Mehrseitige Sicherheitsfunktionen in Telekommunikationsnetzen

Hannes Federrath, Freie Universität Berlin, Institut für Informatik

Abstract-- **Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung. Die mehrseitige Sicherheit verbindet die Sichtweisen von Datenschutz und Datensicherheit zu einem gemeinsamen Konzept.**

Index Terms—**Mehrseitige Sicherheit, Datenschutz, IT-Sicherheit.**

I. Einführung

Informationstechnische Systeme (IT-Systeme) verarbeiten, transportieren und speichern digitale Daten. Die Verarbeitung und der Transport werden immer schneller, Speicher wird immer preiswerter. Es ist innerhalb der nächsten Jahrzehnte zu erwarten, dass immer kleinere und leistungsfähigere Rechner überall zur Verfügung stehen werden. Während früher wenige Großrechner und Datenbanken durch wenige Betreiber, die leicht kontrolliert werden konnten, bedient wurden, sind heute alle Betroffenen selbst Betreiber und Teilnehmer an der Datenverarbeitung. Diese neue Situation führt dazu, dass sich der Teilnehmer auch selbst um seine eigene und die Sicherheit anderer kümmern muss.

Das Konzept der mehrseitigen Sicherheit versucht der neuen Situation Rechnung zu tragen und verbindet die Konzepte des Selbstdatenschutzes und des Systemdatenschutzes, wie sie auch in die neue Datenschutzgesetzgebung, vgl. [1], einfließen sollen.

II. Motivation

Die Großrechner vor 20 Jahren waren streng bewacht, d.h. sie hatten Zugangskontrollmechanismen (Pförtner, Stahltüren etc.), die nicht leicht zu überwinden waren. Die Vernetzung von Rechnern blieb Spezialanwendungen vorbehalten. Da personenbezogene Daten meist auf diesen zentralisierten Datenverarbeitungssystemen gespeichert wurden, waren die Daten, verglichen mit der Speicherung in den heutigen über das Internet verbundenen Systemen, gut gesichert: Mit dem Einzug des Internet und der Mobilkommunikation in alle Bereiche des Lebens fallen personenbezogene Daten in einer noch nie da gewesenen Menge an, deren Schutz selbst von den Betroffenen teilweise erstaunlich locker gesehen wird. Für die Aussicht auf ein kostenloses Goodie werden Adressen und Telefonnummern im Internet preisgegeben; Kreditkartennummern werden über das unsichere Internet übertragen, um Waren und Dienstleistungen im Internet zu bezahlen. Global Unique Identifier, Prozessor IDs und Ethernetadressen können einen Menschen, der einen Großteil seiner Aktivitäten ins Netz verlagert, fast vollständig beobachtbar machen, da sie als Personenkennzeichen fungieren.

Bereits vor 20 Jahren genügte die Speicherkapazität eines tragbaren Mediums (Magnetbandkassette), um die personenbezogenen Daten der Volkszählung von 1987 (knapp 2 Gigabyte) der Bürger der Bundesrepublik aufzunehmen. Auf vergleichbaren, heute verfügbaren tragbaren Speichermedien fänden zusätzlich noch hochauflösende Fotos aller

Bürger mitsamt den Fotos Ihrer Wohnhäuser Platz. Durch die Vernetzung ist es möglich, solche Datenmengen blitzschnell an das andere Ende der Welt zu transportieren. Private Haushalte werden heute mit Übertragungskapazitäten zwischen 500 Kilobit/s und 1 Megabit/s angeschlossen. In ein paar Jahren wird sich die Übertragungskapazität von und zu privaten Haushalten verhundertfacht haben. Die verfügbaren Speichermedien, Netze und Übertragungsgeschwindigkeiten ermöglichen die kostengünstige und schnelle Vervielfältigung und Verbreitung auch von personenbezogenen Daten. Sie sind für den Betroffenen und seine Kommunikationspartner (und ggf. auch Unberechtigte) stets verfügbar, kaum endgültig löschbar, weil vielfach dupliziert, die Integritätssicherung erfordert viel Mühe bzw. ist nicht mehr möglich.

Glücklicherweise existieren einerseits Datenschutzgesetze, andererseits Technik, die den Menschen schützen können. Technik kann dabei Daten und Menschen schützen: Während **Datensicherheit** die Daten schützen soll, schützt **Datenschutz** die Menschen.

III. Mehrseitige Sicherheit

Wenn Technik zur Datenverarbeitung und -speicherung eingesetzt wird, erscheint es eigentlich selbstverständlich, Technik auch zum aktiven Datenschutz und zur Datenvermeidung einzusetzen.

Es ist völlig unklar und unverständlich, warum die rechtmäßige Datenverarbeitung mit Hilfe von Technik gerne genutzt wird, um Kosten zu sparen und effizient handeln zu können, gleichzeitig aber der Aufwand gescheut wird, Technik einzusetzen, mit der Geschäftsprozesse so abgewickelt werden, dass personenbezogene Daten vollständig vermieden oder wenigstens stark reduziert werden. Gesteigerte Effizienz eines Unternehmens durch elektronische Datenverarbeitung darf kein Argument für reduzierten Datenschutz zu Lasten des Betroffenen sein. Zwar kann mit jeder Datenverarbeitung die Einwilligung des Betroffenen eingeholt werden, um auf niedrigem Datenschutzniveau trotzdem verarbeiten zu dürfen; im Endeffekt unterhöhlt aber dieses Vorgehen die Rechte des Betroffenen, weil sie „daran gewöhnt“ werden, dass es ohne die Preisgabe ihrer persönlichen Daten angeblich nicht möglich ist, bestimmte Dienstleistungen in der Informationsgesellschaft in Anspruch zu nehmen.

Die Vertrauensverhältnisse zwischen den verschiedenen beteiligten Instanzen innerhalb eines IT-Systems entscheiden stark darüber, welches Schutzniveau für den einzelnen Beteiligten tatsächlich erreicht werden kann. Nicht selten gilt dabei, wie im wirklichen Leben, dass die Mächtigen ihre Interessen gegen die schwächeren Partner durchsetzen, zumindest solange sie dies auf legaler Basis tun. Man könnte diesen Prozess zwar mit dem evolutionären Grundgedanken, dass der (genetisch) Stärkere den Überlebenskampf gewinnt, erklären, aber keinesfalls billigen. Eine solche Form von Sozialdarwinismus dürfte aber in einer modernen Gesellschaft durchaus fragwürdig sein. Zumindest sollte die Unsicherheit von Informationstechnik nicht zwangsläufig dazu führen, gesellschaftliche Ungleichheiten noch zu verstärken.

Glücklicherweise hat sich in den letzten Jahren eine Gegenströmung im Bereich der IT-Sicherheit etabliert, die dieser einseitigen Betrachtung von Sicherheit und Schutz das Konzept der mehrseitigen Sicherheit entgegenstellt.

Mehrseitige Sicherheit [2,3] bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer

Kommunikationsverbindung. Die mehrseitige Sicherheit verbindet die Sichtweisen von Datenschutz und Datensicherheit zu einem gemeinsamen Konzept.

Während sich Datenschutz hauptsächlich um die Interessen der Betroffenen kümmert, und Datensicherheit vor allem die Interessen der Datenbesitzer und –verarbeiter beachtet, wird bei mehrseitiger Sicherheit in einem Aushandlungsprozess versucht, möglichst Beides, Datenschutz und Datensicherheit zu gewährleisten.

Mehrseitige Sicherheit ist Sicherheit mit minimalen Annahmen über andere:

- Jeder Beteiligte hat Sicherheitsinteressen.
- Jeder Beteiligte kann seine Interessen formulieren.
- Konflikte werden erkannt und Lösungen ausgehandelt.
- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.

Die Realisierung von mehrseitiger Sicherheit führt nicht zwangsläufig dazu, dass die Interessen aller Beteiligten erfüllt werden. Sie gewährleistet jedoch, dass die Partner einer mehrseitig sicheren Kommunikationsbeziehung in einem geklärten Kräfteverhältnis bzgl. Sicherheit miteinander interagieren.

IV. Grundsätze mehrseitiger Sicherheit

Mehrseitige Sicherheit bedeutet aus Nutzersicht, dass sich die Gestaltung von Technik im Hinblick auf die Verarbeitung personenbezogener Daten am Ziel Datenschutz orientiert. Dabei kann Technik einerseits die **Vertraulichkeit** von personenbezogenen Daten schützen, aber auch deren **Korrektheit** (inkl. ihrer Aktualität). Wann immer möglich, sollten Daten vollständig vermieden werden (Datenvermeidung) oder wenigstens so wenig wie möglich Daten verarbeitet werden (Datensparsamkeit):

- **Datenvermeidung:** Die Vertraulichkeit von Daten ist dann am größten, wenn sie vollständig vermieden werden können - was natürlich nur bei nicht für eine bestimmte Zweckerfüllung benötigten Daten möglich ist. Dabei ist erstaunlich, wie viele einen Personenbezug herstellende Daten sich als unnötig herausstellen, wenn nur früh und gründlich genug nachgedacht und das System entsprechend gestaltet wird. Beispielsweise ist es keineswegs erforderlich, dass der einen Telekommunikationsdienst Erbringende erfährt, welche Kommunikationspartner er miteinander verbindet.
- **Datensparsamkeit:** Kann man personenbezogene Daten nicht vermeiden, so ist das Nächstbeste, die Verwendungsmöglichkeit notwendiger Daten einzuschränken bzw. Betroffenen die Möglichkeit zu geben, die Daten insbesondere bei jeder Verwendung auf Richtigkeit und Aktualität zu überprüfen. Das Ziel der Datensparsamkeit umfasst, die Verwendungsmöglichkeit notwendiger Daten einzuschränken.

V. Schutzziele

Schutzinteressen können sich nicht nur auf die über die Netze ausgetauschten Nachrichteninhalte (Vertraulichkeit, Integrität) beziehen, sondern gelten ebenfalls für den Schutz von Kommunikationsumständen: In manchen Anwendungen ist zu schützen, wer wann mit wem kommuniziert hat (Anonymität und Unbeobachtbarkeit), in anderen Anwendungen ist vor allem sicherzustellen, dass eine Nachricht nachprüfbar und beweisbar von einem bestimmten Absender stammt (Zurechenbarkeit).

Die heutigen Computernetze sind meist große heterogene Gebilde mit sehr vielen

Betreibern und Anwendern. Die neuen Kommunikationsmedien sind inzwischen zu einer bedeutenden Infrastruktur gewachsen. Interessengegensätze zwischen Betreibern und Anwendern, aber auch zwischen den Betreibern selbst und natürlich auch zwischen Anwendern werden künftig auch über diese neuen Infrastrukturen ausgetragen. Folglich bedarf es Sicherheitsmechanismen, siehe [4], die niemanden, weder Betreiber noch Anwender, von der Nutzung der neuen Möglichkeiten ausschließen, und auch möglichst keine neuen Risiken mit sich bringen.

Tabelle: Gliederung von Schutzzielen

	Inhalte Worüber?	Umfeld Wer, wann, wo, mit wem, wie lange?
Unerwünschtes verhindern	Vertraulichkeit von Nachrichteninhalten	gegenseitige Anonymität der Anwender; Unbeobachtbarkeit der Anwender durch die Betreiber
Erwünschtes leisten	Integrität von Nachrichteninhalten	Zurechenbarkeit von Nachrichten zu Absendern
	Verfügbarkeit von Daten und Diensten	Erreichbarkeit von Anwendern

Die neuen Kommunikationsmedien sollen zunächst natürlich erwünschte Funktionen leisten, allerdings ebenso unerwünschte Funktionen oder Verhaltensweisen verhindern (siehe Tabelle). Hier zeigt sich der **Gegensatz in den Interessen**. Beispielsweise möchte ein Information Broker über eine Person möglichst schnell und effizient viele aktuelle und richtige Informationen sammeln, während die Person selber möglicherweise ein Interesse und ein Recht an der Privatheit und Vertraulichkeit gegenüber dem Information Broker besitzt.

VI. Zusammenfassung

Die mehrseitige Sicherheit verbindet die Sichtweisen von Datenschutz und Datensicherheit zu einem gemeinsamen Konzept. Während sich Datenschutz hauptsächlich um die Interessen der Betroffenen kümmert, und Datensicherheit vor allem die Interessen der Datenbesitzer und -verarbeiter beachtet, wird bei mehrseitiger Sicherheit in einem Aushandlungsprozess versucht, möglichst Beides, Datenschutz und Datensicherheit zu gewährleisten. Dies trägt der Entwicklung Rechnung, dass aus den bisher lediglich Betroffenen zunehmend informationstechnisch Beteiligte werden können und oftmals werden sollten.

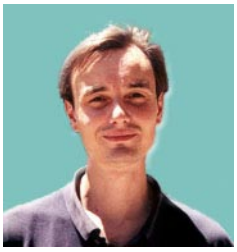
VII. Literatur

[1] Alexander Rossnagel, Andreas Pfitzmann, Hansjürgen Garstka: Diskussionsentwurf des Gutachtens „Modernisierung des Datenschutzrechts, insbesondere grundlegende Novellierung des Bundesdatenschutzgesetzes“, 15. Juni 2001

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

[3] Günter Müller, Kai Rannenberg (Ed.): Multilateral Security in Communications, Addison-Wesley-Longman 1999.

[4] Hannes Federrath, Andreas Pfitzmann: Bausteine zur Realisierung mehrseitiger Sicherheit. in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 83-104.



Hannes Federrath, Dr.-Ing., studierte von 1989 bis 1994 Informatik und promovierte 1998 an der Technischen Universität Dresden auf dem Gebiet der Sicherheit mobiler Kommunikation. Von 1994 bis 1999 war er als wissenschaftlicher Mitarbeiter, seit 1999 ist er als Oberingenieur im Bereich Informations- und Kodierungstheorie bei Prof. Andreas Pfitzmann tätig. Von September 1999 bis August 2000 forschte er als Gastwissenschaftler am International Computer Science Institute Berkeley, Kalifornien. Von September 2000 bis August 2001 forschte und lehrte er am Institut für Informatik der Freien Universität Berlin. Forschungsschwerpunkte sind Sicherheit in verteilten Systemen, Kryptograhie, Steganographie, Anonymität und Unbeobachtbarkeit sowie Mobile Computing.