

Privatsphäre und Sicherheit Ergebnisse aus dem europäischen TA-Projekt PRISE

von Johann Čas, Institut für Technikfolgen-
Abschätzung, Wien

Die rasante technische Entwicklung bei Kommunikationstechnologien und biometrischen Verfahren sowie in der Sensorik und Datenanalyse ermöglicht immer tiefere Einblicke und Eingriffe in die Privatsphäre. Insbesondere bei Anwendungen im Sicherheitsbereich besteht eine große Versuchung, diese Möglichkeiten der Überwachung über Gebühr zu nutzen und das Grundrecht auf Privatsphäre zu verletzen. Im EU-Projekt PRISE (Privacy and Security) wurden mit einer partizipativen Herangehensweise Kriterien und Empfehlungen zu einer grundrechtskonformen Sicherheitsforschung und damit zu einer privatsphärenfördernden Einführung und Nutzung von Sicherheitstechnologien entwickelt.

1 Ausgangssituation

Der technische Fortschritt in den Informations- und Kommunikationstechnologien und die zunehmende Durchdringung des Alltags mit diesen Technologien ist allein genommen schon ausreichend dafür, dass die Menge der generierten personenbezogenen Daten immens anwächst. Die Verbreitung von biometrischen Verfahren und neuen Sensortechnologien ermöglicht es, dass Daten auch ohne aktives Zutun der betroffenen Personen erhoben werden können. Durch immer leistungsfähigere Speichermedien und Prozessoren lassen sich die wachsenden Datenmengen zu sinkenden Kosten praktisch unbegrenzt speichern, miteinander verknüpfen und mit immer effizienteren Algorithmen analysieren. Das Grundrecht auf Wahrung der Privatsphäre gerät dadurch zunehmend unter Druck; wirtschaftliche Interessen, das Versprechen von besseren privaten und öffentlichen Dienstleistungen und Sicherheitsargumente verleiten dazu, die wachsenden technischen Möglichkeiten auch exzessiv zu nutzen.

Die tragischen Ereignisse vom 11. September 2001 und nachfolgende Terroranschläge in Europa haben das politische Interesse an Fragen der öffentlichen Sicherheit beträchtlich erhöht und zur Entwicklung von neuen Sicherheitskonzepten und Sicherheitsstrategien geführt. Diese werten den Sicherheitsaspekt zu-

meist deutlich zuungunsten von Grund- und Menschenrechten auf. Auch in Europa wurden in den letzten Jahren eine Reihe von neuen Sicherheitstechnologien entwickelt und Maßnahmen durchgesetzt, von denen angenommen wird, dass sie die Sicherheit der Bürger Europas erhöhen, diese aber gleichzeitig einer immer höheren Überwachung aussetzen und tiefe Eingriffe in deren Privatsphäre mit sich bringen. Der Schutz der Privatsphäre ist ein Menschenrecht, das sowohl in vielen internationalen Erklärungen, Konventionen und nationalen Verfassungen manifestiert ist, als auch in der Europäischen Union durch die Datenschutzrichtlinie bzw. deren Umsetzung in nationales Recht explizit geschützt ist. Respekt vor der Privatsphäre schützt Bürger vor staatlicher Willkür und ist eine Grundvoraussetzung für die persönliche Freiheit und für demokratische Gesellschaften. Der Schutz vor permanenter Überwachung ist nicht nur eine Bedingung für die freie persönliche Entfaltung, sondern auch für die gesellschaftliche und wirtschaftliche Weiterentwicklung und Innovationsfähigkeit. Damit sind Investitionen in den Schutz der Privatsphäre auch Investitionen in die Zukunft demokratischer Gesellschaften.

2 Projekthintergrund und -ziele

PRISE¹ wurde im Rahmen von PASR² von der Europäischen Kommission gefördert. Durch das PASR-Programm soll die Europäische Kommission bei der Vorbereitung und Ausgestaltung des Themas „Sicherheitsforschung“ im 7. Rahmenprogramm der Europäischen Union unterstützt werden. PRISE war innerhalb dieses Programms das einzige Projekt, das dezidiert dem Schutz von Menschenrechten und dabei insbesondere der Privatsphäre gewidmet war. Das Projekt hatte eine Laufzeit von 28 Monaten und wurde im Sommer 2008 abgeschlossen. Das PRISE-Konsortium³ wurde vom Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften koordiniert.

Die primäre Aufgabe des PRISE-Projekts war es, Kriterien und Richtlinien für Sicherheitstechnologien und -maßnahmen zu entwickeln, welche in Einklang mit Menschenrechten im Allgemeinen und mit dem Schutz der Privatsphäre im Besonderen stehen. Ein Ausgangspunkt war, dass Sicherheitstechnologien, die die Privatsphäre respektieren und fördern,

die Entwicklung von akzeptablen und akzeptierten Sicherheitslösungen ermöglichen. Die Integration des Schutzes der Privatsphäre in das Design von Sicherheitstechnologien soll für die Zukunft mehr Sicherheit ohne Einbußen an Privatsphäre erlauben.

Die in PRISE entwickelten Kriterien für privatsphärenfördernde Sicherheitstechnologien sind unmittelbar als Unterstützung an Antragsteller und Evaluatoren von Sicherheitsforschungsprojekten gerichtet, um bereits in der Phase der Projektkonzeption das Ziel von datenschutzkonformen und privatsphärenfördernden Sicherheitstechnologien ins Zentrum der Aufmerksamkeit zu rücken. Um grundrechtskonforme Sicherheitslösungen erreichen zu können, ist auch ein entsprechender Einsatz dieser Technologien unabdingbar. Die Kriterien sind daher so konzipiert, dass sie auch für die spätere Einführung und Nutzung von Sicherheitstechnologien anwendbar sind.

3 Projektmethoden

Während die Wissensbasis im Wesentlichen mittels traditioneller Methoden wie „Desktop Research“ und der Einbeziehung von Expertenwissen erarbeitet wurde, basierte die Entwicklung der Kriterien und Richtlinien auf einem innovativen Methodenmix unter Einbeziehung partizipativer Verfahren. Zur Wissensbasis selbst zählten

- die Identifikation und Analyse von relevanten Sicherheitstechnologien, wobei sich die Relevanz hier auf potenzielle oder aktuelle Eingriffe in die Privatsphäre bezog
- die Identifikation von technischen, organisatorischen und legislativen Optionen zur privatsphärenfördernden Gestaltung von Sicherheitstechnologien sowie
- die Entwicklung von Szenarien, welche die Einsatzmöglichkeiten und Wirkungen unterschiedlicher Sicherheitstechnologien in einer auch für Laien zugänglichen Weise illustrieren sollten.

Die Einbeziehung von Nutzern und Stakeholdern war eines der wesentlichen partizipativen Elemente von PRISE. In zwei „User- und Stakeholder-Workshops“ wurden Vertretern von Sicherheitsindustrie, Sicherheitsforschung, Datenschutzbehörden, Menschenrechtsorganisationen und Nutzern von Sicherheitstechnologien

die jeweiligen Zwischenergebnisse präsentiert und zur Diskussion gestellt. Mit diesen Workshops wurden mehrere Ziele verfolgt: Einerseits war sicherzustellen, dass alle Gesichtspunkte berücksichtigt werden und Feedback zu vorläufigen Schlussfolgerungen zu bekommen. Andererseits war die Kommunikation und Interaktion der unterschiedlichen Stakeholder-Gruppen zu initiieren und auch die Verbreitung der Ergebnisse von PRISE zu unterstützen.

Das zweite zentrale partizipative Verfahren waren sogenannte „Interview Meetings“. Dabei handelt es sich um eine vom Dänischen Technologierat entwickelte Methode, Bürger in Verfahren der Technikfolgenabschätzung einzubinden. Im Rahmen des PRISE-Projekts wurde dieses Verfahren erstmals simultan in mehreren Staaten durchgeführt. Diese Methode lässt zwar keine für die jeweilige Bevölkerung statistisch repräsentative Aussagen zu, sehr wohl können aber quantitative und qualitative Daten über in der Bevölkerung vorherrschende Meinungen, Haltungen und Argumentationslinien zu einem bestimmten Thema gewonnen werden. Neben den Partnerländern Dänemark, Deutschland, Österreich und Norwegen wurde dieses Verfahren zusätzlich noch in Spanien und Ungarn durchgeführt, um auch Perspektiven aus einem süd- und einem osteuropäischen Staat zu integrieren. In jedem dieser Länder wurde ein Sample von jeweils etwa 30 Personen eingeladen; diese Gruppe wurde zufällig ausgewählt und musste bestimmte demographische Vorgaben erfüllen. Den Teilnehmern wurden vorab Informationen zum Diskussionsthema bereitgestellt. Am Beginn der etwa drei- bis vierstündigen „Interview Meetings“ standen Expertenpräsentationen, die auch die Möglichkeit boten, offene inhaltliche Fragen zu klären. Danach wurden die Teilnehmer gebeten, einen umfassenden Fragebogen auszufüllen. Im Anschluss wurden die Bürger in mehrere Kleingruppen aufgeteilt, um die im Fragebogen formulierten Fragen untereinander zu diskutieren und ihre Antworten zu begründen. Diese Diskussionen wurden transkribiert und analysiert.

4 Ergebnisse der „Interview Meetings“

Für eine Zusammenfassung der Ergebnisse sei auf den „PRISE Synthesis Report – Interview Meetings on Security Technology and Privacy“

verwiesen (Jacobi, Holst 2008). Einige der zentralen Schlussfolgerungen waren:

- Die Bedrohung durch den Terrorismus rechtfertigt keine Verletzungen der Privatsphäre durch Sicherheitstechnologien. Dies ist eine dominante Haltung in allen Ländern, unabhängig davon, ob das jeweilige Land in den letzten Jahren von internen oder externen Terroranschlägen betroffen war – zum Beispiel Spanien – oder nicht.
- Technologien, die in die körperliche Intimsphäre eindringen, werden von einer großen Mehrheit abgelehnt. Ein Beispiel hierfür sind Terrahertzscanner, welche als sogenannte „Naked Machines“ einen Blick durch die Kleidung hindurch auf mitgeführte Gegenstände und den „nackten“ Körper ermöglichen.
- Eine weitere große Sorge betrifft den möglichen Missbrauch von Sicherheitstechnologien. Die Bürger verlangen nach strikten Vorkehrungen, um jegliche Art des Missbrauchs zu vermeiden. Gleichzeitig glauben sie nicht daran, dass diese Möglichkeiten gänzlich verhindert werden können.

Beispiele für Faktoren, die die Akzeptanz von Sicherheitstechnologien erhöhen könnten, sind etwa die Proportionalität der durchgeführten Maßnahmen oder richterliche Anordnungen. Die Proportionalität bezieht sich sowohl auf das Verhältnis von vermuteten Sicherheitsgewinnen zur Schwere der Eingriffe in die Privatsphäre als auch auf das Vorliegen eines konkreten Verdachts. Die Privatsphäre verletzende Maßnahmen werden nur bei begründetem Verdacht als akzeptabel betrachtet, mit richterlicher Anordnung seien dann aber auch schwerwiegende Eingriffe tragbar. Grundsätzlich wurde gefordert, dass Maßnahmen, welche die Privatsphäre einschränken, nur dann getroffen werden dürfen, wenn keine, die Grundrechte nicht einschränkenden Alternativen verfügbar seien.

5 Kriterien für privatsphärenfördernde Sicherheitstechnologien

Die im PRISE-Projekt entwickelten Kriterien⁴ unterscheiden drei Sphären: Die erste betrifft einen Kernbereich an Privatsphäre, der unter keinen Umständen verletzt werden soll, die zweite überprüft die Übereinstimmungen mit den grundlegenden Prinzipien des Datenschut-

zes und die dritte bezieht sich auf kontextabhängige Trade-offs und Abwägungsfragen.

Oft werden Sicherheitstechnologien mit einem oder mehreren dieser Kriterien in Konflikt stehen. Daher werden in den PRISE-Berichten Hinweise auf mögliche Vorkehrungen und Maßnahmen gegeben, wie diese Verletzungen der Privatsphäre verringert oder beseitigt werden können. Diese Maßnahmen setzen auf drei Ebenen an: 1.) technische Vorkehrungen, in erster Linie handelt es sich dabei um den Einsatz von PETs (Privacy Enhancing Technologies), 2.) regulative und gesetzliche Vorkehrungen, die in der Regel in den Verantwortungsbereich der Politik fallen, und 3.) organisatorische Maßnahmen, die sowohl die Entwicklung als auch die spätere Nutzung betreffen können. Ein Ziel ist es, diese Aspekte bereits in das Forschungsdesign zu integrieren, weiters soll in den Begutachtungsverfahren die Beurteilung erleichtert werden, ob wirklich alle notwendigen Vorkehrungen getroffen wurden, um Konflikte mit dem Schutz der Privatsphäre zu vermeiden.

Der Kernbereich des Schutzes der Privatsphäre bezieht sich auf Aspekte der Menschenwürde, der körperlichen Integrität und der persönlichen Lebensführung. Obwohl Einschränkungen der Privatsphäre aus Gründen der Sicherheit erlaubt sein müssen, dürfen diese die Privatsphäre nicht gänzlich aufheben und müssen immer dem Prinzip der Angemessenheit entsprechen. Der Bereich Datenschutzkonformität betrifft Fragen der Legitimität, Zweckbindung, Proportionalität, Transparenz sowie der Qualität und Sicherheit der Daten. Beim dritten Bereich, den kontextabhängigen Trade-offs, ist unter anderem die Effizienz der vorgeschlagenen Technologie oder Maßnahme eine wichtige Frage: Sind tatsächlich Sicherheitsgewinne mit deren Einsatz verbunden und sind zu diesem Zweck Einschränkungen der Privatsphäre wirklich unumgänglich? Dabei muss berücksichtigt werden, dass der Schutz der Privatsphäre selbst eine unverzichtbare Komponente der persönlichen Sicherheit darstellt.

6 Weiterführende Empfehlungen

Um den Schutz der Privatsphäre in einer sicherheitsfokussierten Welt aufrechterhalten zu können, wird eine Vielzahl von weiteren Maßnahmen und Schritten notwendig sein. Folgende Empfehlungen⁵ wurden vom PRISE-Team

und dem wissenschaftlichen Beirat als besonders wichtig eingeschätzt:

- Es sollte ein unantastbarer Kernbereich der Privatsphäre definiert werden. Es werden sich immer wieder einzelne Beispiele finden lassen, die scheinbar auch schwere Eingriffe rechtfertigen. Es gilt daher, im Vorhinein eine Grenze festzulegen, die nicht verletzt werden darf.
- Zwischen Privatsphäre und Sicherheit besteht keine lineare Austauschbeziehung. Während in einigen Fällen mehr Überwachung auch mehr Sicherheit bedeuten kann, gibt es auch die umgekehrte Relation. Der Schutz der Privatsphäre ist ein zentrales Element des Schutzes vor staatlicher Willkür. Das Verhältnis von Privatsphäre und Sicherheit ist daher kein Null-Summen-Spiel.
- Die Minimierung der Verarbeitung von personenbezogenen Daten ist ein wesentliches Prinzip des Datenschutzes. Die Nutzung und Zusammenführung von großen Datenbanken, um das Verhalten der gesamten Bevölkerung ohne spezifische Verdachtslage auf verdächtige Muster hin zu analysieren, verletzt das Grundrecht auf Unschuldsvermutung und das Prinzip der Proportionalität. Privatsphärenfördernde Sicherheitstechnologien müssen darauf abzielen, Datensammlungen zu minimieren und nur bei konkretem Verdacht darauf zuzugreifen.
- Der Schutz der Privatsphäre ist eine gemeinsame Verantwortung aller beteiligten Akteure. Während die Industrie privatsphärenkonforme und -fördernde Sicherheitstechnologien zur Verfügung stellen kann, müssen für deren konforme Nutzung alle involvierten Parteien Verantwortung übernehmen.
- Die Gestaltung von Sicherheitstechnologien sollte darauf abzielen, Eingriffe in die Privatsphäre zu vermeiden. Die gegenwärtige Praxis ignoriert oftmals den Schutz der Privatsphäre in der Entwicklungsphase oder bietet ihn nur als zusätzliche Ergänzung an. Die Übereinstimmung mit und die Förderung des Schutzes der Privatsphäre sollten ein verpflichtendes, nicht funktionales Erfordernis von Sicherheitstechnologien werden.
- Kriterien für privatsphärenfördernde Sicherheitstechnologien müssen kontinuierlich weiterentwickelt werden. Einerseits gilt es mit den stetig wachsenden technischen

Möglichkeiten und den daraus resultierenden potenziellen Verletzungen der Privatsphäre Schritt halten zu können, andererseits wird es nicht immer möglich sein, die Effizienz von Sicherheitstechnologien oder die Verletzungen der Privatsphäre, die mit ihrem Einsatz verbunden sind, im Voraus exakt zu bestimmen. Daher müssen Vorkehrungen getroffen werden, um sowohl gesetzliche Bestimmungen als auch eingeführte Sicherheitsmaßnahmen bei negativer Evaluierung revidieren zu können.

Anmerkungen

- 1) Der Langtitel von PRISE lautet „Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies“.
- 2) Der Langtitel von PASR lautet „Preparatory Action on the enhancement of the European industrial potential in the field of security research“.
- 3) Weitere Projektpartner waren der Dänischen Technologierat, der Norwegische Technologierat und das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein.
- 4) Zu diesen Kriterien siehe Raguse et al. 2008.
- 5) Weitere Informationen zu PRISE sowie sämtliche Projektberichte sind über die Projekthomepage <http://prise.oeaw.ac.at/> abrufbar.

Literatur

- Jacobi, A.; Holst, M.*, 2008: PRISE Synthesis Report – Interview Meetings on Security Technology and Privacy. Deliverable 5.8. Revision April 2008; http://prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf (download 15.12.08)
- Raguse, M.; Meints, M.; Langfeldt, O. et al.*, 2008: Criteria for privacy enhancing security technologies. Deliverable 6.2.; http://prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf (download 15.12.08)

Kontakt

Johann Čas
 Institut für Technikfolgen-Abschätzung
 Österreichische Akademie der Wissenschaften
 Strohgasse 45/3. Stock, 1030 Wien, Österreich
 E-Mail: jcas@oeaw.ac.at

« »