Ralf Bendrath

Digitale Identität – ein Systemfehler oder ein Charakteristikum des Web 2.0?

„Das Internet ist so beschaffen, dass man nicht wissen kann, wer sich mit wem wozu verbindet." Dies ist der erste Satz des Manifests *Laws of Identity*[1], das Kim Cameron, Microsofts Experte für Identitätsmanagement, im Mai 2005 veröffentlichte. An und für sich nichts Neues, da die Online-Anonymität schon seit dem frühen Usenet ein heißes Thema war. 1993 wurde Peter Steiner bei den „Netzbürgern" mit seinem im Wochenmagazin *New Yorker* publizierten Cartoon *On the internet, nobody knows you're a dog* (Im Internet weiß niemand, dass du ein Hund bist) berühmt. Stimmt man dieser Aussage zu, dann stellt sich als nächstes die Frage: Ist das ein Systemfehler oder ein Charakteristikum? Während zumindest die Hunde im Cartoon diese Eigenheit mochten, wird es von Kim Cameron und vielen anderen als Systemfehler betrachtet.

Was ist überhaupt Identität? Eine minimale Definition würde enthalten, dass ein Ding oder eine Person nach Ablauf einer gewissen Zeit immer noch das- bzw. derselbe ist. Dies klingt recht einfach, doch haben sich Philosophen von der Antike bis in die Gegenwart den Kopf darüber zerbrochen. Bereits Buddha stellte die Frage: „Vor Jahren warst du ein kleines Kind, dann ein Knabe, dann ein Jugendlicher und jetzt bist du ein Mann. Sind dieses Kind und der Mann ident?"

Zu kompliziert für die heutige IT-Welt? Lassen Sie mich Ihnen Alice, Bob und Eve vorstellen, die berühmt wurden, weil ein paar Kryptografen ihre Geschichte erzählten.[2] Alice und Bob hatten vor zehn Jahren auf der Highschool eine Affäre, doch dann zog Bob nach Linz, und sie verloren sich aus den Augen. Bob liebt jetzt Eve. Eines Tages kommt Alice nach Linz zu einer Konferenz über elektronische Kunst. Sie geht am Abend aus und sieht einen Mann an der Bar stehen. Sie überlegt: Ist das nicht Bob, meine verflossene High-School-Liebe? Und wenn dieser Mann wirklich Bob ist, ist er dann noch der alte Bob, mit dem sie so oft ins Kino ging? Was, wenn sie nach all den Jahren noch Gefallen aneinander fänden und den einen oder anderen Drink nähmen? Und wenn in dieser Nacht etwas geschehen würde, was Bob am nächsten Morgen bereuen könnte – weil Eve, seine Freundin, nichts davon wissen dürfte?

Der britische Philosoph John Locke beschäftigte sich bereits um 1690 mit solchen Fragen. In seinem Essay „Versuch über den menschlichen Verstand" stellte er die Frage: „Ist ein Mensch dieselbe Person, wenn er betrunken und wenn er nüchtern ist? Warum sonst sollte er für etwas bestraft werden, was er im betrunkenen Zustand getan hat, obwohl er sich gar nicht mehr daran erinnert?" Übertragen auf die Online-Welt ließe sich die Frage so formulieren: Wer ist man, wenn man online ist? Noch dieselbe Person wie im realen Leben? Was wäre, wenn Alice *Second Life* einen Besuch abstatten und dort Bob treffen würde?

Web 1.0 und Web 2.0 – von der Dokumentenverlinkung zur Vernetzung von Personen und Kontexten

Im Web 1.0 stellten sich diese Fragen nicht. Es wurde als gigantischer Server zur Speicherung von Dokumenten, als erweiterter FTP-Server betrachtet. Die Abstimmung der realen Identität auf Online-Aktivitäten war kein Thema. Anonymität und Pseudonyme waren von großer Bedeutung, sie waren cool und eröffneten Möglichkeiten für Experimente. So konnte Bob beispielsweise online in die Rolle von Alice schlüpfen, um herauszufinden, wie man sich als Frau fühlt. Und Eve konnte sich als Mann ausgeben – oder sogar als Hund. Oder wurde Eve gar von einem Hund gespielt?

Es gibt zwei Identifikationssysteme, die im Internet Verwendung finden: Das wichtigere ist die IP-Adresse, über die Computer identifiziert werden und kommunizieren können. In der Zeit vor dynamisch zugewiesenen IP-Adressen und Internet-Cafés konnte sie im Grunde genommen als Identifikationssystem für Personen verwendet werden. Man musste nur herausfinden, welcher Computer welche IP-Adresse hatte (was natürlich nicht besonders einfach ist, wenn der Administrator eines gewissen Adressbereichs sich am anderen Ende der Welt befindet und nicht kooperationsbereit ist). Die zweite Identifikationsmöglichkeit ist das *Domain Name System,* das die eindeutige Benennung von E-Mail-Adressen, Websites und anderen Diensten ermöglicht. Die langwierige Auseinandersetzung innerhalb der ICANN (Internet Corporation for Assigned Names and Numbers), wer weshalb Zugang zur WHOIS-Datenbank hat, zeigt deutlich, dass selbst im Web 1.0 die Anonymität nie zur Gänze gewährleistet, sondern vielmehr stark infrage gestellt war. Als Faustregel gilt, dass man bei dynamischen IP-Adressen und anonymen oder über Proxy-Server registrierten Webdiensten nicht mit Sicherheit herausfinden kann, mit wem man in Verbindung tritt.

Seit dem Web 2.0 ist das anders. Es geht nicht mehr um die Verlinkung von Dokumenten, sondern um die Vernetzung von Personen. Die Menschen scheinen das Bedürfnis zu haben, ihre Online- und Offline-Identitäten aufeinander abzustimmen, diese mit anderen auf nachvollziehbare Weise zu vernetzen und die Welt an dieser Kommunikation teilhaben zu lassen. Und sie scheinen sich vernetzen zu wollen – schließlich ist der Mensch ein Gesellschaftstier. Dies ist vermutlich auch einer der Gründe dafür, warum Netzwerkplattformen wie *MySpace, Xing, Friendster, Facebook* oder selbst das berühmt-berüchtigte deutsche Netzwerk für Studierende *StudiVZ* so beliebt sind.

Auf diesen Plattformen wird nicht nur ein soziales Netzwerk (oder korrekter: das technische Abbild eines sozialen Netzwerks) aufgebaut, sondern auch eine Reputation und ein Image. Wie sieht das Bild eines Mitglieds aus? Wie viele Freunde hat er bzw. sie? Was schreiben diese in sein Gästebuch? Ist das Layout seiner Präsentation ansprechend? Auch als Amazon-Testleser, *eBay*-Verkäufer oder *Flickr*-Fotograf etc. baut man sich einen Ruf auf. Alice überlegte: Wäre es nicht cool, wenn ich mein günstiges Slashdot-Karma für *eBay* verwenden könnte? Oder mein *eBay*-Bewertungsprofil für *MySpace?* Sie fand heraus, dass es keinen wirklichen Standard für den Austausch von Profilen gab. Dies liegt daran, dass Alices Profil bei *Slashdot* nicht viel über ihre Verlässlichkeit als *eBay*-Verkäuferin aussagt. Tatsächlich ermöglicht der Aufbau dieser Identifikationssysteme den jeweiligen Benutzern nur, eine Identität und soziale Beziehungen innerhalb ihrer Systeme aufzubauen, wodurch sie eigentlich zu monolithischen Informationsbunkern werden. Wieder stellt sich die Frage: Ist das ein Systemfehler oder ein Charakteristikum?

Soziologen bezeichnen diese Grundlage komplexer Gesellschaften als „funktionelle Differenzierung". Georg Simmel beschrieb 1907 in seinem Essay „Das Geheimnis und die geheime Gesellschaft"[3] bereits detailliert, wie wichtig es ist, dass verschiedene Menschen unterschiedliche Dinge über einen wissen. Bobs Freundin Eve weiß andere Dinge über ihn als sein Chef, und sein Bankbetreuer wiederum andere Einzelheiten als die Mitglieder seiner Bowlingmannschaft. Man spielt mit verschiedenen Menschen verschiedene Rollen. Und manchmal ist es sogar wichtig, dass diese Rollen nicht miteinander in Verbindung stehen. Ähnlich wie Simmel versuchte Helen Nissenbaum kürzlich eine neue normative Grundlage für „Privatheit als kontextuelle Integrität" zu formulieren: Informationen über Personen entstehen überall, Privatheit beruht aber darauf, dass diese nicht aus ihrem Kontext gerissen werden – oder dass ein Transfer zumindest von dem Betroffenen kontrolliert wird.

Aber wenn nun die Leute die verschiedenen Kontexte, in denen sie aktiv sind, verknüpfen *wollen?*

Es gibt kein definiertes Interface, um das persönliche Profil etwa auf *Xing* mit dem auf *MySpace* zu verknüpfen. Man kann sein Google-Checkout-Konto benützen, um Zugang zu verschiedenen Google-eigenen Diensten zu erhalten, der Zugang zu *Yahoo* oder anderen Systemen bleibt einem aber verwehrt. Aus diesem Grund gibt es einen Trend zu offenen Identifikationsstandards und Protokollen für das Internet, die dem User zusätzliche Kontrollmöglichkeiten bieten und ihm ermöglichen, in diese abgegrenzten Zonen einzudringen. Die Diskussion darüber wird unter dem Schlagwort „benutzerzentrierte Identität" geführt.

Digitale Identität 2.0 – Technologie, neu entstehende Protokolle und Privatheit

Ansätze für eine benutzerzentrierte Identität sind etwa einfache HTML-Tweaks (Mikroformate) wie die vCard, eine maschinenlesbare Visitenkarte, die man auf seine Website stellen kann und die Metadaten-Tags über den User, Kontaktinformationen oder Hinweise auf eine etwaige institutionelle Anbindung enthält. Solche Visitenkarten sind natürlich einfach herzustellen. Jeder kann eine vCard auf seine Website stellen und sich als eine andere Person ausgeben. Sind die Informationen auf der vCard korrekt, dann sind sie auch ein gefundenes Fressen für Spambots. Außerdem weiß man nicht, ob eine vCard für Lieschen Müller sich auf dieselbe Person bezieht wie eine andere vCard auf einer anderen Website, die für besagtes Lieschen Müller andere Kontaktinformationen angibt. Es könnte dieselbe Frau Müller sein, die nun bei einer anderen Firma arbeitet, oder auch eine völlig andere Person. Was hier fehlt, ist ein definierter Adressraum, wie ihn das Domain-Name-System hat.
Ausgeklügeltere Ansätze beruhen auf Methoden, die mit Identifikatoren arbeiten, die URLs ähneln. „iNames" ist ein solches Projekt; es basiert auf Extensible Resource Identifiers (XRI) und wurde vom OASIS-Konsortium entwickelt. Vergleichbar mit Domänennamen kann man seinen iName bei einer zentralen Registrierungsstelle registrieren. Diese Mittler werden im Allgemeinen Identity Provider genannt. Sie bestätigen gegenüber anderen Diensten, dass man berechtigt ist, einen bestimmten Namen oder Identifikator zu verwenden – oder noch einfacher: Sie übernehmen die Authentifizierung einer Person gegenüber anderen Parteien. Im Gegenzug muss man sich natürlich bei jeder Transaktion, die man tätigt, auf diese vertrauenswürdigen dritten Parteien verlassen.
Es gibt einige ähnliche Protokolle und Ansätze, die sich in den letzten Jahren entwickelt haben: MicroID, Lightweight Identity (LID), OpenID, Yadis, Secure Authentication Markup Language (SAML), ID-WSF, Windows Cardspace, Higgins, Shibboleth und andere. Einige davon, wie OpenID, MicroID, LID und Higgins, haben sich aus der Blogger- und Web-2.0-Szene entwickelt. Andere werden von großen IT-Konzernen wie Microsoft (CardSpace) oder der Liberty Alliance, der Sun, Oracle und andere angehören (ID-WSF), forciert. Wieder andere gingen aus diversen formellen oder informellen Organisationen hervor, die sich mit der Weiterentwicklung von Standards für Webdienste beschäftigen, wie OASIS (SAML) oder ITU (X.509). Aufgrund der verschiedenen Ansätze haben einige dieser Organisationen wie etwa W3C, ISO und ANSI vor kurzem Arbeitsgruppen zum Identitätsmanagement eingerichtet. In näherer Zukunft sind also heftige Auseinandersetzungen um die neuen Standards zu erwarten. Die derzeit interessantesten Ansätze im Web-2.0-Kontext verfolgen Microsofts CardSpace, der mit Windows Vista ausgeliefert wird, und OpenID, das sich aus dem losen Netzwerk rund um Identity Gang und die Internet-Identity-Workshop entwickelte. In diesem Zusammenhang ist das technische Design von großer Bedeutung, da es hinsichtlich Rückverfolgbarkeit und Verlinkung große Unterschiede gibt. Es ist inte-

ressant, dass Microsofts „Cardspace“ tatsächlich die Privatsphäre stärker berücksichtigt als der von der Community forcierte Standard OpenID. Während OpenID ein einfacher Single-Sign-On-Dienst ist, bei dem der ID-Provider eine zentrale Rolle spielt und alle Transaktionen kennt, muss der ID-Provider beim Modell Cardspace nicht unbedingt wissen, mit welchem Dienst man sich verbindet, und die verschiedenen Rollen, die man bei diversen Webdiensten spielt, können durch unterschiedliche und nicht miteinander verbundene Identifikatoren strikt getrennt werden.

Namensregeln und digitale ID-Karten – die Regierung als ultimativer Identitäts-Provider

Im Zentrum der Auseinandersetzung rund um das digitale Identitätsmanagement stehen die Identitäts-Provider. Sie registrieren meine unverwechselbare Identität, übernehmen die Authentifizierung gegenüber anderen und können alle meine Aktivitäten nachverfolgen. Corporate-Identity-Management-Systeme identifizieren die Angestellten von Unternehmen bereits seit geraumer Zeit. Sie verwenden Rollenkonzepte, um die verschiedenen Aufgaben, die ihre Angestellten übernehmen können, zu differenzieren. Wer darf das Betriebsgelände betreten? Wer hat Zugang zu welcher Datenbank? Wer kann Bestellungen bis zu welcher Auftragssumme abwickeln? Dies beschäftigte die Big Players wie Oracle, Novell oder Sun. Mit dem Ende der geschlossenen Firma und der Entwicklung der webbasierten Zusammenarbeit verbinden sich die Corporate-Identification-Systeme mit webbasierten ID-Standards. Die Anwendungsfälle der Identifikatoren werden hier normalerweise *Provisioning*, *Identity Federation* oder *Workflow Auditing* genannt. Letzten Endes geht es natürlich um die Kontrolle der Angestellten. Und Kontrolle ist auch eine der wesentlichen Funktionen des Identitätsmanagements.

Doch gibt es noch einen viel wichtigeren Akteur, dessen Rolle in der Identitätsdebatte oft übersehen oder ignoriert wird. Wer war der erste, der Identitätsmanagement und Identifikationssysteme eingeführt hat? Es war der moderne Staat in seiner Frühzeit. Im 15. Jahrhundert wurden die ersten Gesetze in Europa erlassen, denen zufolge es verboten war, seinen Namen im Lauf des Lebens zu verändern. Nun, um anderen zu beweisen, dass man die Person ist, deren Namen zu tragen man vorgibt, benötigt man einen Beweis in Form eines Identitätsnachweises. Erst waren dies offizielle Schreiben oder Siegel, im vergangenen Jahrhundert wurden dann Pässe und Personalausweise entwickelt und verbreitet. Heute wird von Regierungsseite versucht, mittels biometrischer Daten eine Verbindung zwischen dem Pass (der die Richtigkeit eines Namens bescheinigt) und dem Körper des einzelnen Bürgers herzustellen. Doch das Bedürfnis nach einer engeren Verbindung von Identitätsnachweisen (den Identifikatoren) und Personen (den Identifizierten) besteht schon viel länger. Jeremy Bentham, der auch das Konzept des Panoptikums entwickelte, schlug in seinem Essay *The Principles of Penal Law* vor 200 Jahren vor, dass man jedem Bürger seinen Namen auf den Arm tätowieren sollte. Diese Einschreibung eines Identifikators auf den Körper des Identifizierten ist lediglich eine radikalere Version der Fingerabdrücke im Pass. Zu Benthams Zeiten gab es noch keine biometrischen Fingerabdruck-Lesegeräte oder Iris-Scanner, weshalb ein deutlich sichtbarer Identifikator eine nahe liegende Lösung war.

Doch selbst heute wird eine Tätowierung nicht übermittelt, wenn man online ist. Daher wollen manche Regierungen jetzt eine offiziell zertifizierte Verbindung zwischen der realen und der Online-Identität einführen. Die Behörden, die Pässe und Personalausweise ausstellen, könnten dann auch die Identitäts-Provider für das Online-Leben werden. Der feine Unterschied ist: Die Behörden wissen nicht, wem ich meinen Pass zeige. Aber bei den meisten bestehenden digitalen Identity-Management-Systemen würden sie informiert, wenn ich mich gegenüber einer dritten

Partei mit einem von der Behörde ausgestellten digitalen Identitätsnachweis vorstelle. Dies würde offenkundig eine groß angelegte Überwachung und Kontrolle des Online-Verhaltens ermöglichen. Vor allem in Ländern wie Großbritannien und den USA, in denen Personalausweise keine Tradition haben, wehren sich die Menschen gegen die Vorstellung einer verpflichtenden Online-Identifikation.

Was macht also ein Sicherheitspolitiker, der ein solches System einführen möchte? Er beginnt bei Gruppen wie Ausländern oder Kriminellen. Der amerikanische Senat hat jetzt einen Gesetzesentwurf vorgelegt, der alle registrierten Sexualverbrecher zwingen würde, sämtliche E-Mail-Adressen und anderen Online-Identitäten den Behörden zu melden. Es ist ihr bitterer Ernst: Wer sich nicht registriert, dem drohen zehn Jahre Haft. Dies ist nicht etwa die Strafe für Vergewaltigung, sondern für das Vergehen, der Regierung nicht alle Online-User-Namen und Pseudonyme mitgeteilt zu haben.

Andere Länder mit einer längeren Überwachungs- und Kontrolltradition beginnen Online-Identifikationssysteme einzuführen, durch die die Internet-Nutzer gezwungen werden, sich mit ihrem wirklichen Namen zu registrieren. Südkorea entwickelt gerade eine *Real Name*-Regelung für Blogger, die verpflichtet wären, für Blog-Einträge und Kommentare ihren richtigen Namen zu verwenden. Die Volksrepublik China arbeitet an einem „System zur Überprüfung der Namensechtheit" für Blogger, aber auch für Online-Spiele. Dies zeigt erneut die Kontrollfunktion der Identitätssysteme. Neben der Überwachung und der Erstellung von Profilen ermöglicht es sowohl, das Internet in Zonen einzuteilen, als auch eine automatische Zugangskontrolle. Ähnliche Pläne gibt es bereits für das virtuelle Rotlichtviertel in *Second Life*.

Deutschland arbeitet gerade daran, seinen Ruf als hoch bürokratisches Land zu bestätigen. Das Programm *E-Government 2.0,* das das deutsche Innenministerium im September 2006 verabschiedete, enthält ein interessantes Kapitel über elektronische Personalausweise und *e-Identity*-Konzepte. Die Bundesregierung plant die Ausgabe eines elektronischen Ausweises ab 2008, der es Usern ermöglichen wird, sich online mit einem von der Regierung beglaubigten Identitätsnachweis auszuweisen. In Deutschland ist die Registrierung der Online-Identität bei den Behörden nicht „nur für Kriminelle", sondern für die gesamte Bevölkerung vorgesehen. Letzten Endes könnte es so weit kommen, dass die Regierung die Rolle des glaubwürdigen Dritten übernimmt und uns ein perfektes Identitäts-Management-System überstülpt, das jeden erfasst. Viele E-Commerce-Unternehmen wären zweifelsohne begeistert und würden die digitalen Personalausweise verwenden, um Betrügereien und anderen unerwünschten Aktivitäten vorzubeugen. Je nach technischer Auslegung wäre die Regierung als Provider der digitalen Identität dann in der Lage, das Verhalten der Bürger online nachzuverfolgen. Sie wäre jene erwähnte dritte Partei, die höchste Instanz in puncto Glaubwürdigkeit. Noch einmal: Ist das ein Systemfehler oder ein Charakteristikum?

Aus dem Englischen von Martina Bauer

1 *http://www.identityblog.com/stories/2004/12/09/thelaws.html*
2 A. d. Ü.: Alice und Bob sind in der Kryptografie Synonyme für Sender und Empfänger einer Nachricht.
3 Simmel, Georg: in *Soziologie. Untersuchungen über die Formen der Vergesellschaftung,* Duncker & Humblot Verlag, Berlin 1908, S. 256–304