M war es ein technischer Fehler, der private Informationen aller Mitarbeiter des Unternehmens öffentlich zugänglich machte. Die Geldstrafe wurde jedoch nicht wegen des technischen Fehlers verhängt, sondern weil sich durch die Veröffentlichung herausstellte, dass H&M sensible persönliche Daten seiner Mitarbeiter sammelte.
Das Bußgeld von TIM wiederum wurde aus unterschiedlichen Gründen verhängt: Von der unzulässigen Einholung einer Einwilligung zur Datenverarbeitung bis hin zur übermäßigen Datenspeicherung.
Es trifft aber nicht nur die Großen: In Österreich wurde ein Wettbüro mit 5.000 € Strafe für eine illegale Videoüberwachung belegt. In Ungarn verweigerte ein Unternehmen die Herausgabe von Daten und bekam dafür eine Strafe von 6,5% des Jahresumsatzes.
Und es müssen nicht immer Strafen in Millionenhöhe sein: Ein Krankenhaus in Ungarn musste 90€ bezahlen, weil es das Auskunftsrecht eines Patienten verletzte sowie rechtswidrig eine Kopiergebühr erhob.[35] 48€ Strafe ging an die estnische Polizei, weil ein Polizeibeamter die Polizeidatenbank für private Nachforschungen nutzte (unrechtmäßige Nutzung).
Eine Übersicht über die von den europäischen Aufsichtsbehörden verhängten Bußgelder finden Sie auf der folgenden Website:
https://www.enforcementtracker.com/

3.2.3 Kritik

Die Datenschutzgrundverordnung (DSGVO) versucht, unsere Rechte zu stärken. Doch es gibt auch Kritik an der neuen Verordnung. Denn sie ist an vielen Stellen bewusst vage gehalten. Personenbezogene Daten können auf der Grundlage des "berechtigten Interesses" des jeweiligen Unternehmens verarbeitet werden, was im Einzelfall schwierig zu beurteilen ist. Unternehmen sind verpflichtet, "geeignete Maßnahmen" zum Schutz der Daten zu ergreifen, die unter anderem den "Stand der Technik" berücksichtigen. Und unsere Anfragen sollen "ohne unverhältnismäßigen Aufwand" beantwortet werden.

Diese Formulierungen eröffnen Spielraum für Interpretationen. So wird die Datenschutzgrundverordnung in den Mitgliedsstaaten und von den zuständigen Datenschutzbehörden sehr unterschiedlich interpretiert.

Auch ist die Auffassung verbreitet, dass die DSGVO der Komplexität der digital vernetzten Welt nicht gerecht wird. Im Angesicht von vernetzter Applikationen, durch Cloud Computing verteilter Systeme über Ländergrenzen hinweg, sowie dem Überfluss an Daten (Big Data) erscheint die praktische Anwendung der DSGVO als sehr schwierig.

Doch ist die bloße Existenz der DSGVO schon ein wichtiges Schritt im Bereich des Datenschutzes. Wie schwierig und komplex solche Vorhaben sind, lässt sich anhand der geplanten ePrivacy-Verordnung erkennen. Die neue Verordnung soll die bestehende ePrivacy-Richtlinie ersetzen und die Privatsphäre der Bürger online stärken. Thematisch geht es vor allem um Themen rund um das Direktmarketing und die Nutzung von Cookies. Regularien der DSGVO sollen mit der neuen Verordnung konkretisiert werden. Ursprünglich sollte die neue ePrivacy-Verordnung bereits 2018 mit der DSGVO zusammen in Kraft treten. Doch die EU-Mitgliedstaaten konnten sich nicht auf eine gemeinsame Linie einigen. Im November 2020 wurde ein weiterer Kompromissvorschlag abgelehnt.

3.2.4 Problematik: Recht auf Löschung und Vergessenwerden

Die DSGVO stärkt unsere Rechte an unseren Daten durch die Grundsätze der informationellen Selbstbestimmung und der Zweckbindung der Datenverarbeitung. Wir dürfen bestimmen, welche unserer Daten genutzt, verarbeitet und veröffentlicht werden. Unternehmen dürfen unsere Daten nur solange speichern, wie es für den jeweiligen Zweck nötig ist. Entfällt der Zweck, müssen die Daten wieder gelöscht werden. Auch haben wir ein Recht auf die Löschung unserer Daten. Aber inwieweit kann dieses Recht im digitalen Zeitalter auch immer durchgesetzt werden?

Im Jahre 2000 filmte der Kameramann Matthias Fritsch auf eine Technoparade einen muskulösen, leicht bekleideten Mann und stellte das Video im Jahr 2006 auf Youtube. Der auf dem Video gezeigte Mann klagte vor Gericht gegen die Veröffentlichung des Videos, mit der Begründung, dass er einer Veröffentlichung nicht zugestimmt habe. Das Gericht gab ihm Recht und Matthias Fritsch musste das Video wieder von seinem Profil löschen. Allerdings erreichte das Video in der Zwischenzeit in der Internetgemeinde eine Art Kult-Status. Anhang des Aussehen und der Statur des Mannes, wurde das Video unter dem Namen "Techno Viking" bereits mehrfach vervielfältigt, kopiert und in neuen Bearbeitungen wiederveröffentlicht. Obwohl Fritsch das Video auf seinem Kanal löschte, ist das Video bis heute noch über diverse Portale abrufbar. Das Phänomen zeigt die Problematik des Rechts auf Löschung im Zeitalter des Internets. Selbst wenn wir heute all unserer Daten auf einem sozialen Netzwerk löschen, können wir nicht sicher sein, dass damit alle Querverweise und eventuelle Kopien mitgelöscht werden. Löschen wir ein Bild von unserem Smartphone, wird die Kopie, die wir vielleicht zuvor über einen Messenger verschickt haben, nicht automatisch mitgelöscht. Heute existieren unsere Daten meist zeitgleich an verschiedenen Stellen. Eine vollumfängliche Löschung kann oft nicht zu hundert Prozent gewährleistet werden.

Der Streisand-Effekt

Der Streisand-Effekt beschreibt das Phänomen, dass durch einen Versuch eine unliebsame Information zu löschen, genau das Gegenteil erreicht wird und gerade die Aufforderung der Löschung die öffentliche Aufmerksamkeit erregt.
Der Name geht zurück auf die Sängerin und Schauspielerin Barbra Streisand. Auf der Webseite Pictopia.com wurden 12.000 Luftaufnahmen der Küste Kaliforniens veröffentlicht. Die Fotos sollten die Erosion der kalifornischen Küste für das California Coastal Records Project dokumentierten. Auf einem der Bilder entdeckte die Schauspielerin ihr eigenes Haus. Sie forderte die sofortige Löschung des Fotos und verklagte die Webseite und den Fotografen auf 50 Millionen US-Dollar Schadensersatz. Die Klage blieb erfolglos. Aber gerade durch Streisands Klage wurde erst eine Verbindung zwischen dem Foto und ihrem Anwesen hergestellt. In Folge dessen verbreitete sich Foto im Internet

3.3 Datenschutz außerhalb der Europäischen Union

Durch die DSGVO haben wir eine gemeinsame Regelung zum Datenschutz innerhalb der Europäischen Union. Die Verordnung ist in allen Mitgliedstaaten gültig und schützt somit alle personenbezogenen Daten der EU-Bürgerinnen und Bürger, die innerhalb der EU verarbeitet werden. Doch was passiert, wenn wir Dienste nutzen, die nicht in der EU ansässig sind? Letztlich greift auch dann die europäische Datenschutzgrundverordnung nicht.

Das Internet als globales Dorf lässt nationale Grenzen verschwinden. Und es ist für uns oft nicht erkennbar, aus welchem Land ein einzelner Anbieter kommt oder gar in welchem Land unsere Daten gespeichert und verarbeitet werden.

Eines ist jedoch sicher: Wer über das Internet bei einem Anbieter im außereuropäischen Ausland bestellt, genießt nicht die gleichen Verbraucherrechte wie bei einem europäischen Anbieter.

Doch selbst wenn wir unsere Daten einem europäischen Anbieter anvertrauen, heißt das nicht, dass der Anbieter nicht weitere Dienstleister einsetzt, die möglicherweise Zugriff auf unsere Daten haben. Viel wichtiger ist daher die Frage, inwieweit ein Unternehmen mit anderen Unternehmen kooperiert. Ein deutsches Unternehmen mag seinen Hauptsitz in Deutschland haben, aber die Server mit den Kundendaten könnten in einem Rechenzentrum in Straßburg oder Amsterdam stehen und von einem skandinavischen IT-Unternehmen betreut werden. Ebenso könnte das Unternehmen bestimmte Softwarelösungen nutzen, die wiederum von Anbietern mit Sitz in den USA bereitgestellt werden oder auf Call Center mit Sitz im osteuropäischen oder asiatischen Raum zurückgreifen. Hier stellt sich die Frage, inwieweit der Schutz unserer Daten gemäß der DSGVO gewährleistet werden kann.

Die EU hat eine Liste von Ländern definiert, die als sichere Drittstaaten gelten. Dies sind Länder, denen die Europäische Kommission ein angemessenes Datenschutzniveau bestätigt. Das bedeutet, dass diese Länder ein vergleichbares oder besseres Datenschutzniveau umgesetzt haben. Dazu gehören derzeit alle Länder aus dem Europäischen Wirtschaftsraum (Norwegen, Island und Liechtenstein) sowie explizit Andorra, Argentinien, Kanada, Färöer Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Schweiz und Uruguay.

Diese Regelung schließt die Übermittlung von personenbezogenen Daten in andere Länder nicht aus. Der einzige Unterschied ist, dass in diesem Fall der für die Datenverarbeitung Verantwortliche sicherstellen muss, dass die Daten beim Empfänger ausreichend geschützt sind. Um dies zu vereinfachen, hat die EU sogenannte Standardvertragsklauseln entwickelt, die von Unternehmen in Drittländern unterzeichnet werden können. Dort werden dann die entsprechenden Regelungen zum Datenschutz definiert.

Für uns als Endanwender ist es leider oft nicht ersichtlich wohin unsere Daten fließen und wer darauf letztendlich alles Zugriff hat. Trotz aller Regelungen und Vorschriften liegt die Verantwortung darüber, welche Dienstleister wir nutzen und welche personenbezogenen Daten wir diesen zur Verfügung stellen, bei uns selbst.

3.4 Sonderfall USA

Die größten Internet-Unternehmen haben ihren Sitz in den USA. Microsoft, Google, Facebook, Twitter und Co. sind allesamt keine europäischen Unternehmen. In der Regel haben diese Unternehmen zwar eine Niederlassung in der EU, trotzdem kann ein Datentransfer in die USA nicht ausgeschlossen werden. Daher brauchen wir entsprechende Regelungen, die den Schutz der Daten von EU-Bürgerinnen und -Bürgern in den USA sicherstellen.

Lange Zeit gab es entsprechende Abkommen zwischen der EU und den USA. Zunächst gab es seit dem Jahr 2000 das "Safe Harbor"-Abkommen, das es Unternehmen erlaubte, personenbezogene Daten aus einem EU-Land in die USA gemäß den europäischen Datenschutzrichtlinien zu übertragen. Das Abkommen wurde im Jahr 2015 für ungültig erklärt.

Um den Datentransfer zwischen der EU und den USA weiter gewährleisten zu können, wurde 2016 das EU-US Privacy Shield verabschiedet. Dieses wurde 2020 vom Europäischen Gerichtshof für ungültig erklärt.

Beide Fälle gehen auf eine Klage des Österreichers Maximilian Schrems zurück. Kern der Klagen war der Vorwurf, dass die Niederlassung von Facebook in Irland seine Daten mit dem Mutterkonzern in den USA teilt. So werden Daten europäischer Bürger in die USA übertragen. Brisant wurde diese Tatsache im Jahr 2013 durch die Enthüllungen von Edward Snowden (2013). Dieser deckte auf, dass US-Geheimdienste Zugriff auf Server von US-Unternehmen wie Facebook und Google haben. Zuletzt wurde 2018 in den USA der sogenannte CLOUD Act (Clarifying Lawful Overseas Use of Data Act) verabschiedet. Dieses Gesetz verpflichtet amerikanische Unternehmen dazu, US-Behörden Zugriff auf gespeicherte Daten zu gewähren. Die Richter des Europäischen Gerichtshofes erklärten das "Privacy Shield" für ungültig. Mit Blick auf die Zugriffsmöglichkeiten der US-Behörden sind die Anforderungen an den Datenschutz nicht gewährleistet.

Aus datenschutzrechtlicher Sicht ist die Übermittlung personenbezogener Daten daher kritisch zu sehen, auch wenn die aktuellen EU-Standardvertragsklauseln aus rein rechtlicher Sicht noch gültig sind. Die USA ist aktuell nicht als sicheres Drittland anzusehen.

Der US-Bundesstaat Kalifornien zeigt jedoch, dass in dieser Frage viel Bewegung ist. Er hat mit dem California Consumer Privacy Act (CCPA) das bisher strengste Datenschutzgesetz in Amerika umgesetzt. Vorbild für das neue Gesetz war die europäische Datenschutzgrundverordnung.

3.5 Fazit

Die digitalisierte Welt wird zunehmend von Daten bestimmt. Es ist wichtig, dass wir uns über den Wert unserer eigenen Daten bewusst werden. Wir müssen lernen zu verstehen, wann wir welche Daten preisgeben und sensibel mit unseren Informationen umgehen. Mit wem teile ich meine Daten? Zu welchem Zweck? Wo werden sie gespeichert? Werden die angeforderten Daten wirklich benötigt?

Es ist Fakt, dass unsere persönlichen Daten gesammelt werden. Oft geschieht dies mit unserem Einverständnis, auch wenn wir die Tragweite dieser Entscheidung nicht immer erkennen können. In anderen Fällen werden Informationen auch ohne unsere ausdrückliche Zustimmung von uns gesammelt.

Wir müssen uns auch bewusst sein, dass Vorschriften wie die DSGVO nur Regelungen sind. Sie stehen zwar auf dem Papier, schützen uns aber im realen Leben nur bedingt. Wir können nicht überprüfen, ob ein Unternehmen seiner Informationspflicht nachkommt oder sich an geltende Gesetze hält. Alles, was wir tun können, ist, den Anbietern und Aufsichtsbehörden zu vertrauen und kritisch zu bleiben. Das gilt für die E-Mail von unserer Bank, die Freundschaftsanfrage im sozialen Netzwerk ebenso wie für den neu entdeckten Online-Shop. Besser ist es, gründlicher auf Seriosität und Authentizität zu prüfen.

Prinzipien der Datenminimierung lassen sich auch in unserem Alltag umsetzen. Beim Veröffentlichen von Daten in Blogs, Foren, sozialen Netzwerken usw. gilt der Grundsatz, dass wir nichts veröffentlichen sollten, was wir nicht wirklich öffentlich machen wollen. Selbst wenn ein Onlinedienst die Möglichkeit bietet, den Zugriff auf veröffentlichte Informationen auf einen bestimmten Nutzerkreis zu beschränken, sollten wir uns immer gut überlegen welche Informationen wir online stellen. Denn das Internet vergisst nicht.

Letztlich ist es wie im Straßenverkehr. Natürlich kann immer ein Unfall passieren. Aber wenn wir uns umsichtig verhalten und Vorsicht walten lassen, reduzieren wir das Risiko erheblich.

Endnoten

1 https://de.statista.com/statistik/daten/studie/1010134/umfrage/anzahl-der-von-facebook-entfernten-fake-accounts-weltweit/

2 https://www.security-insider.de/was-ist-ein-digitales-zertifikat-a-688440/

3 https://www.datenschutz.org/biometrische-daten/

4 https://www.mimikama.at/fake-gewinnspiele-auflistung/

5 https://www.pcwelt.de/ratgeber/Datenschutz-So-schuetzen-Sie-Ihre-Privatsphaere-im-Web-57287.html

6 https://www.it-zoom.de/mobile-business/e/das-sind-die-dreistesten-datensammler-15442/
https://whotracks.me/

7 https://de.statista.com/statistik/daten/studie/872986/umfrage/anteil-der-spam-mails-am-gesamten-e-mail-verkehr-weltweit/

8 https://www.polizei.bayern.de/kriminalitaet/internet/betrug/index.html/56975

9 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Aktuelle-Beispiele-fuer-Phishing/aktuelle-beispiele-fuer-phishing.html

10 https://www.internet-beschwerdestelle.de/de/beschwerde/einreichen/e-mail-und-spam.html

11 http://www.argedaten.at/php-generiert/datenschutz_seminare_at_Welche_rechtlichen_Schritte_sind_gegen_Spam_m%C3%B6glich.html

12 https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073

13 https://de.statista.com/infografik/23251/anzahl-neuer-malware-varianten/

14 https://www.heise.de/newsticker/meldung/Vor-20-Jahren-Ein-verliebter-Wurm-umrundet-die-Welt-4713566.html

15 https://praxistipps.chip.de/die-5-gefaehrlichsten-viren-aller-zeiten-und-was-sie-angerichtet-haben_42111

16 https://www.heise.de/security/meldung/Virus-oder-Impfstoff-WiFatch-befaellt-Router-und-schuetzt-vor-Malware-2837158.html

17 https://de.statista.com/statistik/daten/studie/1038985/umfrage/betroffenheit-durch-ransomware-nach-umsatzgroessenklasse-der-unternehmen-in-deutschland/

18 https://www.bundespolizei-virus.de/virenschutz/drive-by-downloads/

19 https://www.avg.com/de/signal/windows-10-privacy-everything-you-need-to-know-to-keep-windows-10-from-spying-on-you

20 https://www.brandeins.de/magazine/brand-eins-wirtschaftsmagazin/2019/unabhaengigkeit/smartphones-legaler-lauschangriff

21 https://mobilsicher.de/aktuelles/studie-mehr-als-1000-android-apps-sammeln-daten-ohne-berechtigung

22 https://www.tagesschau.de/inland/cyberangriffe-bka-101.html

23 https://de.statista.com/statistik/daten/studie/193207/umfrage/finanzielle-schaeden-durch-cyberkriminalitaet-in-deutschland/

24 https://www.zeit.de/datenschutz/malte-spitz-data-retention

25 https://www.welt.de/print/die_welt/wirtschaft/article195830359/Was-sind-meine-Daten-wert.html

26 https://de.statista.com/statistik/daten/studie/458825/umfrage/werbeeinnahmen-von-facebook/

27 https://de.statista.com/statistik/daten/studie/75188/umfrage/werbeumsatz-von-google-seit-2001/

28 https://irights.info/artikel/metadaten-fotos-anbringen-loeschen-bearbeiten/26353

29 https://t3n.de/news/smartphone-spionage-alphonso-897108/

30 https://transparency.facebook.com/community-standards-enforcement

31 https://www.handysektor.de/artikel/berechtigungen-was-wissen-meine-apps-ueber-mich/

32 https://de.statista.com/statistik/daten/studie/801670/umfrage/umsatz-mit-mobilen-apps-nach-segmenten-in-deutschland/.

33 https://www.gameswirtschaft.de/wirtschaft/mobilegames-umsatz-deutschland-2019/-

34 https://direc.ircg.ir/wp-content/uploads/2020/01/SuperData2019YearinReview.pdf

35 https://www.dsgvo-portal.de/dsgvo-bussgeld-gegen-krankenhaus-2019-12-09-HU-223.php

65