Datenschutz im Internet und in sozialen Netzwerken

Handout für das DBSV-Seminar
„Fit fürs Web 2.0“ vom 13. bis 15. April 2018 in Münster
von Domingos de Oliveira

Inhalt

Einleitung

Der Datenschutz ist heute ein allgegenwärtiges Thema. Als Außenstehender fragt man sich häufig, warum so viel darüber diskutiert wird. Schließlich leben wir in einer Demokratie. Es ist eher unwahrscheinlich, dass der Staat anfangen wird, uns persönlich auszuspionieren. Und wen interessiert es schon, wo ich gestern Pizza gegessen oder mit wem ich ein Bier getrunken habe?
In diesem Handout sollen drei Dinge vermittelt werden:

- Welche Informationen erhalten die sozialen Netzwerke von dir?
- Was machen die sozialen Netzwerke mit diesen Daten?
- Warum ist es sinnvoll und wichtig, dass du sorgsam mit deinen Daten umgehst?

Soziale Netzwerke sind Netzwerke, auf denen grundsätzlich öffentlich kommuniziert wird. Deswegen wird WhatsApp in diesem Leitfaden nicht ausführlich behandelt. WhatsApp ist eigentlich für die private Kommunikation gedacht, auch wenn viele WhatsApp-Gruppen sehr groß sind. Doch bestehen bei WahtsApp ähnliche Probleme, vor allem, wenn es um den Austausch in größeren Gruppen geht. Häufig sind die Gruppen so groß, dass man nicht mehr alle Teilnehmer persönlich kennt. Durch Einladungslinks zu Gruppen können schnell auch Personen in die Gruppen kommen, die man dort eher nicht sehen möchte.
Es geht nicht darum, gar nicht mehr auf sozialen Netzwerken aktiv zu sein. Es geht um einen bewussten Umgang mit den Daten. Es geht weniger darum, ob du tatsächlich etwas veröffentlichst. Vielmehr sollst du immer die Macht darüber behalten, was über Dich öffentlich wird und was nicht.
Im Datenschutz geht es um zwei grundlegende Bereiche:

1. Welche Daten erhält das soziale Netzwerk?
2. Welche Daten erhalten andere Personen, seien es Freunde, Bekannte oder Fremde?

Im ersten Fall geht es um die Frage, was du auf dem Netzwerk machst und wie du dich verhältst. Wichtig ist dabei die Frage, welche Daten das Netzwerk speichert und was es damit macht.
Im zweiten Fall geht es um die Informationen, welche du für andere Menschen zugänglich machst. Daten können natürlich nicht nur von Unternehmen, sondern auch von einzelnen Menschen missbräuchlich verwendet werden.

Soziale Netzwerke und der Datenschutz

Fast alle Angebote im Bereich Social Media sind kostenlos. Doch handelt es sich um große internationale Unternehmen mit tausenden Angestellten in vielen Ländern. Wie verdienen diese Unternehmen Geld?

Werbung

Sie verdienen vor allem Geld mit Werbung. Sie verkaufen Werbefläche wie eine Zeitung. Dabei wird Werbung umso besser bezahlt, je zielgerichteter sie ausgespielt wird. Die Werbung soll möglichst Personen gezeigt werden, die auch bereit sind, für das Beworbene zu bezahlen. Das nennt sich Targeting. Hast du schon einmal in einem Online-Shop nach einem Produkt gesucht und später auf einer ganz anderen Website Werbung für genau dieses Produkt gesehen? Das ist eine der Funktionen von Targeting.

Deshalb ist es für die sozialen Netzwerke besonders wichtig, viele detaillierte Daten ihrer Nutzer zu sammeln. Oft gibt man das eigene Geschlecht, das Alter, den Beziehungsstatus und viele weitere Informationen freiwillig an, um sein Profil einzurichten. Hinzu kommen die Informationen, die aus den eigenen Beiträgen automatisch gewonnen werden können.

Mit verschiedenen Verfahren ist es heute kein Problem mehr, alle möglichen Informationen über eine Person per Software aus deren Daten zu gewinnen. Man nennt das Data Mining, also quasi das Schürfen in Daten nach wertvollen Informationen. Das geschieht vollautomatisch. Es muss sich also kein Mensch die Daten persönlich anschauen.

Nehmen wir an, du schreibst in einem Beitrag, dass dein Handy kaputt ist. Im Idealfall aus sich des Netzwerkes würden dir Werbung für Handys in deiner Preisklasse angezeigt werden. Die Wahrscheinlichkeit, dass du das beworbene Handy kaufst ist wesentlich größer als bei einer Person, die sich nicht zu ihrem Handy äußert.

Aktuell (März 2018) wird der Datenskandal um Cambridge Analytica diskutiert. Cambridge Analytica hat auf die Daten von fast 100 Millionen Menschen zugreifen können. Ihr Ziel war dabei, den amerikanischen Wahlkampf 2017 zugunsten von Donald Trump zu beeinflussen. Die ganze Tragweite ist bisher noch nicht geklärt.

Verkauf von Daten

Es ist wahrscheinlich, dass die Netzwerke die Daten auch an Dritte verkaufen, zum Beispiel an große Unternehmen. Zwar werden die Daten aggregiert, also es werden die Informationen sehr vieler Personen zusammengefasst. Dennoch weiß niemand, was genau mit diesen Daten passiert und wer alles Zugriff darauf hat. Die Unternehmen wollen zum Beispiel wissen, wie du zu bestimmten Produkten oder Marken stehst oder wofür du dich interessierst. Sie wollen mehr über dich wissen, damit sie dir noch mehr und gezielter Produkte oder Leistungen verkaufen können. Daten sind für viele Unternehmen das wertvollste Gut.

In vielen Bereichen der Wirtschaft sind Daten besonders begehrt. So wollen Organisationen wie die Schufa möglichst viele Faktoren in Betracht ziehen, um zu prüfen, ob jemand kreditwürdig ist. Einige Krankenkassen wollen einen besonders gesunden Lebensstil mit Bonuspunkten belohnen. Dabei sollen etwa Fitness-Tracker zum Einsatz kommen. Sind Daten öffentlich, also grundsätzlich für jeden ohne Anmeldung bzw. auch ohne persönlichen Kontakt sichtbar, ist es auch kein Problem für Dritte, sie über spezielle Programme auszulesen, zu speichern, zu verarbeiten und weiter zu verwenden. Facebook und Co. wollen das nicht, da die Daten für sie wertvoll sind. Doch können sie das nicht immer verhindern. Die Netzwerke liefern sich ein Katz-und-Maus-Spiel mit kriminellen Hackern, die versuchen, die Daten für Spam oder andere Zwecke abzugreifen.

Zudem können Daten aus unterschiedlichen Quellen zusammengeführt werden. InstaGram und WhatsApp etwa gehören zu Facebook. YouTube ist eine Tochter von Google, ebenso wie Blogger.com. Die großen Anbieter wie Google und Facebook haben genügend Geld, um weitere Netzwerke wie SnapChat aufzukaufen. Die zusammengefassten Daten zu einer Person aus unterschiedlichen Quellen sind noch viel wertvoller als die Informationen aus nur einem Netzwerk. Auf WhatsApp oder im Facebook Messenger etwa wird viel intimer kommuniziert als auf Facebook.

Facebook kann nicht nur Texte auswerten. Die Methoden zur Erkennung von Bild- und Video-Inhalten werden immer besser. Du kennst sicherlich die automatisch generierten Bildbeschreibungen von Facebook. Durch die Gesichtserkennung oder auch Markierungen weiß Facebook ungefähr, wer oder was zu sehen ist. Sprache aus Sprachnachrichten oder Videos kann in Text umgewandelt und automatisch ausgewertet werden.

Die Netzwerke sind so konzipiert, dass die Nutzer sich möglichst lange dort aufhalten und möglichst viele

private Informationen über sich verraten. Je mehr Informationen du angibst, desto besser kann Facebook dir zum Beispiel neue Freunde, Gruppen oder Veranstaltungen vorschlagen, die dich wahrscheinlich interessieren. Je interessanter die Inhalte sind, desto mehr Zeit wirst du auf Facebook verbringen. Ganz nebenbei steigt auch die Zahl der Werbeanzeigen, die du siehst, je länger du online bist.

Welche Informationen hat das soziale Netzwerk?

Bei Informationen denken wir zunächst vor allem an die Informationen, die wir selbst einstellen: Unsere Beiträge, Likes, Re-Tweets und so weiter. Doch lassen sich viele Daten auch automatisch abfragen. So ermitteln viele Apps wie Twitter und Facebook bei jedem Zugriff, wo du dich gerade befindest, wenn du die --App aufrufst oder etwas postest. Sie wissen, welches Betriebssystem oder Browser du verwendest und noch einige Dinge mehr.
Zu den Daten, welche die Netzwerke erhalten gehören:

- die Daten aus meinem Profil
- meine Beziehung zu anderen Personen
- wo befindest du dich, wenn du auf die App zugreifst
- was dich besonders interessiert
- mit wem interagierst du besonders viel

Es ist schwierig zu sagen, welche Schlüsse die Netzwerke aus diesen Daten ableiten. Die Auswertungs-Algorithmen sind geheim. Wir wissen aber, dass die Auswertungsmöglichkeiten immer ausgefeilter und leistungsfähiger werden. Facebook beschäftigt eine ganze Abteilung mit Daten-Analysten. Diese Personen tun nichts anderes, als Algorithmen zur Daten-Auswertung zu entwickeln und zu verbessern.
Für die Netzwerke sind Informationen umso interessanter, je persönlicher sie sind. Facebook zum Beispiel möchte erreichen, dass du möglichst viel Zeit dort verbringst. Deshalb möchte es in deiner Chronik möglichst Beiträge anzeigen, die dich interessieren. Um das zu schaffen, muss Facebook natürlich möglichst viel über dich wissen: Was interessiert dich, wo hälst du dich häufig auf, mit wem interagierst du besonders viel. Facebook wird dann versuchen, dir ähnliche Beiträge zu zeigen. YouTube und Twitter funktionieren grundsätzlich genau so, verfügen aber über weniger persönliche Daten.
Facebook weiß relativ viel. Es kennt schon einmal Deine Identität. Es verlangt, dass du dich mit deinem richtigen Namen anmeldest. Auf YouTube oder Twitter ist es deutlich einfacher, nicht mit dem eigenen Namen unterwegs zu sein. Je mehr Zeit du in sozialen Netzwerken verbringst und je mehr Interaktionen du hast, desto mehr weiß das Netzwerk über dich.
Oft wird gesagt, die Algorithmen wüssten Dinge über uns, die wir selber nicht wissen. Das ist übertrieben. Richtig ist aber, dass durch statistische Analysen sehr viel mehr aus den Daten abgeleitet werden kann, als auf den ersten Blick klar wird. Es können zum Beispiel auch Daten zusammengeführt werden, die in einem großen zeitlichen Abstand eingegeben wurden. Den Algorithmen ist es egal, ob zwei Beiträge kurz hintereinander oder über zwei Jahre hinweg geteilt wurden. Du hast den alten Beitrag vielleicht vergessen, für das Analyseprorgramm spielt der zeitliche Abstand aber keine Rolle. Zudem können nicht nur Beiträge aus deiner Chronik, sondern auch aus Gruppen oder aus dem Messenger für die Auswertung herangezogen werden. Schon die Information, in welchen Gruppen jemand ist, sagt Einiges über seine Neigungen und Interessen aus.
Besonders wertvoll für Werber sind zum Beispiel Informationen über das Alter, die finanzielle und persönliche Situation. Wer etwa kleine Kinder hat, ist für Werbung für Spielzeug empfänglicher als ein kinderloser Single. Wer vegan lebt ist wahrscheinlich eher bereit, viel Geld für Bioprodukte auszugeben. Diesen Personen soll entsprechend passende Werbung angezeigt werden.
Der Traum der Netzwerke ist es, Daten aus ganz verschiedenen Quellen zusammenzuführen und zusammenzufassen. Wenn zum Beispiel Daten aus der Google-Suche, Amazon und Facebook aggregiert werden würden, wüssten die Netzwerke eine ganze Menge über die Person, die diese Dienste nutzt.

Messenger

Ein besonders kritischer Punkt sind die Messenger. In den Messengern teilen wir Informationen, die wir nicht öffentlich teilen würden. Deshalb sind diese Informationen für die Netzwerke besonders spannend.
Die beiden wichtigsten Messenger gehören zu Facebook: Die Facebook-eigene App sowie WhatsApp.
Facebook kann grundsätzlich die gleichen Analysemethoden auf diese Daten

anwenden wie auf der eigentlichen Plattform.

Welche Datenschutzregeln gelten?

Der Datenschutz ist in Deutschland relativ streng. Ende Mai 2018 wird die Europäische Datenschutz-Grundverordnung in Kraft treten. Sie enthält strenge Regeln zum Umgang mit persönlichen Daten.

Das Problem besteht darin, dass praktisch alle sozialen Netzwerke ihren Sitz in den USA haben. Die USA haben derzeit deutlich lockere Gesetze zum Datenschutz.

Zwar gelten die deutschen Datenschutzverordnungen für Facebook und Co. Facebook hat auch bereits mitgeteilt, dass es sich an diese Regeln hält. Doch überprüfbar ist das nicht. Die transnationalen Unternehmen haben ihre eigenen Regeln.

Die sozialen Netzwerke sind Blackboxes. Niemand kann überprüfen, ob sie sich an Regeln halten oder was sie mit den Daten machen. Einerseits fürchten sie sich vor einem schlechten Ruf und werden deshalb darauf bedacht sein, sich an die Regeln zu halte. Immerhin kann es passieren, das sich zum Beispiel ein ehemaliger Mitarbeiter als Whistle-Blower betätigt oder eine staatliche Behörde wie jetzt im Rahmen von Cambridge Analytica Ermittlungen einleitet. Dennoch bleibt der Umstand, dass das Verhalten der Netzwerke von außen nicht überprüfbar ist.

Persönlicher Datenschutz

Die sozialen Netzwerke arbeiten vor allem mit Algorithmen und zusammengefassten Daten. Doch ist das nur ein Aspekt des Datenschutzes. Es gibt auch Personen oder Gruppen, die aus verschiedenen Gründen an euren Daten interessiert sein können.

Daten-Diebstähle

Vor allem bei kleineren Netzwerken kommt es häufiger zum Diebstahl von Daten. Dort werden unter anderem auch Nachrichten, Fotos und ähnliche Daten im großen Stil erbeutet. Sie werden oft verkauft, für weitere Hacking-Versuche oder zur Erpressung verwendet.

Der Fairness halber muss man sagen, dass die großen Dienste wie Facebook, Twitter oder Google soweit wir wissen bisher nicht betroffen waren. Zu den prominenten Opfern gehörte der Mail-Anbieter Yahoo.

Es passiert regelmäßig, dass private Profile gehackt und für kriminelle Zwecke verwendet werden. Dazu reicht es schon, wenn euer Smartphone im fremde Hände gerät oder ihr euch einen Computervirus einfangt. Deshalb ist es besser davon auszugehen, dass eure privaten Daten immer in fremde Hände geraten können. Und vergesst nicht: Auch die Profile eurer Freunde könnten geknackt werden. Dann hat der Hacker Zugriff auf alle Informationen, die auch eure Freunde sehen. Wenn das Handy eines Freundes gestohlen oder gehackt wird, sieht der Dieb auch alle Infos, die euer Freund von euch hat, z.B. Fotos aus WhatsApp oder Messages, Facebook-Nachrichten und so weiter. Viele Smartphones sind sicherheitstechnisch nicht mehr auf dem neuesten Stand oder generell schlecht geschützt.

Die Daten werden in der Regel für Spam-Nachrichten verwendet. Oder es wird versucht, mit den gehackten Profilen weitere Profile zu hacken, um weiteren Schaden anzurichten. Ein bekannter Fall sind zum Beispiel Computerschädlinge, welche die Festplatte verschlüsseln und erst gegen Geldzahlung wieder freigeben.

Daten-Missbrauch durch einzelne Personen

Neben diesen Diebstählen durch kriminelle Organisationen können jedoch auch einzelne Personen gezielt einzelne Profile ausspähen. Es soll vorkommen, dass Einbrecher über Facebook herausfinden, dass ihre potentiellen Opfer nicht zuhause sind. Fast jede Frau kann über Belästigung durch unerwünschte Kommentare oder Nachrichten berichten. Das geschieht umso eher, je mehr Informationen über sie öffentlich zugänglich sind. Besonders häufig werden Frauen belästigt, deren Profilbild, Geburtsdatum oder Single-Status öffentlich zugänglich ist.

Vor einiger Zeit gab es ein Feature von einer Tageszeitung. Sie hatte zusammengefasst, welche Informationen sie über eine bestimmte Person eingesammelt hat. Diese Daten ergaben ein detailliertes Profil dieser Person.

Solche Informationen können etwa zum Missbrauch der Daten für Identitäts-Diebstahl verwendet werden. Auch Stalking und Mobbing wird durch öffentlich zugängliche Daten einfacher. Dabei muss es nicht unbedingt um dich persönlich gehen. Die Daten können auch verwendet werden, um an einen deiner Verwandten oder Freunde heran zu kommen. Die Kriminellen haben teils ausgefeilte Strategien entwickelt. Das Stichwort dazu ist social engineering.

Eine weitere Entwicklung sind „Real Fakes“. Dabei handelt es sich um Einzelpersonen, die sich Fake-Profile zulegen. Oft sind sie harmlos. Sie können aber auch negative Absichten haben. Auch deswegen ist es empfehlenswert, nicht jede Freundschaftsanfrage anzunehmen.

Allgemeine Tipps zum Datenschutz

Für die private Kommunikation sollte man überlegen, ob man nicht auf eine Alternative umsteigt oder möglichst viele unterschiedliche Kanäle verwendet. E-Mail, iMessage oder Apps wie Telegramm können sinnvolle Alternativen sein.

Generell ist es sinnvoll, die Datenschutz-Einstellungen eher scharf einzustellen. Im besten Fall sind persönliche Informationen nur für den engsten Freundeskreis sichtbar. Das heißt, auch wenn Du Dir nicht persönlich bekannte Personen zu deinem Freundeskreis hinzufügst, sollten sie nur das sehen, was Du für öffentlichkeitstauglich hälst bzw. was du aktiv mit ihnen teilst.

Als generelles Prinzip wird häufig die Daten-Sparsamkeit empfohlen. Daten sollten möglichst sparsam weiter gegeben werden. Lieber einmal weniger teilen als einmal zu viel. Als kleine Faustregel: Würdest du wollen, dass dein Beitrag von deinem Vater, deinem Nachbarn, deiner Lehrerin oder Chefin gesehen wird? Ist das nicht der Fall, dann solltest du ihn lieber nicht teilen.

Es lohnt sich auch zu prüfen, welche Informationen Fremde und Freunde tatsächlich von euch sehen. Dazu gibt es mehrere Möglichkeiten.

Bittet einmal darum, von einem fremden Konto auf Euer Profil zuzugreifen. Schaut auch einmal, was von eurem Profil zu sehen ist, wenn ihr nicht eingeloggt seid. Häufig ist der erste Treffer bei Google zu eurem Namen euer Profil bei Facebook, Twitter oder YouTube. Wenn ein möglicher Arbeitgeber nach euch googelt, könnte also euer Profil und die öffentlich zugänglichen Infos dort das erste sein, was er von euch sieht.

Betrachtet grundsätzlich alles als öffentlich, was ihr im Internet postet. Das gilt auch, wenn ihr die Privatsphäre-Einstellungen scharf gestellt habt. Alles, was online ist, kann grundsätzlich auch öffentlich werden. Beziehungen und Freundschaften können kaputt gehen und manchmal sind die verschmähten Partner auf Rache aus. Ein Screenshot ist schnell gemacht und geteilt.

Je mehr ihr teilt, desto mehr weiß das Netzwerk über euch. Weniger ist also immer besser.

Denkt immer daran, dass es Bereiche gibt, die ihr nicht kontrollieren könnt. Dazu gehört die Frage, wie eure Freunde mit euren und ihren eigenen Daten umgehen. Du kannst Deine Freundesliste so einstellen, dass sie für niemanden einsehbar ist. Aber dein Freund kann seine Liste so einstellen, dass jeder sieht, dass du mit ihm befreundet bist. Darauf hast du grundsätzlich keinen Einfluss. Deswegen solltest Du auch deine Freunde zur Datensparsamkeit ermutigen.

Die Axiome des Datenschutzes

Alles, was irgendwo digital gespeichert ist, kann grundsätzlich öffentlich werden. Das kann ganz simpel durch Diebstahl deines Handys geschehen. Oder durch Viren auf deinem Computer.

Alles, was einmal im Internet ist, kann nicht mehr zurückgeholt werden. Selbst, wenn man es löschen lässt, kann es sich jemand privat kopiert haben oder es liegt in einem Archiv wie archive.org.

alles, was du veröffentlichst, kann mit dir in Verbindung gebracht werden. Wenn du etwa einen politisch fragwürdigen Inhalt kommentarlos teilst, gehen viele Nutzer automatisch davon aus, dass du dem Geteilten zustimmst.

Jede Information, die das Netzwerk einmal über Dich hat, behält es auch. Die Netzwerke bieten keine unkomplizierte Möglichkeit, einzelne Informationen gezielt zu löschen. Auch wenn Andere oder du selbst die Daten nicht mehr sehen können, sind sie immer noch in den Datenbanken der Netzwerke. Was passiert, wenn das Netzwerk pleitegeht oder von einem anderen Unternehmen aufgekauft wird. Selbst, wenn du dein Profil löschst, werden deine Daten nicht vollständig gelöscht.

alles, was du veröffentlicht, kann eventuell gegen dich oder deine Freunde verwendet werden. Wenn du dich negativ über jemand anderen äußerst und deine Freunde es liken oder weiter verbreiten, kann das die betroffene Person mitbekommen. Dann kann es großen Ärger geben. Das gilt auch und vor allem, wenn es vielleicht scherzhaft gemeint war. Im Internet werden solche ironische Inhalte oft nicht verstanden.

Du bist nicht nur für deinen eigenen Datenschutz, sondern auch für den deiner Freunde verantwortlich. Achte also darauf, welche Beiträge du teilst. Würdest du diesen Beitrag teilen, wenn er über dich handeln würde? Möchtest du wirklich, dass dein nächster Arbeitgeber oder Kunde sieht, wie du eine Wodka-Flasche auf Ex trinkst? Sind deine Freunde auch in 10 Jahren noch dankbar, wenn Party-Fotos mit ihnen in Verbindung gebracht werden?

Alles, was du veröffentlichst, sagt etwas über dich aus. Jede Information ist ein Baustein für ein Gesamtbild über dich. Dabei spielt es keine Rolle, ob die Daten von einem Programm oder von einer Person ausgewertet werden.

Alles, was missverstanden werden kann, wird missverstanden: Ein lustiger, zweideutiger oder ironischer

Spruch ist schnell abgesetzt. Doch gerade in der digitalen Kommunikation kannst du nie beeinflussen, wer etwas wie wahrnimmt. Dann wird aus einem flapsigen Spruch schnell ein Shitstorm. In der digitalen Kommunikation fehlen zusätzliche Informationsebenen wie die Körpersprache oder Stimmlage. Zudem werden Kommunikationen häufig aus dem Zusammenhang gerissen. Dann steht eine Aussage für sich und wird auch so wahrgenommen. Symbole wie Emoticons oder Emojis sind kein Ersatz für Körpersprache oder den Kontext des Beitrags.

Grundsätze des Datenschutzes

Die folgenden Grundsätze sollen dir helfen, deinen Umgang mit deinen persönlichen Daten zu durchdenken.
Teile nichts, was deine Mutter, deine Lehrerin oder dein Nachbar auch sehen dürften, ohne dass es dir peinlich ist.
Sage nichts, was du nicht auch öffentlich sagen würdest.
Sage nichts über jemanden, was du ihm nicht auch ins Gesicht sagen würdest.
Teile nichts, was dir in zehn oder 20 Jahren peinlich sein könnte.
Mache nichts öffentlich wenn du es privat halten kannst.
Im Folgenden gibt es Tipps zu den einzelnen Netzwerken.

Browser als Alternative

Grundsätzlich lassen sich auch einige Funktionen der Netzwerke auch ohne Anmeldung nutzen. Bei YouTube ist das am einfachsten.
Generell bieten die Browser auch für angemeldete Nutzer mehr Schutz-Möglichkeiten als die Apps der Anbieter. Überlegt euch also, ob ihr immer die App verwenden müsst.

Apps

Der erste Ansatzpunkt ist bereits die Frage, welche Zugriffsrechte du der jeweiligen App einräumst. Bestimmte Rechte müssen sinnvollerweise eingeräumt werden. Dazu gehört der Zugriff auf Videos, Kameras oder Mikrofon.
Insgesamt solltest du aber überlegen, welche Rechte du der App einräumst und ob du diese Rechte dauerhaft geben musst. Braucht die App tatsächlich Zugriff auf deine Kontakte oder deinen Standort?

Facebook

Die Datenschutzeinstellungen sind bei Facebook sehr detailliert möglich. Das beginnt schon beim eigenen Profil. Sollen Fremde unbedingt euren Beziehungsstatus, das Geburtsdatum oder den Wohnort sehen? Ist es wirklich wichtig, dass alle Freunde sehen, mit wem ihr noch befreundet seid oder auf welche Veranstaltungen ihr geht?
Facebook verfügt wahrscheinlich über die persönlichsten Informationen. Generell sollten hier die Datenschutz-Einstellungen gründlich durchgesehen werden. Um sicher zu gehen, kannst du eine mit dir befreundete Person fragen, was sie von dir sehen kann. Generell sollten die Datenschutzeinstellungen eher schärfer als schwächer eingestellt werden.

Freunde

Es gibt mittlerweile sehr gut gemachte Fake-Profile auf Facebook. In der Regel sind sie dazu gedacht, Spam zu verschicken oder dienen politischen Zwecken. Facebook versucht, diese Profile möglichst automatisch aufzuspüren. Deshalb versuchen die Bots auch, möglichst natürlich zu erscheinen. Um ein echtes Profil vorzutäuschen, wollen die Bots auch mit realen Menschen befreundet sein. Nehmt also Freundschaftsanfragen nur an, wenn ihr die Personen tatsächlich

kennt oder es eine Verbindung mit diesen Personen gibt. Da manche aus eurem Freundeskreis vielleicht jede Anfrage ohne Prüfung annehmen reicht es nicht aus, dass eine eurer Freunde mit dem Anfragenden befreundet ist.
Auch könnt ihr steuern, welche Freunde welche Informationen sehen. Dazu müsst ihr eure Freunde in Gruppen kategorisieren. Heute ist es üblich, auch Kollegen, die Vorgesetzten oder Nachbarn in der Freundesliste zu haben, also Menschen, denen man persönlich nicht so nahe steht. Teilt ihr private Informationen, könnt ihr in gewissem Maße steuern, wer welche Informationen sieht.
Es kann aber immer passieren, dass die Informationen doch von Leuten gesehen werden, die es eigentlich nicht sehen sollten. Gerade blinden Menschen kann es schnell passieren, dass sie eine Einstellung übersehen und schon ist der private Beitrag öffentlich. Denkbar ist auch ein Software-Fehler von Facebook. Seid also generell umso achtsamer, je persönlicher die Informationen sind. Überlegt euch bei sehr persönlichen Informationen, ob ihr sie überhaupt teilen wollt.
Es ist generell sinnvoll, die Freundesliste nicht öffentlich sichtbar zu machen.

Beiträge

Bei den Beiträgen in eurer Chronik könnt ihr jeweils festlegen, wer die Beiträge sieht. Ist dieser Beitrag oder dieses Foto tatsächlich für die Öffentlichkeit oder euren ganzen Freundeskreis gedacht? Oder sollte das nicht lieber an eine ausgewählte Gruppe gehen?
Facebook erlaubt genau zu steuern, wer eure Beiträge sieht. Ihr könnt auch einzelne Personengruppen erstellen, für die ihr eure Beiträge jeweils freigeben wollt. Es ist nur selten sinnvoll, persönliche Beiträge auf öffentlich zu stellen.

Gruppen

Was in größeren Facebook-Gruppen passiert, sollte grundsätzlich als öffentlich betrachtet werden. Ab einer bestimmten Gruppengröße ist nicht mehr zu verhindern, dass solche Informationen auch von Leuten gelesen werden, die das vielleicht nichts angeht.
Verhaltet euch also in Gruppen immer so, als ob eure Beiträge und Kommentare öffentlich sind und von jedem gelesen werden können. Ausnahme sind private Kleingruppen, wo ihr tatsächlich alle Teilnehmerinnen persönlich kennt.
Facebook erlaubt das Erstellen nicht-öffentlicher Gruppen. Die Gruppen und ihre Inhalte sind dann nicht über die Suche sichtbar.
Wenn du Gruppenbetreiber bist,kannst du die Gruppe so einstellen, dass die Beiträge nur für Mitgleider sichtbar sind. Die Mitglieder öffentlicher Gruppen sind immer auch für Nicht-Mitglieder sichtbar. Wenn sich einer eurer Freunde sich die Liste der Gruppen-Mitglieder ansieht, sieht er euren Namen als Erstes, wenn ihr dort Mitglied seid. Standardmäßig wird er auch informiert, wenn einer seiner Freunde etwas in einer Gruppe postet, in der ebenfalls Mitglied ist.
Bei vielen Gruppen mag dir das recht sein. Aber willst du etwa, dass dein Freund sieht, dass du Mitglied in einer bestimmten politischen Gruppe bist?
Denke auch daran, dass Facebook deinen Freunden Gruppen empfiehlt, in

denen du Mitglied bist. Also auch Freunde, die nichts mit dem Gruppenthema zu tun haben, könnten erfahren, welchen Gruppen du angehörst.

Twitter

Anders als Facebook ist Twitter grundsätzlich für die öffentliche Kommunikation gedacht. Alles, was du selber twitterst, likest oder retweetest kann grundsätzlich innerhalb weniger Sekunden von Anderen wahrgenommen werden. Nicht wenige Karrieren wurden durch unbedachte Tweets beendet.

Wenn du eine Aussage retweetest, gehen alle davon aus, dass du dieser Aussage zustimmst. Ist das nicht so, solltest du den Tweet nicht unkommentiert teilen.

Twitter kann so eingestellt werden, dass nur deine Follower sehen, was du twitterst. Diese Funktion heißt "Deine Tweets schützen". Nimmst du allerdings jeden Follower an, ist dieser Schutz natürlich hinfällig.

Bei Twitter ist es grundsätzlich einfacher als bei Facebook, eine beliebige Identität anzulegen. Du musst also nicht deinen richtigen Namen oder ein reales Foto von dir verwenden.

YouTube/Google

Das Gleiche gilt auch für YouTube. Likes und Kommentare können grundsätzlich von jedem wahrgenommen werden.

Auch hier gilt: Empfiehlst du ein Video kommentarlos weiter, werden viele annehmen, dass du das Video gut findest oder den Aussagen zustimmst.

Da YouTube sich ohne Anmeldung nutzen lässt, sollte man es auch grundsätzlich ohne Anmeldung nutzen. Likes, Kommentare oder eigene Playlists sollten gut überlegt werden.

Bei YouTube ist zu beachten, dass es wie auch blogger.com und einige andere Portale zu Google gehört. YouTube/Google kann auch ohne, dass du einen Google-Account hast oder eingeloggt bist ein Profil erstellen, deine Daten sammeln und auswerten wie Facebook. Das geschieht über Cookies und andere Technologien, die unter dem Stichwort Tracking zusammengefasst werden. Hier helfen nur spezielle Browser-Erweiterungen, die das Tracking verhindern sollen. Diese Möglichkeiten gibt es allerdings nicht in den Apps, sondern nur im Browser.

WhatsApp

WhatsApp ist kein soziales Netzwerk, weil die Kommunikation entweder persönlich oder in nicht-öffentlich zugänglichen Gruppen stattfindet.

Dennoch muss auch WhatsApp Geld verdienen. WhatsApp hat aktuell keine andere Möglichkeit, Geld zu verdienen, als die Daten der Nutzer zu analysieren. Außerdem kann der Eigentümer von WhatsApp, das ist Facebook, die Daten aus beiden Bereichen zusammenführen. Offiziell dürfen sie das in Deutschland nicht. Doch kann niemand überprüfen, ob sie sich daran halten.

Grundsätzlich gilt: Du solltest den Einladungslink zu einer Gruppe nicht öffentlich, etwa auf Facebook oder Twitter teilen. Am besten ist es, gar nicht mit diesen Einladungslinks zu arbeiten. Du kannst nicht kontrollieren, ob deine Freunde den Link nicht selbst weiter geben oder öffentlich teilen. An den Telefonnummern ist

nicht zu erkennen, wer sich dahinter verbirgt. Das Risiko des Ausspionierens ist deutlich geringer, wenn sich die Interessierten bei dir persönlich melden müssen, um in die Gruppe aufgenommen zu werden.

Weitere Infos

Informationen zu aktuellen Debatten zum Datenschutz gibt es im Blog netzpolitik.org.
Jedes große Netzwerk stellt ausführliche Informationen und Hilfen zu den Datenschutz-Richtlinien und Einstellungen bereit:
Facebook: https://www.facebook.com/privacy/explanation
Twitter: https://twitter.com/de/privacy
Google/YouTube: https://policies.google.com/terms?hl=de
Über eine Suchmaschine findest du daneben unabhängige Tipps und weitere Informationen zu den einzelnen Netzwerken.
Weitere Informationen findest Du bei der Datenschutzbeauftragten des Bundes sowie der Bundesländer. Die Website der Datenschutzbeauftragten findest du unter https://www.bfdi.bund.de/DE/Home.
Microsoft gibt Informationen zu Datenschutz-Einstellungen bei Windows 10
https://support.microsoft.com/de-de/help/4014916/windows-10-choose-your-privacy-settings-after-updating
Der Firefox bietet eine Reihe von Erweiterungen für den Datenschutz
https://addons.mozilla.org/de/firefox/extensions/privacy-security/
Das Portal „Mobil sicher“ bietet speziell Tipps zum Datenschutz bei Smartphones: https://mobilsicher.de/.
Beratung bei Problemen mit dem Datenschutz bieten neben den Datenschutz-Beauftragten auch die lokalen Verbraucherzentralen.