Mühlen, den28.04.10

Facebook & Co. kills your life

Ein Essay über moderne Medien

Soziale Netzwerke im Web 2.0

geschrieben von Tibor Weiß

Facebook feiert mehr Seitenaufrufe als Google – Jetzt sollte jedem klar sein, dass das Internet sich nachhaltig verändert hat. Dabei sieht sich Facebook erst am Anfang, und die stark steigenden Nutzerzahlen bestätigen diesen Trend. In Fachkreisen ist die soziale Überwachung schon lange keine Dystopie weniger Datenschützer mehr.

Die Aktivität der Nutzer in den sozialen Netzwerken ist das Öl, welches diese am Leben hält. Teilnehmer sind möglichst ständig online, um auf dem Laufenden zu bleiben und um vermeintlich Wichtiges als erstes zu erfahren. Jeder stellt freiwillig Informationen bereit und 'verteilt' diese -fishing for compliments- an seine Kontakte. Dadurch entsteht eine regelrechte Flut an Informationen. Diese zu verarbeiten bleibt jedem selbst überlassen. Informationen im Internet veralten sehr schnell. So ist die Ebay-Auktion in 2 Minuten vielleicht schon vorbei oder der CSS Fehler auf einer bekannten Internetseite wurde in der Zwischenzeit behoben.

Bei all der Hektik und der Menge an Daten auf den sozialen Plattformen, hoffen wohl viele Teilnehmer, in den anonymen Massen des Internets unterzutauchen. Dies ist aber auf sozialen Plattformen nicht möglich, da jeder Benutzer ein Profil mit persönlichen Informationen unterhält und mit anderen Nutzern interagiert. Auch das automatische erkennen von gleichen Benutzern auf unterschiedlichen Plattformen ist inzwischen möglich. In Casinos wurde Erkennungssoftware eingesetzt, um Leute zu finden, die versuchen ein Hausverbot zu umgehen. Damit die Software die Personen vollautomatisch in allen Netzwerken wiedererkennt, bräuchte sie nur einen freien Zugang zu den Datenbanken. Viele Nutzer sehen das Potential der Daten für eine soziale Überwachung nicht, und scheuen sich daher nicht davor, bestimmte Daten zu veröffentlichen. So scheint beispielsweise die twitter Meldung „Ich bin gerade mit jemanden in der Stadt einkaufen“ an sich ungefährlich. Aber nicht nur Einbrecher wissen gerne, wann welches Gebäude leer steht (der Besitzer kann oft über eine 'whois-abfrage' ermittelt werden), sondern auch die Läden in der Stadt interessiert, wann sie mit einem Ansturm zu rechnen haben, um ihre Preise rechtzeitig anheben zu können.

Über die umfangreichen Daten ist eine soziale Überwachung möglich. Dies beginnt mit den Informationen über die Freundeslisten bis zu den Profilinformationen und den Statusmeldungen. Diese Daten sind für den Betreiber frei zugänglich und auch staatliche Stellen hätten gerne freien Zugriff auf solche Daten. Als Grund wird dabei zum Beispiel das Aufklären von Alkoholmissbruch von Jugendlichen angeführt. In den USA wurden über Bilder, die in Facebook eingestellt wurden, schon Jugendlliche vor Gericht verklagt. Studien belegen, dass die Überwachung von 20% einer Gruppe ausreicht, um Gruppenaktivitäten zu erkennen. Mit anderen Worten, man muss nur 20 von 100 Schüleraccounts überwachen, um mitzubekommen, wann und wo die nächste Party mit illegalem Alkoholkonsum stattfinden wird. Das dieses nicht nur für solche Zwecke verwendet werden kann, sondern zum Beispiel auch

zur Sabotage von Demonstrationen, ist logisch und macht die Gefahr für die freie Meiungsäußerung deutlich.

Wenn man seine Daten nicht preisgeben will, um die eigene Privatsphäre zu schützen, ist der einfachste Tipp diese nicht zu veröffentlichen. Dieser Tipp ist aber ebenso simple wie nutzlos, da Freunde auch über andere berichten. Einmal 'gepostete' Informationen sind aus dem Internet praktisch nicht mehr zu entfernen. Der Satz: „Das Internet vergisst nie.“ hat sich schon zum Nachteil vieler Firmen bewahrheitet. Gewisse Daten wurden zeitweise erfolgreich entfernt, bis sie Jahre später wieder auftauchten. Dass macht deutlich, wie Daten auch über das soziale Umfeld bestimmbar sind. So wurden zum Beispiel die twitter Kanäle von US Parlamentsmitgliedern untersucht bezüglich wer wem 'folgt'. Daraus lies sich bestimmen, welcher Kanal zu welcher Partei gehört. Denkbar wäre auch ein Einsatz für andere Zwecke in anderen sozialen Netzwerken.

An gespeicherte Daten kommt ein versierter Angreifer immer heran, es sei denn, diese sind mit einem sicheren Verfahren und einem gutem Schlüssel verschlüsselt. Da hilft auch kein 'Schutz' alias Daten nur privat zugänglich zu machen. Denn dies ist eine trügerische Sicherheit. Wenn Facebooks Chief Security Officer Max Kelly in einem Vortrag berichtet, dass man lieber Angreifer jage als das man Sicherheitslücken schließe, denn Sicherheitslücken werden immer existieren, dann macht dies deutlich, dass Informationen auf einem fremden Server auch von Fremden gelesen werden können. Dafür muss man nicht gleich Hacken. Das machen die Facebook Apps deutlich, die automatisch auf viele Profilinformationen zugreifen können, oder mehrere erfolgreiche Angriffe auf die Struktur des von der Stiftung Warentest so hoch gelobten SchülerVZ.

Auch wenn die Privatsphäre an vielen Stellen auszuhebeln ist, ist diese die Grundlage für eine informationelle Selbstbestimmung. Dies beginnt mit dem Wissen über die Einstellungen, um genau zu bestimmen, wer was lesen kann und wer nicht. Dies sollte in einem normalen sozialem Umfeld reichen, aber der Personalchef einer Firma hat vielleicht einen Datensatz mit Bildern von Jugendlichen in etwas angetrunkenem Zustand eingekauft und per Gesichterkennungssoftware, wie sie in Picasa (Fotoverwaltung von Google) verwendet wird, kann er den Bewerber innerhalb von wenigen Minuten wiederfinden. Über die Bewerbungsunterlagen kommt ja das perfekte Bild mit. Wie hilfreich soetwas als Hintergrundwissen für den Personalchef ist, muss wohl nicht erwähnt werden.

Warum macht ein Betreiber sich die Arbeit, ein Rechenzentrum zu unterhalten, jede Menge Programmierer, Anwälte und Netzwerkfachleute zu bezahlen? Das Management muss nur Prioritäten setzen, Arbeit gibt es mehr als genug. Dies bedeutet einen recht hohen finanziellen Aufwand, der in der Anfangszeit von Investoren getragen wurde, die inzwischen profitieren

wollen und so sieht sich jede Plattform nach Einnahmequellen um. Xing finanziert sich zum gewissen Teil aus den Premium-Accounts, die meisten anderen müssen Werbung einblenden. Dies geschieht an mehreren Stellen und mit unterschiedlichen Voraussetzungen. So kann ein Werbepartner von Facebook zum Beispiel eine Zielgruppe 'Singles zwischen 35 und 50' definieren, dann wird nur bei diesen die Werbung eingeblendet. Das sichert Facebook höhere Einkünfte pro Seitenaufruf zu als vielen anderen Betreibern. Die Ausmaße wie 'Google Adds' hat es bisher noch nicht erreicht.

Dass Facebook mehr Seitenaufrufe als Google feiern konnte, mag für den einen unverständlich sein, für den anderen ist es eine Revolution, und für den nächsten ist es nur die Konsequenz des Siegeszugs von Facebook. Soziale Plattformen, Facebook als die größte, haben eine riesige Anzeihungskraft auf ihr Clientel. Sie bauen die Nutzergruppe nicht nur ständig aus, sondern sie versuchen die Nutzer immer stärker an ihre Plattform zu binden. Dies ist gut für die Werbeeinnahmen, aber viel wichtiger ist die Macht im Internet. Bisher war Google unangefochten die wertvollste Internetfirma der Welt: ein Unternehmen, das von 2 Studenten vor 25 Jahren gegründet wurde und bis vor kurzem jeden Internetnutzer zu den Internetseiten geleitet hat. Diese Funktion wird ihnen nun durch Facebook streitig gemacht. Allerdings kann ein bei Facebook geposteter Link innerhalb weniger Minuten eine solche Eigendynamik verursachen, dass der entsprechende Server überlastet wird. Für den Server kommt das einer DoS (Denial of Service) Attacke gleich, für den Betreiber kann es den Bankrott bedeuten, wenn zigtausend potentielle Kunden seinen Online-Shop dann nicht erreichen können. Keiner von ihnen wird wiederkommen.

Bei all ihrer Anzeihungskraft, soziale Netzwerke können die Meinungsfreiheit, die Privatsphäre und vieles anderes sehr stark einschränken. Die vorhandenen Daten reichen aus, um weite Teile der Bevölkerung automatisch zu überwachen oder zu steuern. Bücher wie „Little Brother“ von Cory Doctorow zeigen, dass ein Anlass ausreichen könnte um solche Daten gegen Unschuldige zu verwenden. Dies würde nicht nur die Meinungsfreiheit einschränken, sondern auch eine digitale Rasterfahndung möglich machen. Daher ist es eine wichtige Aufgabe jedes einzelnen, die Privatsphäre zu achten, besonders auch die fremder Menschen nicht zu verletzen.

Anlagen

Literatur

diverse Ausgaben der c't (Fachzeitschrift für Computertechnik) vom Heise Zeitschriftenverlag. Insbesondere die Artikelserie über Soziale Netzwerke. Aufgelistet sind die wichtigsten /aktuellsten Artikel.

c't Artikel:
04/2010, Editorial, Big Brother 2.0
06/2010, S. 188, Netz-Sozialisierung
S. 190, Jetzt. Sofort. Alles.
07/2010, Editorial, Fotowilderei
Treffpunkt Netz
S. 104 Soziale Netzwerke verändern die Onlinelandschaft
S. 108 Facebook, twitter & Co. von innen
S: 114 Datenschutz mit Augenmaß
10/2010, S. 44, Schwarz ist out – Die Hackerkonferenz Black Hat wandelt sich