HANSER

Leseprobe

Manuel Ziegler

Facebook, Twitter & Co. - Aber sicher!

Gefahrlos unterwegs in sozialen Netzwerken

ISBN (Buch): 978-3-446-43466-0

ISBN (E-Book): 978-3-446-43474-5

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-43466-0

sowie im Buchhandel.

Mit diesen Tricks manipuliert der Betreiber direkt die einzelnen Benutzer. Man wendet sozusagen seine eigenen Daten gegen ihn an, um ihn dazu zu bewegen, ein bestimmtes Produkt zu erwerben.

Natürlich muss man nicht unbedingt jede Werbung hinnehmen. Mit sogenannten Werbeblockern – das sind Erweiterungen für einen Browser, die Werbung auf Webseiten automatisch herausschneiden – kann die in Facebook geschaltete Werbung blockiert werden.

Adblock Plus[10] ist eine solche Erweiterung für Firefox, Chrome und andere Browser, mit dem Werbeanzeigen auch unter Facebook ausgeblendet werden können. Auch die an späterer Stelle vorgestellten Erweiterung *DoNotTrack Plus* blendet die Anzeigen aus.

3.2 Missbrauch freiwillig veröffentlichter Daten

Freiwillig veröffentlichte Daten werden von den Betreibern der sozialen Netzwerke ausgiebig ausgewertet und genutzt. Unter diesen Daten ist alles zu verstehen, was der Benutzer jemals in sozialen Netzwerken mit anderen Benutzern geteilt hat oder dort auch nur für sich selbst sichtbar gespeichert hat. Das bedeutet, dass die Betreiber von sozialen Netzwerken auch Inhalte persönlicher Nachrichten auswerten könnten. Beweisbar ist das derzeit nicht, aber es gibt einige Indizien, die diese These untermauern. Erwähnt man in persönlichen Nachrichten beispielsweise häufiger Begriffe eines bestimmten Themengebietes, kann man nach einiger Zeit Werbeanzeigen zu diesem Thema auf seiner Seite beobachten.

Zumindest bei Facebook kann der Verdacht, dass der Betreiber speichert und auswertet, wer mit wem wie oft kommuniziert, auf diese Weise gestützt und von jedem nachvollzogen werden. Man kann das recht einfach feststellen: Gibt man oben in das Suchfeld einen Buchstaben ein, wird bereits nach Ausdrücken gesucht, die mit diesem Buchstaben beginnen, und diese in der Vorschau angezeigt. „Seltsamerweise“ werden nach der Eingabe eines beliebigen Buchstabens im Suchfeld die engsten Freunde an oberster Stelle angezeigt beziehungsweise die Personen, mit denen man in Facebook am häufigsten kommuniziert.

Auch die Chat-Funktion auf der rechten Seite enthält an oberster Stelle die Personen, mit denen man sich am häufigsten digital unterhält. Damit ist zwar noch nicht bewiesen, dass Facebook auch den Inhalt der persönlichen Nachrichten ermittelt. Allerdings kann man davon ausgehen, dass die Entwickler von Facebook nicht dumm sind und deshalb eindeutige Rückschlüsse auf Datenspionage verhindern. Nur weil der Dienst dadurch wesentlich benutzerfreundlicher wird, erfährt man, dass Daten über die Kommunikation zwischen den Benutzern gespeichert werden. Der Betreiber riskiert damit zwar,

[10] Für Firefox zu beziehen von https://addons.mozilla.org/de/firefox/addon/adblock-plus/, Homepage auf http://adblockplus.org/de/, die Chrome-Version ist auf http://adblockplus.org/de/chrome erhältlich.

dass misstrauische und technisch versierte Mitglieder sehen können, welche Daten ausgewertet werden. Weil solche Mitglieder aber in der Minderheit sind, werden sie hingenommen. Im Gegenzug wird der Dienst für die große Masse benutzerfreundlicher, und von dieser erfährt der Betreiber größere Zustimmung als vom Rest Ablehnung. Allerdings ändert dies nichts an der Tatsache, dass Facebook riesige Datenmengen gewinnt, die beispielsweise durchaus für eine Psychoanalyse brauchbar wären. Mit diesen Daten und der Flut weiterer Daten, die zusätzlich ermittelt werden, ist es möglich, dass der Betreiber den Benutzer beinahe besser kennt als dieser sich selbst.

BILD 3.1 Es ist zwar komfortabel, Freunde vorgeschlagen zu bekommen (siehe rechts), vor allem dann, wenn man mit diesen auch tatsächlich befreundet ist, allerdings sollte jedem klar sein, dass die sozialen Netzwerke eine Vielzahl von Daten über den Benutzer benötigen, um solche Vorschläge unterbreiten zu können

Welche Informationen die Betreiber sozialer Netzwerke tatsächlich aus den freiwillig gelieferten Benutzerdaten gewinnen können und worauf generell zu achten ist, ist in den folgenden Kapiteln erläutert.

3.2.1 Datenspeicherung verhindern

Um Spionage durch andere Benutzer zu verhindern, wurden in Kapitel 2 die Privatsphäre-Einstellungen empfohlen. Mit dieser Differenzierung der Reichweite können Daten in unterschiedlichen Freundeskreisen veröffentlicht und bestimmte Informationen vor Fremden und entfernten Bekannten verborgen werden. Wenn man die Empfänger sorgfältig filtert, können Informationen, die nicht alle kennen sollen, also getrost publiziert werden.

Allerdings helfen selbst die durchdachtesten Privatsphäre-Einstellungen nicht dabei, Informationen vor dem Betreiber des sozialen Netzes zu verheimlichen – sein langer Arm reicht überall hin. Um ihn kurzzuhalten, hilft nur, vertrauliche Informationen in einem sozialen Netzwerk überhaupt nicht zu verteilen. Schließlich hat der Betreiber die Möglichkeit, sämtliche Angaben zu ermitteln. Egal, ob sie öffentlich oder nur für Freunde sichtbar sind, in persönlichen Nachrichten erwähnt werden oder ausschließlich für den Nutzer selbst sichtbar sind – er kann sie bei Bedarf jederzeit aus seinen Datenbanken abrufen und auswerten.

Das bedeutet für die Nutzer sozialer Netzwerke, dass sie sich bereits mit der Entscheidung zur Registrierung damit abfinden müssen, dass von nun an Daten über sie gesammelt werden, egal wie sehr sie sich bei der Wahrung der Privatsphäre anstrengen. Sobald man Mitglied eines sozialen Netzwerks ist, trägt man automatisch dazu bei, die Datenbank des Betreibers mit persönlichen Daten zu bereichern. Auch Daten nur für den Autor selbst sichtbar zu machen, ist unter diesem Aspekt reine Augenwischerei und zugleich eine freiwillige Fütterung der Datenbank der Netzwerke – sozusagen die Absegnung des Datenmissbrauchs durch den Betreiber.

Besonders bemerkenswert ist es, dass oft Beiträge, die vom Benutzer bereits gelöscht wurden, dennoch in den Datenbanken gespeichert bleiben. Als es vor einiger Zeit einem Studenten der Rechtswissenschaften gelang, die Herausgabe aller ihn betreffenden bei Facebook gespeicherten Daten zu erwirken, stellte er außer der Tatsache, dass seine Daten intern unter insgesamt 57 Kategorien abgelegt waren und 1200 Seiten umfassten, auch fest, dass darunter zahlreiche von ihm in der Vergangenheit gelöschte Beiträge enthalten waren. In einem Interview mit 1Live berichtet der Student Max Schrems von seinen Erkenntnissen[11]. Am 7.2.2012 berichtete die Computerwoche[12] abermals von Daten, die nach der Löschung wieder aufgetaucht waren. Facebook berief sich auf einen Fehler im System – aber für die meisten Datenschützer war damit klar, dass Facebook Daten auch nach der Löschung aufbewahrt, um immer umfassendere Informationen über den Nutzer gewinnen zu können.

Dass es sich keineswegs um einen Fehler handelt, sondern um Absicht – das Einräumen eines Fehlers sollte wohl nur die Mitglieder besänftigen –, verrät das Impressum bzw. die Nutzungsbedingungen von Facebook. Hätten die Datenschützer oder der Student vor

[11] Siehe auch http://www.einslive.de/magazin/extras/2011/09/28/110928_iv_max_ schrems.jsp

[12] http://www.computerwoche.de/netzwerke/web/2504579/

der Mitgliedschaft auf http://www.Facebook.com/legal/terms?ref=pf in Punkt 2.2 nachgelesen, hätten sie folgenden Text gefunden:

> *„Wenn du IP-Inhalte löschst, werden sie auf eine Weise entfernt, die dem Leeren des Recyclingbehälters auf einem Computer gleichkommt. Allerdings sollte dir bewusst sein, dass entfernte Inhalte für eine angemessene Zeitspanne in Sicherheitskopien fortbestehen (für andere jedoch nicht zugänglich sind).“*

Der Recyclingbehälter auf einem Computer entspricht unter Windows dem Mülleimer. Wenn auf einem PC Dateien gelöscht werden, werden sie zuerst automatisch in den Mülleimer verschoben. Wenn danach der Inhalt des Mülleimers gelöscht wird, wird dabei lediglich der zugehörige Verzeichniseintrag gelöscht. Das bedeutet: Die Daten sind weiterhin auf der Festplatte vorhanden und können – solange sie nicht durch neuere Daten überschrieben werden – restauriert werden. Was eine angemessene Zeitspanne ist, wird nicht näher definiert. Dem einen erscheinen zwei Tage wie eine Ewigkeit, der andere, der mit den Daten Geld verdient, hält vielleicht ein Jahr für angemessen. Über diesen Begriff können sich die Betreiber und Mitglieder trefflich streiten.

Allerdings steht in Punkt 2.1 im Impressum/Nutzungsbedingungen von Facebook:

> *„Für Inhalte wie Fotos und Videos („IP-Inhalte“), die unter die Rechte an geistigem Eigentum fallen, erteilst du uns durch deine Privatsphäre- und Anwendungseinstellungen die folgende Erlaubnis: Du gibst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest („IP-Lizenz“). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht.“*

Was genau unter IP-Inhalten verstanden wird, konnte im Impressum nicht eruiert werden. Man sollte vorsichtshalber davon ausgehen, dass davon nicht nur Fotos und Videos betroffen sind, sondern auch die Inhalte aller Beiträge. Schließlich hat der Verfasser/dasMitglied das geistige Eigentum an ihnen, weil er sie geschrieben (und quasi erfunden) hat. Dies bedeutet, dass Facebook die Fotos, Inhalte und privaten Daten, die seine Anwender posten, jederzeit – ohne weitere Genehmigung – an beliebige Firmen oder Privatpersonen weiterverkaufen darf. Und dies ist unter normalen Umständen auch nach ihrer Löschung durch den eigentlichen Urheber möglich, denn dass auch alle seine Freunde die Inhalte löschen, wenn ein Mitglied sein Konto und seine Daten löscht, ist unwahrscheinlich. Punkt 2.1 ist also Facebooks Freifahrschein für das Bunkern und Verkaufen von Daten.

Allerdings wird auf der Impressumsseite https://www.Facebook.com /terms/provisions/german/index.php für deutsche Mitglieder eine Einschränkung getroffen:

> *„Ziffer 2 gilt mit der Maßgabe, dass unsere Nutzung dieser Inhalte auf die Verwendung auf oder in Verbindung mit Facebook beschränkt ist.“*

Deutsche Mitglieder haben also Glück, ihre Inhalte dürfen „nur“ an in Facebook Werbetreibende oder Firmen weiterverkauft werden, die in irgendeiner Form mit Facebook zu tun haben. Und das sind eine ganze Menge.

Die Gruppe http://europe-v-facebook.org warnt jedoch vor allem im Hinblick auf die kürzlich neu eingeführten AGB davor, dass in Zukunft jede Information, die man als Benutzer auf Facebook angibt, der Plattform gehören könnte.

Durch Täuschung des Netzwerkbetreibers

Da man als Mitglied eines sozialen Netzwerks dem Betreiber nicht verbieten kann, bestimmte Informationen über einen zu gewinnen und vorzuhalten, muss man nach anderen Lösungen suchen. Einer der effizientesten, aber auch einer der aufwendigsten Wege ist die systematische Täuschung des Netzwerkbetreibers durch das Veröffentlichen diffuser Daten. Unabdingbar dabei ist, dass man selbst den Überblick über seine publizierten Informationen behält und sie entweder durch entsprechend gegenläufige Informationen egalisiert oder durch eine Vielzahl ähnlicher Informationen dramatisiert und auf diesem Weg das Bild über sich selbst verzerrt. Solche verzerrten Informationen sind für den Netzwerkbetreiber nichts wert.

Der Vorteil dieses Verfahrens ist gleichzeitig sein Nachteil: Je nach Inhalt der Informationen entsteht ein völlig falsches Bild über den Verbreiter der Daten. Weil man aber nur den Betreiber des sozialen Netzwerks und nicht auch noch zusätzlich seine eigenen Freunde täuschen möchte, gilt es einen Weg zu finden, der den eigenen Ruf nicht ruiniert. Die allgemeinen Techniken dafür werden nachfolgend vorgestellt.

Generell sei aber angemerkt, dass das Täuschen laut den Nutzungsbedingungen des jeweiligen Diensts verboten sein kann. Im Impressum von Facebook ist beispielsweise unter Punkt 4.1 zu lesen:

> *„Du wirst keine falschen persönlichen Informationen auf Facebook bereitstellen [....]“*

Wenn ein Mitglied sich nicht an diesen Passus hält, kann es aus dem Netz geworfen werden. Der Grund ist klar: Falsche Informationen sind finanziell wertlos, weil sie nicht verkauft werden können – beziehungsweise dürfen, wenn der Betreiber weiß, dass sie falsch sind. Würde er sie dennoch verkaufen, würde er den Kunden betrügen.

Prinzipiell können Informationen, die Netzbetreiber aus Nachrichten und Beiträgen gewinnen, auf zweierlei Arten verborgen werden:

- Der einfachere Weg ist es, das soziale Netzwerk mit beliebigen Daten zu fluten, die in alle möglichen Richtungen gehen. Dabei werden die tatsächlich relevanten Daten so verborgen, dass ihre Bedeutung mit der Menge der Datenflut abnimmt und schließlich zu vernachlässigen ist.
- Der bessere Weg ist es, gezielt durch selbst veröffentlichte Informationen den vorhandenen Informationen entgegenzuwirken oder solche Informationen zu verfassen, die in die gleiche Richtung wie die ursprüngliche Information gehen und diese weiter dramatisieren. Dadurch entsteht ein verzerrtes Bild der eigenen Identität, das aller-

dings deutlich realistischer wirkt als das mit dem ersten Verfahren erzeugte. Diese Arbeitsweise erfordert allerdings einen erheblich höheren Aufwand als die zuerst geschilderte Variante.

Nachdem ein Beitrag, der eine gewisse Information trägt, im sozialen Netzwerk veröffentlicht wurde, wird sein Inhalt automatisch vom Betreiber ausgewertet. Damit der Betreiber die aus dem Beitrag gewonnenen Erkenntnisse nicht weiter beziehungsweise nicht in entsprechendem Maße weiterverwenden kann, muss der Nutzer Maßnahmen treffen, um die Information dieses Beitrags zu verschleiern. Dazu ein einfaches Beispiel:

Tom schreibt eines Tages in sozialen Netzwerken den Beitrag *Ich bin Vegetarier*. Als er merkt, dass er seit der Veröffentlichung dieses Beitrags immer wieder Werbung für vegetarische Kochbücher und dergleichen bekommt, ärgert er sich und würde seinen Beitrag am liebsten rückgängig machen. Da dies bekanntlich nicht möglich ist, hat Tom zwei Möglichkeiten, um die Werbung für vegetarische Kochbücher zu unterbinden:

- Erstens kann er den Dienst mit uneinheitlichen Informationen fluten. Wenn die Angaben automatisch ausgewertet werden, entsteht ein diffuses Bild über das Mitglied. Der Betreiber kann daraus nicht mehr entnehmen, welche Art von Produktwerbung er Tom anzeigen soll, so dass ihm keine andere Wahl bleibt, als die Anzeigen thematisch zu streuen. Das heißt, dass mehr oder weniger der Zufall entscheidet, zu welchem Thema Tom Werbung angezeigt bekommen wird.
- Oder Tom arbeitet seiner ursprünglichen Aussage inhaltlich entgegen – verbreitet also das Gegenteil – oder spitzt sie zu. Entgegenarbeiten könnte er beispielsweise durch die Aussage *Ich liebe Fleisch*, während er seine Aussage weiter verschärfen könnte mit *Ich bin Veganer*.

Im Folgenden sollen die beiden Möglichkeiten anhand dieses Beispiels genauer betrachtet werden.

Ungerichtete Informationsüberflutung

Bei der ungerichteten Informationsüberflutung des sozialen Netzwerks werden regelmäßig nicht aufeinander aufbauende Beiträge veröffentlicht, die insgesamt den Dienst derart mit Informationen überfluten, dass die inhaltliche Bedeutung eines einzelnen Beitrags in den Hintergrund rückt. Man kennt dies im echten Leben von Briefen oder E-Mails: Je mehr man bekommt und je länger ein Schreiben ist, desto weniger wird sein Inhalt zur Kenntnis genommen.

Die einzige Schwierigkeit bei diesem Verfahren besteht darin, ausreichend Themen für Beiträge zu finden. Wie man solche Themen findet, bleibt jedem selbst überlassen, es empfiehlt sich allerdings ein kurzes Brainstorming, bevor man mit dem Veröffentlichen beginnt. Man sollte sich die Themen notieren und sich auch daran halten, denn andernfalls wird die Mehrzahl der Beiträge sich automatisch mit den Themen befassen, die einen tatsächlich interessieren. Nur wenn man sich an den eigenen Plan hält und etwas Disziplin walten lässt, sind die Beiträge auch tatsächlich ungerichtet.

Welchen Inhalt die Beiträge tatsächlich haben, ist dabei eigentlich gar nicht so sehr von Bedeutung, man kann sie auch lustig schreiben. Auf diese Weise macht man diese Bei-

träge auch für die eigenen Freunde lesbar. Diese Beiträge nur für sich selbst zu veröffentlichen, ist nicht empfehlenswert. Es ist nämlich durchaus möglich, dass einem der Betreiber auf die Schliche kommt und das Täuschungsmanöver erkennt. Er wird dann die Beiträge ignorieren (oder schlimmstenfalls den Urheber sogar aus dem Dienst ausschließen). Ob die Inhalte tatsächlich ignoriert werden, kann man allerdings nicht überprüfen – es ist nur möglich, der Eventualität vorzubeugen. Der Inhalt der Beiträge muss mindestens ein Schlagwort zu einem bestimmten Thema enthalten, so dass das System auf diesen Reiz reagiert und das Thema auch registriert.

Tom hat, nachdem er von dieser Möglichkeit erfahren hat, einige weitere Beiträge veröffentlicht:

Mein neues Auto ist transparent.

Windows ist fehlerfrei!

Der DAX klettert – Na dann wird das Wetter morgen ja schön.

Solche Sprüche reichen durchaus aus, um dem sozialen Netzwerk Anreize für Werbung zu geben, und können ohne weiteres veröffentlicht werden. Sie gelten einfach als Witze oder werden von den meisten Nutzern ignoriert. Toms ursprüngliche Aussage, dass er Vegetarier ist, hat damit für den Auswertungsmechanismus der sozialen Netzwerke nur noch ein Viertel des ursprünglichen Werts, da die anderen Aussagen ebenfalls ausgewertet werden. Als Ergebnis muss Tom jetzt nur noch in jeder vierten Werbeanzeige etwas über Kochbücher für Vegetarier lesen.

Aufbau einer virtuellen Identität

Die zweite Möglichkeit der Egalisierung eines Beitrags besteht darin, sich eine virtuelle Identität aufzubauen. Der Gedanke hinter dem Verfahren ist, dass es belanglos ist, ob die Betreiber persönliche Daten ermitteln können, wenn diese ohnehin nicht stimmen beziehungsweise wenn sie mit dem Ziel, den Betreiber zu täuschen, angelegt wurden.

Dafür ist es allerdings erforderlich, sich genau zu überlegen, wie sich die eigenen Interessen – die man ja schließlich auch noch verfolgen möchte, wenn man mit seinen Freunden kommuniziert – mit einer virtuellen Identität vereinbaren lassen, die mit der eigenen Person möglichst wenige Gemeinsamkeiten hat.

In Toms Beispiel war das die Verzerrung der Information, dass er Vegetarier ist. Er würde demnach entweder angeben, er sei Veganer, oder er würde so tun, als sei er kein Vegetarier. Dieses Verhalten müsste Tom auf alle seine Eigenschaften anwenden: Entweder er verstärkt/dramatisiert eine Eigenschaft oder er stellt sie abgeschwächt dar beziehungsweise egalisiert sie.

Das wichtigste bei beiden Varianten ist es, nie auf eine Werbebotschaft, die tatsächlich interessant ist, zu klicken. Wurde das Interesse wirklich geweckt, kann man das Produkt immer noch in einer Suchmaschine suchen, aber ein Klick auf die Werbeanzeige bestätigt dem Dienstbetreiber das Interesse. Auf diese Weise werden zukünftig verstärkt derartige Werbeanzeigen auch mit Manipulationscharakter angezeigt werden.

Beachten muss man allerdings, dass man die Produkte, die in den in Google-Diensten geschalteten Werbeanzeigen angepriesen werden, natürlich nicht über die Google-Suchmaschine suchen darf, da die Daten aller Google-Dienste zentral zusammengefasst werden. Dies geht indirekt aus den Datenschutzerklärungen Googles hervor[13]. Dort ist nachzulesen, dass Informationen über eine Person von allen Google-Diensten gesammelt und gespeichert werden. Da man in der Regel nur ein Google-Konto besitzt, werden diese Informationen also zusammengeführt.

Möchte man sich ein Produkt, auf das man in einer Werbeanzeige aufmerksam wurde, näher ansehen, sollte man es in einer anderen Suchmaschine suchen. Es bietet sich ohnehin an, regelmäßig die Suchmaschinen zu wechseln, damit die Betreiber nicht allzu viele Daten über ihre Nutzer erhalten. Es gibt eine ganze Reihe von Suchmaschinen, darunter auch sogenannteMeta-Suchmaschinen wie Search.com (leider wurde das hervorragende Scroogle vor einiger Zeit eingestellt).

Stellt man an eine solche Maschine eine Frage, leitet sie die Meta-Suchmaschine an verschiedene Suchmaschinen weiter und zeigt die Ergebnisse dann auf einer Seite an. Auf diese Weise bleibt der Anwender also anonym, selbst wenn die Daten des Anfragenden gespeichert würden. Eine echte anonyme Suchmaschine ist DuckDuckGo.com, sie speichert die Daten der Anfragenden nicht und kann sogar direkt aus dem anonymen TOR-Netzwerk[14] unter der Adresse 3g2upl4pq6kufc4m.onion ohne den Umweg über einen Internet-Gateway angesteuert werden. Normale, aber beliebte Suchmaschinen sind Microsofts Bing, Yahoo, Ask.com, und MSN Live Search. Die Dienste Web.de, GMX und T-Online suchen über Google, sind also als Maßnahme gegen das Datensammeln weniger zu empfehlen. Weitere Suchmaschinen bieten unter anderem Altavista, Fastbot, Freenet-Suche, Hotbot und Wikipedia.

Nutzer von Firefox oder SeaMonkey stellen eine neue Suchmaschine im Eingabefeld rechts oben im Browser ein, sie müssen nur das Pulldown-Feld aufklappen und die Auswahl aus den angebotenen Maschinen treffen.

Es können aber auch Suchmaschinen, die an dieser Stelle nicht voreingestellt verfügbar sind, in den Browser integriert werden, wenn es für sie eine Mozilla-Erweiterung gibt, wie zum Beispiel für DuckDuckGo. Im Dialog Liste der Suchmaschinen verwalten, (Bild 3.2 auf der nächsten Seite) der über das nach unten weisende Dreieck im Suchen-Fenster und dort unter Suchmaschinen verwalten... angezeigt wird, wird die Zeile Weitere Suchmaschinen hinzufügen... angeklickt. Im Hauptfenster öffnet sich die Seite für die Suchmaschinen auf *https://addons.mozilla.org*. Ist die gewünschte Suchmaschine angezeigt, klickt man ihren Button Zu Firefox hinzufügen (oder Zu Seamonkey hinzufügen). Ruft man den Dialog erneut auf, ist die Liste ergänzt (Bild 3.2). DuckDuckGo findet man nicht auf Anhieb, deshalb gibt man in das in Bild 3.2 hinter dem Suchmaschinendialog halb verdeckte Suchfenster mit dem grünen Button den Namen der Suchmaschine ein, die dann in einer Liste passender Addons angeboten wird.

[13] Siehe http://www.google.de/policies/privacy/

[14] Weitere Informationen zu diesem kostenlosen Anonymisierungs-Netzwerk findet man auf seiner Webpräsenz unter https://www.torproject.org/

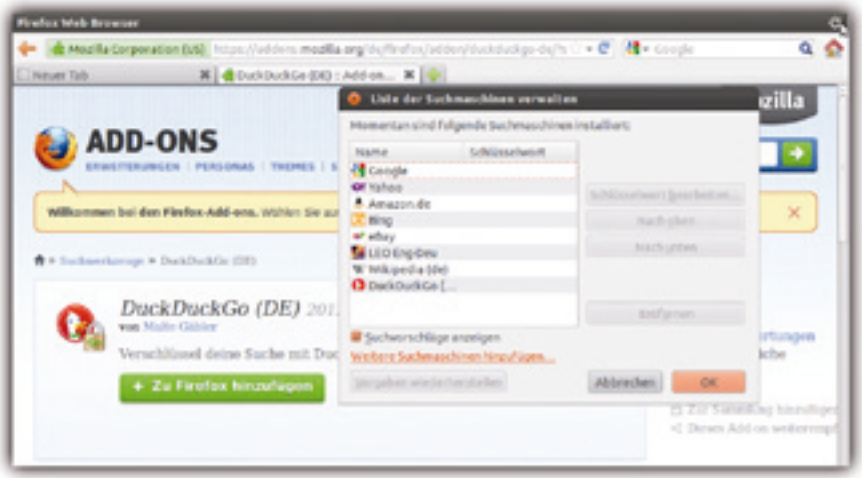

BILD 3.2 So wird im Firefox eine andere Suchmaschine eingestellt

In Browsern, wo es nicht so einfach ist, die Suchmaschine zu wechseln, sollte man die alternative Suche entweder direkt durch die Angabe der URL beginnen oder die Übernahme der Suchmaschinenadresse beispielsweise in die Favoriten überlegen.

Irregeführte Gesichtserkennung

Vor allem in den großen sozialen Netzwerken ist die Gesichtserkennungsfunktion direkt integriert. Der Betreiber kann auf dieser Grundlage mit einer gewissen Sicherheit eine Person namentlich identifizieren, sobald sie einmal markiert wurde[15]. Diese Gesichtserkennungsfunktion kann jedoch ganz einfach getäuscht werden und sogar ohne größeren Aufwand. Dazu benötigt man lediglich ein computergeneriertes Durchschnittsgesicht, das Merkmale möglichst vieler menschlicher Gesichter enthält. Solche Bilder werden durch sogenanntes Morphing erzeugt. Diese spezielle Technik erzeugt Übergänge in Bild (und Farbe). Beim Morphing wird ein Quellbild mit geeigneten Transformationen so verändert, dass daraus ein Zielbild entsteht. Beim Erzeugen eines Durchschnittsgesichtes wird versucht, ein möglichst realistisches Gesicht darzustellen, das so genau wie möglich zwischen zwei Gesichtern liegt. Wird dieses Verfahren auf möglichst viele Gesichter angewandt, erhält man die gemeinsamen Merkmale möglichst vieler Gesichter. Die Ergebnisse dieses Morphing-Schritts werden anschließend auf die gleiche Weise wieder miteinander kombiniert, bis schließlich ein Bild entsteht, nämlich das gesuchte Durchschnittsgesicht. Man kann sich diesen Vorgang wie das Durchlaufen eines Binärbaums in umgekehrter Reihenfolge, also von den Blättern zur Wurzel, vorstellen (Bild 3.3).

[15] Die Biometrie erreicht allgemein eine Trefferquote bis zu 90 Prozent.

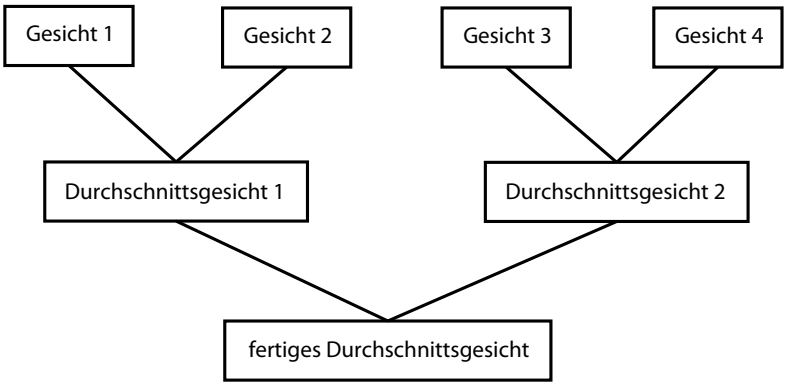

BILD 3.3 Ablauf beim Morphing eines Durchschnittsgesichts

Auf einem solchen Durchschnittsgesicht[16] (Bild 3.4) kann man sich dann als Benutzer verlinken. Die Gesichtserkennung des sozialen Netzwerkes schlägt dann auf nahezu jedes reale Gesicht an und spielt verrückt. Damit die Verlinkung nicht als Täuschung erkannt und verworfen wird, sollte man das entsprechende Gesicht in unterschiedliche Bilder einbetten und sich entweder auf allen verlinken oder sich auf unterschiedliche Durchschnittsgesichter verlinken.

BILD 3.4 Gemorphte Durchschnittsgesichter von http://beautycheck.de/cmsms/index.php/durchschnittsgesichter

[16] Man findet solche Gesichter beispielsweise auf http://beautycheck.de/cmsms/index.php/durchschnittsgesichter

Anschließend ist es für die Gesichtserkennung des sozialen Netzwerkes praktisch unmöglich, sinnvolle Vorhersagen zu machen, ob sich die Person auf einem Bild befindet oder nicht, da nahezu jedes Gesicht Merkmale aufweist, die auch in dem als Nutzer identifizierten Durchschnittsgesicht enthalten sind. Der Benutzer kann nun nicht mehr automatisch identifiziert werden. Es müsste manuell gefiltert werden, was aber viel zu aufwendig ist, weshalb das Morphing für eine gewisse Anonymität sorgt.

Durch Wechsel des Accounts

Nicht jeder möchte regelmäßig Zeit dafür aufwenden, den Betreiber zu täuschen oder möchte es seinen Freunden zumuten, zwischen relevanten und nicht relevanten Inhalten zu unterscheiden. Hier bietet sich das regelmäßige Wechseln des eigenen Benutzerkontos als weitere Möglichkeit an, dem Datenmissbrauch durch die Betreiber vorzubeugen.

Die Idee dahinter ist, dass der Betreiber immer nur über einen relativ geringen Zeitraum Daten sammeln kann, so dass zum Zeitpunkt, an dem das Benutzerkonto wieder gewechselt wird, noch nicht genug Daten vorliegen, um tatsächlich etwas mit ihnen anfangen zu können. Beim neuen Benutzerkonto fängt der Betreiber wieder bei Null an und das Spiel beginnt von vorne.

Soweit zumindest die Theorie. In der Praxis müssen einige Hürden überwunden werden, damit diese Technik auch wirklich zum Erfolg führt.

Besonders wichtig sind unterschiedliche Namen für das alte und das neue Benutzerkonto. Legt man es auf den gleichen Namen an, kann es passieren, dass der Dienst automatisch die Übereinstimmung der realen Personen hinter den beiden Benutzerkonten erkennt und dann die Daten der beiden Konten zusammenführt. Dieses Risiko besteht zwar auch bei der Wahl unterschiedlicher Namen, kann jedoch durch weitere Maßnahmen minimiert werden.

So sollte der Wohnort – wenn man ihn überhaupt angeben möchte – nicht in den beiden Konten identisch sein, ebenso müssen sich die Interessen und das Profilbild auf jeden Fall unterscheiden.

Der größte Schwachpunkt dürfte die nahezu identische Freundesliste beider Konten sein, die sich aufgrund der gleichbleibenden Freunde natürlich nicht verhindern lässt. Daher ist es sinnvoll, auch das alte Konto in die Freundesliste aufzunehmen, so dass es sich beim neuen Konto auch um einen nahen Freund des alten Kontos handeln könnte. Zudem sollten sich die Freundeslisten nie hundertprozentig gleichen. Es ist nicht schwer, einige zusätzliche Freunde zu finden und oft auch keine schwere Entscheidung, einen Freund, mit dem man ohnehin noch nie kommuniziert hat, aus der Freundesliste zu streichen.

Vor allem in Zeiträumen, in denen beide Konten gleichzeitig genutzt werden, sollte man darauf achten, dass vor dem Login in das jeweils andere Konto stets die Chronik sowie die Cookies gelöscht werden oder dass mit unterschiedlichen Browsern gearbeitet wird. Andernfalls können die sozialen Netzwerke gegebenenfalls feststellen, dass vom glei-

chen PC in beide Konten eingeloggt wurde. Dies verhält sich im Grunde ganz ähnlich zu der ab Seite 102 in Kapitel 3.3.1 beschriebenen Technik.

Möchte man sich von einem Account ab- und direkt in einem anderen anmelden, ist zusätzlich darauf zu achten, dass der Betreiber nicht an der IP-Adresse feststellen kann, dass es sich um die gleiche natürliche Person handelt. Daher sollte die Verbindung zum Internet über den Router kurzzeitig getrennt und anschließend wieder neu aufgebaut werden, so dass man vom Internetprovider eine neue IP-Adresse zugewiesen bekommt.

Wie im Browser die Chronik und Cookies gelöscht werden, ist dem Anhang zu entnehmen. Dort ist auf Seite 169 auch beschrieben, wie man eine neue IP-Adresse abruft.

3.3 Missbrauch zusätzlicher Daten

Würden die Betreiber lediglich die vom Benutzer freiwillig angegebenen Daten erfassen, könnte man sich entspannt zurücklehnen und in dem Wissen, dass der Betreiber lediglich die Daten erfährt, die man selbst preisgibt, gemütlich einen Kaffee trinken und sich dabei überlegen, was man denn überhaupt weitergeben möchte. Allerdings haben die Betreiber der sozialen Netzwerke die lästige Angewohnheit, auf eigene Faust Daten zu ermitteln, um zusätzliche Informationen über ihre Mitglieder zu erhalten. Das beginnt bereits in den sozialen Netzwerken selbst. Hier speichern die Betreiber die Zugriffe auf die Profile anderer Personen, obwohl diese zumeist für den Benutzer gar nicht angezeigt werden können. Dadurch erfahren sie, welche anderen Mitglieder einen Benutzer besonders interessieren und können so ihr Bild von ihm, das anhand der Analyse seiner Kommunikation gewonnen werden konnte, weiter präzisieren.

Natürlich ermitteln die Betreiber auch Daten über das Computersystem des Benutzers, so wie es heutzutage von nahezu jeder Website getan wird.

Recht leicht herauszufinden ist, mit welchem Browser der Benutzer den Dienst aufruft. Weil der Browser beim Webserver anklopft und um Übermittlung der Webseite bittet, kann diese Anfrage (genauer: ihr Header) daraufhin untersucht werden, welcher Browser darin vermerkt ist, welches Betriebssystem auf dem PC des Benutzers installiert ist und welche Spracheinstellungen gewählt sind. Wie einfach das ist, kann jeder selbst auf Webseiten wie beispielsweise http://www.ip-secrets.info/ erfahren.

Der IP-Header kann bei einigen Browsern auch unterdrückt beziehungsweise ein alternativer Header kann angegeben werden (Bild 3.5), unter dem dann die Anfragen gesendet werden. Allerdings ist das nicht unbedingt ratsam, da viele Webseitenbetreiber speziell auf bestimmte Browser angepasste Versionen der Seite ausliefern, die dann unter Umständen im tatsächlichen Browser nicht richtig dargestellt werden.

Aber viel bedenklicher als die Browserkennung ist, dass der Betreiber anhand einer IP-Adresse herausfinden kann, wo sich der Benutzer gerade befindet (die sogenannte Lokalisierung beziehungsweise Geo-IP). Diese Abfrage ist keine spezifische Eigenheit