Datenschutzaudit als Konvergenzkriterium zur IT-Sicherheit

Frank Reiländer, Dr. Gerhard Weck[31]

IT Security Solutions
INFODAS GmbH
Rhonestraße 2
50765 Köln
f.reilaender@infodas.de
g.weck@infodas.de

Abstract: Spätestens mit der Novelle vom Mai 2001 orientiert sich der Datenschutz stärker an den Kriterien der IT-Sicherheit, deren Bedeutung im Vergleich mit den juristisch geprägten Organisationsanforderungen deutlich steigt. Das Postulat des Datenschutzaudits quasi als Qualitätskriterium unterstreicht die Herausforderung, sich offensiv mit dem Thema Daten- bzw. IT-Sicherheit auseinander zu setzen. Dieser Beitrag beschreibt die Konvergenz von Auditanforderungen im Datenschutz hin zu bewährten, standardisierten Ansätzen der IT-Sicherheit, praxisnah und projekterprobt mit Industrieunternehmen.

IT-Sicherheitstrends im Datenschutz

Die im Mai 2001 verabschiedete dritte Fassung des Bundesdatenschutzgesetzes (BDSG) ist wesentlich von zwei Faktoren getrieben: Der Umsetzung der EU-Vorgaben aus der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995 und von grundlegenden Überlegungen für ein „modernes Datenschutzrecht“. Wichtige Eckwerte wie die dem Systemdatenschutz zuzurechnenden Prinzipien der Datenvermeidung und Datensparsamkeit, des Datenschutzes durch Technik sowie die Festschreibung eines freiwilligen Datenschutzaudits, das u.a. den Trend zur Stärkung der Selbstkontrolle verdeutlichen soll, wurden darin aufgenommen. Zu den Eckpunkten der Neuregelungen zählen, neben dem erweiterten Geltungsbereich und der erweiterten Transparenz gegenüber dem Betroffenen, erweiterte Verarbeitungsbeschränkungen und eine erweiterte Datenschutzkontrolle. Gerade die beiden letztgenannten Kriterien führen – neben einer Stärkung der Position des betrieblichen Datenschutzbeauftragten – zu einem deutlichen Anstieg hinsichtlich seiner Pflichten und Verantwortung.

[31] Die Autoren arbeiten langjährig im Bereich IT-Sicherheit und Datenschutz und sind vom BSI lizenzierte IT-Grundschutz-Auditoren.

Trends zu Standards in der IT-Sicherheit

In einer vernetzten Welt, die mittels offener Standards interagierende IT-Systeme verbindet, haben sich auch die Regelwerke hin zu IT-Sicherheits-Standards basierend auf Prozessstrukturen und vernetzen Systemen gewandelt. Früher hat sich der Fokus von ITSEC-Kriterien oder BSI-Grundschutzmaßnahmen [GSHB] auf ein einzelnes IT-System bzw. dessen Sicherheitskern gerichtet. Heute wird einer ganzheitlichen Sicht hinsichtlich organisatorischer Regelungen und der gesteigerten Komplexität in Bezug auf Netzstrukturen und Schnittstellen mittels der Protection Profiles in den Common Criteria, der Prozessbetrachtung nach BS 7799 bzw. ISO 17799 und CobiT und durch die Modellierung des IT-Verbunds nach BSI-Grundschutz Rechnung getragen. Das IT-Grundschutz-Zertifikat, das innerhalb des Qualifizierungsschemas den höchsten Grad der Vertrauenswürdigkeit und des Sicherheitsniveaus darstellt, ist somit ein Schritt in Richtung „messbare" Sicherheit [BSI02], basierend auf einem etablierten und praxisbewährten Katalog von Standard-Sicherheitsmaßnahmen.

Datenschutzaudit im Spannungsfeld Datenschutz und IT-Sicherheit

Willenserklärungen und Ansätze zu einem Datenschutzaudit finden sich zahlreich, ob in einschlägigen Studien oder bereits in der Gesetzgebung verankert. Kritisch begleiten die Autoren den Weg, den das Datenschutzaudit unter den Leitmotiven Stärkung der Selbstkontrolle und Erhöhung der Transparenz für den Betroffenen nimmt. Die bereits 1997 in § 17 Mediendienste-Staatsvertrag festgeschriebene Absichtserklärung, dass eine Verfahrensregelung durch ein „besonderes Gesetz" zum Datenschutzaudit erfolge[32], wird seitens der Exekutive im Folgenden alleinig gestützt durch die provet-Studie von Roßnagel [Ro99]. Im Gegensatz hierzu beobachten die Autoren vielfach den Wunsch, als Zielsetzung eines Datenschutzaudits die Unterstützung des betrieblichen Datenschutzbeauftragten in seinem erweiterten Verantwortungsbereich, insbesondere hinsichtlich IT-lastiger Verfahren wie dem Verfahrensverzeichnis und der Vorabkontrolle, in den Vordergrund zu stellen.

Diese Kritik wird auch von Drews/Kranz [DreKra00] vorgetragen. Sie lehnen das Datenschutzaudit gemäß der Roßnagel-Studie als dritte Kontrollebene zusätzlich zu den etablierten Instrumenten des betrieblichen Datenschutzbeauftragten und den Aufsichtsbehörden ab, da dies „ineffizienten Aufwand und eine deutliche Schwächung der weisungsfreien, unabhängigen Stellung des betrieblichen Datenschutzbeauftragten zur Folge haben würde". Sie äußern dabei die Meinung, dass sich das Ziel zur Realisierung von mehr Datenschutz auch ohne Audit erreichen ließe, durch konsequente Anwendung des bestehenden, dualen Kontrollsystems in Form der betrieblichen Selbstkontrolle und Überprüfungen durch die zuständige Aufsichtsbehörde. Die Zielsetzung zur Schaffung von Wettbewerbsvorteilen erachten sie nur für Teilbereiche (IT-Unternehmen) als sinnvoll und sprechen sich in ihrer Kernthese für ein Datenschutzaudit für Spezialgebiete (IT-Bereich, Tele- und Multimediadienste) und

[32] Diese lässt bis heute - zusammen mit gleichlautenden Ausführungen in späteren Gesetzgebungen zum Datenschutz - auf sich warten.

gegen eine generelle Konstituierung des Datenschutzaudits aus und entsprechen damit auch der Meinung der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) [GDD99].

Getrieben von der Ansicht, dass es „nicht an gut gemeinten Ideen und interessanten theoretischen Debatten, wohl aber an Vollzug und Umsetzung“ mangelt [Bäu01], stellt Bäumler einen Praxistest als „neues Instrument auf dem Gebiet des Datenschutzes“ vor (Ziff. A 1.2 [HDSA-SH]), begünstigt durch die schleswig-holsteinische Landesgesetzgebung zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG-SH. Neben diesem Ansatz zur Auditierung organisatorischer Aspekte werden Merkmale des Systemdatenschutzes in einem weiteren, ebenfalls beim Unabhängigen Landeszentrum für den Datenschutz (ULD) durchgeführten Verfahren, der Verleihung des „IT-Gütesiegels“ auditiert, was die Entwicklung datenschutzfreundlicher Produkte gezielt fördern soll. Auch das quid!-Projekt [quid!] geht mit der Verleihung eines weiteren Siegels diesen Weg.

Konvergenz zu bewährten Standards

Alle diese Ansätze stellen Triebfedern zur Förderung eines modernen, technisch unterstützten Datenschutzes dar. Die Autoren stehen diesen Zertifizierungsschemas jedoch insoweit skeptisch gegenüber, als sie neue Prüfverfahren anwenden, deren Transparenz und Akzeptanz als zunächst äußerst gering beurteilt wird. Eine Einführung solch autarker und nur Teilbereiche abdeckender Standards führt so möglicherweise genau zu dem befürchteten „Wildwuchs“ an Datenschutz-Gütesiegeln, den u.a. auch die GI in ihrer Erklärung zum Datenschutzaudit [GI00] anspricht. Mit dem Entwurf eines Datenschutz-Bausteins zum IT-Grundschutzhandbuch des BSI durch den Bundesbeauftragten für den Datenschutz [BfD99] wurde in einem ersten Ansatz die Konvergenz zu bewährten Standards der IT-Sicherheit [GSHB] gesucht. Die offensichtlich aufgrund interministerieller Zuständigkeitsdebatten nicht offiziell verabschiedeten Gefährdungs- und Maßnahmenkataloge zum Datenschutz decken im Wesentlichen die organisatorischen Anforderungen des Datenschutzes ab. In einer Zuordnungstabelle werden erste Ansätze zur Abbildung der „zehn Regeln zur Datensicherung“ gemäß Anlage zu § 9 BDSG (in der Fassung von 1990) aufgezeigt.

Die Autoren haben diesen Ansatz im Januar 2003 aufgegriffen. Mit einem praxisorientierten Vorgehen sollte die postulierte Konvergenz verifiziert werden. Analog zur Abbildungsskizze der „zehn Regeln zur Datensicherung“ gemäß Anlage zu § 9 BDSG (1990) ist eine Verknüpfungstabelle zu den „acht Geboten“ der Datensicherheit gemäß Anlage zu § 9 BDSG (2001) unter Verwendung des Werkzeugs SAVe® [SAVe] entstanden. Jedes Kontrollziel ist in einem analog zum IT-Grundschutzhandbuch erstellten Baustein abgebildet und mit den entsprechenden Gefährdungen und Maßnahmen verknüpft. Im Rahmen eines integrierten und standardisierten Verfahrens sind auch die organisatorischen Aspekte des Grundschutz-Bausteins 3.5 („Datenschutz“) unter der Maßgabe der oben beschrieben, zwischenzeitlichen Tendenzen () weiterentwickelt worden. In Expertenworkshops wird die Zuordnung der technisch-

organisatorischen Schutzmaßnahmen gemäß Anlage zu § 9 BDSG (2001) vor dem Hintergrund neuer Grundschutz-Maßnahmen fortlaufend erweitert.

Fazit

Dieser Praxisbericht macht deutlich, dass sich IT-Sicherheit und Datenschutz in vielen Aspekten ergänzen. In konkreten Einzelfällen liegt das Synergiepotential einer gemeinsamen Bearbeitung auf der Hand und macht die Nutzung einer Werkzeugunterstützung, wie sie in der überwiegenden Zahl aktueller IT-Grundschutz-Projekte angewendet wird, doppelt wertvoll. Das geschilderte Vorgehen setzt nach Meinung der Autoren die nicht geregelten gesetzlichen Forderungen nach einem Datenschutzaudit unter den Aspekten von Selbstkontrolle, Effizienz und Wirtschaftlichkeit sinnvoll in die Praxis um.

Literaturverzeichnis

[Bäu01] Helmut Bäumler, Datenschutzaudit und IT-Gütesiegel im Praxistest, RDV 2001, 167.

[BfD99] Entwurf Baustein 3.5 zum IT-Grundschutzhandbuch des BSI, Bundesbeauftragter für den Datenschutz, 1999, http://www.bfd.bund.de/technik/DS-KAP/35.htm.

[BMI01] Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze, Synopse zu dem am 23. Mai 2001 in Kraft tretenden Änderungen (nur) des BDSG (mit Begründung des Regierungsentwurfs, BT-Drs. 14/4329, und Begründung zur Beschlussempfehlung des BT-Innenausschusses vom 04.04.2001, BT-Drs. 14/5793), Bundesministerium des Inneren, Referat V 7, 118, Ziffer 3.

[BSI02] BSI (Hrg.): Qualifizierung / Zertifizierung nach IT-Grundschutz – Eckpunktepapier, http://www.bsi.de/gshb/zert/eckpunkt.htm, Stand 25.03.2002.

[DreKra00] Hans-Ludwig Drews, Hans Jürgen Kranz, Datenschutzaudit, DuD 4/2000, 226.

[GDD99] GDD-Mitteilungen 2/1999, 3.

[GI00] Vorschlag des Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit" zu einer Stellungnahme der Gesellschaft für Informatik (GI) zur Gesetzlichen Regelung eines Datenschutzaudits, Mai 2000, http://www.gi-ev.de/informatik/presse/krypto5.shtml.

[GSHB] IT-Grundschutzhandbuch, Schriftenreihe zur IT-Sicherheit, Band 3, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Bundesanzeiger-Verlag, Stand Mai 2002, aktuelle Version abrufbar unter http://www.bsi.de/gshb/deutsch/menue.htm.

[HDSA-SH] Hinweise des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG vom 22. März 2001, Amtsblatt für Schleswig-Holstein, 196-200.

[quid!] Projekt quid!, Qualität im betrieblichen Datenschutz, http://www.quid.de

[Ro99] Prof. Dr. Alexander Roßnagel, Datenschutzaudit – Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit, Rechtsgutachten für das Bundesministerium für Wirtschaft und Technologie, Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität GH Kassel, Mai 1999, abrufbar u. a. unter http://www.iid.de/iukdg/gus/DASA.html, Ziffer 3.8.2.

[SAVe] IT-Sicherheitsdatenbank SAVe®, Version 3.0, INFODAS GmbH, 2003, Kurzanleitung, Kap. 8.3, 47, http://www.save-infodas.de.