GEFAHREN VON SOZIALEN NETZWERKEN

In den letzten Jahren hat sich im Web eine Flut von sozialen Netzwerken aufgetan. Viele davon werden auch von der radikalen Linken gerne unhinterfragt verwendet. Es ist mittlerweile leider normal, dass politische Gruppierungen ihre Identität im Web mit Myspace, Facebook oder Twitter/Identica Accounts untermauern. Überlegungen zu Datenschutz, Privatsphäre und die Gefahr der Offenlegung von sozialen Zusammenhängen bleiben meist links liegen. Jedoch verwenden nicht nur 'Linke' das Internet, auch Nazis und Behörden können Computer benutzen und tun dies auch!

Anhand der §278/a/b und §129/a/b Verfahren der letzten Jahre hat sich gezeigt, dass es den Behörden immer ein grosses Anliegen ist, soziale Zusammenhänge auszuforschen. Wenn AktivistInnen observiert werden oder Telefone abgehört werden, dient dies weniger der Aufdeckung oder Prävention von Verbrechen, sondern der Ausforschung von Strukturen. Wer kennt wen wie gut, wer ist mit wem in welchen Zusammenhängen aktiv. Mit diesen Informationen lassen sich sehr schön 'terroristische Vereinigungen' konstruieren. Dabei ist es natürlich schön, wenn die AktivistInnen eine Liste der eigenen FreundInnen ins Netz stellen. So schreibt das Magazin kripo.at (Zeitschrift der Vereinigung Kriminaldienst Österreich): "Der Nutzen des populären 'Gesichtsbuchs' für Kriminalisten ist zweifelsohne bewiesen".
Jedoch nicht nur die Behörden, sondern auch die Nazis interessieren sich brennend für eure Daten. Das soziale Umfeld ist bei der Antiantifa wohl eher zweitrangig. Da die Nazis aber nicht so einfach Zugriff aufs Melderegister und andere Datenbanken haben, sind die sozialen Netzwerke eine Fundgrube, was private Daten, wie zum Beispiel Foto, Adresse, Arbeitsstelle, Schule/Uni/Ausbildungsstelle betrifft.

Oft wird von Gruppen damit argumentiert, dass es nun mal weitaus besser möglich sei, mit sozialen Netzwerken Menschen zu erreichen. Dies mag zwar stimmen, jedoch sollte auch jede Gruppe eine gewisse Verantwortung wahrnehmen. Meist wird der Schutz der Privatsphäre von AktivistInnen als Nebensächlichkeit abgetan. Jedoch sollte jede Gruppe, die im Netz auftritt, auch Verantwortung für die Sicherheit der BenutzerInnen ihres Angebots übernehmen. Ein anderes Argument, welches oft aufkommt, ist die Mögliche Pseudonymität in Sozialen Netzwerken. Doch das Geschäftsmodell von Myspace und Facebook basiert darauf, die Daten der NutzerInnen zu Geld zu machen. Deswegen verwenden sie auch enorm viel Energie darauf, die Privatsphäre der NutzerInnen aufzubrechen auch ohne deren Vor- oder Nachnamen wissen zu müssen.
Wenn politische Gruppierungen sich in sozialen Netzwerken bewegen, wird für AktivistInnen die Hemmschwell niedriger, sich diesen Netzwerken anzuschliessen und private Daten herzugeben. Es ist dann nur noch ein kurzer Weg zu privaten Bildergallerien, wo AktivistInnen identifizierbar sind. Sobald zb. Antifa Gruppen in Facebook eine Gruppe gründen oder Demonstrationen als Event ankündigen, wobei sich leicht nachvollziehen lässt, wer teilnimmt, ist dies ein gefundenes Fressen für die Antiantifa.

Datenverkauf

Wie im letzten Absatz schon erwähnt, basiert das Geschäftsmodell der sozialen Netzwerke auf dem Verkauf von Daten. So kommt nicht nur der Dienst bei dem mensch sich angemeldet hat sondern auch Drittfirmen oft ohne Wissen und explizite Einwilligung des/der NutzerIn in den Besitz von dessen Daten. Da das häufig illegal ist werden die Daten nicht verkauft sondern (gegen Geld) eine Kooperation geschlossen, und dann stellt die Kooperationspartnerin eine Dienstleisterin an die Zugriff auf die Daten bekommen und die verliert sie dann versehentlich- da kann dann natürlich niemensch was dafür. Bei Facebook wurde im November 2010 bekannt, dass EntwicklerInnen von Anwendungen die Daten der NutzerInnen weiterverkauft haben.
Mark Zuckerberg, der Gründer von Facebook, meinte vor einiger Zeit in einem Intview, dass Privatsphäre nicht so wichtig sei. Und mit dieser Einschätzung ist er nicht alleine- auch in anderen Teilen des Netzes geistert mittlerweile die Idee von "Post Privacy" herum, also "Nach der Privatsphäre". Es gibt tatsächlich AktivistInnen(?), die argumentieren, dass es besser für alle sei, wenn wir das Bedürfnis nach Privatsphäre überwinden würden.

Soziale Netzwerke und Behörden

Die Electronic Frontier Foundation hat vor einem halben Jahr Anleitungen veröffentlicht, die von den US Behörden verwendet werden, um in sozialen Netzwerken effektiv Nachforschunge anstellen zu können. Darin werden die FahnderInnen angehalten, die öffentlichen Datenquellen zu nützen. Wenn die Daten nicht öffentlich einsehbar sind, kann immer noch nachgefragt werden. Die Firma Facebook hat sich in dieser Hinsicht bei Schnellanfragen von FahnderInnen häufig kooperativ gezeigt.
In den USA kam ein Aktivist, der auf Bewährung draussen war, wieder in den Knast, weil er auf FB den Friendrequest einer Person akzeptiert hatte, der das Gutheissen von Gewalt vorgeworfen wurde. 2009 wurde ein Aktivist verhaftet und seine Wohnung durchsucht, da er beim G20 die Standorte von Polizeieinheiten über Twitter bekanntgab.

Soziale Netzwerke und die Antiantifa

Natürlich verwenden auch die Nazis zur Recherche soziale Netzwerke und deren Plattformen. So geschieht es immer wieder, dass AktivistInnen geouted werden und die veröffentlichten Daten aus sozialen Netzwerken gewonnen werden. Einfach wird es den Recherche Teams gemacht, wenn sich Antifa Gruppen auf Facebook tummeln und damit AktivistInnen durch 'like this' Buttons oder durch Teilnahme an Demo-Events ihre politischen Kontexte leichter öffentlich machen können.

Zensur

Wie bei allen kommerziellen ServiceanbieterInnen ist die Gefahr, dass zensiert wird, sehr hoch. Dies hat sich erst vor kurzem gezeigt, als der Twitter-Account der Gruppe Anonymous, die zu Attacken gegen verschiedene Firmen und Behörden aufgerufen hatte, gelöscht wurde. Ein weiteres Beispiel ist die Löschung der Facebookseite NPD-Blog.info im Oktober 2010.

Lücken in sozialen Netzwerken

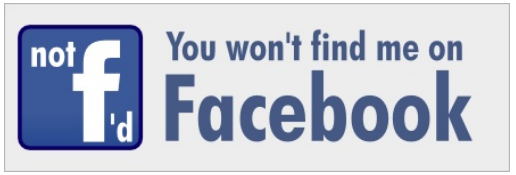
Facebook verschickt Emails, wenn eine Person ein Kommentar postet oder andere Aktionen ausführt. Im Mai 2010 wurde bekannt, dass in diesen Emails die IP Adresse von der Person vermerkt ist. Facebook hat diese Lücke im Schutz der Privatsphäre zwar kurz darauf geschlossen, jedoch werden immer wieder neue Lücken in sozialen Netzwerken bekannt. So schaffen es immer wieder findige ProgrammiererInnen mittels Skripten, die Daten aus sozialen Netzwerken zu extrahieren, wie im Mai 2010 bei SchülerVZ (1,6 Millionen Datensätze) und im Juli 2010 bei Facebook (170 Millione Datensätze). Als Google Buzz (der Kurznachrichtendienst von Google) im Februar 2010 online ging, waren von den NutzerInnen anfangs die am meisten genutzten persönlichen Kontakte einsehbar.
Meist sind dies zwar keine Sicherheitslücken im technischen Sinn, jedoch Fehler im Design der Software- was aber nicht minder gefährlich sein kann.

Alternativen

Beisl, Lokale, Konzerte, Plena, Demos… soziale Kontakte knüpft mensch am besten IRL (in real life, im echten Leben) und nicht im Netz. Es gibt zwar alternative soziale Netzwerke, jedoch sind es dennoch soziale Netzwerke und eignen sich somit gut dazu, unsere Zusammenhänge aufzuzeigen. Ein Beispiel dafür ist die Software Crabgrass, die von Leuten um das Technikkollektiv Riseup herum programmiert wird, und das soziale Netzwerk WE auf we.riseup.net, das diese Software nützt und zur Verfügung stellt. Ein grosses Augenmerk legen die EntwicklerInnen auf das kollaborative Arbeiten. So ist es möglich auf we.riseup.net Gruppen zu bilden, welche über eigene Wikis miteinander arbeiten können. Intensiv wird auch am Schutz der Privatsphäre gearbeitet- die Einstellungen dazu sind jedoch noch schwer zu überblicken. An der Software wird viel programmiert und es ist zu erwarten, dass die gröbsten Fehler und Userinterfacedesign-Schwächen bald ausgemerzt sind.
Ein weiteres soziales Netzwerk, das momentan noch sehr am Anfang der Entwicklung ist, ist Diaspora. Der Schwerpunkt von Diaspora liegt auf der Dezentralisiertheit. Das heisst, das das soziale Netzwerk nicht von einer Anbieterin betrieben und kontrolliert wird. Dabei kann die Software auf vielen Server installiert werden, die dann untereinander kommunizieren. Auch bei Diaspora wollen die EntwicklerInnen sehr auf den Schutz der Privatsphäre der NutzerInnen achten.

Loskommen

Die 'Web 2.0 Suicide Machine' ermöglicht es euch, euch mit wenigen Klicks aus mehreren sozialen Netzwerken zurückzuziehen. Auf suicidemachine.org findet ihr dieses Service, dem ihr eure Zugangsdaten gebt und welches eure Infos dann aus den Netzwerken löscht. Dies ist auch deswegen nett, da viele soziale Netzwerke das Löschen der eigenen Konten sehr schwer und kompliziert macht (was ja auch verständlich ist, die verdienen ja daran).



Suicide Machine:
http://suicidemachine.org
Entwicklung der Facebook Privatsphären Einstellungen:
http://mattmckeon.com/facebook-privacy/
What the New Facebook Privacy Rules Mean for Activists:
http://www.digiactive.org/2009/12/10/what-the-new-facebook-privacy-rules-mean-for-activists/
Dokumente, die zeigen wie Behörden soziale Netzwerke nutzen:
https://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement
Facebook Seite der FSF:
http://www.fsf.org/facebook

tear the system down - bit. by. bit. mailto:bitbybit@riseup.net
technologie in linksradikalen kontexten https://we.riseup.net/bitbybit