Datenschutz – what else?

Christian Wirsig,
Communications Manager, Kaspersky Lab

Über 350 Millionen Nutzer haben ein Facebook-Konto, laden pro Monat rund 1 Milliarde Bilder und 10 Millionen Videos hoch und wissen meist nicht, was mit ihren Daten passiert. Doch Datenschutz-probleme tauchen nicht nur im "Mitmach-Web" auf, denn im Internet lassen sich verschiedenste Quellen einfach verknüpfen – das betrifft jeden Online-Nutzer.

George Clooney ist etwas Besonderes. Nein, diesmal ist nicht gemeint "besonders gutaussehend", sondern er ist besonders vorsichtig im Umgang mit Daten im Internet. Denn Clooney gehört zu den wenigen Stars, die mit sozialen Netzwerken auf Kriegsfuß stehen. So hat er sich kürzlich als Facebook-Hasser geoutet [1], während seine Kollegen Tod & Teufel in sozialen Netzen und Microblogging-Diensten wie Twitter veröffentlichen. Doch Datenschutz und Privatsphäre im Internet sind auch für Otto-Normal-Nutzer derzeit heiß diskutierte Themen. Der Grund: Vor allem soziale Netzwerke wie Facebook und StudiVZ boomen [2], was mit den eingestellten Daten passiert, ist aber allzu oft unklar. Kürzlich hat Facebook-Chef Mark Zuckerberg in einem Interview [3] die Privatsphäre im Internet als alte Konvention bezeichnet. Hintergrund: Facebook hatte kurz vorher die Datenschutzeinstellungen für seine Nutzer so verändert, dass private Informationen über die Facebook-Suche einfacher gefunden werden können. Diese laxere Haltung gegenüber privaten Daten sei nur eine Reaktion auf Veränderungen in der Gesellschaft, erklärte der Facebook-Chef. Fazit: Sie können sich als Internet-Nutzer nicht darauf verlassen, dass die Anbieter von Web-Diensten schon dafür sorgen werden, dass Ihre Daten geschützt bleiben. Sie müssen selbst aktiv werden.

Christian Wirsig
ist seit Januar 2006 bei der Kaspersky Labs GmbH tätig. Zunächst war er als Marketing-Redakteur für Broschüren und Artikel verantwortlich, seit Anfang 2008 betreut er als Communications Manager Central Europe die interne und externe Kommunikation des Unternehmens in Deutschland, Österreich und der Schweiz.

Die Welt entblößt sich

Neben Communities sind auch Homepages oder ein eigener Blog ein gefundenes Fressen für alle Neugierigen. Gefühle, Stimmungen, Ansichten, alles das kriegt man in den Online-Tagebüchern brühwarm und ungefiltert serviert. Dabei sollte dem Verfasser klar sein, dass auch Personalverantwortliche oder Arbeitskollegen auf den Blog stoßen können. Selbst Blogs, die bei einer Google-Recherche nicht gleich zu finden sind, können einfach aufgestöbert werden. Wer etwa eine Mail-Adresse mit eigener Domain nutzt, der kann sich sicher sein, dass www.die_angegebene_domain.de von Empfängern ausprobiert wird. Meist ist dann der Blog nicht weit entfernt.

Heiße Diskussionen

Aber die Diskussion um Datenschutz ist schon so alt wie das Web selbst. Schon lange vor den sozialen Netzwerken und Web 2.0 haben sich Communities mit klassischer Forenfunktion einen Namen gemacht, in denen Nutzer meist Hobbys diskutieren. Den gleichen Ansatz gibt es seit Jahrzehnten in Usenet. Im Hinterkopf sollte man auch dabei haben: Wer in Foren ohne Pseudonym und vielleicht noch mit Foto

allzu wild vom Leder zieht, der kann sich selbst schaden. Denn die Beiträge sind für die Web-Ewigkeit gespeichert. Selbst wenn man als Nutzer einen Beitrag per Foren-Software entfernen kann, taucht er meist immer noch im Cache von Suchmaschinen auf. Auch auf den Beruf können sich solche Netzaktivitäten auswirken, denn der Einsatz von Internet-Tools hat bei Personalern zugenommen. Gut ein Drittel nutzt schon seit Jahren regelmäßig Google & Co. im Rahmen eines Such- und Auswahlprozesses [4]. Um allgemeine Informationen über die Kandidaten zu gewinnen, setzen knapp 30 Prozent das weltweite Netz grundsätzlich immer ein, Tendenz steigend.

Internet gefühlsecht

Auch Partnersuche, Reiseplanung und Einkäufe verlagern sich ins Web. Daran ist zwar nichts Verwerfliches, aber die Angaben bei Flirt-Börsen sind so ziemlich das Persönlichste, was man im Web finden kann. Selbst wenn der Anbieter selbst seriös ist und Ihre Daten schützt, kann ein geklautes Passwort dazu führen, dass diese Daten in falsche Hände geraten. Ebenso verhält es sich bei Online-Reisebüros oder allgemein Online-Shops, in denen etwa schon Kreditkartendaten, Suchprofile oder Interessen hinterlegt sind. Das ist einerseits bequem, weil man mit einem Mausklick bezahlen kann, andererseits kann jeder, der den Zugang knackt auch auf Ihre Kosten einkaufen.

Finden Sie sich selbst

Doch wie kann man den Fluss der Informationen über sich selbst eingrenzen? Als erstes sollten Sie prüfen, wie es um Ihren Online-Ruf bestellt ist. Eine einfache Google-Suche nach sich selbst verrät viel. Welche Profile in sozialen Netzwerken tauchen auf? Wo ist der Link zur privaten Homepage? Vielleicht erscheinen auch Links auf Webseiten Ihres Arbeitgebers. Schnell kriegen Sie einen Eindruck, was man auf die Schnelle über Sie in Erfahrung bringen kann. Wichtig: Sehen Sie sich auch mögliche Verknüpfungspunkte an: So kann man die private Adresse aus dem Homepage-Impressum einfach bei Google Maps eingeben und sich kinderleicht einen Eindruck über Ihre Wohngegend verschaffen. Übrigens können Nutzer von Google-Diensten neuerdings schnell rausfinden, was Google über Sie weiß: Das Dashboard (https://www.google.com/dashboard) zeigt es im Überblick an. Neben Google kann auch ein Besuch bei www.yasni.de nicht schaden. Die Personensuchmaschine wird etwa gerne von Personalberatern genutzt. Sie listet Telefonbucheinträge, Amazon-Wunschzettel, Xing-Profile und weitere Quellen auf.

Daten nachträglich löschen

Unerwünschte Daten im Internet haben sogar schon für das Entstehen einer neuen Dienstleistung gesorgt, dem Online-Reputation-Management. Dabei ist man sich einig, dass es besser ist, erst gar keine unerwünschten Daten zu veröffentlichen. Ist das Kind aber in den Brunnen gefallen, gibt es mehrere Möglichkeiten. Bei Telefonbucheinträgen oder Nutzerprofilen auf sozialen Netzwerken können Sie selbst aktiv werden: Hier reicht meist eine Mail oder ein Fax an den Anbieter oder man kann die Veröffentlichungseinstellungen selbst bearbeiten. Nicht mehr genutzte Accounts bei Web-Diensten kann man meist beim Betreiber löschen lassen. Schwieriger wird es bei Suchmaschinen. Zwar müssen Google & Co. Löschanträge prüfen, nur weil man selbst einen Eintrag als unpassend empfindet, ist aber noch kein Grund dafür, dass dieser Eintrag verschwindet.

Richtiges Verhalten

Wichtiger ist es, in Zukunft das richtige Maß für persönliche Daten im Internet zu finden. Richtig ist der Mittelweg zwischen Hardcore-Gezwitscher und Berghütte ohne Internet-Verbindung: Wer mit Freunden über Facebook Kontakt halten will, der kann das auch guten Gewissens tun. Man sollte sich aber die Zeit nehmen und die Einstellungen zur Privatsphäre prüfen. Dort ist aufgelistet, wer welche Informationen sehen kann. Im Zweifelsfall sollten Sie bei der Angabe und Herausgabe von Infos erst einmal konservativ sein, Schweigen ist hier wirklich

Gold. Wichtig: Achten Sie auch darauf, dass Ihre Freunde genauso umsichtig mit Daten umgehen, denn schnell ist man bei Facebook auf Fotos markiert und taucht in Videos auf.

Bei den meisten Web-Shops ist zwar das Zahlen via Kreditkarte üblich, die Daten sollten Sie aber nicht beim Anbieter hinterlegen. Geben Sie sie nur über eine sichere Internet-Verbindung ein. Sicherer ist natürlich die Bezahlung per Nachnahme oder Rechnung. Auf den ersten Blick praktische Funktionen wie ein öffentlicher Wunschzettel bei Amazon sollten Sie auch immer kritisch sehen, denn so kriegt jeder mit, welchen Hobbys Sie nachgehen. Im Zweifel verzichten Sie einfach auf den Wunschzettel im Web und schreiben eine Mail mit Wünschen.

Passende Schutz-Software

Eine aktuelle Schutz-Software ist für alle Internet-Nutzer Pflicht, vor alle aber für die, die auch viel im Mitmach-Web unterwegs sind. Denn schnell nistet sich sonst ein Schädling ein, der Zugangsdaten zu sozialen Netzwerken und anderen Diensten abgreift. Neben einem Schutzpaket wie Kaspersky Internet Security gehört aber auch eine leistungsfähige Passwort-Verwaltung mit zum Pflichtprogramm. Denn wer kann sich sonst schon zufällig erzeugte Passwörter mit Sonderzeichen, Ziffern sowie Groß- und Kleinschreibung merken? Komfortabel funktioniert hier etwa der Kaspersky Password Manager.

[1] www.people.com/people/article/0,,20304800,00.html

[2] www.facebook.com/press.php#/press/releases.php?p=133917

[3] www.ustream.tv/recorded/3848950

[4] www.bdu.de/presse_321.html