in: Helmut Bäumler (Hrsg.): „Der neue Datenschutz“ – Datenschutz in der Informationsgesellschaft von morgen. Luchterhand, Berlin 1998, 166–172.

IV. Prävention neben Kontrolle

# Die Rolle der Datenschutzbeauftragten bei der Aushandlung von mehrseitiger Sicherheit

Hannes Federrath, Andreas Pfitzmann
Technische Universität Dresden, Fakultät Informatik, D-01062 Dresden
E-mail: {federrath, pfitza}@inf.tu-dresden.de

Datenschutzbeauftragte können bei der Aushandlung von mehrseitiger Sicherheit ihre juristische und technische Kompetenz sowie ihre normativen Einflußmöglichkeiten nutzen: Sie besitzen neben ihren Kontrollaufgaben auch Beratungs- und Empfehlungsmöglichkeiten, können Musterentwürfe für mehrseitig sichere und datenschutzgerechtere Technik erarbeiten und auch verbraucherschützend auftreten. Darüber hinaus sollten sie die Aufgaben eines vertrauenswürdigen Dritten übernehmen, sofern die mehrseitig sicheren technischen Systeme solche Instanzen überhaupt noch erforderlich machen.

## 1 Einführung: Mehrseitige Sicherheit

Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte, etwa beim Entstehen einer Kommunikationsverbindung. Die Schutzziele mehrseitiger Sicherheit können vielfältig sein, wie die folgende Tabelle zeigt.

| **Schutz der Inhalte** | **Schutz der Kommunikationsumstände** |
|---|---|
| *Vertraulichkeit der Inhalte*<br>• Nachrichteninhalte sollen vor allen Instanzen außer dem Kommunikationspartner vertraulich bleiben. | *Anonymität und Unbeobachtbarkeit*<br>• Sender und/oder Empfänger von Nachrichten sollen voreinander anonym bleiben können, und Unbeteiligte (inkl. Netzbetreiber) sollen nicht in der Lage sein, sie zu beobachten. |
| *Integrität der Inhalte*<br>• Fälschungen von Nachrichteninhalten sollen erkannt werden. | *Zurechenbarkeit*<br>• Gegenüber einem Dritten soll der Empfänger nachweisen können, daß Instanz x die Nachricht y gesendet hat.<br>• Der Absender soll das Absenden einer Nachricht mit korrektem Inhalt beweisen können, möglichst sogar den Empfang der Nachricht.<br>• Niemand kann dem Netzbetreiber Entgelte für erbrachte Dienstleistungen vorenthalten. Umgekehrt kann der Netzbetreiber nur für korrekt erbrachte Dienstleistungen Entgelte fordern. |

## 1.1 Das organisatorische Szenario mehrseitiger Sicherheit

Die genannten Schutzziele sind vielschichtig und gelten nicht für alle Beteiligten jeweils gleich stark. Je nach Kommunikationsgegenstand und -umstand werden einzelne Schutzziele sogar für denselben Nutzer eine unterschiedliche Bedeutung haben. Technische Mechanismen zum Erreichen mehrseitiger Sicherheit genügen allein nicht. Der organisatorische Rahmen mehrseitiger Sicherheit muß mindestens folgende Anforderungen erfüllen:

- Klare juristische Regeln müssen definiert sein.
- Rechtssicherheit für alle Beteiligten muß gewährleistet sein.
- Es dürfen keine expliziten Verbote von Schutzmöglichkeiten existieren.

Mit Ausnahme ganz spezieller Instanzen besitzt niemand, weder die Nutzer noch Betreiber von Netzen und Diensten, ein primäres Interesse daran, einfach nur Daten zu sammeln. Im Gegenteil: Je weniger Daten zur Diensterbringung benötigt werden, um so weniger Kosten fallen für deren Verarbeitung (und deren Schutz) an. Damit wird das Ziel von Datenvermeidungs- und Datensparsamkeitstechniken klar, die wesentliche Bestandteile der Methodik „Mehrseitige Sicherheit“ sind.

## 1.2 Das technische Szenario mehrseitiger Sicherheit

Mehrseitige Sicherheit geht davon aus, daß jeder Nutzer seinen eigenen, individuellen Rechner besitzt und für sich selber definiert, wie er sich schützen möchte, was also Sicherheit für ihn ist. Technisch gesehen kommt es darauf an, dem Nutzer Möglichkeiten an die Hand zu geben, Schutzziele zu formulieren und durchzusetzen. Der Nutzer von mehrseitig sicherer Technik besitzt damit idealerweise die Möglichkeit

- Daten in einer persönlichen, sicheren Rechenumgebung zu speichern und zu verarbeiten,
- Schutzziele zu formulieren, zu verstehen und zu beurteilen,
- Schutzziele in einem Aushandlungsprozeß gegenüber anderen Instanzen (Nutzern, Betreibern) zu vertreten.

Wie die Schutzziele von technischer Seite her umgesetzt werden können, findet man z.B. in [1]. Hier findet man auch Informationen zu den Rahmenbedingungen für die Realisierung mehrseitiger Sicherheit.

# 2 Die Rolle der Datenschutzbeauftragten

Der praktische Einsatz mehrseitig sicherer Technik wird von den ökonomischen, sozialen wie juristischen Gegebenheiten abhängen: Sicherheit ist ein Querschnittsthema und erfordert daher einen engen Dialog mit anderen Disziplinen. Hierzu zählen wir insbesondere auch die Datenschutzbeauftragten, die heute mindestens juristische und technische Kompetenz auf sich vereinigen müssen.

Datenschutzbeauftragte besitzen Möglichkeit zur Beratung der Nutzer, können Empfehlungen aussprechen, können Musterentwürfe für mehrseitig sichere und datenschutzgerechtere Technik erarbeiten und auch verbraucherschützend wirken. Als vertrauenswürdige Dritte besitzen Sie aufgrund ihrer allein auf den Datenschutz (und nicht auch auf andere Interessen, z.B. Gewinnstreben, Verbrechensbekämpfung) ausgerichteten Interessen ein hohes Potential für Vertrauenswürdigkeit.

## 2.1 Beratung und Empfehlung

Rechner und Programme werden von den wenigsten Nutzern selber entwickelt und hergestellt. Das Angebot und die Vielfalt an Hardware und Software gibt dem Käufer viele Wahlmöglichkeiten, fordert ihm aber eine Menge an Entscheidungen ab. Ohne entsprechende Beratungsmöglichkeiten ist eine qualifizierte Entscheidung häufig nicht möglich.

Welche Möglichkeiten existieren für den Nutzer, sich von der richtigen (korrekten) und angemessenen (adäquaten) Erbringung der Sicherheitsfunktionalität zu überzeugen? Oder muß er der Sicherheit einfach Vertrauen entgegenbringen? Die zweite Frage enthält offenbar einen Widerspruch: Hat sich ein Nutzer von der Korrektheit der Funktionalität überzeugt, muß er ihr nicht mehr vertrauen. Unsicherheit wurde beseitigt, *Vertrauen* ist nicht mehr nötig, *Vertrauenswürdigkeit* wurde hergestellt. Für die erste Frage existieren folgende Möglichkeiten: a) Überprüfung der Technik durch Dritte, b) Überprüfung durch den Nutzer selbst. Da die Möglichkeit b) mangels Expertise, Zeit, Geld etc. meist unmöglich ist, sucht sich der Nutzer einen Partner, dem er vertraut und der die Überprüfung übernimmt.

Mit der zunehmenden Verarbeitung personenbezogener Daten über informationstechnische Systeme steigt auch die Bedeutung von Sicherheitsfunktionen und der Bedarf an spezieller Beratung für datenschutzgerechte Systeme. Eine Möglichkeit, solche Beratung zu geben, sind die Datenschutzbeauftragten. Die Vorteile sind die relative Nähe zum Bürger und die weitgehende Unabhängigkeit von Herstellern. Förderlich kommt der juristische Hintergrund der Datenschutzbeauftragten hinzu.

Bei der Sicherung eines Systems ist stets die unterstellte Stärke eines Angreifers zu berücksichtigen. Ein solches Angreifermodell kann jedoch nur eine Abstraktion von der Wirklichkeit sein. Die reale Stärke eines Angreifer unterliegt jedoch zeitlichen Veränderungen z.B. durch die Erhöhung der Rechenleistung, aber auch durch neu gefundene Angriffsmethoden. Weit verbreitete, erfolgreich angegriffene Systeme stellen

ein erhebliches Sicherheitsrisiko für die Bereiche dar, in denen ein Angriff bisher nicht stattfand. Die schnelle und zuverlässige Information der Nutzer über neue Sicherheitsprobleme ist daher sehr wichtig und hilft, den potentiellen Verlust von Datenschutz zu verhindern. Datenschutzbeauftragte können und müssen in Zukunft in enger Zusammenarbeit mit den entsprechenden Experten, im Internet sind das z.B. die Computer Emergency Response Teams (CERT, siehe z.B. [2]), eine konsequente Informationspolitik betreiben. Gegebenenfalls sollte dies sogar so weit gehen, daß kompromittierte Systeme durch „Rückrufaktionen“ nachgebessert werden.

## 2.2 Musterentwürfe für mehrseitig sichere Technik

Für viele Lebensbereiche existieren Mindestregeln oder -standards, um die Qualität von Produkten, Dienstleistungen etc. zu sichern. Mehrseitig sichere Technik soll die Interessen nicht nur einer Partei einer Kommunikation sichern. Die normative Kompetenz der Datenschutzbeauftragten, die bisher vor allem die Interaktionen zwischen *Bürger und Staat* unter dem Datenschutzaspekt bestimmt, sollte in Zukunft auch Auswirkungen auf das Handeln zwischen *Bürger und nichtstaatlichen Organisationen* (z.B. Unternehmen) haben. So klafft durchaus noch ein weiter Spalt zwischen den technischen Möglichkeiten zur Realisierung von Datenschutz, speziell Datensparsamkeit und Datenvermeidung, und den industriell bereits umgesetzten Konzepten.

Datenschutzbeauftragte sind geeignet, hier der Industrie auf die Sprünge zu helfen, sie zu überzeugen von der Bedeutung datenschutzgerechter Technologien und Hinweise zu geben, was rechtskonforme Systeme zu leisten haben. Ein Beispiel für die noch fehlende industrielle Verwirklichung von Rechtsnormen ist die im Informations- und Kommunikationsdienstegesetz (IuKDG, siehe [3], [4], [5]) genannte Möglichkeit zur pseudonymen Kommunikation. Obwohl die Konzepte bereits seit Jahren existieren (siehe z.B. [6]), sind sie bisher für den Bürger nicht praktisch nutzbar. Mit dem IuKDG existiert nun sowohl für Hersteller als auch Nutzer solcher Konzepte Rechtssicherheit: Die Nutzer (bzw. der Markt) können die Umsetzung von der Industrie fordern, und die Industrie braucht gegenüber Strafverfolgungsbehörden nicht mehr vorauseilenden Gehorsam zu üben und auf Datensparsamkeit in ihrer Kommunikationstechnik zu verzichten.

Konkret könnte die Aushandlung mehrseitiger Sicherheit durch die Datenschutzbeauftragten unterstützt werden, indem sie

- Vorschläge für Standardkonfigurationen mehrseitig sicherer Technik erarbeiten,
- Standard- bzw. Musterverträge für die Geschäftsbeziehungen zwischen Nutzern und Herstellern/Verkäufern/Betreibern informationstechnischer Systeme erarbeiten, die klare Regeln zur Realisierung von Datensparsamkeit und Datenvermeidung enthalten.

## 2.3 Vertrauen und die Rolle der Datenschutzbeauftragten als vertrauenswürdige Dritte

Viele technische Konzepte der mehrseitigen Sicherheit zielen darauf ab, das *Vertrauen eines Nutzers* in die informationstechnischen Systeme, ihre Hersteller, Betreiber und weiteren Nutzer *so wenig wie möglich* zu *beanspruchen.*

Wenn es beispielsweise technisch möglich ist, eine Teleshoppinganwendung so zu gestalten, daß der Kunde bzw. Händler auch vor Fehlfunktionen oder bewußten Angriffen des jeweiligen Geschäftspartners oder der Bank sicher ist, dann hat sich das Ziel mehrseitiger Sicherheit erfüllt. Konkret sind hier jedoch weitreichende Schutzziele gefragt: Sollte ein Kunde beispielsweise wünschen, daß niemand (weder der Händler noch irgendein anderer Beteiligter) ihn beobachten kann, genügen einfache Konzepte mit *einem* vertrauenswürdigen Dritten allein nicht mehr. Hier ist mindestens *verteiltes Vertrauen* zu fordern, d.h. Viele müssen zusammenarbeiten, um Einen (z.B. Kunde oder Händler) zu beobachten. Diese Möglichkeit zur Beobachtung sichert Andere davor, daß Schutzziele wie Unbeobachtbarkeit dazu mißbraucht werden, selbst Angriffe (z.B. Betrug) erfolgreich durchzuführen. Sie verhindert jedoch die Überwachbarkeit der Nutzer im großen Stil.

Da es offenbar in Kommunikationssystemen nicht völlig ohne vertrauenswürdige Dritte (Trusted Third Parties, TTP) geht, im Gegenteil, beim *Konzept des verteilten Vertrauens* sogar viele unabhängige Dritte erforderlich sind, sollten sich Datenschutzbeauftragte auf jeden Fall daran beteiligen, entsprechende Dienste anzubieten. Für die bisher bekanntesten und verbreitetsten Formen von TTPs, den Zertifizierungsstellen für öffentliche Schlüssel, fälschlicherweise oft mit dem irreführenden Begriff „Trust Center“ bezeichnet, existieren in der Industrie bereits Erfahrungen (siehe z.B. [7], [8]).

Die Zertifizierung von Schlüsseln ist zwar kein direktes Datenschutzproblem, jedoch ist unseres Erachtens die Rolle der Datenschutzbeauftragten auch in dieser Hinsicht in Zukunft weiter zu fassen. Ein Wissens- und Erfahrungstransfer zu den Datenschutzbeauftragten ist mehr als wünschenswert und eröffnet für beide Seiten (Industrie und Datenschutzbeauftragte) die Möglichkeit, auch für den Datenschutz relevante TTP-Dienstleistungen zu erbringen.

Gerade die Datenschutzbeauftragten sind aufgrund des Fehlens offener Interessengegensätze geeignet, Vertrauenswürdigkeit zu repräsentieren. (Das Bundesamt für die Sicherheit in der Informationstechnik BSI ist zum Beispiel durch seine Aufgaben für die Sicherung des Staates in einer Doppelrolle. Es sollte die Interessen der Bürger vertreten, wozu natürlich auch Datenschutz gehört, gleichzeitig arbeitet es aber auch unterstützend für die Sicherung des Staates, etwa im Bereich der Verbrechensbekämpfung. Daß dadurch Interessenkonflikte vorprogrammiert sind, steht außer Frage. Dies wiederum erhöht jedoch nicht gerade die Vertrauenswürdigkeit einer solchen Organisation.)

## 3 Schlußbemerkungen

Die Rolle der Datenschutzbeauftragten ist in Zukunft weiter zu fassen. Entweder sie nehmen ihre neue Rolle wahr, oder ihre Aufgaben werden mehr und mehr assimiliert durch andere Institutionen, beispielsweise Verbraucherschutzorganisationen oder Bürgerinitiativen. Darüber hinaus verliert der Staat durch die Dezentralisierung der Kommunikation, ein Beispiel hierfür ist das weltweite Internet, seine Einflußmöglichkeiten und die Bedeutung des Individuums bzw. der Individualkommunikation (Bürger, schützenswerte Personengruppen etc.) wächst. Somit muß sich auch die Rolle und Einflußnahme der Datenschutzbeauftragten verschieben — von der Beratung und Kontrolle öffentlicher (staatlicher) Stellen hin zu einer Beratung und Unterstützung der Individuen bei deren Selbstschutz.

## 4 Literatur


[1] Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison-Wesley-Longman, 1997.

[2] DFN-CERT: http://www.cert.dfn.de/.

[3] Bundeskabinett: Informations- und Kommunikationsdienste-Gesetz — IuKDG. Datenschutz und Datensicherheit DuD 21/1 (1997) 38-45.

[4] Stefan Engel-Flechsig: Teledienstedatenschutz. Datenschutz und Datensicherheit DuD 21/1 (1997) 8-16.

[5] Ulrich Wuermeling: Datenschutz bei Telediensten. Datenschutz-Berater 20/12 (1996) 1-6.

[6] Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

[7] Deutsche Telekom AG, Produktzentrum Telesec, Trust Center: http://www.telesec.de/trust.htm.

[8] Competence Center Informatik GmbH (CCI GmbH), Trust Center CCI: http://www.cci.de/cci/no-frames/arbeit-themen-itsicherheit-4.html.