In welchen Situationen könnte meine Privatsphäre gefährdet sein?



Deine **Privatsphäre** kann im Netz an sehr vielen Stellen gefährdet sein. Hier sollen **einige wichtige Beispiele** genannt und erklärt werden. Die einzelnen Abschnitte **überschneiden** sich teilweise, weil z.B.

- soziale Netzwerke (Abschnitt 1) auch
- Geodaten (Abschnitt 2),
- biometrische Methoden (Abschnitt 3) und
- Cookies (Abschnitt 4)

verwenden. Sei Dir also bewusst, dass die folgenden Situationen zusammen spielen.

(I) Soziale Netzwerke

Bei der Benutzung von sozialen Netzwerken wie Facebook oder SchülerVZ kann Deine Privatsphäre auf verschiedene Art gefährdet sein.

1. Du könntest **versehentlich Informationen über Dich dem »falschen« Personenkreis preisgeben**, weil die Privatsphäre-Einstellungen nicht so sind, wie Du das möchtest oder wie Du glaubst.
2. Du **gibst grundsätzlich alle Informationen dem Anbieter des Netzwerks preis**, der dann wiederum weitreichende Möglichkeiten für die Verwendung (Werbung, Verkauf Deiner Daten etc.) oder des Missbrauchs hat.
3. Deine Daten könnten **durch Hacker gestohlen** und dann zu Geld gemacht werden, wenn diese durch Sicherheitslücken große Mengen von Datensätzen aus den Datenbanken eines Netzwerks stehlen, was immer wieder vorkommt.

Informationen für die »falschen« Leute sichtbar

Die Anbieter von Sozialen Netzwerken verdienen am meisten Geld, wenn Du möglichst viele Informationen über Dich möglichst öffentlich zeigst. Dann bist Du für die Anbieter von Werbung am attraktivsten und diese sind bereit mehr Geld für die Werbung an das soziale Netzwerk zu bezahlen. Daher werden in den meisten Netzwerken die Einstellungen für die Privatsphäre in regelmäßigen Abständen geändert. Das klingt dann meistens so:

> Um Dir die Benutzung unseres Dienstes noch einfacher zu machen, haben wir die Seite mit den Privatsphäre-Einstellungen überarbeitet und vereinfacht. Du kannst nun … bla bla bla …
>
> Wir wollen, dass Du genau kontrollieren kannst, mit wem Du Informationen teilst … bla bla bla …

Außerdem folgt eine Menge weiterer Text, in dem irgendwo versteckt auch steht, dass von nun an alle Fotos öffentlich sind oder dass alles, was Du nicht innerhalb von vier Wochen als »privat« kennzeichnest, für immer öffentlich sein wird – oder etwas Ähnliches.

Der Zweck dieser Änderungen ist *oft* genau das Gegenteil von dem, was der Anbieter sagt: Es geht nicht darum, dass Du möglichst gut kontrollieren kannst, mit wem Du etwas teilst, sondern darum, dass Du den Überblick über die ganzen Einstellungsmöglichkeiten verlierst und außerdem die *wichtigen* Änderungen (z.B. öffentliche Fotos) nicht bemerkst. Du sollst ja schließlich in Zukunft möglichst vieles möglichst öffentlich posten.

Wenn Du schon etwas länger bei einem Sozialen Netzwerk wie z.B. Facebook angemeldet bist, hast Du bestimmt schon mehrere solcher Änderungen mitbekommen. **Kennzeichnend ist, dass man immer von *Dir* verlangt, dass Du Dich *aktiv* mit den Einstellungen auseinandersetzt und etwas tust.** Wenn Du nichts tust, werden die weniger strengen Einstellungen übernommen und Deine Informationen sind künftig einem größeren Kreis von Personen zugänglich.

Damit hast Du auch schon eine **Möglichkeit, die Vertrauenswürdigkeit eines Netzwerk-Anbieters zu beurteilen**: Wenn *Du* die ganze »Arbeit« machen musst, wenn Du nach Informationen über Änderungen suchen musst oder die Einstellungen extrem kompliziert sind, ist der Anbieter *nicht vertrauenswürdig*, denn er setzt offensichtlich auf Deine Unkenntnis und möchte, dass Du möglichst *nicht* genau weißt, mit wem Du welche Informationen teilst.

Weitere Informationen

- Facebook will noch mehr Nutzerdaten weitergeben
- Datenschützer besorgt über Änderungen bei Facebook
- Facebook will Lebensarchiv werden
- Facebook aktiviert Gesichtserkennung in Deutschland
- Für den Facebook-Chef ist Privatsphäre nicht mehr zeitgemäß
- Facebook nervt Nutzer mit verschleierter Werbung



Wie kannst Du Dich schützen?

- Wenn Dir Deine Privatsphäre wichtig ist, bleibt Dir nur, Dich *tatsächlich* aktiv mit den Privatsphäre-Einstellungen auseinanderzusetzen und nach jeder Änderung wieder neu zu kontrollieren, ob alles so offen oder privat ist, wie Du das möchtest.
- Wenn ein Anbieter mehrfach sehr respektlos mit Dir als Nutzer umgeht, kannst Du natürlich auch überlegen, ob Du diesem Anbieter weiterhin Deine Daten anvertrauen möchtest oder das Netzwerk nicht doch lieber verlässt.

Hier sind noch einige Artikel, die Dir helfen können, die Einstellungen und Hintergründe in Deinem Netzwerk besser zu verstehen:

- Sicherheit in sozialen Netzwerken
- Materialien zum Schutz der Privatsphäre in Sozialen Netzwerken - Facebook, dort die PDF-Datei Profilinformationen und Inhalte, die du teilst
- Datenschutz in sozialen Netzwerken – Meine Daten gehören mir
- Privatsphäre in Facebook-Chronik

Der Netzwerk-Anbieter weiß alles über Dich

Wenn Du Daten in ein soziales Netzwerk hochlädst oder Informationen über Dich postest, gibt es natürlich immer Personen, die grundsätzlich **alles** sehen können. Denn um das Netzwerk technisch zu betreiben, die Software zu programmieren, die Server zu warten etc. müssen zumindest einige Personen uneingeschränkten Zugriff haben.

Außerdem sind Deine Daten attraktiv, weil man mit ihnen Geld verdienen kann. Es besteht also immer die Versuchung, heimlich Deine Privatsphäre-Einstellungen zu ignorieren und Deine Daten z.B. an andere Firmen zu verkaufen. Du würdest davon in der Regel nichts merken, weil Du kaum wissen kannst, woher jemand, der Dir z.B. eine Werbe-Mail schickt, Deine E-Mail-Adresse hat. Oder warum Du auf einer bestimmten Website ausgerechnet eine Werbeanzeige über Fußballschuhe oder Nagellack siehst, nachdem Du einem Freund oder einer Freundin beim Facebook davon erzählt hast, dass Dich das interessiert.

Grundsätzlich bist Du also darauf angewiesen, dem Anbieter eines sozialen Netzwerks zu **vertrauen**, weil dieser im Prinzip alles mit Deinen Daten machen kann solange er sich nicht dabei erwischen lässt, gegen Gesetze zu verstoßen.

Ob dieses Vertrauen gerechtfertigt ist, kann man nicht immer leicht beurteilen. Du kannst Dir aber überlegen, wie der Anbieter in verschiedenen Regeln oder Regeländerungen mit Dir als Nutzer umgegangen ist.

- Wurdest Du gut und rechtzeitig informiert?
- Hat man Dir die Möglichkeit gegeben, Deine Meinung angemessen zu äußern?
- Gibt es Möglichkeiten, den Netzwerkanbieter schnell und unkompliziert zu kontaktieren?
- Wenn man eine Mail schreibt, bekommt man dann zügig Antwort?

Die Antworten auf solche Fragen geben einen Hinweis darauf, ob der Anbieter Dich als Nutzer respektiert oder ob er Dich eher als »Ware« ansieht, mit der er möglichst problemlos Geld verdienen möchte.

Weitere Informationen

- Was Facebook über dich weiß
- Facebook: Deine Daten gehören(!) uns. (Wirklich.)
- Was Vorratsdaten über uns verraten (hier geht es um einen Telefonanbieter, die Situation und die Konsequenzen sind aber mit einem sozialen Netzwerk vergleichbar)

Wie kannst Du Dich schützen?



- **Sei sparsam mit Deinen Daten**. Poste nur das, was Du für absolut wichtig hältst und lasse die übrigen Felder frei. Je weniger jemand über Dich weiß, desto weniger Informationen kann er missbrauchen.
- Achte auf die Art, wie der Anbieter eines Netzwerks mir Dir kommuniziert. Wenn Du das Gefühl hast, Du wirst nicht respektiert, solltest Du nicht darauf vertrauen, dass der Anbieter mit Deinen Daten verantwortungsvoll umgeht.
- Informiere Dich, ob es die Möglichkeit gibt, dass Du die von Dir gespeicherten Informationen einsehen kannst. Mit der Zeit verliert man den Überblick, was



man alles gepostet hat. Wenn diese Möglichkeit *nicht* besteht, ist das ein weiteres Anzeichen dafür, dass dem Anbieter der Datenschutz und der respektvolle Umgang mit Dir nicht wichtig ist.

Datendiebstahl

Es kommt immer wieder vor, dass Hacker in soziale Netzwerk »einbrechen« und große Mengen von Daten stehlen. Das ist kriminell und es sind Kriminelle, die so etwas tun. Insofern kann man davon ausgehen, dass diese Leute auch kriminelle Handlungen mit den gestohlenen Daten vorhaben. Sie werden versuchen, möglichst viel Geld dafür zu bekommen.

Auch in diesem Bereich musst Du auf die Verantwortung des Netzwerkanbieters vertrauen:

- Tut dieser sein Möglichstes, um Sicherheitslücken der Software (und die gibt es *immer*) möglichst schnell zu schließen?
- Informiert er seine Nutzer, wenn Daten abhanden gekommen sind, damit diese sich schützen können?
- Kommt Datendiebstahl häufiger vor oder bleibt er eine Ausnahme?

Weitere Informationen

- Reihenweise Sicherheitslücken in sozialen Netzen
- Über 1 Million Datensätze bei SchülerVZ abgesaugt
- SchülerVZ-Datenlecks: auch geschützte Informationen ausgespäht
- SchülerVZ-Daten: Der florierende Markt für Datensammelprogramme
- Hotmail-Hacking für 20 US-Dollar



Wie kannst Du Dich schützen?

- Achte darauf, ob in den Medien Berichte über Datendiebstahl in Deinem sozialen Netzwerk auftauchen. Eine gute Quelle für solche Informationen sind z.B.
  - heise security
  - Golem
- Falls Du berichte über Datendiebstahl findest, verfolge sie und überlege Dir, wie der Anbieter damit umgeht.
  - Ist er offen oder versucht er, die Vorfälle zu verschleiern?
  - Wie schnell werden die Sicherheitslücken geschlossen?
- **Sei sparsam mit Deinen Daten** – auch hier gilt wieder: Was Du nicht gepostet hast, ist am besten vor Diebstahl und Missbrauch geschützt.

(II) Geodaten

Viele Handys und auch Kameras können feststellen, an welchem Ort sie sich gerade befinden. Sie tun

das mit Hilfe des so genannten Global Positioning System (GPS) und in der Regel speichern sie diese so genannten »Geodaten« (also Deine geographische Position beim Fotografieren) »in« das Foto.

Die Geodaten können später wieder ausgelesen werden, wenn Du z.B. ein Foto zu Facebook hochlädtst. Facebook erkennt, an welchem Ort das Foto aufgenommen wurde. Da auch Aufnahmedatum und -uhrzeit mit dem Foto gespeichert wurden, kann man nun also genau sagen, an welchem Tag, zu welcher Uhrzeit sich das Handy oder die Kamera an welchem Ort befunden hat.

Aber nicht nur das: Man kann nun z.B. auf einer Karte anzeigen, an welchen Orten Du häufig Fotos machst und wann. Insgesamt kann man mit Hilfe von Geodaten ein sehr genaues »Bewegungsprofil« über Dich erstellen und damit sichtbar machen, wo Du Dich wie häufig aufhältst, zu welchen Zeiten Du typischerweise an welchen Orten bist etc. Somit könnte z.B. jemand sehen, dass Du häufig Samstag Abends Fotos in einer bestimmten Disco machst und nun wissen, dass er Dich zu dieser Zeit also dort abpassen könnte.

Weitere Informationen

- Facebook spinnt das Hier-bin-ich-Netz
- Das ignorierte Risiko Geodaten
- Facebook bringt Places jetzt auch nach Deutschland
- Dank "Places" mit dem Finger auf andere zeigen
- Die stille Angst des Weltkonzerns



Wie kannst Du Dich schützen?

- Du kannst prüfen, ob die **Geodaten-Funktion** man bei Deinem Handy oder Deiner Kamera **abschalten** kann.
- Wenn Du Fotos zu einem Online-Dienst hochlädtst, kannst Du prüfen, ob es eine Funktion gibt, die **»Geodaten nicht speichern«** oder **»Geodaten nicht mitzuschicken«** oder ähnlich heißt und diese aktivieren.
- Du kannst genau darauf achten, wer **Zugang zu Deinen Fotos** hat und entsprechend möglicherweise Geodaten daraus entnehmen kann.



Letzlich muss Dir bewusst sein, dass **jedes mit einem Handy aufgenommene Foto möglicherweise Geodaten enthält**. Sobald Du ein solches Foto bei einem Online-Dienst hochlädtst, besteht die Gefahr, dass das Foto einem bestimmten Ort (und durch das Aufnahmedatum auch einem Zeitpunkt) zugeordnet werden kann.

(III) Biometrie

»Biometrie« bedeutet, dass man mit Hilfe von Computern versucht, biologische Merkmale einer Person zu erkennen, um damit die Person zu identifizieren. Dazu kann man z.B. Merkmale benutzen wie das Gesicht, den Fingerabdruck oder die Iris des Auges. Die Idee ist, dass man den Zugang zu bestimmten Orten oder auch Diensten dann genau für die Personen freigeben könnte, die dazu berechtigt sind. Eine Kamera am Haus könnte z.B. erkennen, ob der Mensch, der vor der Tür steht,

hier wohnt und eintreten darf oder ob er ein Fremder ist und klingeln muss.

Darüber hinaus sind natürlich Internetdienste ebenfalls daran interessiert, Biometrie-Daten zu nutzen. Facebook scannt zum Beispiel alle hochgeladenen Fotos und versucht zu erkennen, ob die darauf abgebildeten Personen im Netzwerk bereits bekannt sind. Falls ja, können sie gleich mit Namen getaggt werden. (siehe z.B. Facebook aktiviert Gesichtserkennung in Deutschland).

Du kannst Dir die (zukünftige[1)]) Anwendung – etwas überspitzt – vielleicht so vorstellen:

> Du kommst auf eine Party und siehst einen Jungen/ein Mädchen, den/das Du attraktiv findest. Du machst aus einigem Abstand ein Foto des Gesichts und lässt die Facebook-App auf Deinem Handy das Foto scannen. Die Person ist bei Facebook, Du siehst, wie sie heißt und dass ihr Beziehungsstatus »Es ist kompliziert« lautet. Nun kannst Du also abschätzen, ob es sich lohnt, den Jungen/das Mädchen anzusprechen …
> In jedem Fall könntest Du dabei schon mal den Namen der Person verwenden und vielleicht auch schon mal auf gemeinsame Interessen eingehen oder andere Informationen nutzen, die Du dem Facebook-Profil entnehmen konntest.

Weitere Informationen

- EU-Datenschützer warnen vor neuen Gefahren beim Biometrie-Einsatz
- Datenschützerin kritisiert Gesichtserkennung
- Gesichtserkennung mit dem Handy
- Zahlen per Fingerabdruck: Zwischen Alltagstauglichkeit und Datenschutzbedenken
- Britische Biometrie-Ausweise in wenigen Minuten geknackt
- Biometrische Gesichtserkennung in Laptops gehackt

(IV) Cookies

> Ein Cookie […] ist in seiner ursprünglichen Form eine Textdatei auf einem Computer. Sie enthält typischerweise Daten über besuchte Webseiten, die die Browser-Software beim Surfen im Internet ohne Aufforderung speichert.
> — Wikipedia: Cookie.

Cookies sind als Dateien harmlos: Sie können auf Deinem Rechner keinen Schaden anrichten. Allerdings kann man mit Ihnen ausspähen, auf welchen Websites Du surfst und noch einiges mehr, das Du online tust.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat **gut verständliche Informationen zum Thema Cookies**.

Cookies werden heute praktisch von allen großen Websites benutzt. Shops nutzen Cookies, um Dir z.B. Produkte zu zeigen, die Du kürzlich angeschaut hast. Soziale Netzwerke nutzen Cookies, um Deine Anmeldedaten zu speichern oder auch um zu erfahren, auf welchen Websites Du einen »Like-Button« angeklickt hast. Cookies sind nichts Schlimmes, aber ein Shop oder ein soziales Netzwerk können damit auch sehr genau nachvollziehen, was Du online tust, welche Produkte Dir gefallen, welche Interessen Du hast etc. Man erhält mit Hilfe von Cookies ein recht genaues Bild Deiner Person und Deiner Interessen. Ideal, um Dir – »zufällig« – genau die Produkte im sozialen Netzwerk per Werbung anzubieten, für die Du Dich bei einem Online-Shop interessiert hast.



Wie kannst Du Dich schützen?

- Lies die Informationen zum Thema Cookies gründlich, so dass Du in eigenen Worten erklären kannst, was Cookies sind und inwiefern sie problematisch sein können.
- Informiere Dich, wie Du Deinen Browser so einstellst, dass Cookies nur begrenzt gespeichert werden können: Wie kann ich meine Daten im Internet schützen?
- Mach den Browser-Sicherheitscheck des Bundesamtes für Sicherheit in der Informationstechnik und überprüfe, wie Dein Browser aktuell eingestellt ist.
- Wenn Du Dich noch etwas genauer informieren möchtest, lies die Beiträge Cookie und Flash-Cookie in der Wikipedia.

Vertiefung

Es gibt natürlich noch weitere Situationen, in denen Deine Privatsphäre gefährdet sein kann. Hier findest noch einige Informationen und Tipps dazu:

- Tipps für mehr Privatsphäre
- Überwachung im Netz

privatsphaere, reflexion, medien, datenschutz

1)

WICHTIG: die hier geschilderte Situation ist technisch heute noch nicht möglich, aber in nicht allzu ferner Zukunft denkbar