

(Deine) Spuren im Internet

facebook, twitter, ICQ oder schuelervz - wer kennt sie nicht? In sozialen Netzwerken bewegen wir uns tagtäglich, indem wir die neuesten Bilder von der letzten Party hochladen, peinliche Momente von anderen Freunden kommentieren oder aber auch einfach nur mit Freunden chatten. Aber nicht nur in sozialen Netzwerken hinterlassen wir Spuren. Auch wenn wir nur unsere Mails checken oder etwas über eine Suchmaschine suchen, wird alles über unser Verhalten im kleinsten Detail protokolliert. Dieser Artikel soll dich nicht dazu bringen, jegliche Kommunikation mit Freunden über soziale Netzwerke oder sonstige Tätigkeiten im Internet zu beenden oder dir vielleicht sogar Angst einjagen. Er soll lediglich zur Aufklärung und zum besseren Verständnis dienen.

Zuerst einmal muss ich sagen: Das Internet ist eine tolle Sache. Täglich haben wir mit dem Internet zu tun, sei es beim Nachschauen der aktuellen Fußballergebnisse oder bei der Vorbereitung auf das nächste Referat. Es erleichtert uns das Leben maßgeblich und bietet uns tolle und neue Möglichkeiten der Kommunikation. Diese Abhängigkeit wird aber leider auch von vielen Firmen sehr zu unserem Nachteil genutzt. Wie dies geschieht, werde ich mit Hilfe einiger Beispiele erläutern.

Bestimmt habt ihr schon einmal etwas von den sog. *AGB* gehört. Aber was ist denn die *AGB* oder heißt es der *AGB*, vielleicht aber auch das *AGB*?? Die Allgemeinen Geschäftsbedingungen (kurz: *AGB*) sind eine Art Vertrag, den man bei Installation einer Software, aber auch bei Eintritt in ein soziales Netzwerk, akzeptieren muss. Meist sind die *AGB* extrem lang (locker mal 20.000 Wörter) und mit juristischen Fachwörtern gefüllt, sodass es dem normalen Nutzer schier unmöglich ist, den Inhalt zu verstehen...und seien wir ehrlich: wer hat Lust das auch noch alles durchzulesen!? - Und genau das denkt sich auch der Verfasser. Da kommen dann schon einmal Sätze wie *„Des Weiteren stimmen Sie zu, dass ICQ Inc. befugt ist, nach eigenem Ermessen jegliches gesendete Material oder gesendete Informationen in jeder Art und Weise zu benutzen, beispielsweise, aber nicht ausschließlich, indem es das Material veröffentlicht oder verbreitet“* vor. Oder der Nutzer übergibt *„ein unwiderrufliches, fortwährendes, nicht-exklusives, übertragbares, voll bezahltes, weltweites Recht“* an facebook. Selbst beim Todesfall eines Benutzers handelt facebook in eigenem Ermessen, was schon wirklich makaber klingt: *„Wenn wir eine Information über den Tod eines Benutzers erhalten, werden wir, obwohl wir nicht dazu verpflichtet sind, das Konto des betreffenden Benutzers für einen von uns definierten Zeitraum in einem speziellen Gedenkstatus aktiv lassen, um anderen Benutzern die Möglichkeit zur Abgabe und Einsichtnahme von Kommentaren zu geben“*. Nun denkst du vielleicht: „Dann setz ich das Häkchen das nächste Mal einfach nicht“. Stimmt - musst du nicht, aber wenn du es nicht machst, kannst du das Produkt nicht nutzen. Bei Software, welche du auf deinem Computer installierst, ist das nichts anderes. Wenn du die *AGB* nicht akzeptierst, kannst du das Programm nicht installieren. Wie du nun bemerkt hast,

beginnt da schon die Trickserei. Leider haben wir, sofern wir die sozialen Netzwerke bzw. Software nutzen möchten, keine andere Wahl und müssen mehr oder weniger den Inhalt der AGB hinnehmen, ohne uns eigentlich im Klaren darüber zu sein, was in diesen geschrieben steht.

Was gibt es aber für Gründe, Daten über uns zu sammeln? Wie so oft ist auch hier das große Geld ein wichtiger Punkt - nämlich Werbung. Durch sie verdient man heutzutage richtig viel Kohle, dass hier mit deinen persönlichen Daten gehandelt wird, interessiert dann keinen mehr. Der andere Standpunkt ist die Sicherheit, wobei man bei dem Wort „Sicherheit“ vorsichtig sein muss. Jeder hat eine andere Ansicht, ob das Sammeln bestimmter Daten wirklich zur Sicherheit beiträgt oder nicht. Das am häufigsten genannte Argument ist: Für den Fall, dass etwas passiert, kann man mit Hilfe der gespeicherten Daten bei der Problemlösung helfen und möglicherweise wichtige Hinweise geben. Soweit das Argument.

Grob kann man zwischen zwei Gefahren bei der Verbreitung persönlicher Daten durch soziale Netzwerke unterscheiden: Zum Ersten sind das Informationen, die du selbst über dich preis gibst, deren genaue Verbreitung du in einem gewissen Umfang kontrollieren kannst („Was trage ich in mein Profil ein?“). Das Zweite sind Informationen, über die du keine Kontrolle der Veröffentlichung hast und durch Annahme der AGB (Allgemeine Geschäftsbedingungen) zustimmst - sprich, der Websitebetreiber kann mit deinen Daten so ziemlich alles machen, was er will, sofern er es in den AGB erwähnt hat.

Es gibt sogar Firmen, die sich darauf spezialisiert haben, komplette Profile von Personen zu erstellen. Deren Datenbank umfasst dann mal locker 1 Milliarde (!) Profile - und du weißt selber nicht, ob du in dieser Datenbank aufgelistet bist. Da stehen dann Sachen drin wie Alter, Lieblingsessen, Automarken, Geschlecht, Lieblingsfilme/serien, Hobbies, politische Einstellung, Einkommen, ob du Raucher bist oder nicht,... . So sammeln sich schnell mal Hunderte von Informationen über dich an. Erschreckend, nicht wahr?

Wie kommen die bloß an meine Daten dran?

Es gibt viele verschiedene Möglichkeiten, an deine Daten zu kommen. Bei den meisten weißt du es nicht mal - das ist wohl das Schlimmste. Einige dieser Möglichkeiten werden wir uns nun etwas genauer anschauen.

Das beginnt schon bei Smartphones. Smartphones sind sehr leistungsstarke Handys, schon fast vergleichbar mit kleinen Computern. Sie bieten ein enormes Leistungsspektrum an Funktionen (meistens mehr, als wir überhaupt brauchen) und sie bieten die Möglichkeit des nachträglichen Installierens sog. „Apps“. „Apps“ sind kleine Programme, die deinem Smartphone noch mehr Funktionen geben, wie z.B. einen schicken Terminkalender, coole Spiele oder auch lustige Fotobearbeitungen. Leider gibt es auch bei den Apps die schwarzen Schafe - nämlich diese, die einfach mal beliebige Daten, die du in deinem Smartphone hast, weiterleiten - ohne dass du das weißt. Da landen dann schnell mal ganze Adressen bei Firmen oder deine aktuelle Position wird (mit Hilfe von GPS) an Firmen geschickt - sprich, die wissen, wo du dich aufgehalten hast.

Oder gehörst du auch zu denen, die gerne mal Fotos ins Internet hochladen? Das ist eine coole Sache, schließlich können sie dann deine Freunde kommentieren, vielleicht sind sie sogar auch drauf. Was deine Freunde aber auch machen können, ist das Foto

herunterladen. Wenn das Gerät, mit dem du das Foto gemacht hast, dann auch noch über einen GPS Empfänger verfügt (eine Vielzahl der aktuellen modernen Handys tut dies), bemerkst du gar nicht, dass in dem Foto auch noch der Ort abgespeichert wird, wo du das Foto gemacht hast. Dein Freund kann also gemütlich dein Foto vom letzten Urlaub herunterladen und auf einer Karte genau sehen, wo dieses Foto gemacht wurde. Nehmen wir mal an, du bist in Rom, knippst dort viele Fotos von allen möglichen Sehenswürdigkeiten und lädst diese Bilder hoch. Der Websitebetreiber holt sich deine Bilder (steht ja in den AGB, dass er das machen darf), schaut, wo du diese aufgenommen hast und kann auch noch den Ort dieser Bilder nachschauen (ist ja im Bild abgespeichert). Nun sieht er, dass du in Rom warst und dir Sehenswürdigkeiten angeschaut hast. Also wird dir Werbung über Städtereisen in deinen Nachbarländern eingeblendet oder auch Werbung für Reiseführer angezeigt.

Vielleicht ist dir das auch schon mal aufgefallen: Du willst deine Mails checken, gehst auf die Homepage, loggst dich ein und bist im Posteingang. An der Seite findest du Werbung zu verschiedenen Artikeln. Interessanterweise sind da sehr viele Dinge dabei, die dich wirklich interessieren oder mit denen du in letzter Zeit in irgendeiner Art und Weise zu tun hattest.

Eines steht fest: Dies ist vom Betreiber der Website gewollt und das Ergebnis tiefer, persönlicher Recherche über dich. Da kann es schon mal vorkommen, dass dein Mailprovider deine (!) Mails auf bestimmte Schlagwörter durchsucht und somit perfekt auf dich abgestimmte Werbung einblendet. Wenn du also in ein paar Mails über den letzten Mallorca-Urlaub schreibst, ist es nicht verwunderlich, dass du auf einmal Angebote über Mallorca-Kreuzfahrten eingeblendet bekommst. Doch wenn du jetzt denkst: „Hey, das darf der doch gar nicht.“, liegst du leider falsch. Schließlich hat der Provider/Hersteller es in seine AGB geschrieben, welche du ja akzeptiert hast, indem du das Häkchen gesetzt hast.

Social Networking

Soziale Netzwerke dienen dazu, Informationen mit anderen Freunden zu tauschen und halten uns auf dem aktuellen Stand (wer ist mit wem in einer Beziehung und wie war eigentlich die letzte Party). Alleine in Deutschland gibt es momentan 149 soziale Netzwerke, deren Firmensitz sich in Deutschland befindet. Das ist eine ganze Menge. Da verliert man schnell mal den Überblick. Viele von euch werden vermutlich bei mehreren Netzwerken angemeldet sein - schließlich will man jede Möglichkeiten nutzen, um auf dem aktuellsten Stand zu bleiben.

Doch leider besteht genau darin auch eine große Gefahr - wenn du nämlich beginnst dein Profil auszufüllen, also die Informationen, die du über dich weitergeben willst. Zum einen willst du ja viele Informationen über dich ins Profil schreiben, damit die anderen viel über dich erfahren, zum anderen sollten sie aber auch nicht zu viel über dich wissen. Wie du merkst, bist du da ganz schnell in einer Zwickmühle.

Anhand mehrerer Statistiken sieht man deutlich, wie stark das Sammeln von Benutzerinformationen in den sozialen Netzwerken zugenommen hat. Grob gesagt kann man sagen, dass es sich ca. verfünffacht hat. Der Grund liegt auf der Hand: immer mehr Menschen treten in soziale Netzwerke ein und schreiben wie wild alles in ihr Profil. Um an diese Daten zu kommen, benötigt man meist nur ein Profil im Netzwerk des Betroffenen und es ist erstaunlich, an wie viele Informationen man kommt, ohne selbst mit der Person befreundet zu sein.

Möglicherweise hast du das auch schon erlebt: Erst vor kurzem habe ich eine Anfrage bei ICQ bekommen, dass mich ein mir unbekannter Benutzer mit dem Namen „SEXY“ in die Kontaktliste aufnehmen will. Ein kurzer Blick in die Benutzerinformationen bestätigte die Vermutung: es war ein Link hinterlegt, in der Hoffnung, dass ich auf diesen klicke. Wenn man sich den Link genauer anschaut, kann man daraus schließen, dass dieser zu einem Benutzerprofil eines sozialen Netzwerkes in einem Osteuropäischen Land führt, wo es andere Internetgesetze gibt. Ebenso hätte sich eine Spyware (das sind Programme, die deinen Computer im Hintergrund ausspionieren und Daten an andere Computer auf der Welt schicken ohne dass du etwas davon bemerkst!) installiert. Auf Grund von Erfahrung in der Anwendung dementsprechender Programme konnte ich dies aber verhindern. Richtige gemeine Spyware ist, wenn diese alle Tastenschläge auf deiner Tastatur aufnimmt und weiterleitet. Wenn du dich dann in deinem sozialen Netzwerk, oder schlimmer noch, beim Online Banking anmeldest, hat man automatisch deine Zugangsdaten und man kann mit deinen Zugangsdaten anstellen, was man will.

Ein ebenso denkbare Szenario wäre, dass du peinliche Bilder von dir im Internet hast bzw. hattest und dein zukünftiger Chef dich vor dem Bewerbungsgespräch einfach mal mit einer Suchmaschine sucht. Wenn er dieses Bild dann findet, sieht's eher schlecht für dich aus - und heraus bekommst du das Bild „aus dem Internet“ schwer bis gar nicht mehr.

Was kann man mit deinen Daten anfangen?

Zum Ersten könnte man deine Daten verkaufen. Wie wir schon mitbekommen haben, gibt es Firmen, die richtig scharf auf deine Informationen sind. Die zahlen gerne mal mehrere Hundert Euro für dein Profil. Ebenso besteht die Möglichkeit, dass man sich als dich ausgibt - sprich deine Identität stiehlt. Wenn man also genug Informationen über dich hat, könnte man dich z.B. auf irgendeiner Website anmelden und richtigen Unfug damit treiben. Das kann dann zu finanziellem Schaden führen und deine (persönliche) Zukunft wäre mehr oder weniger ruiniert. Wenn diejenigen, die das vorhaben noch „nett“ sind, melden sie sich noch vorher bei dir und bieten dir gegen Geld an, es nicht zu tun...aber nur wenn sie nett sind.

Wie du siehst, gibt's eine Menge, was man mit deinen Daten anstellen kann. Vielleicht fallen dir selber noch ein paar Sachen ein.

Was kann ich an meinem Verhalten ändern?

Die sicherste, einfachste und beste Lösung wäre vermutlich, auf eine einsame Insel auszuwandern, auf der es keine technischen Geräte gibt. Dann wäre das Sammeln deiner Daten nicht mehr möglich. Da du aber vermutlich keine Lust hast, auf eine einsame Insel auszuwandern (ich übrigens auch nicht :-)), schauen wir uns einfach mal ein paar nützliche Tipps an, die dir helfen können:

Das Allerwichtigste ist natürlich, dass du zurückhaltend mit deinen persönlichen Informationen sein solltest.

Ebenso solltest du nicht wahllos irgendwelche fremden Leute als Freunde annehmen, nur damit du mehr Freunde in deiner Liste hast als dein Freund. Jedes soziale Netzwerk bietet die Möglichkeit, (dir unbekannte) Personen, die dich regelmäßig versuchen zu kontaktieren, zu melden.

Sprich doch einfach mal mit anderen Freunden darüber, was sie in ihrem Profil so über sich preisgeben und weise sie auf mögliche Gefahren hin.

Ein großer Fehler, den leider immer noch viele machen, ist das Klicken auf unbekannte Links, schließlich will man ja wissen, was sich dahinter verbirgt. Dies kann aber dann schnell dazu führen, dass sich Spyware installiert, die deinen Computer ausspioniert. Also sei vorsichtig und klicke nicht wild auf jeden dahergelaufenen Link.

Ebenso solltest du gegenüber deinen Freunden Respekt zeigen - das heißt, keine unschönen Dinge auf die Pinnwand des anderen schreiben oder jemanden einfach ohne ihn vorher zu fragen, auf einem Foto verlinken - du würdest das auch nicht wollen!

Ein wichtiger Punkt ist natürlich auch noch, dass du niemals und ich meine wirklich unter keinen Umständen, auf Treffen mit unbekanntem Personen eingehst - solche Menschen suchen gezielt in sozialen Netzwerken nach Opfern, weil sie sich dort als jemand anderer ausgeben können, ohne dass du ihre wahre Person kennst. Das kann sehr gefährlich werden!

Eigentlich sollte man sich auch die AGB durchlesen, was aber kaum jemand macht, aus welchen Gründen auch immer. Hier empfiehlt es sich, einfach mal mit Hilfe einer Suchmaschine (z.B. in google eingeben: „facebook agb“) wichtige Inhaltspunkte nachzuschauen. Es finden sich eine Menge Zusammenfassungen, welche die wichtigsten Punkte ansprechen.

Fazit

Entweder gehörst du nun zu denjenigen, die sich von allen diesen Informationen nur schwer beeindruckt lassen und weiterhin wild ihr Profil ausfüllen und alle möglichen Bilder ins Internet hochladen oder aber, du machst dir nun etwas mehr Gedanken darüber, was du ins Internet schreibst oder hochlädst.

Fakt ist, dass du die Datensammlung eigentlich nicht verhindern kannst. Wo du aber mit eingreifen kannst, sind die Informationen, die du freiwillig über dich preisgibst, indem du dein Profil mit persönlichen Daten füllst. Überleg einfach mal, ob es wirklich notwendig ist, jedes Detail über dich zu veröffentlichen und mach dir Gedanken über die möglichen Folgen. Schließlich hast du eine Persönlichkeit, welche du vermutlich gerne behalten möchtest. Wenn du aber leichtsinnig damit umgehst, kann man dir ohne große Mühe diese Persönlichkeit nehmen und unschöne Dinge damit machen - das Internet vergisst nichts und löschen kannst du sowieso nichts.

Tim Seyler, München

Studium der Elektro- und Informationstechnik

Mitarbeiter der Api-Konfifreizeit und Seminarreferent beim LaJu 2011