Der Landesbeauftragte
für den Datenschutz Rheinland-Pfalz

Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Datenschutzförderndes Identitätsmanagement

Arbeitskreis „Technik“
der Datenschutzbeauftragten
des Bundes und der Länder

Version 1.0
Stand: 5. März 2008

Datenschutzförderndes Identitätsmanagement

Hintergrundpapier zur Entschließung

„Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen“

der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 3./4. April 2008 (siehe Anlage)

(http://www.datenschutz.rlp.de/de/ds.php?submenu=grem&typ=dsb&ber=075_idman)

Autoren: Marit Hansen (ULD Schleswig-Holstein)
Martin Rost (ULD Schleswig-Holstein)
Gabriel Schulz (LfDI Mecklenburg-Vorpommern)
Sven Thomsen(ULD Schleswig-Holstein)
Rüdiger Wehrmann (Der Hessische Datenschutzbeauftragte)

Datenschutzförderndes Identitätsmanagement

Einleitung

Es gibt vielfältige Definitionen für Identitätsmanagementsysteme. Jedoch nicht alle Systeme, die Identitäten – in welch komplexer Form auch immer – verwalten, sind allein deshalb schon als Identitätsmanagementsystem zu bezeichnen. Eine mögliche Definition liefert Wikipedia: Identitätsmanagement ist demnach ein zielgerichteter und bewusster Umgang mit Identität, Anonymität und Pseudonymität. Aus datenschutzrechtlicher Sicht gehört zum Identitätsmanagement aber insbesondere die Möglichkeit, über die Verwendung seiner eigenen Identitätsinformationen selbst entscheiden bzw. verschiedene Identitäten zu unterscheiden und zwischen diesen auswählen zu können.

Der in den aktuellen Diskussionen zum Thema Identitätsmanagement oft erweckte Eindruck, es handele sich dabei um eine neue Entwicklung, ist nicht richtig. Ein Ziel des Datenschutzes war es schon immer, Persönlichkeitsprofile zu verhindern. Keinesfalls sollten Daten einer Person verknüpft werden können, die in verschiedenen Anwendungsfällen mit kontextspezifischen Identitäten agiert. Ohne Identitätsmanagement ist dieses Ziel kaum zu erreichen.

In vielen Gesetzen ist das Grundprinzip von Identitätsmanagement bereits umgesetzt. Es gibt zahlreiche Regelungen, nach denen Betroffene nur in einem bestimmten Kontext durch die ihnen zugeordneten Daten identifiziert werden dürfen. Die Verknüpfung von Daten aus mehreren Bereichen wird dort untersagt. Beispiele hierfür sind das Personalausweisgesetz (PersAuswG), die Abgabenordnung (AO) oder das Telemediengesetz (TMG):

• Im PersAuswG wird geregelt, dass die Seriennummer nicht zum Abruf personenbezogener Daten oder zur Verknüpfung verwendet werden darf; Ausnahmen sind im Gesetz abschließend aufgeführt.

• Die AO legt fest, dass die Steuer-Identifizierungsnummer nur im steuerlichen Kontext genutzt werden darf.

• Im TMG wird gefordert, die Nutzung von Telemedien auch anonym oder pseudonym zu ermöglichen, soweit es technisch möglich und – für den Anbieter – zumutbar ist. Im Falle von pseudonymen Nutzungsprofilen dürfen diese nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden.

Hieran wird deutlich, dass eine kontextspezifische Identität eher der Regelfall als die Ausnahme sein soll. Weder Behörden noch Firmen sollen Daten aus verschiedenen Bereichen einfach verketten oder verknüpfen können und dürfen. Wirtschaft und Verwaltung speichern und verarbeiten jedoch immer häufiger personenbezogene Daten in digitaler Form, ohne die Grundsätze des Identitätsmanagements zu berücksichtigen. So entstehen gerade im Umfeld von Egovernment und E-Commerce viele Sammlungen personenbezogener Daten in öffentlichen und privaten Datenbanken, die zumindest aus technischer Sicht Verknüpfungen einfach zulassen. Es muss aber auch künftig möglich

sein, sich unter einer Identität beispielsweise in Chatrooms zu unterhalten, unter einer anderen Identität Musik herunterzuladen und mit einer dritten unabhängig davon Landkarten zu bestellen.

Damit Daten nur im jeweiligen Zusammenhang einer bestimmten Identität und damit Person zugeordnet werden können, müssen technische Verfahren entwickelt und zur Verfügung gestellt werden, die die Nutzerinnen und Nutzer unterstützen. Müssen Betroffene in einer bestimmten Anwendung beispielsweise nachweisen, dass sie volljährig sind, so sollen sie wie im täglichen Leben trotzdem ohne Preisgabe ihrer Personalien handeln können. Dazu müssen sie aber in die Lage versetzt werden, ihre verschiedenen digitalen Identitäten sicher zu verwalten.

Technische Systeme, die Nutzerinnen und Nutzer dabei unterstützen, sind bereits verfügbar. So können schon jetzt Anonymisierungsdienste genutzt werden und es gibt bereits zahlreiche Entwicklungen, die ein datenschutzgerechtes Identitätsmanagement ermöglichen. Beispielsweise können mit so genannten Credentials elektronischen Beglaubigungen ausgegeben werden, die etwa die Volljährigkeit nachweisen, ohne weitere persönliche Daten preiszugeben.

Entscheidend für den Erfolg solcher Entwicklungen werden jedoch Art und Details der jeweiligen Umsetzungskonzepte sein. Würden Beglaubigungen zentral ausgegeben und die ausgebende Stelle würde für jede Person erfahren, wann sie welche Beglaubigung für welchen Zweck benötigt, wäre eine Profilbildung leicht möglich. Solche Konzepte wären mit Datenschutzgrundsätzen nicht vereinbar. Würde die Steuerung hingegen allein durch Betroffene selbst erfolgen, wäre die Gefährdung der Verfügbarkeit nicht auszuschließen.

Diese Beispiele verdeutlichen, dass die Datenschutzbeauftragten bereits bei der Normung und Spezifikation solcher Verfahren beratend tätig werden sollten, um für den Bürger datenschutzgerechte und praktikable Lösungen zu finden.

Das Papier soll den engen Zusammenhang zwischen Datenschutz und Identitätsmanagement verdeutlichen und aufzeigen, welche Vorgehensweise die Datenschutzbeauftragten empfehlen. Dazu wird nach einer Definition des Begriffs Identitätsmanagement auf mögliche Ausprägungen eingegangen, es werden Lösungen beschrieben und Maßnahmen vorgeschlagen.

Was ist Identitätsmanagement?

Der Begriff Identitätsmanagement (englisch: „Identity Management“) wird in vielen Variationen und mit durchaus unterschiedlicher Bedeutung und Zielrichtung verwendet. Identitätsmanagement wird häufig als zusammenfassende Beschreibung für die Prozesse der Authentifizierung (englisch: „Authentication“), der Autorisierung (englisch: „Authorization“) und einer Protokollierung (englisch: „Accounting“) aufgefasst. Diese auch als Triple-A oder AAA bezeichneten Prozesse bilden die Grundlage sämtlicher geordneter Datenverarbeitung.

Die Authentifizierung bildet hierbei die Grundlage für alle weiteren Schritte. Durch Eingabe einer Benutzerkennung und eines geheimen Passworts oder ergänzend durch biometrische Verfahren weisen die Nutzenden gegenüber dem System nach, dass wirklich sie den Zugang beispielsweise zu einem Rechnersystem erhalten möchten (Zugangskontrolle).

Aufbauend auf einer Authentifizierung werden den Nutzenden dann Berechtigungen zum Beispiel zur Verarbeitung personenbezogener Daten gewährt. Häufig werden hierzu Rechte- und Rollenmodelle verwendet, die einer Zugangskennung eine Rolle zuweisen. Der Rolle sind dann spezifische Rechte zur Datenverarbeitung zugewiesen (Zugriffskontrolle).

Die bei der Datenverarbeitung durchgeführten Schritte oder Operationen werden dann zusätzlich protokolliert. Die Protokollierung kann hierbei die Aufzeichnung lediglich ändernder Operationen im Sinne einer „Administrator-Protokollierung“ oder aber auch einen vollständigen Mitschnitt aller Nutzungsaktivitäten umfassen.

Beispiel: Eine Sachbearbeiterin in einer öffentlichen Verwaltung meldet sich mit Benutzername und Passwort an ihrem PC-Arbeitsplatz an. Der hierfür verwendeten Kennung sind Berechtigungen in der Dateiablage, dem Gruppenkalender und in einzelnen Fachverfahren zugeordnet. Zur Berechtigungsverwaltung wird ein Verzeichnisdienst verwendet, der zentral sämtliche Informationen über Zugangsberechtigungen vorhält und zur Modellierung eines Rechte- und Rollenmodells genutzt wird. Die Anbieter solcher Verzeichnisdienste vermarkten ihre Lösungen häufig unter dem Begriff „Identitätsmanagement“. Die Zugriffe auf einzelne Bereiche der Dateiablage – zum Beispiel Personaldaten – sowie Aktionen in Fachverfahren – zum Beispiel in einem Kassenverfahren – werden protokolliert.

Datenschutzrelevante Aspekte ergeben sich bei dieser Form des Identitätsmanagements zum Beispiel im Bereich des Mitarbeiterdatenschutzes beim Verhindern einer automatisierten Verhaltens- und Leistungskontrolle. Eine andere Ausprägung des Identitätsmanagements befasst sich mit dem Umgang mit personenbezogenen Informationen vor allem im Bereich der Werbung. Diese häufig als „Profiling“ bezeichnete Datenverarbeitung dient vor allem dazu, die über eine Person vorhandenen Daten zusammenzuführen und gemäß charakteristischen Merkmalen zu gruppieren. Häufig werden hierzu Daten aus unterschiedlichen Quellen zusammengeführt.

Der Umgang mit Identitäten, das Anreichern des Datenbestands durch Verketten mit anderen Informationen, die Profilbildung und die gezielte Weiterverwendung wird auch unter dem Begriff Identitätsmanagement zusammengefasst.

Beispiel: Ein Kunde einer Warenhauskette verfügt über eine Bonuskarte. Durch das Vorzeigen der Bonuskarte wird jede vom Kunden gekaufte Ware personenbezogen mit ihm verbunden. Die Daten der hierfür verwendeten Kassensysteme werden zentral zusammengeführt. Aus den einzelnen Transaktionen wird dann ein Profil gebildet, welches beispielsweise für gezielte Werbeaktionen genutzt werden kann. So könnte eine Werbeaktion für eine neue Generation von Abspielgeräten gezielt auf die Gruppe der

häufigen Käufer von Filmen ausgerichtet werden. Häufig werden jedoch auch Daten von Dritten mit den vorhandenen Daten verknüpft. Dadurch können dann genauere Aussagen über den Kunden getroffen werden: Wo wohnt der Kunde? Welche Rückschlüsse lässt dies auf seine finanzielle Situation zu? Ist der Kunde auch bei Partnerunternehmen aktiv? Was hat er dort gekauft?

Datenschutzrelevante Aspekte ergeben sich bei dieser Form des Identitätsmanagements vor allem im Bereich des Kundendatenschutzes bei der Gestaltung einer transparenten Datenverarbeitung und -weitergabe. Eine weitere Variante des Begriffs Identitätsmanagement befasst sich mit der Steuerung der Preisgabe personenbezogener Informationen durch den Nutzer. Dieses nutzergesteuerte Identitätsmanagement soll es einer Person ermöglichen, das Recht auf informationelle Selbstbestimmung gerade in komplexen und in allen Auswirkungen nicht mehr durchschaubaren Verfahren der automatisierten Datenverarbeitung auszuüben.

Beispiel: Einfache Varianten des nutzergesteuerten Identitätsmanagements finden sich bereits in aktuellen Browsern und E-Mailprogrammen. Die Anwendenden können beim Start oder bei der Benutzung des Programms unterschiedliche Identitäten – manchmal auch Profile genannt – auswählen. Mit diesen Profilen ist dann eine bestimmte Menge an personenbezogenen Daten verknüpft, die beispielsweise beim E-Mailprogramm die Absenderadresse und den Abspann einer E-Mail setzen. Ein anderes Beispiel sind Funktionen des Browsers zum halbautomatisierten Ausfüllen von Formularen. In Abhängigkeit der gewählten Identität werden Registrierungsformulare ausgefüllt, aber auch andere persistente Informationen wie Cookies verwaltet. Es gibt bereits Ansätze, diese Art des Identitätsmanagements in den verwendeten Betriebssysteme zu verankern oder aber als Dienstleistung im Netz anzubieten.

Datenschutzrelevante Aspekte ergeben sich bei dieser Form des Identitätsmanagements vor allem bei Design und Umsetzung von datenschutzfördender Technik (englisch: Privacy Enhancing Technologies, PET).

Was ist datenschutzförderndes Identitätsmanagement?

Wie bei jeder Datenverarbeitung mit Personenbezug ist auch beim Einsatz von Identitätsmanagementsystemen generell das Datenschutzrecht zu beachten, insbesondere mit seinen Anforderungen an Zulässigkeit der Verarbeitung, Erforderlichkeit, Zweckbindung, Transparenz, Wahrung der Betroffenenrechte sowie technischorganisatorischen Maßnahmen.

Beim nutzergesteuerten Identitätsmanagement steht das Recht der Nutzenden auf ihre informationelle Selbstbestimmung im Vordergrund. Die folgenden Bausteine sind wesentlich für ein umfassendes nutzergesteuertes Identitätsmanagementsystem. Sie wurden prototypisch im Projekt „PRIME – Privacy and Identity Management for Europe“ im Zusammenspiel von Client- und Serversoftware realisiert, sind aber auch losgelöst von der technischen Implementierung für Identitätsmanagementsysteme allgemein relevant:

Kontrolle durch die Nutzenden beim Verwalten ihrer digitalen Identitäten

Die Nutzenden sollen so detailliert wie möglich steuern können, wem sie welche Daten unter welchen Bedingungen herausgeben. Das kann je nach Kommunikationspartner völlig unterschiedlich sein. Im Arbeitskontext verhalten sich Nutzende beispielsweise meist anders als in ihrer Freizeit. Bedingung ist ein hohes Maß an Transparenz in Bezug auf die personenbezogenen Daten und ihre Verarbeitung. Wenn Nutzende keine Wahlmöglichkeiten haben (z.B. in vielen E-Government-Prozessen, in denen gesetzlich vorgegeben ist, welche Daten zu nennen sind), sollen sie zumindest wissen können, was mit ihren Daten geschieht. Einige nutzergesteuerte Identitätsmanagementansätze unterstützen die nötige Transparenz wesentlich, indem transaktionsbezogen protokolliert wird, welche Daten herausgegeben wurden. Diese Protokollierung ermöglicht den Nutzenden ein späteres Nachvollziehen, wem sie was unter welchen Bedingungen offenbart haben. Auch Datenschutzerklärungen einer datenverarbeitenden Stelle lassen sich hier mitspeichern.

Separierung unterschiedlicher Bereiche

Die Datensparsamkeit wird auch unterstützt durch die Separierung von Kontexten, d.h. die Trennung von Daten in verschiedenen Domänen. Ziel ist die Kontrolle einer möglichen Verkettung von Informationen über verschiedene Bereiche hinweg. Das Grundkonzept wurde bereits Mitte der 1990er Jahre von John Borking im Rahmen des von ihn skizzierten
„Identity Protectors“ vorgeschlagen (Borking, 1996; Hes/Borking, 1998): Logisch trennbare Bereiche werden auch technisch separiert, z.B. indem Kennungen und Identifikatoren nicht mit globaler Gültigkeit (und globaler Verkettbarkeit) verwendet werden, sondern unterschiedliche Bezeichner pro Bereich eingesetzt werden. Diese Bereiche kann man als verschiedene „Pseudonym Domains“ (ULD/SNG, 2003) verstehen, in denen Bezeichner („Pseudonyme“ im allgemeinen Sinn) lokale Gültigkeit haben. Sie können Schnittstellen zueinander haben, an denen in vordefinierten Fällen Bezeichner durch technische oder organisatorische Maßnahmen umgerechnet werden können. Auf diese Weise lassen sich Workflows generell daraufhin analysieren, wo sich Aufgabenbereiche und zugehörige personenbezogene Daten voneinander abgrenzen lassen.

Eine technische Separierung verschiedener Bereiche sollte durch eine organisatorische Trennung unterstützt werden, z.B. durch Festlegung getrennter Verantwortlicher mit eben nicht übergreifenden Zugriffsrechten oder sogar durch die Erbringung der Aufgaben durch verschiedene juristische Personen, die nicht bereichsübergreifend zuständig sind.

Anonyme oder pseudonyme Nutzung

Sobald personenbezogene Daten herausgegeben sind, kann die Nutzenden sie nicht mehr selbst vor Missbrauch schützen. Daher ist Datensparsamkeit Primärziel: Es soll verhindert werden, dass Unberechtigte Daten zu einem Nutzer oder auch Datensätze untereinander verketten können. In vielen Konstellationen sind identifizierende

Informationen für die Inanspruchnahme von Diensten in der Online-Welt auch gar nicht nötig. Ist eine längerfristige Kommunikationsbeziehung gewünscht, sollten Pseudonyme verwendet werden, die möglichst spezifisch für den jeweiligen Anwendungszusammenhang sind (kontextspezifisch), um eine übergreifende Verkettung und damit eine umfassendere Profiling-Möglichkeit zu erschweren.

Einsatz von Credentials

Immer wieder ist es in der Online-Welt notwendig, dass Nutzende Berechtigungen, so genannte Credentials, nachweisen, z.B. über die Volljährigkeit, Mitgliedschaften, Berufsgruppenzugehörigkeit o.ä. Bei so genannten privaten Credentials (auch: „pseudonymous convertible credentials“) können Transaktionen, die von ein und demselben Nutzer ausgeführt werden, nicht unmittelbar verkettet werden – sie kombinieren Zurechenbarkeit und Datensparsamkeit (Chaum, 1985; Camenisch/Lysyanskaya, 2000). Basierend auf kryptographischen Protokollen leiten die Nutzenden ihre privaten Credentials von einem Masterzertifikat ab. Die privaten Credentials können sie an verschiedene Pseudonyme binden. Dadurch erreicht man, dass ein mehrfaches Vorzeigen eines solchen Zertifikats in Form von verschiedenen Credentials für den Empfänger der Daten oder Beobachter nicht verkettbar ist. In vorher zu definierenden Fällen von Missbrauch kann reagiert werden, indem eine eingeschaltete vertrauenswürdige Stelle den Namen der Nutzenden aufdeckt oder indem ein Mehrfachverwenden des Zertifikats technisch unterbunden wird, ohne die Anonymität der Nutzenden aufzuheben.

Transparenz über Datenschutzbedingungen und Aushandlungsmöglichkeiten

Die Bedingungen, unter denen Nutzende ihre Daten offenbaren sollen, werden heutzutage meist vom Diensteerbringer vorgegeben. Sie stehen in der Regel in sog. Datenschutzerklärungen („Privacy Policies“), werden aber oft gar nicht zur Kenntnis genommen. Um diese Datenschutzerklärungen verständlicher zu gestalten und die wichtigsten Fakten auf einen Blick sichtbar zu machen, hat die Art. 29-Datenschutzgruppe den Einsatz strukturierter, mehrstufiger Erklärungen („Layered Policies“) vorgeschlagen (Art. 29-Datenschutzgruppe 2004, Arbeitspapier 100 vom 25.11.2004). Ein nutzergesteuertes Identitätsmanagementsystem soll die Policies mit den Vorgaben der Nutzenden automatisiert abgleichen und ihn bei Abweichungen warnen. Die vereinbarten Datenverarbeitungsregeln werden zur besseren Nachvollziehbarkeit mitgespeichert. Auch Aushandlungen sollen möglich sein, wobei jedoch darauf zu achten ist, generell ungünstige Kompromisse zu Lasten der Nutzenden zu vermeiden. Hier ist für echte Wahlmöglichkeiten der Nutzenden zu sorgen – dies kann auch bedeuten, dass alternative Verfahren oder Ausweichstrategien (Fallback-Lösungen) zur Anwendung kommen
müssen.

Durchsetzen der vereinbarten Datenverarbeitungsregeln

Auf Seiten der datenverarbeitenden Stelle sollten Garantien gegeben werden, dass tatsächlich die Daten so verarbeitet werden, wie es gesetzlich vorgegeben und mit den Nutzenden vereinbart wurde. Hier können sog. „Sticky Policies“ zum Einsatz kommen,

die an den personenbezogenen Daten über den gesamten Lebenszyklus im Bereich der datenverarbeitenden Stelle kleben und stets mit ausgewertet werden (Karjoth/Schunter/Waidner 2002; Casassa Mont/Pearson/Bramhall 2003). Insgesamt ist eine Prüffähigkeit der verwendeten Verfahren und IT-Systeme vonnöten.

Sensibilisierung der Nutzenden

Vielen Nutzenden ist weder bewusst, mit welche Risiken sie in der Online-Welt umgehen müssen, noch welche Datenschutzrechte sie haben. Das nutzergesteuerte Identitätsmanagementsystem kann hier hilfreich sein: Die Gestaltung der Benutzungsoberflächen muss sich an dem Ziel orientieren, ein Höchstmaß an Transparenz und Bedienbarkeit zu ermöglichen. Eigene Funktionen können die Nutzenden bei der Wahrnehmung ihrer Rechte unterstützen, z.B. durch gesicherte Online- Auskunftsersuchen, und für den Fall, dass den Nutzenden ihre Rechte verwehrt werden, an die zuständigen Aufsichtsinstanzen verweisen. Bei jeglicher Einbindung von anderen Parteien zur Unterstützung der Nutzenden beim Identitätsmanagement können Versagen oder Missbrauch nicht vollständig ausgeschlossen werden. Dies zeigt sich ganz klar bei zentralisierten Datenbeständen, aber auch beim Zusammenführen dezentraler Daten. Das Verlagern aller Identitätsmanagementfunktionalität allein auf die Schultern der Nutzenden bringt wiederum andere Probleme mit sich: Ohne Technikunterstützung ist ein Identitätsmanagement zumindest unbequem oder aber zu aufwändig; für Konzepte wie private Credentials ist die Verwendung von technischen Systemen Bedingung. Jede technische Hilfe für Nutzende birgt aber das Risiko eines Ausfalls oder einer Fehlfunktion; heutige IT-Systeme sind selbst für professionelle Systemadministratoren kaum sicher zu betreiben, so dass Privatnutzer erst recht Probleme haben, ihre technischen Systeme wirklich zu beherrschen.

Ausblick

Das aus Datenschutzsicht wünschenswerte nutzergesteuerte Identitätsmanagement ermöglicht im Idealfall eine einfache und leicht verständliche Nutzerkontrolle der Bedingungen, unter denen einzelne Aktionen wie Kommunikationsvorgänge, Handlung(skett)en, Orte (Adressen), Personen-(bezeichner) wie zum Beispiel Namen von Dritten miteinander verknüpft werden können. Die Anforderungen an Systeme, die ein nutzergesteuertes Identitätsmanagements umsetzen sollen, müssen von Datenschützern mitformuliert werden. Der operative Dreh- und Angelpunkt des Identitätsmanagements in Nutzerhand ist dabei die technische Unterstützung bei der Verwendung (Verwaltung, Erzeugung, Löschung etc.) von Pseudonymen. Es ist absehbar, dass es noch lange dauern wird, bis kulturell bzw. psychisch dem technisch gestützten Benutzen von Pseudonymen im Alltag nichts Anrüchiges, Unaufrichtiges, Feiges mehr anhaften, sondern sich die Funktionalität für eine moderne Gesellschaft erweisen wird. Damit der Umgang mit Pseudonymen zur alltäglichen Selbstverständlichkeit werden kann, muss gesellschaftlich-infrastrukturell sowie computertechnisch eine Menge passieren. Aufgabe der Datenschutzbeauftragten wird es sein, spezielle Anforderungen für nutzergesteuertes Identitätsmanagement zu formulieren. Planer müssen künftig die Anforderung des Identitätsmanagements von vornherein in die Betriebssysteme, Kommunikationssoftware, Bürgerportale oder Public-

Key-Infrastrukturen integrieren. Kommunikationsbeziehungen sollten nicht nur mit anonymen Credentials oder Pseudonymen oder zumindest mit komfortablen Login- und Passwortverwaltungen moderner Webbrowser unterstützt werden. Vielmehr sollten derartige Technolgien als Standards gleich in die Technik eingebaut werden. Künftig sollten Kommunikationspartner bei der Nutzung des Internet selbst entscheiden können, inwieweit sie einander selbstbestimmt ihre Identität offenbaren. Dafür muss die Netzkommunikation jedoch technisch auf einer Anonymität gewährleistenden Infrastruktur aufsetzen. Die Aufhebung dieser Anonymität ist dann allein rechtstaatlich zu regeln, und darf nicht von technischen Unzulänglichkeiten oder schlechtem Systemdesign abhängen. Zudem dürfen Konzeption und Betrieb einer solchen technischen Infrastruktur auch nicht von den ökonomischen Interessen einzelner Unternehmen abhängen. Das bedeutet, dass für technische Vielfalt und Interoperabilität zwischen verschiedenen technischen Systemen und Formaten zu sorgen ist.

Das Kommunikationsverhalten der Nutzenden hängt entscheidend davon ab, mit wem sie kommunizieren. Verwandte, Freunde, Nachbarn oder Kollegen kommunizieren anders miteinander als Kunden, Bürger oder Patienten mit einer Organisation. Die Bedienung der Applikationen zum Kommunikationsmanagement muss daher für die Nutzenden einfach sein. Erste Ideen und Untersuchungen zeigen, das bereits auf der Betriebssystemebene den verschiedenen Anforderungen des Kommunikationsmanagements Rechnung getragen werden kann. Der PC kann den Nutzende beispielsweise mit intuitiv anwählbaren Domainen mit unterschiedlichen Datenschutz-Niveaus (vgl. „Stadtmetapher“) schon sehr weit entgegenkommen (vgl. Bergmann/Rost/Pettersson 2005).

Auch durch datenschutzfördernde Ausgestaltung von Protokollen oder WebServices kann das Nutzen von Identitätsmanagement unterstützt werden. So kann sowohl auf Senderals auch auf der Empfängerseite ein bestimmter Typ von Kommunikation festgelegt werden, dem ein bestimmter Datenschutzkontext zugeordnet ist (vgl. Hansen/Rost 2003).

Dadurch können die Nutzenden an bereits erfolgreich vollzogene Transaktionen oder an eine bereits durch andere Interaktion aufgebauten Reputation anknüpfen. Kennt man sich dagegen nicht, fiele die Justage der Kommunikation anders aus. Hier wäre denkbar, dass bspw. zwecks Beweissicherung die Datenbank eines digitalen Notars automatisiert eingebunden würde. Realisieren ließen sich derartige Aushandlungen beispielsweise über WebService-Policies.

Das Datenschutz-Ziel des nutzergesteuerten Identitätsmanagements besteht darin, datenschutzfördernde, alternative Handlungsmöglichkeiten beim Umgang mit digitalen Identitäten anzubieten. Wesentliche Voraussetzung für die Akzeptanz nutzergesteuerten Identitätsmanagements ist jedoch, dass die heute selbstverständlichen, kulturellen, psychischen, politischen oder verfahrenstechnischen Verknüpfungen von Personen, Namen bzw. Bezeichnern und deren Aktivitäten gelöst werden, um sie im Rahmen des an Datenschutz orientierten Identitätsmanagements flexibel, funktional, zweckgerichtet, fair und gesetzeskonform und dann technisch unterstützt neu zusammenzusetzen. Nur dann wird es gelingen, den Organisationen, die bspw. über Scoring-Verfahren oder

Data-Warehouses mit Data-Mining-Techniken zur hochauflösenden Profilbildung verfügen oder die beispielsweise global vernetzt auf dem Electronic Product Code aufsetzen, geeignete Alternativen anzubieten.

Literaturhinweise

• Art. 29 Datenschutzgruppe (2004): Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten, 25. November 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_de.pdf.
• Bergmann, Mike; Rost, Martin; Pettersson, John Sören (2005): Exploring the Feasibility of a Spatial User Interface Paradigm for Privacy-Enhancing Technology, Proceedings of the Fourteenth International Conference on Information Systems Development (ISD´2005),Karlstad: Springer-Verlag.
• Borking, John J. (1996): Der Identity Protector, in: DuD 1996/11: 654-658.
• Camenisch, Jan; Lysyanskaya, Anna (2000): Efficient non-transferable anonymous multishow credential system with optional anonymity revocation, Research Report RZ 3295 (# 93341), IBM Research, Nov. 2000.
• Cameron, Kim (2005): The Laws of Identity, Version May 12, 2005, http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.
• Casassa Mont, Marco; Pearson, Siani; Bramhall, Pete (2003): Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services, Trusted Systems Laboratory, HP Laboratories Bristol, HPL-2003-49, http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf.
• Chaum, David (1985): Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, Vol. 28, No. 10, Oct. 1985, S. 1030-1044,
http://chaum.com/articles/Security_Wthout_Identification.htm.
• Gundermann, Lukas (2003): Sozialhilfe für Dagobert Duck – Sind Anonymität und Pseudonymität im E-Government möglich?, in DuD 2003/05: 282-286.
• Hansen, Marit; Rost, Martin (2003): Nutzerkontrollierte Verkettung – Pseudonyme, Credentials, Protokolle für Identitätsmanagement; in: DuD – Datenschutz und Datensicherheit, 27. Jahrgang, Heft 5, Mai 2003: 293-296
• Hansen, Marit; Meissner, Sebastian (Hrsg.) (2007): Verkettung digitaler Identitäten, Untersuchung für das Bundesministerium für Bildung und Forschung, https://www.datenschutzzentrum.de/projekte/verkettung/.
• Hes, Ronald; Borking, John J. (1998): Privacy Enhancing Technologies: The Path to Anonymity. Überarbeitete Fassung einer Studie von 1995, College Bescherming Persoonsgegevens, Background Studies & Investigations 11. http://www.dutchdpa.nl/downloads_av/AV11.PDF.
• Karjoth, Günter; Schunter, Matthias; Waidner, Michael (2002): Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data, 2nd Workshop on Privacy Enhancing Technologies (PET 2002), LNCS 2482, Springer, S. 69-84.
• Leenes, Ronald; Schallaböck, Jan; Hansen, Marit (Hrsg.) (2007): PRIME White Paper V2, Juni 2007, https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V2.pdf.
• Pfitzmann, Andreas; Hansen, Marit (2007): Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Working Paper v0.30, 26 Nov. 2007, http://dud.inf.tudresden.de/Anon_Terminology.shtml.
• Rost, Martin; Meints, Martin, 2005: Authentisierung in Sozialsystemen – Identitytheft strukturell betrachtet, in: DuD, Heft 04, April 2005: 216-218,

http://www.fidis.net/fileadmin/fidis/publications/2005/DuD04_2005_216.pdf.
• Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) / Studio Notarile Genghini (SNG) (2003) Identity Management Systems (IMS): Identification and Comparison Study, Studie im Auftrag des Institute for Prospective Technological Studies, Joint Research Centre Seville, Spanien.
http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf.
• FIDIS – Future of Identity in the Information Society: http://www.fidis.net/.
• PRIME – Privacy and Identity Management for Europe: https://www.prime-project.eu/.

Anlage

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Berlin, 4. April 2008

Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms "Technologien für die Informationsgesellschaft" gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter

möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z.B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.