Marcus Lindemann, Jan Schneider

Datenschutz-Fallrückzieher

Ein Netizen entdeckt den Wunsch nach Privatsphäre

Für diesen Artikel haben wir beispielhaft das Profil einer realen Person erstellt, indem wir frei verfügbare Informationen im Internet suchten und verknüpften. Als Protagonisten wählten wir einen Mitarbeiter eines Internet-Unternehmens. Der hatte damit zunächst kein Problem – bis er den fertigen Artikel sah. Dann bekam er kalte Füße.

Millionen Nutzer legen in sozialen Netzwerken ihr Privatleben offen. Foto-Websites platzen vor Urlaubsbildern, auf denen ganze Familien zu sehen sind. Arglos twittert der moderne Mensch, wo er sich gerade aufhält. Jemanden, der so naiv mit den neuen Medien umgeht, durch gezielte Recherche bloßzustellen, wäre billig.

Wir wollten an einem Beispiel zeigen, wie sich die Spuren, die man über Jahre im Netz hinterlässt, zu einem Profil verdichten lassen. Dafür suchten wir jemanden, der einerseits genau weiß, dass sich Informationen im Internet aufspüren und verknüpfen lassen, andererseits aber auch nicht gerade aktive Datenvermeidung praktiziert.

Mario R. (Name von der Redaktion geändert) schien perfekt zu passen. Er bekleidet bei einem Internet-Unternehmen einen verantwortungsvollen Posten. Außerdem kokettierte er on- wie offline gerne damit, auch Privates in seine Online-Präsenz einfließen zu lassen. Ganz Mensch 2.0 soll so das Profil im Netz authentischer wirken.

Und wir wurden fündig: Profanes wie den Arbeitgeber und die berufliche Karriere, Banales wie Hobbys und Urlaubsreisen, aber auch Privates über Familienmitglieder, Freunde und vieles mehr. R. war zunächst nicht überrascht, als er von unserer Recherche erfuhr und sah keine Probleme in der Veröffentlichung. Als er allerdings den fertigen Artikel sah, widersprach er der Veröffentlichung. Wir haben daher die konkreten Details entfernt, die Rückschlüsse auf die Person erlauben. Dennoch erfahren Sie, was wir wie herausgefunden haben.

Spitzname

Die Suchmaschine Google verrät über Mario R. vor allem berufliche Details. Sein Werdegang von der Schule bis zur heutigen Anstellung lässt sich schnell mit ein paar Klicks nachvollziehen. Man findet zahlreiche private Fotos von ihm. Auch sein Alter und Geburtsdatum sind im Netz kein Geheimnis. Fotos vom Geburtstag, vom eigenen Kind, das gratuliert, und auch Namen von Freunden, die mit dabei waren – alles steht im Netz.

In einem sozialen Netzwerk hat R. sehr viele Kontakte, in einem anderen dagegen deutlich weniger. Offenbar vernetzt er sich beruflich fleißig und privat nur mit guten Bekannten. Das ist etwas merkwürdig, denn Mario R. scheint ansonsten kaum etwas zu privat zu sein, um es öffentlich zu machen. Besonders auf Twitter vermengt er Beruf und Privatleben, und bei mindestens noch einem Dutzend Plattformen hat er eigene Accounts, unter seinem vollen Namen oder seinem Nickname, den wir ihm schnell zuordnen können.

Viele Internetnutzer sind parallel unter ihrem richtigen Namen und einem Nickname unterwegs. Der richtige Name ist heute notwendig geworden, wenn man im Web 2.0 auch beruflich Kontakte pflegen und gefunden werden will. Der Nickname dagegen entspricht noch ganz den Benimmregeln des Web 1.0, als private E-Mail-Adressen keine Klarnamen enthielten – eine Mail-Adresse zum Chatten, um bei eBay Gebrauchtes zu verkaufen oder um bei Amazon Bücher zu bewerten. Und wenn der Nickname häufig ist, hängt man halt Zahlen dran – Geburtsjahr, Geburtsdatum, Teile einer Postleitzahl. So hält das auch R.

Dieses doppelte Spiel ist riskant, denn kaum jemandem gelingt es auf Dauer, diese beiden Welten konsequent zu trennen. Irgendwann kommt man durcheinander und verrät den richtigen Namen bei einem Account, der unter dem Nickname läuft. Oder Dritte stellen die Verbindung zwischen realem Namen und Nickname her, indem sie Profilfotos auf mehreren Plattformen vergleichen. Danach können sie alle anderen privat gehaltenen Dinge mit dem richtigen Namen verknüpfen.

Ortsbesichtigung

Mario R. hat kein Problem damit, dass sein Nickname öffentlich ist. Er scheint nicht besorgt, dass die Informationen, die er veröffentlicht, für ihn zum Problem werden könnten. Sicher, seine Begeisterung für den Lieblingsverein etwa ist harmlos. Aber man erfährt, wann er im Stadion ist oder ob er zu Hause zuschaut.

Was, wenn jemand die Informationen gezielt nutzt, Schlüsse zieht, Informationshappen miteinander verbindet? Abwegig ist das nicht – auf der Internetseite http://pleaserobme.com haben sich die Macher schon mal einen Spaß daraus gemacht, alle Tweets, die auf Urlaub oder Abwesenheit von zu Hause hindeuten, unter der Überschrift „Please rob me" zu sammeln: eine Warnung, nicht alles mit allen zu teilen.

Aus R.s Tweets lässt sich ziemlich genau sehen, wann er in Urlaub fährt, wohin er reist und meistens auch wie lange und mit wem. Während des Urlaubs twittert er wenig, seiner Frau zuliebe, ab und zu gibt es aber auch Fotos. Für Einbrecher ist aber nicht jeder Urlaub eine Gelegenheit – R. lässt ab und zu auch seine Frau zurück, etwa wenn er mit seinem Kind oder mit Freunden verreist.

Außerdem müssten Einbrecher wissen, wo Mario R. wohnt. Beim Einwohnermeldeamt kann jeder die Adresse erfragen, für diesen Artikel haben wir uns aber auf Online-Quellen beschränkt. Im Telefonbuch ist R.s Adresse nicht eingetragen, aber in einem ortsbezogenen sozialen Netzwerk nennt er einen Ort, der für jedermann sichtbar ist und Rückschlüsse auf seine Adresse zulässt. Die Adresse passt zu den GPS-Koordinaten, die R. seinen Tweets manchmal beifügt. Über die Adresse lässt sich übrigens auch ein guter Freund von R. ausfindig machen, der ihn öfter besucht.

Außerdem passt die recherchierte Adresse gleich zu mehreren anderen Informationen aus seinen Tweets: Die Kirche, die die Familie besucht, oder die Foto-Location nach der Hochzeit. Ansehen konnten wir uns das Haus aus der Vogelflugperspektive bei Bing, in Google Street View ist es verpixelt. Die Haustür passt zu der, die wir auf einem seiner Videos sehen.

Das Stockwerk, auf dem R. wohnt, lässt sich anhand von Fotos und Tweets leicht erraten. Wir finden schnell auch einiges über die Fahrzeuge heraus, die R. besitzt. Das Kennzeichen der Familienkutsche finden wir ebenfalls auf einem Foto.

In der Wohnung lebt R. mit Frau und Kind. Beide darf jeder online kennenlernen – die Familie erlaubt Einblicke in ihren Alltag. Auf Videos und Fotos kann man sich in der Wohnung umschauen. Auch hier passt das Gesehene perfekt zu verschiedenen Tweets. Die Musikanlage ist eher einfach, der Geschmack von R. bleibt uns nicht verborgen: lange Playlisten, Lieblingssongs, Konzertbesuche.

Familienbande

Doch wer sucht, findet mehr als nur ein paar Einblicke in die Wohnung. So erfahren wir etwas über Haustiere. Das Kind lernen wir auf unzähligen Fotos kennen: in der Badewanne, die Taufe, aus dem Urlaub. Selbst ein Foto von Mutter und Kind, das nach der Geburt entstand, ist den R.s nicht zu privat, um es online zu stellen.

An seinem Familienglück darf jeder teilhaben, weltweit über das Netz. Wir erfahren, was R. seinem Kind vorgelesen hat. Mutter und Vater haben ihm bereits ein Blog angelegt. Über die Nicknames der Familie lassen sich auch noch viel heiklere Informationen aus dem Privatleben finden, die selbst für eine anonyme Beschreibung zu persönlich sind, weil sie unstrittig die Intimsphäre betreffen.

R.s Frau ist auch oft online und twittert fleißig. Sie trägt damit wertvolle Informationen zu unserer Recherche bei. Über sie erfahren wir viel, nachdem wir ihren Nicknamen gefunden haben: Alter, Beruf, Mädchenname, Arbeitgeber, Hobbys, Ergebnisse von Sportwettbewerben, wie sie sich die Zeit vertreibt, was sie besonders gut kann. Wir spüren Foreneinträge auf, in denen es um Sport und Schwangerschaft geht – ein vager Hinweis auf die Familienplanung. Und auch von der Vorgeschichte finden wir Bruchstücke online: R. und seine Frau haben sich online kennengelernt, sogar der Zeitraum lässt sich eingrenzen. Gemeinsamer Urlaub, die Geburt des gemeinsamen Kindes. Auch hier wieder: Jede einzelne Information ist unproblematisch, kombiniert man sie aber, entsteht ein Bild wie hier die Liebesgeschichte eines Pärchens. Und auch die Vorgeschichte lässt sich aus Bruchstücken zusammensetzen.

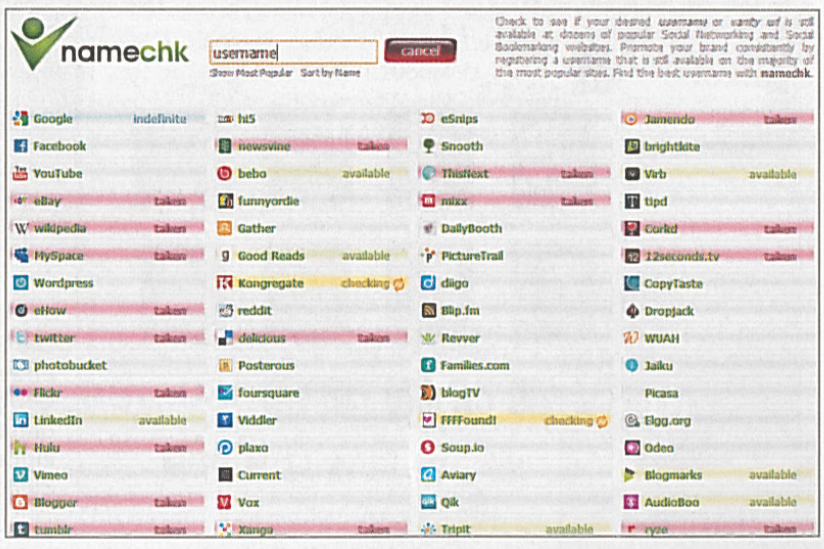
Wir finden ein Foto, auf dem ein weiteres Kind bei der Familie ist. Auf Twitter hatte R. berichtet, dass er mehrere Kinder hat. Wir entdecken das zweite Kind auf so vielen Fotos, dass wir schnell auch die Frau ausmachen können, die seine Mutter sein dürfte. Auf einem Bild sitzt sie neben dem Mann, den wir als R.s Bruder identifiziert haben. Gehört das Kind zu ihm oder zu R.? In der Bildunterschrift unter einem weiteren Foto gibt sich R. als Vater zu erkennen. Die Namen der Kinder nennt er bewusst nicht, die Zuordnung gelingt uns über die Bilder – ein Verknüpfungsweg, den man oft nicht auf dem Schirm hat.

Wir recherchieren nach der Mutter des Kindes und erkennen sie auf einem Foto in einem sozialen Netzwerk. Über ihren Namen finden wir zu einer Website mit ihrer Adresse. Wir besichtigen ihr Haus online, erfahren ihren Geburtstag und ihre Geschenkwünsche, die sie bei einem Online-Shop veröffentlicht hat.

Doch selbst solche Informationen sind an sich harmlos – in den meisten Fällen werden sie folgenlos bleiben. Das ändert sich schlagartig, wenn man an mögliche Bedrohungsszenarien denkt: Stalking, eifersüchtige Partner/Ex-Partner, Wirtschaftsspionage oder dergleichen. Durch die Fülle an Informationen kann jeder über das Netz Gewohnheiten, Tagesabläufe und allerhand andere private Dinge nachvollziehen, ohne dass der Betroffene das verhindern kann oder auch nur erfährt.

Abschluss

Dies ist nur ein grober Abriss der Informationen, die wir ermittelt haben. Am Ende der Recherche hatten wir Hunderte von Texten und Fotos sowie etliche Videos zusammengetragen. Dabei haben wir uns auf frei zugängliche Informationen aus dem Netz beschränkt. Selbst die Bankverbindung ließe sich mit einem ganz legalen Trick herausbekommen, etwa wenn der gesuchte Mensch auf eBay Dinge verkauft. Auf den beschriebenen Wegen gelang es uns, noch mehr Perso-



Wo wird ein Nickname verwendet? namechk überprüft Dutzende Dienste.

nen aus R.s engem Familien- und Freundeskreis aufzuspüren.

Der nächste Schritt wäre gewesen, mit diesen Personen – online oder offline – in Kontakt zu treten. Ein Vorwand dafür ließe sich mit den gewonnenen Informationen schnell finden. So kann man bei diesem Social Engineering auf Schulen und Mitschüler, Hobbys oder angebliche gemeinsame Bekannte zurückgreifen. Die meisten der gefundenen Informationen ließen sich anhand weiterer Online-Quellen auf Plausibilität überprüfen.

Rückzieher

Als wir R. den fertigen Artikel vorlegten, untersagte er uns, ihn mit den gefundenen Informationen zu veröffentlichen. Dieser Sinneswandel hat uns verblüfft. Schließlich waren alle Angaben, die wir zusammengetragen hatten, frei zugänglich – das meiste hatten R. und seine Frau selbst veröffentlicht. Zwar bezog sich ein Teil des Materials auf Dritte, etwa die eigenen Kinder, aber das hatten sie gewusst, als sie es im Netz veröffentlichten.

Zunächst hatte R. angekündigt, einige unserer Funde aus dem Netz zu entfernen. Doch das zuverlässige Löschen bereits länger online verfügbarer Bilder und Texte ist problematisch (siehe S. 112). Später hinterfragte er, ob der Artikel jemandem nützt. Wir haben dies bejaht, denn offenbar hat er bereits bei R. eine Wirkung erzielt. Er zeigt plastisch, warum man persönliche Informationen über sich und andere sparsam veröffentlichen sollte.

R. befürchtet, dass der Artikel zur Nachahmung anregt und sieht sich und seine Familie dadurch gefährdet. Diese Gefahr mag bestehen, allerdings nicht nur durch den Artikel. R. selbst bräuchte ebenso wie jeder erfahrene Internetnutzer keine Anleitung, um ein solches Profil zu erstellen – umso erstaunlicher, wie freizügig er das Netz mit Daten über sich und andere füttert.

Dies ist ein Einzelfall, gleichzeitig aber auch ein Symptom. Selbst erfahrene Netznutzer verlieren leicht den Überblick darüber, was sie tun. Die Faszination über technische Möglichkeiten drängt gesunde Vorsicht zurück. Es ist eine Grundhaltung der Branche: Datenschutz hemmt den Fortschritt und ist die verstaubte Idee rückständiger Street-View-Verpixler. Bis es dann um die eigene Haut geht – dann wird der Ruf nach Privatsphäre laut. (jo)

www.ct.de/1101108

Recherchetipps

Ausgangsbasis für die Recherche war eine Google-Abfrage. Aber nur mit R.s Namen fanden wir zunächst, abgesehen vom Link zum Twitter-Account, nichts Privates, sondern nur sehr viele Treffer, die seine berufliche Tätigkeit betreffen. Einschlägige Personensuchmaschinen wie Yasni oder 123people lieferten ähnliche Ergebnisse.

Der Nickname bei Twitter war aber eine große Hilfe: Wird der noch bei anderen Netzwerken verwendet? Das lässt sich über namechk.com herausfinden: Eigentlich ist die Site wohl dafür gedacht, herauszukriegen, ob der ausgesuchte Nickname in möglichst vielen Netzwerken noch frei ist. Aber das funktioniert auch umgekehrt: Hat man einen Nickname, kann man sehen, wo er noch verwendet wird – von eBay bis zu YouTube. Um die Tweets auszuwerten, haben wir mit einem PHP-Skript Hunderte heruntergeladen.

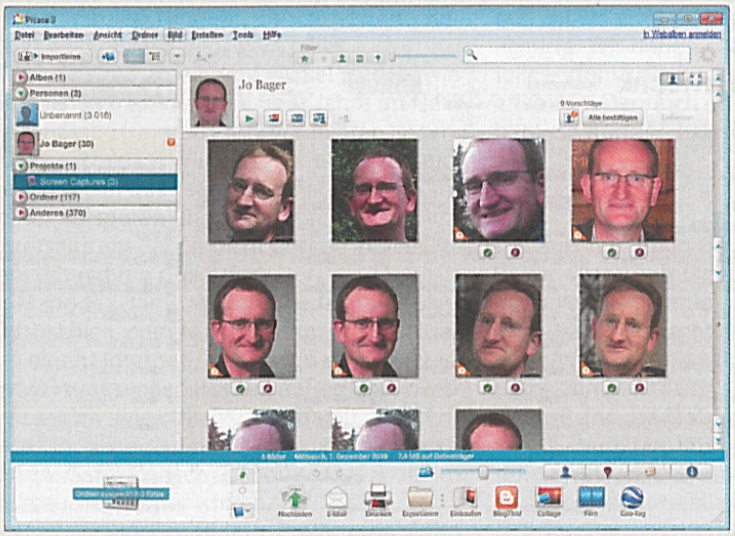
Besonders viel über eine Zielperson herausfinden lässt sich über andere, die ihr wichtig sind – Familie, Freunde, Kollegen. Dabei können auch die Verknüpfungen in sozialen Netzwerken helfen. Diese Informationen haben wir allerdings für unsere Recherche nicht genutzt; R. hat für eine manuelle Auswertung zu viele Kontakte. Wer tiefer nach besonders interessanten Kontakten in sozialen Netzwerken sucht, der kann sich von Online-Werkzeugen unter die Arme greifen lassen. TweetStats zum Beispiel liefert für einen Twitterer die Nutzer, mit denen er sich besonders häufig austauscht – und auch die Hashtags der wichtigsten Themen.

Neben den Kontakten helfen die in den Status-Updates veröffentlichten Informationen bei den sozialen Netzen. Selbst wenn die Zielperson etwa auf Facebook ihre Pinnwand für Mitglieder außerhalb ihres Freundeskreises gesperrt hat, lassen sich Kommentare auf Seiten finden, die frei zugänglich sind, etwa mit dem Google-Operator „site:facebook.com". So kann man beispielsweise herausfinden, wo genau jemand im Urlaub war oder welche Schule er besucht hat. Solche Fundstücke liefern wiederum Input für Suchbegriffe mit der Google-Suche, die zu privaten Informationen führen.

Viele gute Informationen stecken in Daten, die Suchmaschinen für das Web (noch) nicht auswerten können – in Bildern etwa. Doch man kann eine Bildersammlung herunterladen, um mit dem Programm Picasa Gesichter zuzuordnen. Hat dieses ein Gesicht auf einer Auswahl von Bildern gelernt, erkennt es die Person auf weiteren Bildern automatisch. Das klappt nicht immer perfekt, man sollte auf jeden Fall die Bilder selbst auch noch ansehen – auch weil man auf diese Weise noch weitere interessante Informationen findet. So haben wir neue, gute Suchbegriffe gefunden.

Der Fotograf, der Mario R.s Hochzeit fotografierte, hat nur acht Fotos zur Veröffentlichung ausgewählt und verlinkt. Zuvor hat er aber offensichtlich alle gelungenen Aufnahmen auf seine Website hochgeladen – unverlinkt, aber frei zugänglich. Mit einem Klick auf eines der verlinkten Fotos erfährt man, in welchem Verzeichnis die Fotos liegen und wie sie benannt sind.

Endet ein Foto auf 4810.jpg, lässt sich der Dateiname in der URL manipulieren, aus der 10 eine 11 oder 09 machen – und siehe da: auch Bilder mit anderen Ziffern sind online. Einfacher geht das mit dem Firefox-Plug-in Firefusk: Mit einem Rechtsklick lässt sich festlegen, welche Ziffern im Dateinamen es noch ausprobieren soll, etwa „+/- 9999". So haben wir über 300 Fotos gefunden, die Menschen darauf konnten wir mit Bildern der Kontakte in sozialen Netzwerken vergleichen – auch dabei wurden wir fündig. c't



Die Gesichtserkennung von Googles Bilddatenbank Picasa eignet sich zur Zielfahndung.