„Zukunftsfaktor Datensicherheit – nationale und internationale Herausforderungen“

Michael Hange,
Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Thesen zum Vortrag im Rahmen der Sommerakademie des ULD am 30.08.2010 in Kiel

- Datenschutz und IT-Sicherheit sind heute nicht mehr voneinander zu trennen. IT-Sicherheit wird als unverzichtbarer Bestandteil ganzheitlicher Informationssicherheit verstanden, die neben dem technischen Schutz vor IT-Angriffen, auch den sicheren Umgang mit Daten berücksichtigt. Vertraulichkeit, Verfügbarkeit und Integrität gelten als grundlegende Schutzziele für Datenschutz und IT-Sicherheit gleichermaßen.

- Informations- und Kommunikationstechnik wie auch die Bedrohungen für die IT-Sicherheit haben heute globalen Charakter.
  Insbesondere gibt es weltweit agierende kriminelle Strukturen – zum Teil in einer globalisierten Schattenwirtschaft organisiert – die Staat, Wirtschaft und Gesellschaft in der Daten- und IT-Sicherheit vor neue Herausforderungen stellen. Aufgrund dieser Entwicklung ist davon auszugehen, dass die Bedeutung internationaler Standards sowohl beim Datenschutz als auch bei der IT-Sicherheit weiter zunehmen wird. Nationales Agieren ist vor diesem Hintergrund immer im internationalen Kontext zu betrachten. Werden weiterhin nationale Standards entwickelt, müssen diese international durchsetzbar sein, um nachhaltig Bestand zu haben.

- Nationale Standards wie im DIN, aber auch internationale wie bei der ISO entwickelt, können mit den Innovationszyklen in der IT häufig nicht mithalten. Technologien wie RFID oder Entwicklungen im Web 2.0 und in sozialen Netzen werden oftmals nur nachvollzogen und können nicht aktiv mitgestaltet werden. Unterschiedliche politische Rahmenbedingungen wie auch unterschiedliche Rechtsverständnisse führen auf technischer Ebene auch zu unterschiedlichen Sicherheitsniveaus. Um so mehr liegt es im deutschen Interesse, international abgestimmte Prozesse zur Standardisierung verstärkt voran zu treiben. Hier bietet die EU aufgrund gemeinsamer Werte und Ziele den Rahmen für abgestimmtes, supranationales Vorgehen.

- Ihrerseits haben Hersteller – insbesondere international agierende – ein Interesse an proprietären Standards, um damit Marktanteile zu sichern. Marktbeherrschende Unternehmen schaffen sogar Quasi-Standards.

- Eine klassische Forderung des Datenschutzes ist die Bereitstellung datenschutzfreundlicher Technologien; d.h. insbesondere Berücksichtigung der Prinzipien „Privacy by design“ und „Privacy by default“. Dies sind zum einen Anforderungen an die Entwicklung von sicheren Produkten wie auch Anforderungen an den sicheren Einsatz von Produkten. Hier sind Standards sowohl für sichere Produkte, als auch für deren sicheren Einsatz unverzichtbar.

- Der Beitrag des BSI setzt strategisch an drei Stellen an:

Erstens: Das BSI wirkt aktiv in nationalen und internationalen Standardisierungsgremien mit. So arbeitet das BSI in den relevanten ISO-Gremien mit, wie
- ISO/IEC SC 27 (IT-Sicherheitsverfahren),
- ISO/IEC SC 37 (Biometrie) und
- ISO/IEC SC 17 (Karten und persönliche Identifikation).
Auf diese Weise konnte u.a. erreicht werden, dass Forderungen des

deutschen Datenschutzes in entsprechenden Sicherheitsstandards berücksichtigt werden konnten.

Zweitens: Über Zertifizierungsprozesse mit Vorgabe von Schutzprofilen und Technischen Richtlinien kann Datensicherheit und Compliance in IT-Produkten und -Systemen verankert werden („Privacy by design“). Mit international anerkannten BSI-Zertifikaten wird ein nachweisbares, einheitlich hohes Sicherheitsniveau erreicht, das nicht zuletzt im Sinne der Exportfähigkeit auch ein industriepolitisches Argument und einen Wettbewerbsvorteil für deutsche Unternehmen darstellt.

Drittens: Der IT-Grundschutz des BSI berücksichtigt insbesondere den Aspekt „Privacy by default“. Das modular aufgebaute Konzept des IT-Grundschutzes zeigt auf, welche Sicherheitsmaßnahmen umzusetzen sind und wie ein Produkt im Kontext des Gesamtsystems sicher zu betreiben ist. Durch klare Anforderungen schafft die Vorgehensweise nach IT-Grundschutz Verbindlichkeit und durch die Zertifizierung nach ISO 27001 auch internationale Anerkennung.

- Über den IT-Grundschutz wurde eine Brücke zum Datenschutz geschlagen. Der Baustein zum Datenschutz wurde in enger Zusammenarbeit mit den Datenschützern des Bundes und der Länder entwickelt, so dass die Grundschutzkataloge heute einen hohen Referenzwert auch in der Datenschutzpraxis haben.

- Der deutsche Datenschutz steht für Anspruch und Qualität. Diese Ausgangsposition ermöglicht – mit Blick auf die internationalen Entwicklungen – auch ein initiatives nationales Handeln. Projekte wie der neue Personalausweis, die elektronische Gesundheitskarte und die De-Mail sind ambitionierte Beispiele dafür. Datenschutzerfordernisse werden in Verbindung mit den funktionalen Anforderungen an die IT-Sicherheit unter anderem durch das BSI durch Sicherheitsstandards in Form Technischer Richtlinien durchgesetzt. Die Einbindung des BSI erfolgt unter anderem durch spezialgesetzliche Regelungen.

- In besonderem Fokus der IT-Sicherheit und damit des BSI stehen IT-Massenanwendungen, insbesondere wenn sie als kritische Infrastruktur zu bezeichnen sind. Im Rahmen der Anstrengungen des Energiesparens zum Beispiel hat die EU mit der Herausgabe einer Direktive den Anstoß zur Entwicklung so genannter Smart Grids und Smart Meters gegeben. Bei der Realisierung ergeben sich Sicherheitsanforderungen aus funktionalen Erfordernissen, als kritische Infrastruktur und aus dem Datenschutz.
  Es bestehen hier besondere Herausforderungen an Betreiber, Datenschützer und staatliche Stellen, Konzepte zu entwickeln und umzusetzen, die die Aspekte des Energiesparens mit den Aspekten des Datenschutzes und der IT-Sicherheit sowie mit den ökonomischen Zielsetzungen in Einklang bringen.

- Es liegt im Interesse des BSI, den Dialog mit dem Datenschutz zu verstärken und das vorhandene Know-how im Bereich der Standardisierung einzubringen, um damit den nationalen und internationalen Herausforderungen an die Datensicherheit gerecht zu werden.

- Datensicherheit als Zukunftsfaktor erfordert ein frühzeitiges Identifizieren von Handlungsfeldern und ein vorausschauendes Zusammenwirken rechtlicher und technischer Akteure. Kooperatives Zusammenwirken aller Beteiligten schafft die Voraussetzung für durchsetzungsfähige Lösungen auch im internationalen Kontext.