Datenschutz in Sozialen Netzwerken – Meine Daten gehören mir

Autorin: Valie Djordjevic

Soziale Netzwerke gehören zum Alltag. Dabei sammeln die Anbieter jede Menge Daten. Worauf sollten Nutzer achten? Wie können sie Einfluss nehmen und ihre Daten vor Missbrauch schützen?

Die verschiedenen Sozialen Netzwerke haben unterschiedliche Schwerpunkte: Facebook spricht überwiegend Privatnutzer an, Xing oder LinkedIn helfen beim Aufbau eines Business-Netzwerks. Bei Instagram oder YouTube stehen die präsentierten Fotos oder Videos im Vordergrund. Das gilt auch für Apps wie Snapchat, die dabei aber mehr auf den schnellen Austausch im Freundeskreis zielen. Messenger-Dienste wie WhatsApp sind zwar keine Sozialen Netzwerke im engeren Sinn, haben aber teils ähnliche Funktionen, etwa Postings für bestimmte Gruppen.

So oder so gilt jedoch: Nutzt man die Dienste, sammeln die Anbieter mehr oder weniger umfangreiche Datenbestände. Auch wenn die Nutzung der Dienste in der Regel kostenlos ist, wollen die Anbieter natürlich Geld verdienen. Das geschieht meist entweder dadurch, dass für erweiterte Funktionen bezahlt werden muss, zum Beispiel bei Xing oder LinkedIn. Oder die Anbieter verwenden die gesammelten Daten, um ihren Nutzern zielgerichtete Werbung anzuzeigen, so etwa Facebook. Daneben gibt es einige Mischformen.

Wozu Datenschutz?

Wozu überhaupt Datenschutz? Ich hab doch nichts zu verbergen! So denken viele, aber es gibt schnell Situationen, in denen man doch lieber Kontrolle darüber hätte, was mit den eigenen Daten geschieht. Wenn einmal etwas veröffentlicht wurde, ist es nicht selten schwer, es wieder vollständig und dauerhaft aus dem Netz zu entfernen. Das gilt besonders, wenn Dateien über Messenger-Apps versendet werden. Sie befinden sich dann nicht mehr nur auf dem Server des Anbieters, sondern zusätzlich auf allen angeschriebenen Geräten.

Wer bei Sozialen Netzwerken sinnvoll mitmachen will, muss einiges von sich preisgeben. Das fängt häufig mit dem Realnamen an und hört bei Wohnort, Beziehungsstatus und Lieblingsmusik noch lange nicht auf. Es gibt stets Risiken im Umgang mit privaten Daten bei solchen Diensten, aber das heißt nicht, dass man deshalb gar keine Sozialen Netzwerke nutzen sollte. Allerdings sollte man sich vorher gut überlegen, welche und wie viele

Informationen man bei welchem Dienst über die eigene Person preisgibt. Eng mit Datenschutzaspekten verbunden ist die Frage nach der Datensicherheit, also nach dem Schutz vor unbefugtem Zugriff auf die Daten.

Worauf sollten Nutzer achten, damit die Privatsphäre geschützt bleibt?
Wer Soziale Netzwerke nutzt, sollte die folgenden Punkte im Hinterkopf behalten:

- Den Begriff der Datensparsamkeit: Welche Infos sind wirklich notwendig, um einen Dienst zu benutzen?
- Könnten die Informationen, die ich ins Netz gestellt habe, mir später unangenehm werden, wenn sie zum Beispiel mein Arbeitgeber sieht oder andere Stellen? Könnten mir Nachteile dadurch erwachsen?
- Wer kann die Informationen sehen? Welche Einstellungsmöglichkeiten gibt es?
- Welche Rechte und Befugnisse beanspruchen die Anbieter für sich?

Diese Punkte schauen wir uns im Folgenden genauer an, oft an Beispielen aus Facebook, dem mittlerweile „klassischen“ Sozialen Netzwerk. Darüber hinaus gibt es Tipps zu verbreiteten Diensten wie Instagram und Snapchat.

Datensparsamkeit fängt beim Registrieren an
Bei den wenigsten Sozialen Netzwerken ist es wirklich notwendig, seinen vollen Namen, die echte Adresse oder die Telefonnummer anzugeben, um den Dienst nutzen zu können. Schließlich kauft man dort – zumindest derzeit noch – in der Regel nicht ein oder erhält Rechnungen, wofür der Anbieter Geschäftsdaten benötigen würde. Dennoch fragen viele Sozialen Netzwerke recht umfassend sehr unterschiedliche Daten ab.

Hier empfiehlt es sich, selektiv und sparsam mit den eigenen Angaben und Daten umzugehen. Facebook will seine Nutzer dazu verpflichten, bei der Anmeldung einen echten Namen anzugeben. Das ist rechtlich umstritten, Facebook versucht jedoch bis auf weiteres, Konten mit Pseudonymen herauszufiltern und – zumindest temporär – zu sperren. Das gelingt dem Dienst desto besser, je eher es sich erkennbar um Phantasienamen handelt.

Daneben wird beim Registrieren für Soziale Netzwerke meist ein Geburtsdatum, eine E-Mail-Adresse oder eine Handynummer abgefragt. Einige dieser Angaben können nach der Anmeldung versteckt werden, sodass Dritte sie nicht sehen können – diese Möglichkeit sollte man nutzen. Es kann besser sein, für Registrierungen eine zweite E-Mail-Adresse zu benutzen, um die persönliche Adresse zu schützen.

Vor allem mit Telefonnummern und Wohnadressen sollten Nutzer vorsichtig sein: Sind sie einmal in die Öffentlichkeit gelangt, wird es schwierig, das ungeschehen zu machen. Das muss nicht zwangsläufig zum Problem werden, aber es kann: Mit den Daten können sich zum Beispiel Kriminelle als jemand anderes ausgeben und die fremde Identität zu Straftaten benutzen (Identitätsdiebstahl). Aber auch sonst möchte man vielleicht nicht der ganzen Welt verraten, wo man wohnt und wie man angerufen werden kann. Hier gilt: Nach Möglichkeit gar nicht angeben oder zumindest die Sichtbarkeit einschränken.

Bei vielen anderen Diensten ist es nicht nur problemlos möglich, sondern auch recht verbreitet, ein Pseudonym zu verwenden. Das gilt zum Beispiel für Instagram. Seit der Dienst von Facebook aufgekauft wurde, wird er allerdings zunehmend mit dem Sozialen Netzwerk verzahnt. Wer Wert darauf legt, seine Profile getrennt zu halten, sollte daher beispielsweise von vornherein eine andere E-Mail-Adresse bei Instagram hinterlegen als bei Facebook. Nicht allen Nutzern ist bekannt, dass neben den Daten, die sie aktiv beisteuern, sehr viele weitere gesammelt werden. Das sind etwa Daten darüber, wann sie den „Gefällt mir“-Button von Facebook klicken, welche Links sie in ihrem Facebook-Feed anklicken und welche Webseiten außerhalb von Facebook sie besuchen. Mehr Informationen über die Datensammlung und -verwendung finden sich im Artikel „Datenschutz auf Facebook“ (siehe die weiterführenden Hinweise unten).

Adressbuch-Zugriff und Einladungsfunktionen

Im Zentrum Sozialer Netzwerke stehen die Kontakte. Bei Facebook werden sie „Freunde“ genannt, bei Twitter und Instagram „Follower“. Von Kollegen über entfernte Bekannte bis hin zu reinen Online-Bekanntschaften ist alles dabei. Grundsätzlich sollte man sich überlegen, wen man in seine Kontaktliste aufnimmt. Bei Kontaktanfragen von Unbekannten gilt: Nicht wahllos akzeptieren, sondern erst einmal nachfragen oder überprüfen, um wen es sich handelt.

Wenn man sich neu anmeldet, hat man häufig erst einmal gar keine Kontakte. Manche Dienste bieten bei der Neuanmeldung an, das persönliche Adressbuch hochzuladen. Solche Angebote sollte man ausschlagen und lieber von Hand Kontakte suchen. Bekannt wurde hier besonders der „Freundefinder“ von Facebook: Vielen Nutzern war nicht klar, dass Facebook bei Nutzung des „Freundefinders“ nicht nur Zugriff auf das Adressbuch des E-Mail-Kontos erhielt, sondern automatisiert Einladungsmails an das gesamte Adressbuch verschickte. Nach einem Rechtsstreit mit Verbraucherschützern bewertete der Bundesgerichtsgerichtshof die Funktion Anfang 2016 als unzumutbare Werbebelästigung. Facebook hat die Funktionsweise zwar entsprechend geändert, grundsätzlich aber ist es immer ratsam, Daten von Dritten nicht ohne ihr Einverständnis auf Webseiten einzugeben oder hochzuladen.

Auch die mobilen Apps von Sozialen Netzwerken und Messenger-Diensten wollen nach der Installation meist auf die Kontaktliste und zum Teil weitere Inhalte und Funktionen des Smartphones zugreifen. Hier besteht in der Regel zwar keine Gefahr unverlangt versandter E-Mails. Wenn Apps aber allzu neugierig erscheinen und weitgehende Berechtigungen erfragen, die für die Funktionen der App nicht notwendig sind, sollte man genau hinsehen.

Bei den aktuellen mobilen Betriebssystemen – so in Apples iOS und Android ab Version 6.0 – können einzelne Berechtigungen meist verweigert oder zumindest nach dem Installieren wieder entzogen werden. Manche Apps funktionieren auch ohne entsprechende Freigaben gut. Andere – etwa Messaging-Dienste wie WhatsApp – lassen sich ohne den Zugriff auf das Adressbuch nicht sinnvoll nutzen. Nutzer können aber schrittweise vorgehen, die Berechtigungen zunächst abwählen und sie nur freischalten, wenn sie für eine bestimmte Funktion wirklich benötigt werden.

Sichtbarkeit für Inhalte richtig einstellen

Die verschiedenen Netzwerke bieten mehr oder weniger detaillierte Auswahlmöglichkeiten, welche der eigenen Informationen für andere zu sehen sind. Dabei sollte man sich bei keinem Anbieter auf die Voreinstellungen verlassen, sondern gezielt nachschauen, wer was sehen kann und welche Einstellungen es gibt. Manche Anbieter ändern gelegentlich von sich aus die eine oder andere Voreinstellung oder die vom Nutzer gewählte Einstellung, zum Beispiel im Rahmen von Aktualisierungen. Daher ist es zu empfehlen, diese von Zeit zu Zeit zu überprüfen.

Freundeslisten auf Facebook

Wenn die Freundes- beziehungsweise Kontaktliste so weit angewachsen ist, dass sich dort nicht nur die engsten Freunde, sondern auch entfernte Bekannte und Kollegen tummeln, ist es empfehlenswert, sich mit Freundeslisten zu beschäftigen. Facebook erlaubt darüber eine sehr detaillierte Kontrolle, wer welche Inhalte sehen darf.

So lässt sich beim Posten einstellen, welche Gruppe von Kontakten was sehen darf. Wenn man zum Beispiel jeweils eine Gruppe für enge Freunde und für berufliche Kontakte hat, lässt sich einstellen, dass nur die engen Freunde die Partyfotos vom Wochenende zu sehen bekommen. Trotz allem sollte man bedenken: Was mit geposteten Inhalten passiert, lässt sich über Freundeslisten und ähnliche Einstellungen zwar zu einem gewissen Grad steuern, aber nie vollständig kontrollieren. Der beste Schutz davor, Inhalte ungewollt öffentlich zu machen, liegt darin, sie nicht zu posten – auch nicht beschränkt.

Instagram und Snapchat: Öffentlich oder privat posten?

Weniger umfangreich, dafür aber übersichtlicher sind die Einstellungen zur Sichtbarkeit bei Snapchat und Instagram. In der Voreinstellung von Snapchat sind neue Fotos und Videos nur für Freunde sichtbar. Umgekehrt ist es bei Instagram: Wer seine Inhalte nicht öffentlich wissen will, aktiviert in den Einstellungen unter „Konto“ die Option „privates Konto“, um diese nur bestätigten Kontakten anzuzeigen.

Neben Snapchat haben auch Instagram und WhatsApp Postings eingeführt, die nach einer bestimmten Zeit automatisch verschwinden (bei letzteren „Stories“ und „Status“ genannt). So laden sie besonders dazu ein, Inhalte für den Moment zu verbreiten, ohne sich ständig Gedanken darüber machen zu müssen, wie man sich dauerhaft im Netz zeigt. Gleichwohl sollte man sich bewusst sein, dass die geposteten Inhalte über Screenshots, Zusatzfunktionen oder Dienste von Drittanbietern länger verfügbar bleiben oder neu abgespeichert werden können.

Unabhängig von der gewählten Einstellung gilt: Vorher nachdenken, was man veröffentlicht. Denn auch wenn man sich in seinem Online-Freundeskreis wie zu Hause fühlt, könnte es doch sein, dass nicht alle einem gleich wohlgesonnen sind. Kontrollfragen sind:

- Könnte es mir später peinlich sein oder unangenehme Konsequenzen haben?
- Könnte dadurch ein anderer geschädigt werden?

Personen auf Fotos markieren

Viele Dienste bieten an, Personen, die man auf eigenen oder fremden Fotos erkennt, mit Namen zu identifizieren. Beim Klick auf die Markierung wird man dann gleich auf das Profil der abgebildeten Person weitergeleitet. Sie kann die Markierung meist auch wieder entfernen – allerdings erst im Nachhinein. Beispiel Facebook: Man kann in den Privatsphäre-Einstellungen unter anderem festlegen, dass man jede Markierung überprüfen muss, bevor sie auf der eigenen Chronik veröffentlicht wird (unter „Einstellungen“, „Chronik und Markierungen“). Auf dem jeweiligen Profil, auf dem sie hochgeladen worden sind, ist sie allerdings nach wie vor zu sehen. Facebook arbeitet auch mit einer automatischen Gesichtserkennung. In Europa wurde die automatische Markierung bei der Gesichtserkennung nach Protesten von Datenschützern Anfang 2013 gestoppt.

Anzeige des Profils in Suchmaschinen steuern

Mit einer weiteren Option, die von manchen Netzwerken angeboten wird, lässt sich einstellen, dass die Profilseite zwar beim Suchen auf der Plattform angezeigt wird, aber nicht auf den Ergebnisseiten von Suchmaschinen wie Google oder Bing. So wird man nur von Mitgliedern innerhalb des Sozialen Netzwerks gefunden.

Bei Facebook findet sich die Option unter „Einstellungen“, „Privatsphäre“ im Punkt „Wer kann nach mir suchen?“. Wer Instagram mit sogenannten Web-Viewern verwendet, macht die einzelnen Postings häufig auch für Suchmaschinen zugänglich. Nutzt man diese nicht, so ist bei öffentlichen Instagram-Profilen zumindest die Profilseite über Suchmaschinen auffindbar.

Öffentlich gepostete Inhalte auf Twitter sind grundsätzlich auch für Suchmaschinen zugänglich, werden jedoch nur teilweise angezeigt. Twitter bietet keine spezifische Einstellung, um Suchmaschinen auszuschließen, aber die Option, das gesamte Konto auf privat zu schalten (in den Einstellungen unter „Datenschutz und Sicherheit“, „Meine Tweets schützen“). Dann sind die eigenen Tweets nur für Follower einsehbar, die man bestätigt hat.

Virengefahr nicht nur per E-Mail

Auch Spam und Schadprogramme können über Soziale Netzwerke verbreitet werden. Über Anhänge in Nachrichten oder gefälschte Links können Angreifer das eigene Konto kapern, um die Nachrichten weiterzuverbreiten oder Schadsoftware zu installieren. Spam auf Facebook verbreitet sich oft über massenhafte Markierungen von Kontakten. Wer etwa in einem Beitrag markiert wird, der mit angeblich reduzierten Markensonnenbrillen wirbt, sollte nicht auf den Link klicken, sondern die Markierung entfernen. Bei der Gelegenheit lässt sich auch einstellen, Markierungen von Facebook-Kontakten zu überprüfen, bevor sie in der Chronik erscheinen (siehe oben).

Ein prüfender Blick empfiehlt sich, wenn im Sozialen Netzwerk Links auf besonders reißerische Bilder oder Videos auftauchen. Eine vergleichbare Spielart sind gefälschte Nachrichten von Freunden, die einen Bild- oder Video-Link mit Fragen wie „Bist du das?“ enthalten. Wer auf den Link klickt, verbreitet ihn oft ungewollt weiter. Im schlimmsten Fall kann man sich Schadsoftware einfangen, die private Daten abfischt. Wer versehentlich Opfer wurde, sollte das eigene Profil auf gefälschte Postings und Nachrichten überprüfen und das Passwort ändern. Häufig ist es ratsam, den eigenen Browser auf unbekannte Erweiterungen und den Computer mit einem aktuellen Antivirenprogramm zu prüfen.

Anwendungen mit Bedacht verwenden

Ebenfalls sollte man aufpassen, welche Anwendungen und Webseiten mit dem eigenen Konto verknüpft werden. So lässt sich das Facebook-Konto oftmals verwenden, um sich bei anderen Diensten im Web anzumelden. Dritt-Anwendungen wiederum helfen zum Beispiel beim Posten auf Facebook, Instagram oder Twitter und stellen Zusatzfunktionen bereit.

Doch nicht alle Anbieter gehen mit den gewonnenen Daten und Berechtigungen so um, wie man es erwartet. Es ist ratsam, in Abständen zu überprüfen, welchen Dritt-Anwendungen Zugriff gewährt wurde und nicht mehr benötigte Apps zu entfernen. Bei Twitter und Facebook findet sich die Option unter „Einstellungen“, „Apps“, bei Instagram unter „Profil bearbeiten“ im Punkt „Autorisierte Anwendungen“.

Allgemeine Geschäftsbedingungen und mehr Kleingedrucktes: Was dürfen Anbieter und Nutzer?

Wer sich bei Sozialen Netzwerken anmeldet, muss in der Regel den Nutzungsbedingungen der Anbieter zustimmen und seitenlange Datenschutzerklärungen zur Kenntnis nehmen. Aber wer hat solche allgemeinen Geschäftsbedingungen (AGB) und andere Bestimmungen im Kleingedruckten wirklich gelesen?

Dabei können sie für die eigenen Rechte und Befugnisse entscheidend sein: AGB sind Vereinbarungen, die Nutzer mit den Diensteanbietern schließen. Auch wenn die Regeln meist einseitig diktiert werden, handelt es sich rechtlich betrachtet um einen Vertrag. Darüber wollen sich die Anbieter meist in alle Richtungen absichern und sich entsprechende Befugnisse für den Betrieb des Dienstes einräumen.

Datenschutzbestimmungen wiederum haben eine andere Funktion: Sie dienen in erster Linie dazu, bestimmte Informationspflichten der Betreiber gegenüber ihren Nutzern umzusetzen. Sie werden häufig geändert und ergänzt. Hintergrund solcher Änderungen können zum Beispiel Änderungen an Firmenstrukturen sein oder das Vorhaben der Anbieter, Daten an Partnerunternehmen weiterzureichen.

Nutzer sitzen bei der Frage, ob sie die AGB akzeptieren, meist am kürzeren Hebel. Wer nicht zustimmt, kann einen Dienst normalerweise auch nicht nutzen. Weil der Einzelne auf AGB kaum Einfluss nehmen kann, sieht das Gesetz eine sogenannte Inhaltskontrolle vor: Nicht alles, was Anbieter sich im Kleingedruckten herausnehmen wollen, ist auch rechtlich wirksam. Gelegentlich gehen Verbraucherschützer gegen einzelne, für Nutzer besonders nachteilige Klauseln vor und haben teilweise erreicht, dass sie nicht mehr verwendet werden dürfen.

Datenlecks: Ein Risiko bleibt

Gegen den unbefugten Zugriff auf Nutzerdaten treffen die Sozialen Netzwerke zahlreiche Vorkehrungen. Das Restrisiko eines Datenlecks bleibt aber letztlich immer bestehen, sobald Daten durch elektronische Netze wandern. So tauchten 2014 etwa Hunderttausende Snapchat-Fotos im Netz auf. Ursache waren wahrscheinlich Sicherheitslücken bei

„Snapsaved“, einem Zusatzprogramm zum dauerhaften Speichern der geposteten Inhalte. Auch LinkedIn forderte 2016 Millionen seiner Nutzer auf, ihr Passwort zu ändern. Durch ein Datenleck waren die Zugänge unsicher geworden.

Grundlegende Vorsichtsmaßnahmen bei der Internetnutzung gelten auch bei Sozialen Netzwerken. Dazu gehört etwa, ein sicheres Passwort zu wählen, es regelmäßig zu ändern und es nicht für unterschiedliche Dienste zu verwenden. Eine Anmeldung in zwei Schritten – auch Zwei-Faktor-Authentifizierung genannt – erhöht die Sicherheit vor unbefugtem Zugriff. Zum Anmelden wird dann neben dem Passwort ein zusätzlicher, auf dem Handy sichtbarer Code benötigt. Die meisten gängigen Dienste, darunter Facebook, Twitter, Instagram, Snapchat, WhatsApp und LinkedIn bieten diese Option. Ganz grundsätzlich lohnt es sich, sich mit den Datenschutzmöglichkeiten des eigenen Rechners oder Smartphones und des Browsers zu beschäftigen.

Soziale Netzwerke stehen oft in der Kritik wegen ihres Umgangs mit den Daten der Nutzer. Ein Text wie dieser kann nur als erster Hinweis dienen, sich weiter damit zu beschäftigen, wie man seine Daten schützen kann. Da sich die Plattformen weiterentwickeln, sollten Nutzer auch immer wieder abwägen, welche Konsequenzen sie daraus für die eigene Nutzung ziehen.

Mehr Informationen

- www.klicksafe.de/irights – Schwerpunkt: Datenschutz auf Facebook – Wem gehören meine Daten?
- www.klicksafe.de/themen/datenschutz – Tipps und weitere Materialien zum Thema Datenschutz
- www.mobilsicher.de/datenschutz/5560 – Infos und Anleitungen zu App-Berechtigungen auf dem Smartphone unter iOS und Android

Aktualisierte Version 2017