SocietyByte
Wissenschaftsmagazin des BFH-Zentrums Digital Society
https://www.societybyte.swiss

Vertrauen lässt sich nicht herbeikonstruieren

Autor : Hubert Rötzer

Datum : 27. September 2018

Bürgerinnen und Bürger können erst dann in die Verwendung ihrer elektronischen Identitäten und personenbezogenen Daten vertrauen, wenn sie ihr Grundrecht auf Schutz der Privatsphäre gewahrt wissen. Solches Vertrauen kann nicht durch technische Massnahmen hergestellt werden. Wenn aber der Umgang mit elektronischen Identitäten so gestaltet wird, dass er genauso anfühlt, wie bei klassischen Identifizierungsmitteln und wenn Informatiker und Juristen eine gemeinsame Sprache finden, um miteinander die geeigneten IT-Systeme zu entwerfen, dann kann solches Vertrauen entstehen.

Informatiker verstehen unter dem Begriff «CIA-Triad» das Sicherheitsdreieck Confidentiality – Integrity – Availability, also Vertraulichkeit, Integrität und Verfügbarkeit. Dieses sind die klassischen Schutzziele für IT-Systeme und elektronische Datenbestände. Technisch erreicht man Vertraulichkeit und Integrität durch Verschlüsselung. Verfügbarkeit stellt man durch systemische Redundanzen und Schutzmassnahmen gegen Cyber-Attacken sicher.

Neu hinzu kommt der Persönlichkeitsschutz. Es geht hier nicht um Maschinen, sondern um das Grundrecht real existierender Personen auf Schutz ihrer Privatsphäre. Diese haben das Recht auf die Hoheit über alle ihre persönlichen Informationen und Daten, soweit nicht gesetzliche Einschränkungen bestehen oder Nutzungsrechte vertraglich an Dritte übertragen wurden. Vertrauen können nur natürliche Personen aufbringen, einerseits gegenüber den Organisationen, welche Daten über sie sammeln, andererseits gegenüber den IT-Systemen, welche diese Daten speichern und verarbeiten.

Digitale Identität(en) von Personen

Natürliche Personen haben normalerweise eine Hauptidentität, welche an den Staat und den Wohnort gebunden ist und durch einen Pass oder eine Identitätskarte ausgewiesen wird. Das Vertrauen beruht auf der Fälschungssicherheit solcher Dokumente. Im Hintergrund findet eine Registrierung in einem Einwohnerregister statt. Es entsteht auf diese Weise ein weltumspannendes nicht hierarchisch koordiniertes und bisher nicht vollständig digitalisiertes System zur Identifizierung und Registrierung aller Erdenbürger. Die Digitalisierung hat zur Folge, dass die Teile dieses Systems untereinander und mit anderen Datenbanken verknüpfbar werden. Speziell durch Einführung eindeutiger elektronischer Identitäten wird es möglich, personenbezogene Daten aus verschiedenen Datenquellen den Individuen der Realwelt zuzuordnen.

Allgemein benötigen Personen ihre Identität für zwei Hauptzwecke, nämlich um sich auszuweisen (Identifizierung und Authentisierung) und ausserdem für Signaturen, also den Nachweis der Originalität von Dokumenten. Für Individuen bringt die Digitalisierung eine geradezu inflationäre Vielfalt von Systemen, bei denen sie sich registrieren, Daten hinterlegen und Authentifizierungsnachweise beziehen. Jede Person in der Schweiz hat neben den offiziellen Ausweisen noch weitere Identitätsausweise, wie einen Batch vom Arbeitgeber, den Krankenversicherungsausweis, den Führerschein, den SwissPass, diverse Bankkarten und Kundenkarten von Handelsunternehmen. Die Digitalisierung ist in all diesen Bereichen weit fortgeschritten. Die Diskussion, ob es Aufgabe des Staates oder eher eine Aufgabe Privater ist, digitale Identitäten bereitzustellen, kreist um das allesentscheidende Wort «Vertrauen».

Vertrauen auf die digitale Welt übertragen

Vertrauen in technische IT-Systeme gewinnt man, indem man Risiken bestimmt und Schutzmassnahmen ergreift. Für einen Authentifizierungsprozess lassen sich verschiedene Vertrauensstufen ausweisen. Die niedrigste gebräuchliche Stufe für die Vergabe einer elektronischen Identität ist die Verifizierung einer E-Mail-Adresse. Die höchste wäre persönliches Erscheinen und Vorlegen eines amtlichen Ausweises, womöglich mit biometrischen Merkmalen. Für rechtswirksame Transaktionen wird eine 2-Faktoren-Authentifizierung verlangt. Für den sicheren Transport und die sichere Ablage von personenbezogenen Daten werden kryptographische Verfahren eingesetzt. Vertrauen lässt sich aber durch Einsatz von Technologie nicht herbeikonstruieren. Dass Personen elektronischen Systemen mit Misstrauen begegnen, liegt an der Nichtbegreifbarkeit der Systeme. Eine Unterschrift zu leisten, ist eine physisch wahrnehmbare, manchmal geradezu rituelle Handlung.

Die Abgabe einer elektronischen Signatur ist ein abstrakter Vorgang, welcher für viele Personen intuitiv nicht erfassbar ist. Wer aber kein Gespür für den Umgang mit solchen Systemen entwickeln kann, wird Mühe bekunden, deren Sicherheit einzuschätzen.

Vertrauen kann man aufbauen, indem man das Allgemeinwissen über digitale Systeme fördert. Ein solides Verständnis, was eine digitale Identität ist, was man damit Gutes anstellen kann und vor welchen Risiken man auf der Hut sein sollte, wäre eine solide Basis für die Diskussion darüber, welchen Organisationen man wie viel Vertrauen entgegenbringen kann.

Wer ist für die elektronische ID zuständig?

Ist es tatsächlich erwünscht, dass der Staat den Bürger*innen eine elektronische Identität anbietet oder gar vorschreibt? Oder ist dies eine Aufgabe, die an Private übertragen werden sollte? Es ist ein enormes Unbehagen gegenüber grossen Datensammlungen in den Händen von Konzernen spürbar, kann doch von solchen Konzernen keinerlei Commitment eingefordert werden ausser der Einhaltung selbstgegebener ethischer Grundsätze und - häufig extraterritorialer - gesetzlicher Vorgaben, welche weder prüfbar noch durchsetzbar sind. Jedes Unternehmen hat die Möglichkeit, mit personenbezogenen Daten praktisch nach Gutdünken zu verfahren. Häufig geht es letztlich um ökonomische Interessen.

Hier zeichnet sich in der Diskussion der Konsens ab, dass die Ausstellung einer elektronischen Identität nicht auflagenlos privatisiert werden sollte. Es muss aber ausdiskutiert werden, ob es eine eindeutige ID für jede Bürgerin und jeden Bürger geben soll, die in allen Domänen der öffentlichen Verwaltung verwendet wird. Wenn beispielsweise Steuerregister, Strafregister, Wählerverzeichnis sowie Personeneinträge in Grundbüchern, KFZ-Registern, Handelsregister dieselbe E-ID verwenden, dann sind diese direkt verknüpfbar. Man kann darin eine Verletzung des Prinzips der «Separation of Concerns» sehen. Ob dies allgemein so gewollt ist, muss auf politischer Ebene festgelegt werden.

Gemeinsame Sprache von Juristen und Informatikern

Die entscheidende Voraussetzung, um solche Diskussionen überhaupt führen zu können, ist eine gemeinsame Sprache zwischen den Juristen, welche die gesetzlichen Vorgaben machen, und den Informatikern, welche die IT-Systeme bauen und betreiben. Die Einführung der DSGVO (Datenschutzgrundverordnung) hat im Wesentlichen dazu geführt, dass die Anwender in Webauftritten Datenschutzerklärungen abklicken. Juristische Texte, die kaum zu Transparenz beitragen, zumal Informatiker und Juristen nicht einmal bei so grundlegenden Begriffen wie «Identifizieren» und «Authentisieren» zu einem gemeinsamen Verständnis gefunden haben. Eine Ontologie, welche beispielsweise die Begriffswelt des Standards eCH-0107 «IAM-Gestaltungsprinzipien» mit jener aus dem E-ID-Gesetz (BGEID) verknüpft, könnte solche Unterschiedlichkeiten überwinden helfen.

Vertrauen müssen zuerst die Anspruchsgruppen untereinander finden. Danach erst können sie Vertrauen zu den Organisationen schöpfen, welche mit den Abläufen zur Verwaltung von Identitäten und Daten betraut werden. Und erst zuletzt geht es um das Vertrauen auf

technischer Ebene zu den IT-Systemen. Ausbildung, eine gemeinsame Sprache, Information und Transparenz sind die Schlüssel hierzu.