Oliver Günther

Die Vorstandsperspektive

„Wir wissen schon alles über Sie"

„No need to send a resumé – we already know everything about you." Dieser Satz ist nicht wirklich von der amerikanischen National Security Agency, die neuerdings auch in Deutschland jeder kennt. Er ist auch nicht aus neuerer Zeit. Vielmehr begrüßte er mich 1984 in meinem Doktorandenbüro an der University of California in Berkeley. Ein unbekannter Kommilitone hatte ihn auf einen kleinen Aushang gekritzelt, der an dem im Büro befindlichen Schwarzen Brett mit einer Reißzwecke befestigt war. Dieser Aushang war tatsächlich von der NSA – sie suchte amerikanische Informatiker als Mitarbeiter „to serve your country". Ob sie damit im liberal gesinnten Berkeley große Erfolge hatte, weiß ich nicht. Als ich ahnungsloser Deutscher einen gerade anwesenden amerikanischen Kommilitonen fragte, was es mit der NSA denn auf sich habe, meinte er verschmitzt „NSA? You mean: No Such Agency"?

Wer also meint, die NSA und die vielen anderen Geheimdienste dieser Welt sammeln erst seit der Breitennutzung des Internets massiv und systematisch Kommunikationsdaten, muss der Naivität bezichtigt werden. Selbstverständlich sammeln Geheimdienste von jeher Daten. Das ist ja ihr Job. Meistens, aber nicht immer, bewegen sie sich dabei auf dem Boden ihrer nationalen Gesetze. Nationale Gesetze bilden freilich die nationale Kultur ab. Sie passen nicht unbedingt auf andere Länder, und sie räumen Ausländern oft weniger weitreichende Rechte ein als den eigenen Bürgern. All das ist weder überraschend noch verwunderlich. Aber es ist der Grund für die aktuelle Aufregung.

Als Bürger, als Unternehmen, als Behörde ist man gut beraten, sich aktiv und realistisch mit der aktuellen Situation auseinanderzusetzen. Andernfalls läuft man in der Tat schnell Gefahr, die Kontrolle über die eigenen Daten zu verlieren. Manchen mag das egal sein. Mir nicht. Und Unternehmen und Behörden kann *es nicht egal sein.*

Was heißt es nun, sich realistisch *mit der aktuellen Situation auseinanderzusetzen? Es ist ja nicht immer einfach, die sich im Internet präsentierenden Risiken zu erkennen und richtig einzuschätzen. Wie auch die Forschungsarbeiten meiner eigenen Arbeitsgruppe immer wieder zeigten, haben wir Menschen große Probleme mit dieser Form der Risikoeinschätzung. Unsere Gene haben sich seit dem Leben in der Savanne nicht wesentlich verändert. Für ein Leben im Internet, oder allgemeiner: für ein Leben in unserer modernen Zivilisation, sind sie nicht optimiert. Deswegen unterschätzen wir manche Risiken (so das Risiko, in einem Verkehrsunfall verletzt oder eben in der persönlichen Kommunikation überwacht zu werden), überschätzen andere Risiken (so das Risiko, der Rinderseuche oder einem terroristischen Anschlag zum Opfer zu fallen) und landen so in einem Dilemma, wo unser Verhalten unsere Präferenzen nur unzureichend widerspiegelt.*

Die Probleme mit der Einschätzung der im Internet präsenten Risiken haben sich nach den Aufdeckungen von Snowden & Co. verschärft. Wobei die Aufdeckungen für eine offene Gesellschaft wie die unsrige ausgesprochen wichtig waren, denn nur mit dem Wissen um diese Umstände ist es für Bürgerinnen und Bürger möglich, die angesprochenen Risiken realistisch einzuschätzen, über adäquate Konsequenzen nachzudenken und diese Überlegungen mit ihren Parlamentariern zu teilen. Nur so kann sichergestellt werden, dass die Geheimdienste wirklich so agieren, wie es dem Willen des Volkes entspricht. Dies darf nicht mit dem Wunsch nach der Abschaffung aller Geheimdienste verwechselt werden. Letzteres ist weder realistisch noch wünschenswert, denn auch eine offene Gesellschaft braucht

DOI 10.1007/s00287-013-0743-7

Geheimnisse. Sie braucht auch Geheimdienste. Aber eben auch die Möglichkeit für jeden und jede, Geheimnisse sicher zu verwahren. Denn wie sagte der Kollege Dan Kaminsky kürzlich so richtig: „If security is outlawed, only outlaws will have security."

Diese Möglichkeit ist uns im Internet vorerst verwehrt. Wir wissen nun, dass ausländische Geheimdienste über Projekte wie PRISM *den Großteil unserer digitalen Kommunikation ohne Gerichtsbeschluss überwachen können und dies auch tun. Wir wissen, dass gängige Verschlüsselungsprotokolle wie* https *bereits geknackt worden sind. Anbieter sicherer Dienste wie* TOR *oder* Lavabit *werden massiv unter Druck gesetzt, Hintertüren einzubauen, die Regierungsbehörden den Datenzugriff ermöglichen. Die Frage ist freilich, welche Rechtsprechung dann gilt. Constanze Kurz und Frank Rieger haben recht, als sie kürzlich in der FAZ schrieben: „Unter amerikanischer Jurisdiktion Dienste mit Privatsphären-Garantie anbieten zu wollen, ist schlicht nicht mehr möglich."*

Mathematisch fundierte Verschlüsselungsmechanismen wie Public Key Encryption *haben an ihrer nachgewiesenen Sicherheit nichts eingebüßt, aber sie müssen vor dem Hintergrund der stark angestiegenen verfügbaren Rechenleistung neu bewertet werden. (Zur Erinnerung: Je kürzer der Schlüssel, desto weniger Rechenleistung ist erforderlich, um das System zu knacken.) Außerdem werden derartige „mathematisch sichere" Verfahren oft dadurch kompromittiert, dass sie von Laien nur schwer sicher umzusetzen sind. (Was nützt* PKE*, wenn der Schlüssel auf einem Post-It am Desktop steht? Oder gar per E-Mail verschickt wird) Und schließlich stellt sich auch hier die Frage möglicher Hintertüren, also eines Generalschlüssels für Dritte.*

Letztlich zeigt sich hier einmal mehr, dass das Internet nicht für den Zweck entworfen wurde, für den es jetzt genutzt wird. Als Protokolle wie sendmail *oder* http *entworfen wurde, waren weder die Größenordnung noch die Vielfalt der Internetnutzung abzusehen. Aber wie soll man sich eine Substitution des Internets durch ein neues System vorstellen? Der* Clean-Slate-*Ansatz klingt theoretisch gut, wirft aber viele praktische Fragen auf. Und an den Ansprüchen der Geheimdienste würde er auch nichts ändern.*

Viele offene Fragen, zu deren Beantwortung die GI auch weiterhin beitragen wird. Ein erster Schritt ist unsere kommentierbare Liste von Antworten auf häufig gestellte Fragen, siehe https://www.gi.de/themen/ueberwachungsaffaire-2013.html. Weitere Schritte erwägen wir zur Frage der Zertifizierung von Mails und dem Bedarf nach einer nationalen Zertifizierungseinrichtung.

Eigentlich wollte ich diese Kolumne dazu nutzen, einen Rückblick auf die Arbeiten des GI-Vorstands in den letzten zwei Jahren vorzunehmen. Die aktuellen Ereignisse schienen mir dann aber wahrlich von höherer Relevanz, zumal unser Jahresbericht (www.gi.de/service/downloads) ausführlich über die laufenden GI-Aktivitäten berichtet. Erlauben Sie mir hier nur eine kurze Zusammenfassung. Zwei Ziele standen in den letzten Jahren der GI-Arbeit im Vordergrund:

Erstens mussten die Mitgliederleistungen verbessert werden, um die GI für jetzige und zukünftige Mitglieder attraktiver zu machen. Unsere Präsenz auf den (aus Datenschutzsicht natürlich problematischen) sozialen Netzwerken ist hier ein wichtiges Element, ebenso wie der neue „GI-Radar", das neue praxisorientierte Magazin „Digital" sowie unsere digitale Publikationsplattform www.gi.de/portal. Leistungen für Mitglieder aus der industriellen Praxis standen hierbei im Vordergrund. Denn die GI darf kein „Professorenverein" sein. Sie muss auch für die vielen Informatikerinnen und Informatiker, die in Unternehmen und Behörden arbeiten, ein attraktives Leistungsangebot bereithalten.

Zweitens haben wir die GI politischer gemacht. Wie meine vorigen Ausführungen zeigten, ist Informatik heute wahrlich nicht nur eine technische Wissenschaft. Informatik durchdringt alle relevanten Dimensionen unseres Lebens: Politik, Wirtschaft und eben auch unser persönliches Leben – ja, unsere intimste Privatsphäre. Dies muss sich in der Arbeit der GI zunehmend niederschlagen. Deswegen haben wir ein Berliner Büro eröffnet, das sich intensiv der Vernetzung mit den Regierungseinrichtungen und mit den Hauptstadtrepräsentanzen der Unternehmen und der NGOs zuwendet. Diese Art von Lobbyarbeit im besten Sinne ist für eine Gesellschaft wie die GI essenziell. Auch das neue GI-Junior-Fellow-Programm ist durchaus in diesem Kontext zu sehen. Auch hier geht es darum, mit exzellenten jüngeren Informatikerinnen und Informatikern Ideen zur Positionierung der Informatik in Wissenschaft und Gesellschaft zu entwickeln und umsetzen.

Auf diese Weise werden wir auch zunehmend nicht mehr als rein technisch orientierte Organisation wahrgenommen, sondern als Teilnehmer und Mitgestalter des öffentlichen Diskurses zu dem durch Informatik

mitausgelösten gesellschaftlichen Wandel. Die GI muss diesen Wandel verinnerlichen und darf die Diskussion hierüber nicht den anderen überlassen.

Zum Schluss ist es mir noch ein wichtiges Anliegen, Ihnen allen zu danken für Ihre Treue zur GI und Ihren Einsatz für unser Fach. Besonderer Dank gebührt den Mitarbeiterinnen und Mitarbeitern in der Bonner Geschäftsstelle und unserem Hauptstadtbüro, meinen Kolleginnen und Kollegen im Vorstand und Präsidium der GI sowie den vielen anderen, die in der GI Verantwortung tragen. Ohne diese von vielen Schultern getragene Mitverantwortung gäbe es die GI nicht. Ich danke Ihnen für Ihre Mitarbeit und für Ihr Vertrauen.

Mit den besten Grüßen,
Ihr Oliver Günther
(Dezember 2013)

Oliver Günther,
Präsident der Gesellschaft für Informatik e.V. (GI),
Universität Potsdam,
oliver.guenther@gi.de