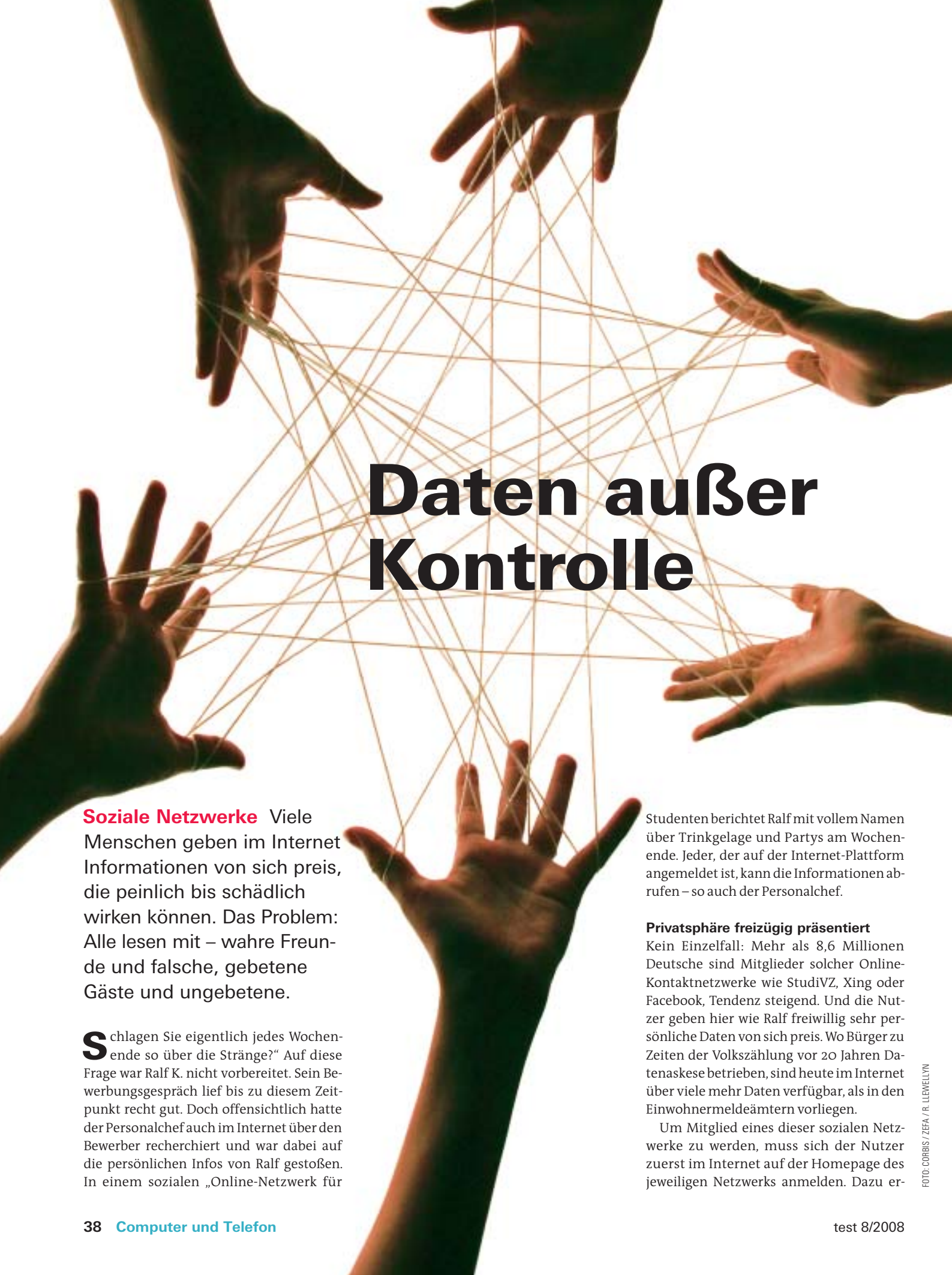


Daten außer Kontrolle

Soziale Netzwerke Viele Menschen geben im Internet Informationen von sich preis, die peinlich bis schädlich wirken können. Das Problem: Alle lesen mit – wahre Freunde und falsche, gebetene Gäste und ungebetene.

„Schlagen Sie eigentlich jedes Wochenende so über die Stränge?“ Auf diese Frage war Ralf K. nicht vorbereitet. Sein Bewerbungsgespräch lief bis zu diesem Zeitpunkt recht gut. Doch offensichtlich hatte der Personalchef auch im Internet über den Bewerber recherchiert und war dabei auf die persönlichen Infos von Ralf gestoßen. In einem sozialen „Online-Netzwerk für Studenten berichtet Ralf mit vollem Namen über Trinkgelage und Partys am Wochenende. Jeder, der auf der Internet-Plattform angemeldet ist, kann die Informationen abrufen – so auch der Personalchef.

Privatsphäre freizügig präsentiert

Kein Einzelfall: Mehr als 8,6 Millionen Deutsche sind Mitglieder solcher Online-Kontaktnetzwerke wie StudiVZ, Xing oder Facebook, Tendenz steigend. Und die Nutzer geben hier wie Ralf freiwillig sehr persönliche Daten von sich preis. Wo Bürger zu Zeiten der Volkszählung vor 20 Jahren Datenaskese betrieben, sind heute im Internet über viele mehr Daten verfügbar, als in den Einwohnermeldeämtern vorliegen.

Um Mitglied eines dieser sozialen Netzwerke zu werden, muss sich der Nutzer zuerst im Internet auf der Homepage des jeweiligen Netzwerks anmelden. Dazu er-

FOTO: CORBIS / ZEFA / R. LLEWELLYN

stellt er ein Profil, also einen Steckbrief, von sich selbst. Notwendige Angaben sind meist Name, E-Mail-Adresse, ein ausgedachter Nutzername, der auf der Homepage erscheint, sowie ein Passwort. Eventuell müssen noch mehr Daten preisgegeben werden, das variiert von Plattform zu Plattform jedoch stark.

Auf seiner Seite stellt sich der Nutzer vor: Wie er heißt, was er macht, wo er wohnt. Meist kann er dort auch Fotos, Musik und Videos hochladen, die dann für andere Nutzer zugänglich sind. Außerdem hat er die Möglichkeit, andere Mitglieder in seine „Freundesliste" einzutragen und Nachrichten auf Profilseiten der anderen Nutzer zu hinterlassen. Sie schicken sich untereinander persönliche Nachrichten oder verlinken die ins Internet gestellten Fotos.

Alle lesen mit

Diese Art der Kommunikation führt dazu, dass die Nutzer große Datenmengen von sich preisgeben. Sie schreiben, was sie lieben, was sie hassen, schwatzen über ihre Hobbys, klagen öffentlich ihr Leid und geben ihre politische Einstellung preis.

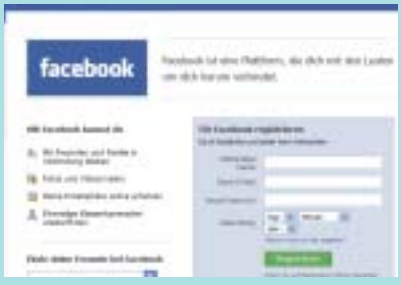
Was früher am Telefon, über Briefe oder per E-Mail stattfand, geschieht heute zum großen Teil für jeden angemeldeten Nutzer sichtbar auf den sozialen Plattformen im Netz. Hier werden Verabredungen für Kino, Grillabend oder Brunch getroffen. Welcher Club gerade angesagt ist, wird mit wenigen Zeilen auf die Profilseite des besten Freundes geschrieben. Bekannte berichten von ihren Wochenendaktivitäten, einige laden Fotos von Clubbesuchen oder der Geburtstagsfeier hoch. Geschäftspartner versenden Messe- und Kongresseinladungen über die Netzwerke und Schüler verraten in ihren Steckbriefen, welche Fächer oder Lehrer sie nicht mögen.

Dazugehören ist alles

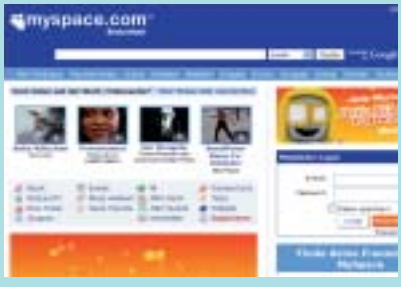
Die Motivationen, sich in den sozialen Netzwerken anzumelden, sind sehr unterschiedlich: Neue Freunde finden, mit alten Bekannten wieder in Kontakt treten oder neue Geschäftsbeziehungen knüpfen. Gerade junge Erwachsene verbringen einen Großteil ihrer Zeit in den virtuellen Gemeinschaften. Sind Freunde oder Kollegen in den Netzwerken aktiv, wollen sie auch dabei sein – zum Mitmachen wie auch Mitreden. Dazugehören ist alles. Täglich meldet sich eine Vielzahl neuer Nutzer auf den Plattformen an. Rund 6,5 Milliarden Seitenabrufe gab es allein im März auf der Platt- ►

Wichtige soziale Netzwerke im Überblick

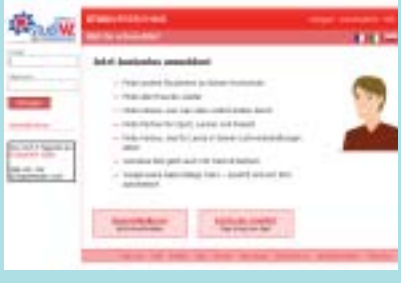
Xing
Das Business-Netzwerk ermöglicht es, berufliche und geschäftliche Kontakte zu knüpfen. Es hat mehr als 5,71 Millionen Mitglieder weltweit. Nutzer suchen Kontakte, Informationen, Mitarbeiter, Jobs oder Kunden. Funktionen wie die erweiterte Suchfunktion stehen nur Premiummitgliedern zur Verfügung. Die Premiummitgliedschaft kostet 5,95 Euro pro Monat. **www.xing.com**



Facebook
Gegründet im Februar 2004, weltweit 80 Millionen aktive Nutzer. Die Benutzer sind in „kleine" Netzwerke eingeteilt. Es gibt Universitäts-, Schul-, Arbeitsplatz- und regionale Bezirksgruppen. Facebook verfügt über einen Marktplatz, auf dem Anzeigen aufgegeben werden können. Durch eine Beobachtungsliste wird man über Neuigkeiten von Freunden informiert. **www.facebook.com**



MySpace
Die Plattform wurde 2003 in den USA gegründet. Über 200 Millionen Jugendliche und Erwachsene sind hier zu finden. Darunter viele, denen die Plattform zum Selbstmarketing dient: Models, Musiker oder Politiker. MySpace erlaubt es, die eigene Seite kreativ zu gestalten: Farben und Formen können geändert, Fotos, Musik und Videos eingebaut werden. **www.myspace.com**



StudiVZ (Studenten Verzeichnis)
Richtet sich hauptsächlich an Studierende und Absolventen. Mit seinen zirka 5,6 Millionen Mitgliedern erlebte es in den letzten zwei Jahren einen regelrechten Boom. Nutzer plaudern über Vorlesungen, Professoren oder private Interessen. Laut der StudiVZ-Homepage ist die Plattform für viele zum festen Bestandteil des täglichen Campus-Lebens geworden. **www.studivz.net**

SchülerVZ (Schüler Verzeichnis)
Der kleine Bruder des StudiVZ hat mehr als 3,6 Millionen Mitglieder. Das seit Februar 2007 bestehende Netzwerk richtet sich an Schüler ab zwölf Jahre. Wer sich registrieren möchte, braucht die Einladung eines aktiven SchülerVZ-Nutzers. Schüler kommunizieren mit Freunden, indem sie Diskussionsgruppen gründen oder Pinnwandeinträge verfassen. **www.schuelervz.net**

form „SchülerVZ“ (Schüler Verzeichnis). Im Vergleich dazu hatten Seiten wie „Spiegel Online“ oder „Yahoo!“ in diesem Zeitraum „nur“ etwa 160 bis 230 Millionen Abrufe.

In einigen Netzwerken können die Mitglieder selbst Diskussionsgruppen gründen oder diesen beitreten. In Businessnetzwerken wie Xing haben sie harmlose Namen wie „Hamburg@work“ oder „JungeWirtschaft“ und dienen meist der beruflichen Vernetzung. Bei Facebook, StudiVZ oder SchülerVZ sieht das schon etwas anders aus. Die öffentlichen Gruppen heißen beispielsweise „Wer tanzt, hat nur kein Geld zum Saufen“ oder „Ich bleibe lange wach und tue nichts Produktives“. Was für einige spaßig sein mag, ist für Personalchefs alles andere als witzig.

Beispiele von Schadensfällen

Daten gestohlen

Mai 2008: „Facebook“ wies eine Sicherheitslücke auf, Angreifer hätten so Daten stehlen können. Mittlerweile soll die Lücke behoben sein.

Januar 2008: Durch eine Sicherheitslücke bei „MySpace“ wurde etwa eine halbe Million privater, nichtöffentlicher Fotos heruntergeladen. Mehr als 44 000 Nutzerkonten der Plattform waren davon betroffen. Später standen die Bilder als Dateien zum Download im Internet bereit.

Dezember 2007: Ein Java-Script-Wurm infizierte innerhalb von 24 Stunden fast 700 000 Profile von „Orkut“ – ein vor allem in Südamerika verbreitetes Netzwerk. Der Wurm richtete keinen weiteren Schaden an, zeigte jedoch, dass es Schwachstellen in der Technik von Orkut gibt, die sich auch für Schlimmeres ausnutzen lassen würden.

Februar 2007: Das Studentennetzwerk „StudiVZ“ wurde Opfer eines Hackerangriffs. E-Mail-Adressen, Zugangsdaten und Freundschaftsverbindungen wurden ausgelesen. Die StudiVZ-Betreiber setzten alle Kennwörter der Nutzer komplett zurück.

Tipps

Spitzname: Handelt es sich nicht um ein geschäftliches Netzwerk, ist es ratsam, sich unter einem fiktiven Namen anzumelden. So lassen sich von Dritten schwerer Rückschlüsse auf die eigene Person ziehen.

Konfigurieren: Stellen Sie ihr Netzwerkprofil so ein, dass nur Freunde darauf zugreifen können. Klicken Sie dazu in den Profileinstellungen „Privatsphäre“ oder „Privacy“ an. Für alle anderen Nutzer sind Ihre Daten dann nicht ohne weiteres sichtbar.

Daten: Veröffentlichen Sie auch im „privaten Bereich“ (Privacy) nicht wahllos alles Mögliche von sich. Geben Sie keine Informationen wie politische Neigungen, Adressen, Telefonnummern, Kontodaten, das Geburtsdatum oder den Mädchennamen der Mutter (benutzen viele als Kennwort) an. Sämtliche Informationen können durch andere Nutzer, Plattformanbieter oder Hacker unter Umständen missbraucht werden.

Bilder: Überlegen Sie gut, welche Fotos und Videos Sie online stellen. Personalchefs suchen im Internet nach Informationen. Veröffentlichen Sie nichts, was Ihre Chancen auf einen Job gefährden könnte.

Blauäugige Nutzer

Für Datenschützer sind diese Netzwerke ein Horrorszenario, und gerade durch Pannen beim Datenschutz haben sie einen schlechten Ruf bekommen *(siehe „Daten gestohlen“, links unten)*. Nutzer geben hier ohne Umschweife Daten wie ihren echten Namen oder ihr echtes Geburtsdatum an, Ralf K. ist da kein Einzelfall.

Für Datendiebe ist es daher ein Kinderspiel, diese Informationen mit Daten aus anderen im Internet frei verfügbaren Quellen zu kombinieren. Sie erhalten auf diese Weise umfangreiche Datensätze, mit denen sie zum Beispiel weitere, nichtöffentliche Daten über Personen herausfinden können. Deshalb rücken soziale Netze immer mehr ins Visier von „Cyberkriminellen“.

So können sich die Täter persönliche Profile real existierender Personen zusammensuchen. Die Daten lassen sich weiterverkaufen, etwa die von Bewerbern an Rekrutierungsfirmen. Auf den Internetplattformen tummeln sich auch Personen, die nur zu gern erfahren würden, wann jemand in den Urlaub fährt. Die Adresse und der Wohnort der betreffenden Familie sind schnell herausgefunden. Und nach der erholsamen Reise ist im schlimmsten Fall die Wohnung leergeräumt. Doch nicht nur Kriminelle, auch legale Firmen, wie beispielsweise Auskunfteien, nutzen die Daten zur Bewertung der Kreditwürdigkeit.

Ebenfalls nicht zu vergessen ist, dass die meisten Plattformen kostenlos und die Netzwerkbetreiber somit auf Einnahmen aus der Werbung angewiesen sind. In Zukunft wird es deshalb immer mehr personalisierte Werbebanner auf den Profilseiten geben. Das Interesse der Werbeindustrie an den Plattformen wächst und darf nicht unterschätzt werden. Es könnte zu einer Zweckentfremdung der Daten kommen: Profile über Einkaufsgewohnheiten oder Vorlieben können damit erstellt werden. Dann erhalten Geburtstagskinder von unbekannten Firmen Werbemails oder man wundert sich, weshalb spezielle Reiseprospekte im Briefkasten landen.

Gelöscht, aber nicht verschwunden

Einmal ins Netz gestellte Informationen sind nur schwer wieder zurückzuholen. So weiß der Nutzer nie, ob die Daten nicht in der Zwischenzeit kopiert wurden: Hacker

können private Daten klauen, Netzwerkanbieter kopieren das Profil auf ihre Server oder der ungeliebte Klassenkamerad hat die Partyfotos schon längst auf seinem Rechner archiviert. Die Daten können also weiterexistieren, selbst wenn das eigene Profil längst komplett gelöscht wurde.

Mit Informationen geizen

Was also kann der Nutzer tun, um sich zu schützen? Gerade für Jugendliche sind die Onlineprofile ein wichtiges Mittel des Selbstausdrucks und der Identitätsdarstellung. Es wäre falsch, ihnen die Anmeldung in den Netzwerken zu verbieten, denn sie wollen dabei sein und mitreden.

Verbraucherschützer und Experten fordern, die Medienkompetenz der Nutzer zu fördern *(siehe Interview rechts)*. Wichtig ist, gerade Kinder und Jugendliche zuhause und in der Schule für das Thema Datenschutz zu sensibilisieren. Auch die Polizei hat eine Broschüre zum Thema herausgegeben, sie heißt „Im Netz der Neuen Medien“ (www.polizei-beratung.de).

Jeder sollte sich darüber im Klaren sein, dass sich seine Spuren im Netz nur schwer verwischen lassen. In den Profileinstellungen ist deshalb immer der Schutz der Privatsphäre zu aktivieren. Hier legt der Nutzer selbst fest, wer seine Seite sehen darf und welche Informationen angezeigt werden. Mitglieder sollten sich überlegen, wen sie in ihre Freundesliste aufnehmen. Persönliche Dinge sollten die Nutzer lieber per Mail austauschen als auf den Pinnwänden oder mit den Kommentarfunktionen der Netzwerke, die jeder lesen kann. Fotos und Videos sollten nur Freunden und nicht der Allgemeinheit zur Verfügung stehen. Auch sollten Nutzer keine fremden Fotos ins Netz stellen, wenn sie selbst nicht die Rechte an ihnen besitzen. Sonst flattert vielleicht eine Abmahnung ins Haus.

Kein Hort für Privates

Gerade Personalabteilungen verschaffen sich heute schon bei jedem vierten Bewerber über Onlinerecherche Informationen. Einmal ins Web gestellte private oder gar peinliche Inhalte können auch von Menschen eingesehen werden, die sie besser nicht sehen sollten. Das Internet ist eben kein sicherer Hort für Privates. Das hat Ralf K. nun auch verstanden: Er hat seinen Nutzernamen bei StudiVZ geändert, sein Profil können nur noch seine Freunde bestaunen, alle Partyfotos sind hoffentlich nachhaltig gelöscht. Jetzt muss er nur zum nächsten Bewerbungsgespräch eingeladen werden. ■

Interview

„Das eigene Abbild kontrollieren“

Prof. Hendrik Speck, Dozent für Interaktive Medien an der Fachhochschule Kaiserslautern.

Nutzer geben viele Daten von sich in Netzwerken preis. Besteht keine Angst vor Datenmissbrauch?

Ein Großteil der Anwender ist sich des Risikos nicht bewusst oder schätzt es falsch ein. Viele wissen gar nicht, was mit ihren veröffentlichten Daten geschehen kann. Die Netzwerke sind Herr unglaublich großer Nutzer-Datenmengen und oft ist es nicht nur für Hacker ein Leichtes, an sie heranzukommen.

Welche Daten sollten Nutzer niemals dort preisgeben?

Weder das eigene Geburtsdatum noch der Mädchenname der Mutter sollten veröffentlicht werden. Denn dies sind beliebte Passwörter, die auf diesem Wege schnell in die Hände von Datendieben fallen können. Auch vertrauliche Informationen wie Telefonnummern oder Kontonummern haben in sozialen Netzwerken nichts zu suchen.

Worauf ist noch zu achten?

Potenzielle Arbeitgeber suchen auf Websites nach Informationen. Nutzer sollten also nichts veröffentlichen, was ihre Chancen auf die neue Stelle gefährden könnte. Auf Plattformen, die der beruflichen Vernetzung dienen, ist es nicht sinnvoll, eine falsche E-Mail-Adresse, einen aufgemotzten Lebenslauf oder einen verniedlichten Profilnamen wie etwa „Schmusi“ anzugeben. Bei Netzwerken wie MySpace oder StudiVZ ist das wiederum durchaus vertretbar. Denn mit ihren Freunden können sie deshalb trotzdem noch in Kontakt stehen, meist kennt man die Profilnamen des Freundeskreises.

Welche Grundeinstellungen sollte der Anwender vornehmen?

In den Profileinstellungen sollte der Schutz der „Privatsphäre“ beziehungsweise „Privacy“ aktiviert werden. Hier legt der Nutzer selbst fest, wer seine Seite sehen darf und welche Informationen angezeigt werden. Das geschieht vonseiten der Plattformbetreiber nicht automatisch, der Nutzer muss selbst aktiv werden.

Wo lauern Gefahren für den Nutzer?

Dritte können veröffentlichte Daten, Bilder oder Videos ohne das Wissen des Nutzers verwenden und/oder verfälschen. So kann er mit etwas in Verbindung gebracht werden, was nicht der Wahrheit entspricht, beispielsweise einer radikalen Vereinigung. Auch harmlose Lästereien, schwere Beleidigungen oder gar „Hetze“ gegen Privatpersonen oder Lehrer – wie beispielsweise im SchülerVZ schon der Fall – können vorkommen. Inhalte über den Nutzer werden veröffentlicht, obwohl der nichts davon weiß und auch nicht seine Zustimmung dazu gegeben hat. Er hat keine Kontrolle mehr über seine veröffentlichen Daten. Im schlimmsten Fall kann dies dem Nutzer privat oder sogar beruflich schaden.

Was tun, wenn es schon zu Datenmissbrauch gekommen ist?

Betroffene sollten sich unverzüglich an die in jedem Bundesland vertretenen Datenschutzbeauftragten (Landesbeauftragte für den Datenschutz) oder an die Verbraucherzentralen wenden. Handelt es sich um einen besonders schweren Fall, sollte ein Anwalt zurate gezogen werden.

Was kann jeder im Vorfeld tun?

Jeder Nutzer sollte ein aktives Identitätsmanagement betreiben, also regelmäßig das eigene Abbild im Netz kontrollieren. Dazu sollte der eigene Name in eine Suchmaschine eingegeben und die Ergebnisse überprüft werden: Mit welchen Themen wird er in Verbindung gebracht und auf welche Fotos ist er verlinkt. Wichtig für jeden einzelnen Nutzer, vor allem jedoch bei Kindern, ist die Entwicklung einer entsprechenden Medienkompetenz: ein Bewusstsein dafür zu erlangen, welche Daten preisgegeben werden können und welche auf keinen Fall in die Netzwerke gehören.