

# **Gefahren der sozialen Netzwerke**

## **Wer sollte dies unbedingt lesen?**

**Jeder, der in sozialen Netzwerken unterwegs ist.**

**Jeder, der bei der Polizei eingestellt werden will.**

**Jeder, der bei der Polizei beschäftigt ist.**

**Jeder, der aus den Erfahrungen anderer lernen möchte.**

Stand: 05.03.2010

## **Gefahren der sozialen Netzwerke**

Die VZ-Gruppe, Xing oder Facebook, alle soziale Netzwerke sind voll im Trend. Hier gehen täglich Menschen neue Freundschaften per Mausklick ein. Freundschaften können so unkompliziert und über weite Entfernungen geknüpft und gepflegt werden. 400 Freunde nehmen Zeit in Anspruch und manche Nutzer/innen sind sich nicht sicher, ob sie alle ihrer 400 Freunde kennen. Andere akzeptieren diese Freundschaften um niemanden zu beleidigen, aber eigentlich wollen sie nicht drin sein. Es ist in, es ist ein Muss. Doch der Zeitaufwand wird größer: „Weltweit verbringen 175 Millionen aktive Nutzer knapp drei Milliarden Minuten täglich in dem Facebook- Netzwerk. Auf den einzelnen Nutzer gerechnet sind das durchschnittlich 102 Sekunden täglich.“<sup>1</sup>

Wir dürfen nie vergessen: Bei diesen Sozialen Netzwerken geht es ums Geld. So setzte allein Facebook 500 Millionen € in diesem Jahr. Twitter sucht einen neuen Sponsor im dreistelligen Millionenbereich.

Vor diesem Hintergrund sollten Nutzerinnen und Nutzer sehr genau hinschauen, wie soziale Netzwerke funktionieren, was steht oder was steht nicht in den AGB und wie verhält es sich mit dem Datenschutz.

## **Surfer haben Rechte**

Der Verbraucherzentrale Bundesverband<sup>2</sup> (vzbv) nahm im Sommer 2009 die Anbieter Sozialer Netzwerke ins Visier. Gegen die Plattformen MySpace, Facebook, lokalisten.de, wer-kennt-wen.de und Xing leitete der Verband Unterlassungsverfahren ein. In der Kritik standen Vertragsbedingungen und Datenschutzbestimmungen, die Nutzer benachteiligen und den Betreibern weitgehende Rechte einräumen. Gegenstand der aktuellen Verfahren sind insbesondere Regelungen zur umfassenden Datennutzung und -verarbeitung. Diese erfolgen oft ohne Einwilligung des Nutzers und weit über den eigentlichen Zweck hinaus.

Der Verbraucherzentrale Bundesverband forderte die Anbieter auf, Voreinstellungen für die Datennutzung schon bei der Registrierung nutzerfreundlich zu gestalten. Die Betreiber müssen sicherstellen, dass Daten nur verwendet werden dürfen, wenn der Nutzer ausdrücklich einwilligt hat. Dies gelte zum einen für jede Form der Werbung. Zum anderen aber

<sup>1</sup> <http://www.zeit.de/online/2009/12/social-network-studie?page=2>

<sup>2</sup> <http://www.vzbv.de/go/presse/1180/index.html>

müssten die Verbraucher auch darüber entscheiden können, ob sie möchten, dass ihre Daten über Suchmaschinen aufzufinden sind. Auch beim Urheberrecht liegt hier einiges im Argen: einige Anbieter lassen sich laut AGB vom Nutzer umfängliche Rechte an von ihnen erstellten Inhalten übertragen. Daraufhin können sie mit den Inhalten nach Belieben verfahren, etwa könnte ein Privatfoto ungefragt in einer Zeitung oder im Fernsehen landen. Außerdem behalten sich einige Anbieter das Recht vor, "aus beliebigen Gründen" Inhalte zu löschen oder gar "ohne vorherige Mitteilung" und "ohne Angabe von Gründen" den Zugang für Mitglieder zu sperren. Trotz der Kampagne hat sich technisch nicht viel getan. Wir Nutzer werden eben dazu aufgefordert, möglichst viel von sich in Sozialen Netzwerken preiszugeben.

### **Karriere-Killer Internet**

Das Internet ist seit vielen Jahren schon eine zusätzliche Informationsquelle für Personalabteilungen. Die unbekümmerte Preisgabe persönlicher Daten im Netz kann zum Stolperstein für die berufliche Karriere werden: Eine Umfrage im Auftrag des Bundesverbraucherschutzministerium (BMELV) zeigt, dass über ein Viertel der befragten Unternehmen das Internet systematisch für Personalentscheidungen nutzen. Fast 80 Prozent von ihnen bereits vor der Einladung zum Vorstellungsgespräch. Bei einem Viertel der Unternehmen kommt es vor, dass Bewerber wegen Informationen aus dem Internet nicht eingestellt werden.

Zwar beschränkt sich derzeit noch die Mehrzahl der Unternehmen auf allgemein zugängliche Informationen, aber immerhin ein Drittel bezieht auch soziale Netzwerke ein. Umso wichtiger wird es, sehr bewusst zu entscheiden, welche Inhalte man hier einstellt und wer diese sehen können soll.

Einträge, Bilder, Kommentare in sozialen Netzwerken haben auch schon Auswirkungen auf Versetzungen und Beförderungen gehabt.

### **Soziale Netzwerke und Polizei**

Die Neuseeländische Polizei stellte das Bild eines Verbrechers bei Facebook ein und innerhalb von 24 Stunden konnte der Täter identifiziert werden.<sup>3</sup>

Wir können sicher sein, dass das polizeiliche Gegenüber die sozialen Netzwerke für seine Zwecke ebenso nutzt, sprich die Identifizierung von Polizistinnen und Polizisten.

<sup>3</sup> <http://presstext.de/news/090114016/polizei-nutzt-facebook-zur-einbrecherjagd/>

Wir können auch sicher sein, dass Benutzerprofile und geschlossene Nutzergruppen nicht sicher sind.

Daher kein leichtfertiger Daten-Strip im Netz.

## **Erfahrungen von KollegInnen für KollegInnen**

Die folgenden Beispiele zeigen, dass die Beteiligung mit sozialen Netzwerken Folgen haben kann.

### **Beispiel 1**

Ein Kollege hat im ersten Jahr bei einer entsprechenden Plattform ([www.gesichterparty.de](http://www.gesichterparty.de)) Fotos vom Grillen nach einem Seminar eingestellt. Darunter war auch ein Foto auf dem ein Mitarbeiter des Praxisamtes abgebildet war, der eine Flasche Bier in der Hand hielt. Das Foto soll einen Untertitel gehabt haben „ So arbeitet die Polizei“.

Das wurde der Dienststelle bekannt. Der Kollege bekam ein Diszi, das erst nach über einem Jahr abgeschlossen wurde und mit einer schriftlichen Rüge und einem Eintrag in die Personalakte endete. Folge war, dass der Kollege eine Sperrfrist von zwei Jahren bekam und erst ein Jahr später als seine Lehrgangskollegen zum Kommissar ernannt wurde. Umgerechnet bedeutete dies eine Geldstrafe von rund 9600,-€ (12 x 800,-€), da ihm das Geld natürlich verloren ging.

### **Beispiel 2**

Hier sind zwei Fälle bekanntgeworden, die eine andere Art der "Gefährlichkeit" zeigen.

- 1.) Nachdem eine Kollegin Fotos vom normalem (!) Schießtraining (wohlgemerkt, es waren auch keine polizeitaktischen Dinge darauf zu erkennen) in ihr StudiVz Fotoalbum stellte, folgte sogleich ein persönliches Zwangsgespräch mit dem PI-Leiter mit dem Hinweis, dass eine disziplinarrechtliche Überprüfung stattfindet. Da kam nichts bei rum.
- 2.) Infolge des Punkt 1.) registrierten diverse Kollegen, dass die PI-Leitung offensichtlich systematisch diverse StudiVz-Konten "durchforstete". Man konnte dies an den letzten erfassten Besuchern erkennen. Das Ziel ist unbekannt!

Also immer schön die eigenen Konten vor unbefugten Zugriffen schützen.

### **Beispiel 3**

Ich bin seit 2006 Mitglied bei den Lokalisten und hatte dort anfangs den Benutzernamen "Bullen...". Diesen Spitznamen habe ich im engeren Freundeskreis bekommen, er ist eine Mischung aus meiner schönen Herkunft und meinem Beruf. Ich finde den Spitznamen einfach nur sehr lustig und habe ihn deshalb auch als Benutzernamen gewählt. Zu Beginn meiner Mitgliedszeit waren bei den Lokalisten noch bedeutend weniger User registriert und das Ganze hatte einen familiären Charakter. Ich hatte dort lediglich mit Personen Kontakt, die ich kenne. Meinen Beruf hatte ich zu keiner Zeit in meinem Profil angegeben.

So nach und nach (v. a. mit ansteigender Zahl der Registrierungen, Freundschaftsanfragen von mir völlig unbekanntem Personen usw.) ist mir alles allerdings etwas unheimlich geworden und ich habe immer mehr Daten herausgenommen oder Aussagen abgeschwächt. Irgendwann im Laufe des Jahres 2008 bekam ich eine Nachricht über das lokalisteneigene Nachrichtensystem mit den Worten: "werd Sie gleich festnehmen ... " (ohne Anrede oder ähnliches). Die Person, die mir die Nachricht geschrieben hatte, konnte ich als einen ganz entfernten Bekannten identifizieren, der zu Grundschulzeiten in der Klasse eines Freundes war. Diese Person ist bekannt dafür, sozial nicht unbedingt besonders integriert zu sein, um es mal vorsichtig auszudrücken. Ich hatte zu dieser Person niemals engeren Kontakt.

Daraufhin habe ich sämtliche Bilder von mir herausgenommen, meinen Benutzernamen geändert und jegliche Aussagen, die mich eindeutig identifizieren könnten, gelöscht. Seither habe ich keine Probleme mehr gehabt und ein gutes Gefühl dabei. Hierbei kommt mir auch mein "Allerweltsname" zu Gute. Such mal bei Lokalisten nach Personen mit Nachname: N. und Vorname: N. Das Ergebnis sind 195 Treffer ;).

Hier kann mich nur eine Person identifizieren, die mich wirklich kennt und z.B. darüber hinaus mein Geburtsdatum kennt. Aber selbst das ist schwierig, weil ich keine Bilder mehr von mir eingestellt habe. Mein bisheriger Freundesbaum bleibt natürlich bestehen und ich kann weiterhin zu den Personen Kontakt haben, zu denen ich Kontakt haben möchte.

Ich habe auf lokalisten.de spaßeshalber mal nach Kollegen gesucht und war wirklich erschrocken, was für Informationen hier zum Teil preisgegeben werden. Fotos von Frau und Kindern usw. Das ist für mich undenkbar.

## Beispiel 4

Ein Landesjugendvorstand hat sich vor zwei Jahren im Rahmen einer Sitzung dazu entschlossen, dass sich alle Vorstandsmitglieder bei StudiVZ anmelden, um dort als Gewerkschafts-"Nasen" ansprechbar zu sein.

Ich war dort auch angemeldet und habe auch entsprechende Gewerkschaftsgruppen eingerichtet. Irgendwann bekam ich die Bitte aus dem Innenministerium (ich sag nur "Bitte") mich mit Blick auf meine Bewerbung doch dort wieder abzumelden. Begründet hat man das mit taktischen Gesichtspunkten (Einsatz VE - wäre bei mir so was von lächerlich, aber na ja). Darüber hinaus hat man mir einen Verstoß gegen das Urheberrecht unterstellt, da ich so viele Bilder von Gewerkschaftsveranstaltungen dort eingestellt hatte. So nach dem Motto: "Wenn die da so viele Bilder drin haben, dann muss ja jemand abgebildet wurden sein, der das gar nicht wollte." Darüber habe ich mich am Meisten geärgert, weil ich vorher immer jeden frage, ob er mit der Veröffentlichung des Bildes einverstanden ist.

Ergebnis der ganzen Debatte: Ich habe mich in allen sozialen Netzwerken wieder abgemeldet.

Kernaussage: In unserem Bundesland wird es überhaupt nicht gerne gesehen, wenn sich Polizistinnen und Polizisten dort anmelden.

Persönliche Erfahrung: Ich bin ganz froh, dass ich nicht mehr angemeldet bin, denn zum Schluss wurde ich von "potentiellen" Kunden angeklickt, nicht gerade angenehm :-)

## Tipps<sup>4</sup>

### Grundregeln

- Gib keine Daten an (z.B. in Profilen), durch die man Dich im realen Leben finden kann!
- Veröffentliche nur Dinge, auf die Du auch noch in 3 Monaten und sogar in 5 oder 10 Jahren stolz sein kannst!
- Das Internet kennt leider keine „Gnade des Vergessens“.
- Stell Dir folgendes plastisch vor: Alles, was Du heute schreibst, lesen ...
  - alle Deine Mitschüler und Lehrer.
  - ein späterer Arbeitgeber.
  - Deine zukünftigen Schwiegereltern.
- Was Du einmal veröffentlicht hast, kannst Du sehr wahrscheinlich

<sup>4</sup> [www.lrz-muenchen.de/services/security/gefahren/gefahren\\_handzettel\\_kids.pdf](http://www.lrz-muenchen.de/services/security/gefahren/gefahren_handzettel_kids.pdf)

nicht mehr zurückholen! Es ist oft für jeden lesbar, der sich für Dich interessiert. Und diejenigen reagieren möglicherweise unangenehm! Ein zuverlässiges Löschen ist meist nicht möglich.

- Selbst wenn Du den Zugriff eingeschränkt hast, können vertrauliche Daten in die falschen Hände gelangen!

### **Konkrete Regeln**

- Keine Strandbilder und –filme
- (Private) Tagebücher gehören nicht ins Internet!
- Keine unvoreilhafteten oder (ganz) privaten ...
  - Fotos oder Filme veröffentlichen.
  - Kommentare zu Fotos schreiben.
  - Pinnwandeinträge schreiben.
- Diskriminierende Gruppen, wie z.B. über rechtsradikale Themen oder zum Mobbing von Lehrern/Mitschülern:
  - Nicht beitreten!
  - Niemals gründen!

### **Besonders Wichtig:**

Gib zu Deiner eigenen Sicherheit niemals Deine private Adresse an, d.h. keinesfalls die Straße und den Wohnort (nur bei großen Städten)!