

Konsumentenschutz
Prinz-Eugen-Straße 20-22
A-1041 Wien
Tel: ++43-1-501 65/2144 DW
E-Mail: konsumentenpolitik@akwien.at



06/2010
Jänner/2010

TEST SOZIALE NETZWERKE

ZUSAMMENFASSUNG DER ERGEBNISSE

18.1.2010

Durchgeführt vom Österreichischen Institut für angewandte Telekommunikation (ÖIAT) im Auftrag der AK

Facebook, MeinVZ, Netlog, Szene1: vier verschiedenen soziale Netzwerke, vier verschiedene Übungsparcours für den mehr oder weniger datenschutzbewussten Nutzer. Welche Informationshilfen findet er auf den Seiten vor, wenn er die voreingestellten Datenschutzstandards nicht ändert, was wenn er im Netzwerk nicht mehr präsent sein möchte oder wenn er von anderen Teilnehmern belästigt wird bzw. gar ein Dritter unter seinem eigenen Namen auftritt und ihm damit gewissermaßen seine Identität „klaut“?

Diese Szenarien wurden beispielhaft in einem Test durchgespielt, um auf Basis der dabei gewonnenen Erfahrungen Verbesserungsmöglichkeiten aufzuzeigen. Die Schlussfolgerungen wurden bewusst allgemein, und nicht Plattform-spezifisch, gezogen, da allein aufgrund der überwältigenden Zahl an täglichen Kommunikationsvorgängen singuläre Testerfahrungen bei eingeschränkten Testkriterien im einzelnen zwar aufschlussreich aber nicht repräsentativ sind.

Die wichtigsten Ergebnisse

- **Die Standard-Einstellungen zum Schutz der Privatsphäre - worum geht's:** Sich mit einzelnen Konfigurationen zum Schutz der eigenen Daten zu beschäftigen, ist nicht jedermanns Sache. Der Anbieter gibt deshalb ein Sicherheitslevel vor, dass individuell verändert werden kann.

Die „Schärfe“ der Standardeinstellungen variiert netzwerkabhängig sehr: Profilfotos und Fotoalben sind entweder nur für deklarierte „Freunde“ sichtbar oder aber allen Plattformnutzern bzw. überhaupt allen InternetnutzerInnen zugänglich. Details zum eigenen Profil (z.B. Interessen, Beziehungsstatus, Wohnort) sind teilweise für alle Internet-NutzerInnen sichtbar. Die Einstellungen zum Schutz der Privatsphäre sind zu wenig spezifisch: Nutzer können nicht bei allen Plattformen

selbst entscheiden, welchen Ausschnitt der Profilangaben sie wem sichtbar machen wollen.

Fazit: Es sollten jeweils spezifische Einstellungsmöglichkeiten vorhanden und die sichersten Optionen automatisch vorausgewählt sein.

- **Profil und Beiträge löschen - worum geht's:** „Besen, Besen seids gewesen“ – wie wird man sein Profil und eigene Einträge wieder los und zwar restlos? Denn Achtung: Auch gepostete Nachrichteninhalte (etwa in Gästebüchern oder auf Pinnwänden), die bei einem Plattformausstieg anonymisiert werden, können Rückschlüsse auf den Verfasser geben.

Wo ist bitte die Löschfunktion?: Auf zwei Plattformen ist sie nicht direkt, sondern nur über eine Suche in der Hilfe auffindbar.

Datenreste: Plattform-Betreiber klären nicht immer aktiv darüber auf, wie umfangreich gelöscht wird und dass Datenspuren bei außerhalb des eigenen Profils veröffentlichten Nachrichten übrig bleiben. So bleiben oft gepostete Beiträge erhalten, wobei der Name bspw. durch den Hinweis „anonymer Nutzer“ ersetzt wird. Teilweise wird nur die Verknüpfung zum gelöschten Profil gekappt und sowohl der Beitrag als auch der Benutzername bleiben erhalten.

Fazit: Die Löschfunktion für das eigene Profil muss leicht auffindbar sein. Aufklärung darüber, welche Datenreste zurückbleiben, ist notwendig.

- **Verstöße melden - worum geht's:** Auf Plattformen werden erfreulicherweise viele Freundschaften geschlossen, hin und wieder aber auch Feindseligkeiten ausgetragen. Beleidigungen können dabei ein Ausmaß annehmen, dass von Cyber-Mobbing die Rede sein kann.

Wer rasch hilft, hilft doppelt: Die Bandbreite der Reaktionszeiten bei den gespielten Testsituationen reicht von wenigen Minuten bis hin zu gar keiner Reaktion seitens eines Plattformbetreibers. Teilweise wurden auch nicht alle beanstandeten Inhalte entfernt (z.B. nur bloßstellende Fotos aber nicht die herabwürdigenden Kommentare).

Fake-User melden - worum geht's: Soziale Netzwerke können für Identitätsdiebstahl missbraucht werden. Oft erweisen sich Ex-FreundInnen oder SchulkollegInnen als Übeltäter, die über Fake-Profile Schaden anrichten, etwa in dem sie kompromittierende echte oder gefälschte Fotos und Texte mit Bezug zum Opfer veröffentlichen.

Hilfe für Opfer: Anleitungen und Tipps, was gegen Fake-User unternommen werden kann, sind rar. Opfer von Identitätsdiebstahl können nicht auf allen Plattformen eine Meldung abgeben, ohne sich selbst registrieren zu müssen. Die Bandbreite an Reaktionen auf Meldungen reicht von erfreulich prompter Löschung des gefälschten Profils bis zu keiner Reaktion.

Fazit in beiden Fällen: Die plattformseitigen Hilfestellungen sind verbesserungswürdig.

Inhalt

1. Testdesign	4
2. Testszenario „Verstöße melden“	4
3. Testszenario „Profil löschen“	6
4. Testszenario „Fake-User melden“	9
5. Testszenario „Standard-Einstellungen zum Schutz der Privatsphäre“	10
6. Zusammenfassende Darstellung der wichtigsten Verbesserungspotenziale.....	13

1. Testdesign

Vorbemerkung:

Ziel dieses exemplarischen Tests ist es anbieterunabhängig Verbesserungspotenziale zu identifizieren, die aus der Sicht durchschnittlicher NutzerInnen bei der sicheren Verwendung Sozialer Netzwerke als relevant zu betrachten sind.

Eine Vergleichbarkeit der für diesen Test ausgewählten Plattformen auf Basis dieser Erhebung ist nicht intendiert und mangels Repräsentativität auch nicht möglich. Zu den Gründen dafür zählen die geringe Anzahl an Stichproben, mangelnde Vergleichbarkeit der unterschiedlichen Plattformfunktionalitäten und die eingeschränkte Auswahl an Testkriterien.

Getestete Plattformen:

- Facebook
- MeinVZ
- Netlog
- Szene1

Testzeitraum:

November 2009 bis Jänner 2010

Testscenarien:

1. Verstöße melden
2. Profil löschen
3. Fake-User melden
4. Standard-Einstellungen zum Schutz der Privatsphäre

Methode:

Praxistests mit Hilfe von exemplarischen Stichproben

2. Testscenario „Verstöße melden“

Problemdarstellung

Studien, zB JIM 2008 des Medienpädagogischen Forschungsverbundes Südwest (www.mpfs.de), belegen die Zunahme von Mobbing und Belästigungen in Sozialen Netzwerken. Demnach kann ein Viertel der befragten Jugendlichen zwischen 12 und 19 Jahren bestätigen, dass im Bekanntenkreis schon einmal jemand in einem Sozialen Netzwerk von Mobbing betroffen war. Angesichts dieser Entwicklung soll die Unterstützung Betroffener durch die Betreiber der Sozialen Netzwerke untersucht und dokumentiert werden.

Testaufbau

Aufbau von zwei nachgestellten Cyber-Mobbing Situationen in jedem der getesteten Sozialen Netzwerke und Meldung von Beschwerden an die Betreiber.

Zwei männliche jugendliche Täter belästigen das Opfer, einen ebenfalls männlichen Schulkollegen, auf den Sozialen Netzwerken mittels:

- Beleidigungen, Beschimpfungen etc.
- Veröffentlichung je eines neutralen und eines bloßstellenden Fotos (Anspielung auf sexuelle Vorlieben) mit Nennung des vollen Namens des Opfers
- Androhung der Verbreitung von Fotos an SchulkameradInnen und weiterer Verleumdungen

Ablauf:

- Registrierung von 3 Plattform-Nutzern.
- „Freundschaftliche“ Interaktionen zwischen den 3 zuvor registrierten und ausgewählten anderen Plattform-NutzerInnen über einen Zeitraum von 1 Woche, danach während 3 Wochen stetige Steigerung der Belästigungen mittels Nachrichten und Fotos auf Guestbooks, Pinnwänden etc.
- Meldung der schriftlichen Belästigungen und der beanstandeten Fotos an den Plattform-Betreiber mit Hilfe der auf den Plattformen angebotenen „Melde“-Funktionalitäten.
- Auswertung der Rückmeldungen und der getätigten Aktionen der Plattform-Betreiber.

Testkriterien

Getestet wurde entlang folgender Kriterien (in Klammer sind jeweils die Bewertungskategorien angegeben):

1. Auffindbarkeit der Meldefunktion (leicht/schwer)
2. Gestaltung des Meldevorganges, Kategorisierung der Meldungen (einfach/kompliziert, mit/ohne Kategorisierung)
3. Reaktionszeit bis zur Löschung (Stunden bzw. Tage, betrug die Reaktionszeit mehr als 7 Tage erfolgte die Bewertung mit „keine Reaktion“)
4. Möglichkeit von wiederholten Meldungen des gleichen Sachverhalts (ja/nein)
5. Entfernung der beanstandeten Inhalte (ja/nein)
6. Benachrichtigung von Täter bzw. Opfer (keine/beide/nur Täter/nur Opfer)
7. Inhaltliche Qualität der Rückmeldung (Beschreibung).

Ergebniszusammenfassung:

Anmerkung:

Die Tests in diesem Szenario wurden mit zwei Testfällen pro Plattform durchgeführt. Bei Übereinstimmung der Ergebnisse in beiden Testfällen, ist das Ergebnis in nachfolgender Tabelle nur einmal angeführt.

	Facebook	meinVZ	Netlog	Szene1
1) Auffindbarkeit der Meldefunktion	Leicht	Leicht	Leicht	Leicht
2) Gestaltung des Meldevorganges, Kategorisierung	Einfach, mit Kategorien	Einfach, mit Kategorien	Einfach, ohne Kategorien	Einfach, mit Kategorien
3) Reaktionszeit (Test 1 / Test 2)	keine Reaktion / keine Reaktion	2 Tage / 5 Tage	4 Tage / 9 Minuten	2 Tage / 2 Tage
4) Möglichkeit von wiederholten Meldungen	Nein	Ja	Ja	Ja
5) Entfernung der beanstandeten Inhalte	Nein	Bilder entfernt, beleidigende Kommentare blieben jedoch erhalten	Ja	Bilder entfernt, beleidigende Kommentare blieben jedoch erhalten
6) Benachrichtigung von Täter bzw. Opfer *	Keine	Täter und Opfer	nur Täter	nur Opfer
7) Inhaltliche Qualität der Rückmeldung	-	Klare und sinnvolle Antworten	Klare und sinnvolle Antworten	Klare und sinnvolle Antworten (1 x erst nach Nachfragen)

*... Anmerkung: Antworten der Betreiber erfolgten immer gleichzeitig mit der Löschung (sofern durchgeführt).

Verbesserungsmöglichkeiten:

- Beschleunigung der Reaktionen auf Beschwerdemeldungen
- Umfang der Entfernung der beanstandeten Inhalte

3. TestszENARIO „Profil löschen“

Problemdarstellung

Viele Internet-NutzerInnen wissen nicht, wie man das eigene Profil auf Sozialen Netzwerken löschen kann und stellen sich darüber hinaus die Frage, wie vollständig eine Löschung bzw. Deaktivierung ist.

Testaufbau und Ablauf

- Anlegen eines NutzerInnen-Profiles (mit Profilfoto und Personenbeschreibungen mit Hilfe der jeweils vorgegebenen Beschreibungsfelder)
- Durchführung von Plattform-Aktivitäten: Hochladen von Fotos, Hinterlassen von öffentlichen Nachrichten auf eigenem und anderem Profil (mit Fotos, wenn möglich)
- Löschung des NutzerInnen-Profiles durch den Nutzer selbst

- Überprüfung, ob alle Daten, d.h. die im eigenen Profil angegebenen Informationen und auf anderen Profilen geposteten Einträge und Fotos gelöscht werden bzw. inwieweit für andere Plattform-NutzerInnen diese Daten noch einsehbar sind.

Testkriterien

Getestet wurde entlang folgender Kriterien (in Klammer sind jeweils die Bewertungskategorien angegeben):

1. Auffindbarkeit der Löschfunktion (leicht/schwer)
2. Benachrichtigung von "Freunden" über Löschung (ja/nein)
3. Reaktivierbarkeit (ja/nein, wie lange)
4. Gestaltung des Löschvorganges (Beschreibung)
5. Verzögerung der Wirksamkeit der Löschung (sofort, Anzahl der Stunden/Tage bis zur endgültigen Löschung)
6. Umfang der Löschung der Profildaten und der außerhalb des eigenen Profils auf Pinnwänden und in Gästebüchern öffentlich geposteten Inhalte. Private Nachrichten sind nicht berücksichtigt. (alles/unvollständig).

Ob seitens der Betreiber tatsächlich eine umfassende physische Löschung von nicht mehr angezeigten Inhalten durchgeführt wurde, konnte nicht erhoben werden.

	Facebook	meinVZ	netlog	Szene1
1) Auffindbarkeit der Löschfunktion	Schwer für Löschung (leicht für Deaktivierung)	Leicht	Schwer	Leicht
2) Benachrichtig von „Freunden“ über Löschung/Deaktivierung	Nein	Nein	Nein	Nein
3) Reaktivierbarkeit	Immer bei Deaktivierung, bis zu 14 Tage bei Löschung	Nein	Ja, 14 Tage	Nein
4) Gestaltung des Löschvorganges	Formular, ohne Email-Bestätigung	Formular, ohne Email-Bestätigung	Formular, ohne Email-Bestätigung	Formular, mit Email-Bestätigung
5) Verzögerung bis zur Wirksamkeit der Löschung	Sofort (allerdings vorerst nur Deaktivierung)	Sofort (Hinweis, dass Löschung bis zu 48 Stunden dauern kann)	Sofort	Sofort
6) Umfang der Löschung *	Vollständig	Unvollständig außerhalb des eigenen Profils	Unvollständig außerhalb des eigenen Profils	Unvollständig außerhalb des eigenen Profils

* *Detailinformationen zum Umfang der Löschung:*

Facebook:

Das Profil und die außerhalb des eigenen Profils geposteten öffentlichen Beiträge werden gelöscht.

Es wird zwischen einer „Deaktivierung“ und einer „Löschung“ unterschieden. Bei einer Deaktivierung bleiben die Daten auf Betreiberseite gespeichert. Man scheint jedoch beispielsweise nicht mehr auf Freundeslisten auf und öffentliche Nachrichten auf fremden Profilen werden nicht mehr angezeigt.

Eine Deaktivierung wird nach einem erneuten Login sofort aufgehoben. Im Gegensatz zur Deaktivierung findet bei einer Löschung die tatsächliche Entfernung aller Daten statt (zumindest aus der Sicht von Plattform-NutzerInnen) - dies allerdings erst innerhalb eines Zeitraumes von 14 Tagen nach einer Löschung („...wird innerhalb von 14 Tagen dauerhaft gelöscht...“). In diesem Zeitraum entspricht der Status einer Löschung dem einer Deaktivierung.

Auszug aus Datenschutzrichtlinien: „Selbst nach dem Entfernen von Informationen von deinem Profil oder Löschen deines Kontos werden Kopien dieser Informationen u.U. weiterhin an anderer Stelle angezeigt, sofern sie mit anderen ausgetauscht, gemäß deinen Privatsphäre-Einstellungen übermittelt oder von anderen Nutzern kopiert oder gespeichert wurden. Dein Name wird jedoch nicht mehr mit diesen Informationen auf Facebook verknüpft. (Wenn du beispielsweise etwas im Profil eines anderen Nutzers veröffentlichst und dann dein Konto löschst, bleibt dieser Beitrag u.U. weiterhin bestehen, ist jedoch mit dem Namen „Anonymer Facebook-Nutzer“ verknüpft.) Darüber hinaus können wir bestimmte Informationen zur Vermeidung von Identitätsbetrug oder anderem missbräuchlichen Verhalten speichern, selbst wenn sie gelöscht werden sollten.“

meinVZ:

Das Profil wird zur Gänze gelöscht, die außerhalb des eigenen Profils geposteten öffentlichen Beiträge bleiben anonymisiert erhalten.

Auszug aus den Allgemeinen Geschäftsbedingungen: „Mit der erfolgreichen Abmeldung eines Nutzers werden der Account des Nutzers und alle personenbezogenen Daten des Nutzers dauerhaft gelöscht. Diejenigen Beiträge, die der Nutzer vor der Abmeldung über das Netzwerk öffentlich zugänglich gemacht hat (z.B. auf der Pinwand eines anderen Nutzers oder innerhalb einer Gruppe), bleiben nach der erfolgten Deaktivierung weiterhin abrufbar – dies jedoch ohne Angabe des Namens und ohne Angabe des Fotos sowie mit dem Hinweis, dass der Beitrag von einem inzwischen gelöschten Nutzer stammt.“

netlog:

Das Profil wird zur Gänze gelöscht. Die Inhalte der außerhalb des eigenen Profils geposteten öffentlichen Beiträge bleiben inklusive BenutzerInnenname, Geschlecht und Alter weiterhin sichtbar. Der BenutzerInnenname ist nicht mehr mit dem (bereits gelöschten) Profil verknüpft.

Auszug aus Datenschutzerklärung: “Informationen, die von dir hochgeladen wurden: gespeichert für einen Zeitraum von 6 Monaten nachdem du diese Informationen oder deinen Account gelöscht hast. (Beachte: du kannst deinen Account jederzeit löschen. Wenn du dich in einem Zeitraum von zwei Jahren nicht in dein Profil einloggst, wird es automatisch gelöscht.)“

Szene1:

Das Profil wird zur Gänze gelöscht. BenutzerInnenname und Inhalt von außerhalb des eigenen Profils geposteten Nachrichten sind bei Empfängern noch lesbar, bei einem Klick auf den BenutzerInnennamen erscheint „User existiert nicht“.

Auszug aus Allgemeinen Geschäftsbedingungen: „Im Fall der Beendigung der Nutzung werden auf Wunsch des Users sämtliche zu ihm gespeicherten personenbezogenen Daten gelöscht, sofern diese nicht mehr z.B. für Abrechnungszwecke erforderlich sind.“

Verbesserungsmöglichkeiten:

- Auffindbarkeit der Löschfunktion
- Vollständigkeit der Löschung
- Leichtere Verfügbarkeit von Informationen über den Löschvorgang (Wie kann eine Löschung des Profils durchgeführt werden? Was wird gelöscht und was nicht?)

4. Testscenario „Fake-User melden“

Problemdarstellung

Fake-User Accounts sind NutzerInnen-Profilen auf Sozialen Plattformen im Internet, mit denen reale Identitäten, oft von Ex-FreundInnen, SchulkollegInnen oder Prominenten vorgetäuscht werden. Durch einen solchen Identitätsdiebstahl kann z.B. Schaden durch Beschimpfungen und Belästigungen im Namen des Opfers oder die Zur-Schau-Stellung von kompromittierenden echten oder gefälschten Fotos verursacht werden.

Testaufbau und Ablauf

- Anlegen eines Fake-Profiles: TäterIn legt unter dem Namen eines fiktiven 15-jährigen Opfers ein neues Profil auf den Plattformen an, inklusive Foto mit eindeutig nachteiliger Darstellung und den „echten“ Kontaktdaten des Opfers. Die Veröffentlichungen finden auf der eigenen Profilsseite statt.
- TäterIn veröffentlicht Beschimpfungen und Verunglimpfungen von SchulkollegInnen und LehrerInnen wegen schlechter Noten auf dem Fake-Profil.
- Opfer meldet das Fake-Profil dem Plattformbetreiber, zuerst nur per Email, da es von einer Freundin vom Fake-Profil erfahren hat und kein eigenes Profil auf der jeweiligen Plattform angelegt hat.
- Danach wird die Meldemöglichkeit innerhalb der Plattform getestet.

Testkriterien

Getestet wurden folgende Kriterien und Funktionen (in Klammer finden sich jeweils die Bewertungskategorien):

1. Möglichkeit der Suche von NutzerInnen mit Vor- und Nachnamen ohne Registrierung (ja/nein)
2. Hilfestellung für eine Meldung von „Fake-User“ ohne Registrierung auf Plattform vorhanden? (ja / nein)
3. Wird das Fake-Profil auch dann entfernt, wenn die Meldung ausschließlich per Email – ohne Registrierung auf der Plattform – gemacht wird? (ja / nein)
4. Reaktionszeit bis zur Löschung des Fake-Profiles (Stunden bzw. Tage). Betrug die Reaktionszeit mehr als 7 Tage, wurde mit „keine Reaktion“ bewertet.
5. Umfang der Löschung (Beschreibung)

Anmerkung:

Die Tests in diesem Szenario wurden mit zwei Testfällen pro Plattform durchgeführt. Bei Übereinstimmung der Ergebnisse in beiden Testfällen, ist das Ergebnis in nachfolgender Tabelle nur einmal angeführt.

	Facebook	meinVZ	netlog	Szene1
1) Möglichkeit der Suche von NutzerInnen mit Vor- und Nachnamen ohne Registrierung	Ja (abhängig von Einstellungen zur Privatsphäre)	Nein	Ja (immer sichtbar: Profilfoto, Name, Benutzer-Innenname, Ort, Geschlecht, Alter; restliche Angaben: abhängig von Einstellungen zur Privatsphäre)	Nein (nur mit BenutzerInnen-namen)
2) Hilfestellung für eine Meldung von „Fake-User“ ohne Registrierung auf Plattform vorhanden	Ja (mit Meldeformular)	Nein (nur Hinweis wie Meldung nach Registrierung funktioniert)	Ja (es wird Email-Adresse für Missbrauch genannt)	Nein (nur Hinweis wie Meldung nach Registrierung funktioniert)
3) Entfernung des Fake-Profiles auch bei Meldung ausschließlich per Email	Nein	Nein	Ja	Ja
4) Reaktionszeit bis zur Löschung *	Keine Reaktion / 12 Stunden	1 Tag / keine Reaktion	3 Tage / 1 Tag	1 Tag / 2 Stunden
5) Umfang der Löschung	- / vollständig	Vollständig / -	Vollständig	Vollständig

*... Anmerkung: Antworten der Betreiber erfolgten immer gleichzeitig mit der Löschung (sofern durchgeführt).

Verbesserungsmöglichkeiten:

- Reaktion auf Beschwerden
- Möglichkeit einer „Fake-User“-Beschwerde auch ohne Registrierung auf der Plattform
- Einfach auffindbare Hilfestellung zum Thema „Fake-User“ ohne erforderliche Registrierung auf Plattform

5. Testszenario „Standard-Einstellungen zum Schutz der Privatsphäre“

Problemdarstellung

Ein wichtiges Instrument zum Schutz persönlicher Daten in Sozialen Netzwerken sind die Einstellungen zur Privatsphäre. Viele NutzerInnen sind sich jedoch der Einstellungsmöglichkeiten und der jeweiligen Auswirkungen nicht bewusst. Vor diesem Hintergrund ist ein wichtiger Aspekt welche Standard-Einstellungen durch den Betreiber eines Sozialen Netzwerks standardmäßig festgelegt sind – für den Fall, dass sich die

NutzerInnen mit diesen Konfigurationsmöglichkeiten nicht beschäftigen und die Standardeinstellungen unverändert übernehmen.

Nachfolgend sind für alle getesteten Sozialen Netzwerke zu den drei beispielhaft ausgewählten Punkten:

1. Einstellung der Sichtbarkeit von Fotos
2. Einstellung der Sichtbarkeit von persönlichen Daten im Profil (Email, Geburtstag, Tel.Nr., ...)
3. Auffindbarkeit durch Suchmaschinen

...die Standardeinstellungen sowie, in Klammer, die verfügbaren Einstellungsoptionen dargestellt. Alle Angaben beziehen sich auf erwachsene NutzerInnen (Abweichungen bei minderjährigen NutzerInnen sind möglich).

Facebook

1) *Standard-Einstellung der Sichtbarkeit von Fotos:*

Das Profilfoto ist automatisch für „alle“ (alle Internet-NutzerInnen) sichtbar. Es werden keine anderen Optionen angeboten.

Bei Anlegen eines neuen Fotoalbums ist „alle“ (alle Internet-NutzerInnen) vorausgewählt (**Alle**, Freunde von Freunden, nur Freunde, Benutzerdefiniert).

2) *Standard-Einstellungen der Sichtbarkeit von persönlichen Daten im Profil (Email, Geburtstag, TelNr, ...):*

Angaben unter „Über mich“, „Persönliches (Interessen, Aktivitäten, Favoriten)“, „Familie und Beziehung (Familienmitglieder, Beziehungsstatus, ‚Interessiert an‘ und ‚Auf der Suche nach‘)“ sind für „alle“ (alle Internet-NutzerInnen) sichtbar (**Alle**, Freunde von Freunden, Freunde, Benutzerdefiniert).

Der Geburtstag ist für „Freunde von Freunden“ sichtbar (Alle, **Freunde von Freunden**, Freunde).

Kontaktdaten wie Handynummer und Email-Adresse sind für „Freunde“ sichtbar (Alle, Freunde von Freunden, **Freunde**, Benutzerdefiniert)

3) *Auffindbarkeit durch Suchmaschinen:*

Informationen, die für „alle“ (alle Internet-NutzerInnen) freigegeben sind, sind standardmäßig auch Suchmaschinen zugänglich. Dies kann von der/dem Nutzer/in deaktiviert werden.

meinVZ

1) *Standard-Einstellung der Sichtbarkeit von Fotos:*

Das Profilfoto ist für „Freunde“ sichtbar (Alle, Alle Leute in meiner Region und meine Freunde und deren Freunde, meine Freunde und deren Freunde, **nur meine Freunde**).

Fotoalben können entsprechend der Voreinstellung von „allen“ (allen Plattform-NutzerInnen) eingesehen werden (**Alle**, meine Freunde, nur mich selbst).

2) *Standard-Einstellung der Sichtbarkeit von persönlichen Daten im Profil (Email, Geburtstag, TelNr, ...):*

Name und Region sind für alle Plattform-NutzerInnen sichtbar (**Alle**, Alle Leute in meiner Region und meine Freunde und deren Freunde, meine Freunde und deren Freunde, nur meine Freunde).

Account-Informationen, Allgemeines, Persönliches, Karriere, Gruppen, Fotos, Pinnwand und Freunde sind für „Freunde“ sichtbar (Alle, Alle Leute in meiner Region und meine Freunde und deren Freunde, meine Freunde und deren Freunde, **nur meine Freunde**).

Geburtstag wird „nicht angezeigt“ (Geburtstag und –Jahr, nur Geburtstag (ohne Jahr), **Nicht anzeigen**).

Kontaktdaten sind nur für „Freunde“ sichtbar (keine Optionen).

3) *Auffindbarkeit durch Suchmaschinen:*

Keine Einstellungsmöglichkeit. Eine Information bei den Einstellungen zur Privatsphäre beinhaltet den Hinweis: „An Suchmaschinen werden keine Informationen ausgegeben“.

Netlog

1) *Standard-Einstellung der Sichtbarkeit meiner Fotos:*

Das Profilfoto ist für jede/n Internet-Nutzer/in sichtbar.

Bei Hochladen eines neuen Fotos ist standardmäßig „jedem“ (jedem Internet-NutzerIn) ausgewählt (**jedem**, nur deinen Freunden, nur für mich).

2) *Standard-Einstellung der Sichtbarkeit meiner persönlicher Daten im Profil (Email, Geburtstag, TelNr, ...):*

„Jeder“ (jede/r Internet-NutzerIn) hat Zugang zum gesamten Profil mit Ausnahme der Email-Adresse (**Jeder**, nur Netlog-Mitglieder, nur bestimmte Netlog-Mitglieder, Freunde)

3) *Auffindbarkeit durch Suchmaschinen:*

Die Profile sind Suchmaschinen standardmäßig zugänglich (Option ausgewählt). Dies kann von der/dem Nutzer/in deaktiviert werden.

Szene1

1) *Standard-Einstellung der Sichtbarkeit meiner Fotos:*

Es sind keine Einstellungsmöglichkeiten zum Profilfoto vorhanden.

Die Vorauswahl beim Anlegen eines neuen Fotoalbums ist „Community“ (**Community**, Userpage, Friends, versteckt, Passwort).

2) *Standard-Einstellung der Sichtbarkeit meiner persönlicher Daten im Profil (Email, Geburtstag, TelNr, ...):*

Keine Einstellungsmöglichkeiten. Jede/r Internet-NutzerIn hat Zugang zum Profil, es werden Daten wie z.B. Alter, Herkunft, Sternzeichen, Aussehen, Liebesstatus, Interessen,... angezeigt – Name, Adresse, Telefonnummer, Email-Adresse und Geburtsdatum beispielsweise.

3) Auffindbarkeit durch Suchmaschinen:

Freigegeben ist die Suche nach Vor- und Nachname nur für das „Szene1- und Weblife1-Netzwerk“ (nicht freigegeben, **Freigegeben nur für „Szene1- und Weblife1-Netzwerk“**, öffentlich freigegeben).

Die Suche nach Email-Adresse ist standardmäßig „nicht freigegeben“ (Freigegeben nur für „Szene1- und Weblife1-Netzwerk“, **nicht freigegeben**).

6. Zusammenfassende Darstellung der wichtigsten Verbesserungspotenziale

In der Folge genannte Verbesserungspotenziale beziehen sich nicht auf alle der exemplarisch getesteten Sozialen Netzwerke. Es handelt sich um eine summarische Darstellung.

1. Einstellungen zum Schutz der Privatsphäre

Es sollten umfangreiche Einstellungsmöglichkeiten zum Schutz der Privatsphäre für sämtliche Inhalte, die in einem Sozialen Netzwerk veröffentlicht werden, angeboten werden.

Viele NutzerInnen sind sich der Einstellungsmöglichkeiten zum Schutz der Privatsphäre nicht bewusst und ihnen ist unklar für welche NutzerInnen-Gruppen veröffentlichte Inhalte sichtbar sind. Vor diesem Hintergrund ist ein wichtiger Aspekt welche Standard-Einstellungen durch den Betreiber eines Sozialen Netzwerks festgelegt worden sind – für den Fall, dass sich die NutzerInnen mit diesen Konfigurationsmöglichkeiten nicht beschäftigen und die Standardeinstellungen unverändert übernehmen. Es sollten daher jeweils die sichersten Einstellungen automatisch vorausgewählt sein.

Beispiel:

In mehreren Sozialen Netzwerken sind hochgeladene Fotos für alle Plattform- oder sogar für alle Internet-NutzerInnen standardmäßig sichtbar und z.B. nicht nur für Freunde oder einen selbst. Auch die Angaben im eigenen Profil (z.B. Interessen, Beziehungsstatus, Wohnort...) sind teilweise für alle Internet-NutzerInnen entsprechend der Voreinstellungen einsehbar. In einem Fall trifft das auch auf die Standardeinstellungen für Geburtsdatum und ausgewählte Kontaktdaten zu.

Darüber hinaus können NutzerInnen nicht bei allen Plattformen selbst entscheiden, welchen Ausschnitt der Profilangaben sie wem sichtbar machen wollen. Die Einstellungen zum Schutz der Privatsphäre sind zu wenig spezifisch.

2. Hilfestellung zu den Themen Privatsphäre und Fake-User

Die nutzerInnenfreundliche Aufbereitung von Informationen und konkreten Tipps zum Schutz der Privatsphäre und möglichen Problemen wie Identitätsklau in Verbindung mit „Fake-Usern“ ist verbesserungswürdig.

Beispiel:

Es ist in der Regel für durchschnittliche Internet-NutzerInnen schwer nachzuvollziehen welche in den Sozialen Netzwerken veröffentlichten Angaben für wen genau sichtbar sind und für wen nicht. Auch die genauen Auswirkungen der jeweiligen Einstellungen zum Schutz der Privatsphäre sind oft mangelhaft erläutert. Zudem gibt es kaum prominent platzierte und leicht verständliche Informationen sowie Tipps für NutzerInnen wie sie ihre Privatsphäre den eigenen Interessen entsprechend schützen können.

Opfer von Identitätsdiebstahl in Form von „Fake-User“-Profilen werden außerdem nicht von allen Plattformen dabei unterstützt eine Meldung von „Fake-Profilen“ ohne sich selbst beim Sozialen Netzwerk registrieren zu müssen.

3. Unterstützung bei Löschung des eigenen Profils

Die Löschfunktion für das eigene Profil sollte einfach auffindbar sein und die NutzerInnen sollten in einfach nachvollziehbarer Weise informiert werden, wie vollständig die Löschung des eigenen Profils und von außerhalb des eigenen Profils veröffentlichten Daten unter Nutzung der unterschiedlichsten Plattformfunktionen tatsächlich ist.

Beispiel:

In zwei Sozialen Netzwerken ist die Löschfunktion nur über eine Suche in der Hilfe auffindbar. Plattform-Betreiber machen darüber hinaus in der Regel nicht aktiv darauf aufmerksam wie umfangreich die Löschung tatsächlich ist und dass oftmals Datenspuren weiterhin bestehen, die mit der eigenen Person in Verbindung gebracht werden können. Dazu sind beispielsweise außerhalb des eigenen Profils veröffentlichte Nachrichten zu zählen, deren Inhalte in Verbindung mit den BenutzerInnenamen noch erhalten bleiben. Auch die Inhalte der Nachrichten können unter Umständen auf den/die VerfasserIn konkrete Rückschlüsse geben.

4. Reaktion auf Beschwerden

Auch bei der vorliegenden exemplarischen Erhebung von Reaktionen auf Beschwerden bei Belästigungen und Cyber-Mobbing zeigt sich eine große Bandbreite der Reaktionszeiten.

Eine rasche Reaktionszeit ist für Opfer von Bloßstellungen und Belästigungen eine wichtige Unterstützung.

Beispiel:

Die Bandbreite der Reaktionszeiten reicht von wenigen Minuten bis hin zu gar keiner Reaktion seitens eines Plattformbetreibers. Teilweise wurden auch nicht alle beanstandeten Inhalte entfernt (z.B. nur bloßstellende Fotos aber nicht die herabwürdigenden Kommentare).

Nutzertipps

- Müssen es hundert „Freunde“ im Netz sein? Reagieren Sie nicht auf jede x-beliebige Kontakteinladung – denn je größer und unübersichtlicher das Netzwerk, umso mehr Gedanken sollten Sie sich über Ihre Privatsphäre machen.
- Ihre Privatsphäre ist schützenswert: Wählen Sie auf den Netzwerkseiten scharfe Sicherheitseinstellungen: Einträge sollen nur Ihre Freunde sehen. Ihr Profil wird auch über Suchmaschinen gefunden? – Bei vielen Netzwerkseiten lässt sich einen Suchmaschinenzugriff unterbinden. Nähere Anbieterinfos finden Sie dazu meist in der Rubrik „Datenschutz“
- Wenn Sie persönliche Daten öffentlich zugänglich machen, fragen Sie sich, wie Ihr elektronisches Profil bspw auf kritische Betrachter, etwa Arbeitgeber, wirkt.
- Überlegen Sie vor jedem Eintrag, wie offenherzig Sie sein wollen. Jeder Beitrag sollte so gestaltet sein, dass Sie oder die Empfänger kein Problem damit haben, wenn er auf Umwegen an die Öffentlichkeit gelangt. Nicht nur Texte auch Bilder können bloßstellen: wählen Sie Ihre Worte und Aufnahmen sorgfältig.
- Achten Sie auch auf die Rechte Anderer. Fragen Sie um Erlaubnis, bevor Sie bspw Bilder, die Dritte zeigen ins Netz stellen oder Materialien veröffentlichen, an denen Dritte Urheberrechte besitzen.
- Immer öfter gibt es auf Netzwerkseiten Anwendungen Dritter, bspw Spielapplikationen. Aufpassen: diese Anbieter können in der Regel auf viele Ihrer Daten zugreifen.
- Weitere Infos und Tipps auf <http://www.arbeiterkammer.at/konsument/datenschutz.htm> bzw www.saferinternet.at