BSI IT-Grundschutztag in Bremen am 13. Juni 2012
„Die Welt wird digital – wem kann man noch trauen?“

Keynote

Die digitale Welt – und wie hilft IT-Grundschutz?

Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Wer zu einem IT-Grundschutztag einen Datenschutzbeauftragten einlädt, der zudem Jurist und nicht Informatiker ist, der wird nicht erwarten, dass in einer Keynote einfach ein Loblied auf den IT-Grundschutz gesungen wird.
Als Leiter des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, das eine stark technisch-organisatorische Ausrichtung hat, könnte ich Ihnen natürlich von meinen InformatikerInnen vorschwärmen. Es ist tatsächlich ein Segen für unsere Aufgabenerfüllung als Datenschutzbehörde insgesamt, dass drei meiner Mitarbeiter BSI-Grundschutzauditoren sind. Das ULD macht äußerst positive Erfahrungen mit der Grundschutz-Beratung, -Ausbildung und -Zertifizierung. Unsere Leute von der Technik sind aber insofern sprechfähiger als ich.
Meine Kompetenz und mein Anliegen liegen eher darin, den IT-Grundschutz in unserer globalen digitalen Welt unter dem besonderen Datenschutzaspekt, oder etwas weiter greifend, unter dem Aspekt des digitalen Grundrechtsschutzes zu verorten. Dies ist mein persönliches wie mein professionelles Interesse. Es gibt hier noch viel zu tun - aus Sicht des Datenschutzes wie aus Sicht der Informationssicherheit. Dies gilt für alle Bereiche: die Ebene der Gesetze, die Ebene der Organisation, die der Technikgestaltung und der Standards, bis hin zum Betrieb der einzelnen Systeme - und schließlich hinsichtlich des Bewusstseins aller Beteiligten.

Datenschutz verfolgt grundsätzlich einen interdisziplinären Ansatz und hat ökonomische, kulturelle, pädagogische und psychologische Komponenten. Ich will mein heutiges Thema nicht noch komplizierter machen, als es ohnehin schon ist: Zentrale Kernkomponenten sind die Technik und das Recht. Selbst diese Erkenntnis hat sich in der Praxis von uns Datenschutzjuristen erst Mitte der 90er Jahre des letzten Jahrhunderts richtig durchgesetzt. Eine tatsächliche Emanzipation der Technik vom Recht und dessen Gleichberechtigung hinsichtlich der personellen und finanziellen Ausstattung, etwa in Aufsichtsbehörden, steht immer noch in den Sternen. In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sitzen gerade mal zwei Technikleute als stellvertretende Leiter – die absolute Mehrheit kommt aus dem Recht oder der allgemeinen Verwaltung.

Als jemand, der seit über 20 Jahren im Bereich des Datenschutzes aktiv ist, durfte ich viel mit InformatikerInnen zusammenarbeiten. Ich habe sehr viel dabei gelernt, auch über das Verhältnis von Sicherheitstechnik und Datenschutz.

Grundanliegen des Datenschutzes seit den 70er Jahren des letzten Jahrhunderts war es, den Menschen vor einem informationstechnisch überlegenen Datenverarbeiter zu schützen. Schutzziel ist nicht die Technik und deren Funktionieren, sondern der einzelne Mensch, den wir "Betroffener" nennen. Es geht darum, die negativen Auswirkungen der Informationstechnik auf das Individuum zu

vermeiden. Nicht nur als Schutzobjekt, sondern auch in den datenschutzrelevanten Prozessen spielt der Betroffene als Subjekt eine wesentliche Rolle.

Der ursprüngliche Ansatz der Informatiker ist genau der Entgegengesetzte: Als Schutzziele wurden und werden immer noch die Technik und die diese betreibende Organisation gesehen. Das Individuum ist der potenzielle Angreifer. Ziel unserer Informatiker ist es regelmäßig, durch Technik den Risikofaktor Mensch so weit wie möglich auszuschließen. Der Ansatz der Sicherheit der Organisation, etwa eines Unternehmens, wird auch mit dem IT-Grundschutzhandbuch verfolgt.

Diese unterschiedlichen Ansätze machen - neben der andersartigen Sozialisation und der oft sehr unterschiedlichen Terminologie - die Kommunikation zwischen Juristen und Informationstechnikern manchmal nicht einfach. Inzwischen haben wir in unseren Datenschutzstrukturen in Deutschland aber Dialogverfahren entwickelt, mit denen diese Ansätze zusammengeführt werden können und auch tatsächlich zusammengeführt werden. Förderlich für diese Entwicklung war die Einsicht der Juristen in die Technikabhängigkeit und Technikgetriebenheit ihres Tuns.

Insbesondere seit dem Aufkommen des Internet sind die Grundrechtsschützer darauf angewiesen, dass die rechtlichen Ziele, etwa Zweckbindung, informationelle Gewaltenteilung, Datensparsamkeit oder die Wahrnehmung von Betroffenenrechten - also Auskunft, Löschung, Berichtigung und Feststellung der Verantwortlichkeit - technisch übersetzt werden. Mit dem Internet veränderte sich die Bedrohungslagen für Datenschützer wie für IT-Sicherheitsleute: Risiken für den Datenschutz können plötzlich von allen Beteiligten ausgehen, auch von Einzelpersonen; die IT-Sicherheit ist auch bedroht von kriminellen Organisationen, fremden Staaten, von der Technik selbst. Für Juristen wie für Informatiker wird offenbar, dass die eigene Profession zur Problemlösung nicht genügt. Globalität, Ubiquität, Universalität und Konvergenz sowie weitgehende Intransparenz des Internet machen interdisziplinäre Ansätze und Instrumentenmixe nötig. Die gegenseitige Abhängigkeit von Recht und Technik hat massiv zugenommen.

Der technische Wandel verändert auch das Datenschutzrecht. Die Technikregulierung des Datenschutzes war ursprünglich auf einen technisch-organisatorischen Maßnahmenkatalog beschränkt, der in seiner Struktur aus den 70er Jahren stammt und der inhaltlich z. B. in § 9 BDSG bis heute überlebt hat. Egal ob in dieser Auflistung der technisch-organisatorischen Maßnahmen nun 8 oder 10 Grundmaßnahmen aufgeführt waren oder sind, unbefriedigend sind sie wegen ihrer zumindest teilweise fehlenden Technikangepasstheit, ihrer mangelnden Systematik und dem Ausblenden von Schutzzielen, ja letztlich auch des Ziels des Schutzes der informationellen Selbstbestimmung der Menschen.

Diese Defizite haben einige technikorientierte Datenschützer erkannt und den Gesetzgebern aufgegeben, das Regelungskonzept weg von Maßnahmen und hin auf operationalisierte Schutzziele umzustellen. Dieser Prozess wurde durch eine Änderung des Landesdatenschutzgesetzes, des LDSG, von Nordrhein-Westfalen bestimmt. Ursprünglich standen neben den klassischen IT-Schutzzielen der CIA - also Confidentiality, Integrity und Availability - die Transparenz bzw. die Revisionsfähigkeit. Vorläufig abgeschlossen wurde die Weiterentwicklung mit dem LDSG Schleswig-Holstein, wo im Jahr 2011 die Ziele "Intervenierbarkeit" und "Nicht-Verkettbarkeit" hinzugefügt wurden. Mit diesen technischen Schutzzielen sollen

insbesondere der Schutz der Betroffenenrechte und die Zweckbindung operationalisiert werden.

Es ist insbesondere Martin Rost in meiner Dienststelle zu verdanken, dass wir so eine adäquate Verknüpfung von Recht und Technik gefunden haben, die weder von den konkreten aktuellen Anwendungen, noch von den konkret eingesetzten Techniken abhängig sind. Derzeit versuchen wir als Datenschützer, diesen Regulierungsansatz in das neue geplante Regelwerk der Europäischen Kommission zum Datenschutz, in die Europäische Datenschutz-Grundverordnung zu integrieren.

Lassen Sie mich nun versuchen, die Entwicklung aus Sicht der IT-Sicherheitstechniker darzustellen: Die Attraktivität des Datenschutzes lag für diese von Anfang an auch darin, dass hier ein gesetzliches Regelwerk vorhanden ist, das eine Legitimationsbasis für die eigene Tätigkeit bot. Tatsächlich interessierten sich die Techniker aber zumeist weniger für das Anliegen des Grundrechts- und Freiheitsschutzes. Hierfür hatte und habe ich auch viel Verständnis. IT-Sicherheit kann auch ganz anderen materiell-rechtlichen Werten dienen und lässt sich professionell zur Erreichung dieser Werte betreiben.

Es kommt nicht von ungefähr, dass das BSI eine seiner historischen Wurzeln im Staatsschutz hat. Mit der Digitalisierung aller Lebensbereiche, insbesondere auch der Verwaltung und der Wirtschaft, haben wir inzwischen einen riesigen und bunten Strauß weiterer juristischer Schutzziele: vom Urheber-, Marken- und Patentschutz hin zum weiten Feld des Schutzes von Betriebs- und Geschäftsgeheimnissen bis hin zu - so zunächst für Techniker exotisch erscheinenden - Zielen wie Jugendschutz oder Suchtprävention. Mit dem Aufkommen der Diskussion über Cyber-Terrorismus und Cyber-War spielt der Infrastruktur-Schutz eine immer wichtigere Rolle.

Diese weiteren rechtlichen und gesellschaftlichen Legitimationsmuster für die Tätigkeit von IT-Sicherheit trugen wohl dazu bei, dass das Interesse am Datenschutz begrenzt blieb. Doch will ich dieses Interesse nicht kleinreden, zumal ich es ja weiterentwickeln möchte. Aber es ist mir klar, dass IT-Sicherheitsleute einer Vielzahl unterschiedlicher Herren dienen können, deren Aufgabe nicht als weniger wichtig zu bewerten ist als das Ziel des Datenschutzes oder weiter gefasst des digitalen Grundrechtsschutzes.

Umso löblicher bewerte ich das Unterfangen des BSI, gemeinsam mit den Datenschutzbeauftragten des Bundes und der Länder ein Datenschutzkapitel in das IT-Grundschutzhandbuch zu integrieren. Erlauben Sie mir aber, dass ich die ketzerische Behauptung aufstelle, dass diese Integration wohl gut gemeint und auch ein guter erster Ansatz war, dass dieser aber längst nicht mehr den heutigen Anforderungen genügt. Dies liegt nicht nur daran, dass der Baustein "Datenschutz" im IT-Grundschutz nur ein "Kann-Baustein" ist, der für die Herstellung der Grundschutzkonformität nicht umgesetzt werden muss und im Rahmen einer Grundschutzzertifizierung keine verpflichtende Anwendung ist.

Ähnlich wie die Regelung des technisch-organisatorischen Datenschutzes aus den 70er Jahren ist der Baustein „Datenschutz“ unsystematisch und unvollständig. Wohl liefert er eine Art Checkliste, worauf man beim Datenschutz als IT-Sicherheitsbeauftragter achten sollte. Aber letztlich ist der Baustein nicht viel mehr als eine fortgeschrittene Themen- und Gedankensammlung, bei der zwischen den

Ebenen Daten - Verfahren - Organisation wild hin- und hergesprungen wird wie zwischen den Stadien Planung - Entwicklung - Test - Dokumentation - Betrieb und Evaluation. Dies ist der Grund, weshalb der Arbeitskreis Technik der Datenschutzkonferenz darüber diskutiert, diesen Baustein zu überarbeiten.

Dabei sollte es nicht darum gehen, die datenschutzrechtliche Rechtmäßigkeit und die Ordnungsgemäßheit der Datenverarbeitung in das Prüfverfahren nach Grundschutz zu integrieren. Hierfür haben wir eigenständige Datenschutz-Audits. Wohl aber kann eine Verbindung hergestellt werden, indem die auch das materielle Recht erfassenden Datenschutz-Audits oder sonstige Prüfmechanismen sowie die Ansichten der eigenen Datenschutzbeauftragten oder der Aufsichtsbehörden einbezogen werden.

Inzwischen ging und geht die Diskussion weiter, insbesondere hier in Deutschland. Im Vordergrund stehen dabei nicht mehr einzelne Schutzmaßnahmen, sondern die sechs genannten Schutzziele. Mit ihnen lassen sich Technik und Recht weiter zusammenführen. Dabei habe ich nicht nur den Datenschutz im Blick, sondern potenziell die von mir oben erwähnten weiteren rechtlich geschützten Güter, vom Staatsschutz bis hin zum Jugendschutz.

Dessen ungeachtet kommt dem Schutz auf informationelle Selbstbestimmung eine zentrale Funktion beim rechtlichen Schutz vor informationstechnischen Bedrohungen zu. Dies liegt daran, dass das Recht auf informationelle Selbstbestimmung eine dienende Funktion für alle anderen Grundrechte hat, etwa wenn das Grundrecht auf Unversehrtheit der Wohnung durch den technischen Lauschangriff bedroht wird oder das Recht auf Versammlungsfreiheit durch extensive Videoüberwachung. Eine zentrale rechtliche Schutzaufgabe sehe ich im Grundrecht auf informationelle Selbstbestimmung auch, weil ihm, wie das Bundesverfassungsgericht immer wieder betont, eine gesamtgesellschaftliche Funktion zukommt: Es geht nicht nur um den Schutz des Individuums, sondern auch um den einer demokratisch offenen und freien Informationsgesellschaft.

Und damit kommen wir zu einem Topos, der so alt ist wie die Geschichte der Technik und der Naturwissenschaft generell. Es geht um die dienende Rolle der Technik und deren Verantwortung für die gesellschaftlichen, politischen, ökonomischen und sozialen Verhältnisse. Was schon Galilei bewegt hat, bewegt uns, getrieben durch die technische Entwicklung, seit dem 20. Jahrhundert, in immer mehr Bereichen. Die Verantwortung der Technik für die Gesellschaft wird zu Recht thematisiert im Hinblick auf den Einsatz bei der Atomtechnik, der Chemie oder der Medizin. Auch die Informationstechnik hat insofern eine rasant steigende gesellschaftliche und politische Bedeutung. Dies gilt nicht nur wegen des schieren Ausmaßes, der Durchdringung aller Lebensbereiche und der Vernetzung. IT bestimmt zunehmend die Qualität unseres gesellschaftlichen Zusammenlebens, sie gibt also Antworten auf die zentralen Fragen des Ressourceneinsatzes, der Gerechtigkeit, der Wahrnehmung von Freiheiten, der demokratischen Partizipation. Insofern ist sie wohl die gesellschaftliche Schlüsseltechnologie des 21. Jahrhundert. Schon allein deshalb darf sich diese Technologie nicht naturwüchsig entwickeln, sie muss vielmehr demokratisch und grundrechtsverträglich gestaltet werden.

Gnadenlos und unverantwortlich ist die weit verbreitete Ansicht "Code is law". Diese Behauptung wird leider von vielen Informatikern, dann aber auch von geldgierigen

Geschäftsleuten aus der IT-Branche verbreitet. Google, Apple oder Facebook und viele ihrer kleineren Brüder programmieren Datenbanken, Anwendungen und Netzwerke, die funktional und nützlich und damit auch profitabel sein mögen. Diese Unternehmen dürfen aber nicht die Macht haben, Menschen oder ganze Gesellschaften zu programmieren.

Insofern sind IT-Sicherheitsbeauftragte Sozialingenieure - ob Sie dies nun wollen oder nicht. Das Werkzeug kann hierfür nicht mehr allein der IT-Grundschutz sein. Der ist und bleibt ein wichtiges Instrument. Der IT-Grundschutz muss aber integriert werden in einen breiteren Instrumentenmix, bei dem zweifellos weiterhin die klassischen Schutzgesetze wie das Datenschutzrecht eine wichtige Rolle spielen. Daneben benötigen wir aber weitere ergänzende und unterstützende Instrumente, mit denen unsere rechtlichen und gesellschaftlichen Schutzziele durch Technik- und Prozessgestaltung instrumentalisiert werden. Eine wichtige Herangehensweise ist dabei die Prüfung von Verfahren nach den oben dargestellten Schutzzielen hinsichtlich technischer Verfahren und konkreter Datenverarbeitung. Dabei können und müssen anwendungs- und technikbezogene Schutzprofile, sog. Protection Profiles, erarbeitet und anwendet werden. Hierin liegt eine gewaltige gemeinsame Herausforderung für Techniker und Juristen. Themen wie Profiling, Scoring, Tracking und die darauf aufbauende Mustererkennung und -auswertung sind noch nicht ansatzweise disziplinübergreifend erforscht. Entsprechendes gilt z. B. für digitale Identifizierungs-, Bedien- oder Bezahlverfahren.

Für die Erarbeitung von solchen Schutzprofilen können auf einer höheren Ebene technische Standards, die heute zumeist international sein müssen, dienlich sein. Auch insofern haben wir einen gewaltigen, bisher noch nicht ansatzweise befriedigten Diskussions- und Regelungsbedarf. Nicht nur die konkreten Technikanwendungen, sondern auch die Technikorganisation kann und muss derart neu geordnet werden. Dies bedeutet z. B., dass das Datenschutzmanagement nicht als Unterpunkt im Datenschutzkapitel des IT-Grundschutzes versteckt, sondern in das IT- und das IT-Sicherheitsmanagement integriert wird.

Der IT-Sicherheit kommt heute eine Bedeutung zu, die vielen Praktikern nicht bewusst sein und die bei diesen wohl auch keine durchgehende Begeisterung auslösen dürfte. IT-Leute verstehen sich zumeist eher als Bastler und Tüftler und nicht als Soziologen, Philosophen, Pädagogen oder gar Politiker - also als Sozialingenieure. Doch eben hier liegt deren wichtige aktuelle gesellschaftliche Aufgabe. So wie Menschen lernen müssen, sich sicher im Straßenverkehr sicherheitsbewusst zu verhalten, so müssen sie dies nun hinsichtlich des Datenverkehrs. Um sich diese Kulturtechnik anzueignen, müssen Sicherheits-Werkzeuge erforscht und entwickelt, anwendungsfreundlich gestaltet, den Nutzenden vermittelt und deren Nutzung überwacht werden. Es müssen Regelwerke erarbeitet werden, und zwar sowohl Best-Practice-Beispiele wie auch zwingende Verhaltenspflichten, deren Einhaltung mit Kontrolle und Sanktionen erzwungen werden.

Zwingende Regelwerke bedürfen demokratischer Legitimation. Diese müssen erarbeitet und beschlossen werden. Dies geht nicht ohne die Vermittlung von IT-Sicherheitskompetenz als Bestandteil einer umfassenderen Medienkompetenz auch bei den Politikern. Lange Zeit wurde von den meisten Menschen angenommen, Medienkompetenz sei eine Generationenfrage, die sich durch Aussterben der

digitalen Immigranten von allein erledigt, weil die digitalen Natives damit spielerisch und souverän umgehen könnten. Der Siegeszug der Piraten scheint ein Beleg für diese These zu sein. Diese These ist aber tatsächlich ein gewaltiger Irrtum. Verantwortungsvoller und sicherer Umgang mit IT ist nicht eine Frage des Alters, sondern eine Frage der Erziehung und letztlich der Kultur. Es versteht sich von selbst, dass diese Erziehung IT-Sicherheitskompetenz vermitteln muss wie auch die Kompetenz des Schutzes der durch digitale Technik bedrohten sozialen Werte.

Solange IT-Anwendungen wie das Facebook-Netzwerk den Standard für IT-Einsatz wesentlich mitbestimmen, sowohl im Hinblick auf die IT-Sicherheit wie auch im Hinblick auf Datenschutz und soziale Verantwortung, solange gibt es hier viel zu tun.

Deshalb möchte ich bei Ihnen dafür werben, dass Sie sich in die aktuellen Diskussionen über IT-Politik einmischen – also zu Themen wie Urheberrechtsschutz, zu Transparenz, zu Anonymität im Netz, zur Bekämpfung von Kinderpornografie oder Cyber-Terrorismus, natürlich zum Datenschutz, etwa bei Social Media oder zum Streben nach Sicherheit über Maßnahmen der Vorratsdatenspeicherung. Die Öffentlichkeit ist wie die Politik auf Ihre Expertise angewiesen.

Ich wurde eingangs gefragt: Wie hilft IT-Grundschutz? Meine Antwort ist: IT-Grundschutz ist wichtig und hilfreich, aber nur, wenn er als Bestandteil einer umfassenderen Aufgabe verstanden wird. Dieses umfassendere Verständnis vermisse ich heute bei den IT-Sicherheitsleuten wie auch bei den Datenverantwortlichen noch all zu oft. Für dieses umfassendere Verständnis habe ich deshalb umso lieber in dieser Keynote geworben.