Der Schlüssel-Meister

Jan Camenisch entwickelt Code, mit deren Hilfe wir uns im Internet ausweisen können – und trotzdem anonym bleiben

VON SIMONE LUCHETTA (TEXT) UND BRUNO SCHLATTER (FOTO)

Egal, was Jan Camenisch tut: Er tut es mit Ausdauer und Beharrlichkeit. «Was mich von anderen Verschlüsselungsforschern unterscheidet ist, dass ich seit zwölf Jahren zusammenhängend an einem Thema forsche», sagt er. Im Zentrum seiner Arbeiten steht die Frage, wie sich Benutzer im Internet sicher ausweisen können, ohne dabei detaillierte persönliche Daten weiter zu geben. Für sein «Lebenswerk» hat der erst 42-jährige Bündner kürzlich vom weltgrössten Verband für Informatik den «Outstanding Innovation Award» erhalten. Camenisch legte damit den Grundstein für die Identitätskarte der Zukunft.

Der renommierte Preis, eine gravierte Messingplatte auf dunkelbrauner Holztafel, hängt prominent neben bunten Zeichnungen und Fotos seiner beiden Töchter. Das kleine Büro im IBM Forschungsinstitut in Rüschlikon ist tipptopp aufgeräumt. Auf dem Pult stehen vier weitere Skulptürchen, die ihm ebenfalls für sein herausragendes Schaffen verliehen wurden. «Die anderen sind dort oben.» Er grinst und zeigt auf das Gestell, wo sich gerahmte Anerkennungen bis an die Decke stapeln.

Jan Camenisch ist in der Kryptografieforschung weltweit ganz vorne dabei. Und noch nie waren seine Fragestellungen so aktuell wie heute. «Vor 10 Jahren schliefen die Zuhörer bei meinen Vorträgen ein; heute haben viele das Problem erkannt und wollen mit uns zusammenarbeiten», sagt er.

Das «Problem» ist, dass wir immer häufiger online einkaufen, chatten, Flüge buchen oder Einzahlungen erledigen und jedes Mal ein persönliches Profil erstellen müssen; dabei geben wir oft mehr private Daten preis als für eine Dienstleistung nötig wären. Ganz zu schweigen von sozialen Netzwerken, wo Leute freiwillig Details verraten. Gleichzeitig ist der Identitätsdiebstahl das am schnellsten wachsende Internet-Verbrechen. Und die Angst vor Datenmissbrauch ist gemäss einer neuen Erhebung des Bundesamtes für Statistik in den Schweizer Haushalten sehr verbreitet.

Da kommen die von Camenisch entwickelten kryptografischen Algorithmen wie gerufen. Auf der einen Seite garantieren sie dem Dienstleister grösstmögliche Sicherheit, auf der anderen garantieren sie dem Benutzer den Datenschutz.

In den nächsten vier Jahren wird die Technik erprobt

Das Prinzip ist relativ einfach erklärt: Das System kann Daten in elektronischen Zertifikaten so verschlüsseln, dass zwar eine Aussage über den Besitzer gemacht wird, diese aber keine Rückschlüsse auf die genaue Identität ermöglicht. Die eingesetzten Algorithmen agieren dabei wie eine Art Mittelsmann, der zwar alles weiss, aber nur die Infos weitergibt, die für die Nutzung einer Dienstleistung nötig sind.

So bestätigt das System etwa, dass ein Mädchen einer Altersgruppe im Chat unter 14 Jahren angehört, das genaue Geburtsdatum wird aber verschwiegen. Gleichzeitig ist sichergestellt, dass sich ein über 14-Jähriger nicht in diesen Chat einloggen kann. Ebenso kann die Technologie etwa den Wohnort des Inhabers nachweisen, ohne gleich Adresse und Namen offenzulegen.

Derzeit führt Camenisch seine Forschung in der europäischen Forschungsinitiative ABC4Trust weiter. Er leitet eine Gruppe mit Leuten von Microsoft, anderen Firmen, Universitäten und Datenschützern: «In den nächsten vier Jahren geht es darum, die Verschlüsselungstechnik in der Praxis zu erproben und zu zeigen, dass sie funktioniert.»

Die Forscher verfolgen zwei Pilotprojekte: An einer Schule in Schweden können sich die Schüler sicher in Dienste der Schule einloggen und mit Sozialarbeitern oder Lehrern persönliche Fragen diskutieren – anonym. An der Patras-Universität in Griechenland bewerten Studenten auf dieselbe Weise ihre Dozenten und Kurse.

Über seine Erfolge zu reden, fällt dem Sohn einer Stockholmerin und eines Bergbauern nicht ganz leicht; man muss schon reichlich bohren, will man erfahren und einordnen, was der Mann aus Langwies erreicht hat. Der Spitzenkryptograf ist viel unterwegs, leitet Sitzungen, betreut Doktoranden und hält Vorträge. Zum Ausgleich spielt er Bassgitarre in einer Band und treibt Sport – die Marathonbestzeit liegt bei drei Stunden. Ein Tag pro Woche bleibt ihm für sein «Handwerk»: «Dann ziehe ich mich mit Bleistift und Block zurück und knoble an einem mathematischen Problem.»

Erstmal müssen Regierungen und Unternehmen zustimmen

Schon bald könnte uns der Tüftler eine weitreichende Erfindung bescheren. Ziel der europäischen Forschungsinitiative ist es, ein «übergeordnetes Managementsystem für Identitäten» zu schaffen. «Das könnte eine global einsetzbare Identitätskarte sein», so Camenisch.

Bis wir so einen elektronischen Ausweis im Portemonnaie haben, sind noch einige Hürden zu nehmen. So ist derzeit unklar, wer eine solche eID zuerst ausstellen soll. Es könnte ein privates Unternehmen sein: «Ich tendiere aber eher zu einer Regierungsstelle.» Zudem muss Camenisch Firmen und Regierungen überzeugen, die Verschlüsselungstechnologie in ihre Systeme und Ausweise einzubauen und sie als Standard zu etablieren.

Schwierig dürfte das besonders bei Firmen wie Facebook sein, die mit den Daten Geld verdienen. «Das wird wohl nur auf Druck von aussen möglich sein, sei es politisch, gesellschaftlich oder rechtlich», ist er sich bewusst. Dabei sei es schon heute möglich, auch Facebook, wo sich die Leute ja zeigen wollen, sicher und gleichzeitig datenschutzfreundlich zu bauen.

Unsicher ist, wann es so weit sein wird. Laut Camenisch könnten wir in 6 bis 7 Jahren eine eID besitzen, die – anders als die heutige Suisse ID (*siehe Kasten*) – auch die Privatsphäre schützt. Sicher ist: Camenisch bleibt dran.

Datenschutzexperte: Jan Camenisch im IBM-Forschungsinstitut

Camenisch: Suisse ID schützt die Privatsphäre nicht

Jan Camenisch entwickelt Verschlüsselungs-Algorithmen für den «Nachfolger der Suisse ID», wie er selbst sagt. An diesem im Mai 2010 vom Bund lancierten elektronischen Ausweis bemängelt er, dass er zwar die Identität zweifelsfrei nachweise, aber die Privatsphäre des Karteninhabers nicht schütze. Im Gegenteil: Dieser muss sich immer vollständig ausweisen, egal für welche Dienstleistung. Bis Ende 2010 wurden 271 000 Suisse IDs bestellt, davon nur 20 000 von Privaten. Bislang sind 118 Anbieter an Bord, vor allem Städte und Gemeinden. Dem Seco sind Einzelheiten der IBM-Forschung noch nicht bekannt; es kann deshalb keine Stellung nehmen.

Der «Huffington Post» droht die Zähmung

Blogger schimpfen über den Verkauf der Onlinezeitung an den Internetgiganten AOL – sie haben Angst, die linke Ausrichtung gehe verloren

Die Fronarbeiter begehren auf. Kaum wurde der Verkauf des Blogportals «Huffington Post» für 315 Millionen Dollar an den Onlinegiganten AOL am Montag bekannt, regte sich Widerstand unter den Tausenden von Bloggern, deren Texte die Spalten der Huffpo füllen.

Bislang habe sie gern gratis beigetragen, denn «die Huffpo schien mir ein grossartiges, neues, frisches Projekt», so Bloggerin Mya Guarnieri. «Ich bin nicht 100 Prozent sicher, ob ich das ohne Entgelt für einen Riesenkonzern tun will.» Blogger Tara Dublin wurde konkreter: «Ich finde, Beitragsleistende sollten bezahlt werden.»

AOL-Chef Tim Armstrong, Arianne Huffington FOTO: GETTY

Unzufriedenheit macht sich auch unter Huffpo-Lesern breit. In den ersten 24 Stunden gaben sie 7000 Kommentare zum Kauf ab – zu 81 Prozent negative, wie Thedailybeast.com zählte. Auf dem Kurznachrichtendienst Twitter rufen Zehntausende Nutzer in Einträgen mit dem Schlagwort Huffpuff zum Boykott auf – eine Anspielung an das Kindermärchen «Die drei kleinen Schweinchen», in dem der Wolf droht: «Ich werde husten (huff) und prusten (puff) und dir dein Haus zusammenpusten.»

Der Unmut beweist, dass die vor fünf Jahren gegründete Huffpo für viele nicht nur eine Newsquelle ist, sondern vor allem als Onlinetreffpunkt dient. Für die Attraktivität spielt die progressivlinke Ausrichtung eine Schlüsselrolle. Jetzt erwarten viele der 20 Millionen monatlichen Nutzer, dass die fortschrittliche Orientierung unter dem Dach des gemässigt-konservativen Internetgiganten AOL verloren gehen könnte.

«Huffington Post» könnte zu totem Rummelplatz werden

Die Angst vor einem Kulturkonflikt ist gerechtfertigt. Denn umgekehrt scheint bei manchen zahlenden AOL-Abonnenten schlecht anzukommen, dass künftig die Huffpo-Gründerin Arianna Huffington alle AOL-Inhalte kontrollieren wird. Die nach dem Verkauf um bis zu 100 Millionen Dollar reichere Huffington wie auch AOL-Chef Tim Armstrong wollen nichts von Risiken wissen. Sie predigen das Wachstum des kombinierten Unternehmens, planen billig produzierte Inhalte in grosser Zahl, damit Inserate die unaufhaltsam schwindenden Aboeinnahmen von AOL wettmachen können.

Das Risiko ist dennoch hoch, dass die Huffpo sehr schnell zum toten Rummelplatz wird, wenn sie sich zu sehr AOL anpasst.

MARTIN SUTER