Das digitale Ich im Cyberspace

13.03.2015 | 18:49 | Martin Walpot (Die Presse)

Sicherheitsforschung. Eine österreichische Studie durchleuchtet digitale Identitäten im technischen, sozialen und rechtlichen Kontext. Der Umgang mit persönlichen Daten im Internet muss sicherer und selbstbestimmter werden.

Facebook, E-Banking oder Online-Shopping. Jeder von uns benutzt tagtäglich digitale Identitäten. Durch den Wandel von analog zu digital nimmt die Zahl der digitalen Identitäten (ID) weiter zu, was viele Grundfragen aufwirft: Wie können wir uns in Zukunft gegenseitig identifizieren? Wie sicher sind derzeitige ID-Technologien? Wie sehen rechtliche Rahmenbedingungen aus? Was tun Entscheidungsträger, Industrie und die Forschungsgemeinschaft, um uns auf den risikobewussten und verantwortungsvollen Umgang mit ID vorzubereiten?

Die Studie „DigID – Digitale Identitäten" widmete sich den Fragen – durchgeführt vom Austrian Institute of Technology AIT und dem Wiener Zentrum für sozialwissenschaftliche Sicherheitsforschung Vicesse, gefördert vom Sicherheitsforschungsprogramm Kiras des Technologieministeriums. „Wir haben soziale, rechtliche, technische und sicherheitsrelevante Aspekte angeschaut und eine Roadmap erstellt, die in Österreich eine vertrauenswürdige Umgebung für ID bereitstellen soll", so Thomas Bleier vom AIT.

Digitale Identitäten haben viele Vorteile: Einzelpersonen können persönlichen Geschäften online nachgehen, Unternehmen Geschäftsmodelle im Internet entwickeln, Regierungen ihre Online-Dienste erweitern, um Bürgern mehr Effizienz und Transparenz zu ermöglichen. Außerdem erschweren IDs die Cyberkriminalität, indem sie Probleme wie Identifizierung und Zugriffskontrolle lösen.

Ihr Nachteil: Die Identitätstechnologien müssen zuverlässig sein. Reinhard Kreissl, CEO von Vicesse: „Heute gibt es zwei Hauptkräfte, die die Sicherheit von digitalen Identitäten vorantreiben: Der Staat und die Privatwirtschaft."

Staat und Industrie nutzen ID

Staatliche Unternehmen nutzen nationale ID-Programme, die Daten abfragen, wie sie in Ausweisdokumenten vorkommen: Sie unterliegen der höchsten Sicherheitsstufe und werden bei Steuererklärungen oder E-Votings abgefragt. Identity-Provider der Privatwirtschaft hingegen nutzen persönliche Informationen, wie es sie in Social Media, E-Mails oder Online-Shopping-Profilen gibt. Zum Datenschutz werden unterschiedliche Mechanismen eingesetzt: darunter kryptographische Verschlüsselungsmechanismen, die eine Zugangsbeschränkung einrichten.

Um die Sicherheit zu erhöhen, sollen künftig weniger Informationen gespeichert werden. Die Selbstbestimmung des Einzelnen über die Verbreitung persönlicher Daten muss gewahrt sein. Ein Stufen-System soll es Anwendern ermöglichen, selbst zu bestimmen, was an Dritte weitergegeben werden darf. „Aber Technik allein ist zu wenig, um das Vertrauen in den Cyberspace zu fördern und nicht den fälschlichen Eindruck des ‚gläsernen Menschen' entstehen zu lassen", meint Kreissl. Dazu sind Gesetze, reaktive Kontrollen, angemessene Strafen und Aufklärungsarbeit für einen selbstbestimmteren Umgang mit ID notwendig.