Datum: 02.06.2010

netzwoche

Netzmedien AG
8005 Zürich
044/ 355 63 63
www.netzwoche.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 7'896
Erscheinungsweise: 25x jährlich

Themen-Nr.: 1.1
Abo-Nr.: 1083040
Seite: 37
Fläche: 48'441 mm²

Wie viel normative Sicherheit erträgt die ICT, wie viel braucht der User?

Auf Einladung der ICT-Kommission der SATW diskutierten rund 50 Exponenten aus Forschung, Bildung, Politik und Wirtschaft über «Digital Identity, Trust und Confidence». In einem Punkt war man sich einig: Das Thema wird von der surfenden Mehrheit unterschätzt. Thomas Brenzikofer

Am diesjährigen Workshop der ICT-Kommission der Schweizerischen Akademie der technischen Wissenschaften (SATW) in Münchenwiler ging es gleich zu Beginn hoch hinaus. In seinem Einführungsreferat brachte Gregory Neven von IBM Research Zürich einen treffenden Vergleich: Bekanntlich seien Neil Armstrongs Fussabdrücke auf dem Mond wegen der geringen Erosion immer noch sichtbar. Das Gleiche gelte auch für die Spuren, die wir in der digitalen Welt hinterlassen, auch diese lassen sich kaum mehr verwischen.

Speichern aus Prinzip

Somit war das Thema gesetzt: Im 24-stündigen Workshop, an dem rund 50 Vertreter aus Politik, Wirtschaft, Ausbildung und Forschung sowie von Behörden partizipierten, wurde die Frage erörtert, wie mit unser aller digitalen Identität in Zukunft umzugehen ist, damit das Grundrecht auf Schutz der eigenen Privatsphäre gewahrt werden kann. Dabei dürfte sich die Problematik, wie Neven ausführte, in den nächsten Jahren nochmals drastisch verschärfen. Verantwortlich dafür sind zwei Entwicklungsachsen: Zum einen werden Speicherkapazitäten immer günstiger und mächtiger, was dazu führt, dass heute schon in vielen Unternehmen das Prinzip «Storage by default» angewendet wird.

Die andere Entwicklungsachse betrifft das, was sich mit den gesammelten Daten anstellen lässt. Auch die Kunst des Data Minings hat sich in den vergangenen Jahren mächtig entwickelt. So werden immer mehr selbstlernende Algorithmen auf die Datenberge angesetzt. Dabei ist man gemäss Neven heute schon so weit, dass nicht mehr genau nachvollziehbar ist, nach welchen Strategien ein Algorithmus zu seinen Ergebnissen kommt.

Digitale Fremdbestimmung

Eine Blackbox stellt letztlich auch Google dar. Auch hier lässt sich kaum kontrollieren, welches Resultat die Suchmaschine zur eigenen Person ausspuckt. Dies kann unangenehme Folgen haben, vor allem dann, wenn die Ergebnisse von Medien, Behörden oder einem potenziellen Arbeitgeber unkritisch verwendet werden. Noch perfider sind Social-Media-Sites. Diese machen es einem zwar denkbar einfach, sich als User zu registrieren. Den Wenigsten ist indes bewusst, dass damit ein Committment auf Lebenszeit eingegangen wird. Zwar kann man seinen Account abmelden, die Daten jedoch bleiben ungelöscht. Aber auch die Hoheit darüber zu behalten, wer was vom eigenen Profil sehen darf, ist auf vielen Social-Media-Plattformen ein schwieriges wenn nicht gar unmögliches Unterfangen.

Plädierte dafür, das Neue ins Alte zu integrieren: Ethiker Alberto Bondolfi am SATW-Workshop

Bildquelle: SATW

Datum: 02.06.2010

netzwoche

Netzmedien AG
8005 Zürich
044/ 355 63 63
www.netzwoche.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 7'896
Erscheinungsweise: 25x jährlich

Themen-Nr.: 1.1
Abo-Nr.: 1083040
Seite: 37
Fläche: 48'441 mm²

Kein rechtloser Raum

So stellte sich die Frage, inwiefern der Staat auch dem Internet-Citizen das Recht zu garantieren hat, wo nicht die Kontrolle, so doch die Transparenz über seine digitale Identität zu erlangen. Festzustellen ist indes, dass es offensichtlich die wenigsten Social-Web-Aficionados kümmert, als Marketingobjekt ausgeschlachtet zu werden. Dabei ist es meist Unwissenheit, die in digitale Fremdbestimmung führt. Sollte also der Gesetzgeber eingreifen?

Eine ethische Frage, zu der am SATW-Workshop auch ein Ethiker Stellung nahm. Alberto Bondolfi von der Universität Lausanne vertrat die Ansicht, das Neue möglichst in die bestehende Rechtsprechung zu integrieren und nicht umgekehrt. Erst wenn eine neue Technologie eine konkrete Spezifität ins Feld führe, sei Handlungsbedarf gegeben. Meistens handle es sich indes um die gleichen Delikte, nur deren Form würde sich verändern. So könne es eben zu Beschuldigungen kommen, weil ein vermeintlicher Tatbestand als solcher falsch erkannt wurde, oder umgekehrt, sei es schwierig, Missbrauchsfälle als Delikte zu identifizieren, was dann eben dem digitalen Wilden Westen Vorschub leiste.

Während nicht nur die Gesetze, sondern auch Technologien vorhanden wären, um den Persönlichkeitsschutz auch in der digitalen Welt zu bewahren, fragt es sich, warum diese kaum eingesetzt werden. Im Zentrum des Interesses steht dabei die frisch lancierte SuisseID. Diese könnte durchaus als starke Authentifizierung bei Social-Media-Plattformen und anderen sensitiven Onlinetransaktionen ihre Verwendung finden. Nur: Wie kann der User davon überzeugt werden, sich – gegen Geld! – eine SuisseID zu besorgen, vorausgesetzt auch die Anbieter würden die Technologie adaptieren.

Präzedenzfälle schaffen

Letztlich, so eine mögliche Quintessenz aus allen eingebrachten Empfehlungen, verbleibt dem Staat einzig die Rolle des Sensibilisierers und Aufklärers. Allenfalls könnte er den Gesetzen in gesteigertem Masse Nachdruck verleihen. Zu überlegen wäre etwa, ganz bewusst Präzedenzfälle zu schaffen mit dem Ziel, in der Öffentlichkeit eine erhöhte Aufmerksamkeit gegenüber dem Thema zu erzeugen, sodass sich Unternehmen durch den Einsatz von Technologien wie die SuisseID einen Reputationsgewinn erhoffen könnten.

Dabei liesse sich der legislative Schraubstock (für die Unternehmen) noch etwas anziehen, indem man gesetzlich das Prinzip instauriert, dass bei Onlinetransaktionen nicht sämtliche Risiken dem User überantwortet werden dürfen. Ebenfalls denkbar wäre es, bei Anwendungen, in denen digitale Identitäten involviert sind, ganz bestimmte Benutzungsregeln vorzuschreiben. Allerdings muss dann auch die Frage ausdiskutiert werden, ob es sich lohnt, durch dieses normative Sicherheitsdenken die Innovationskraft der Informations- und Kommunikationstechnologie aufs Spiel zu setzen. <