Gisela Quiring-Kock

Anforderungen an ein Datenschutzmanagementsystem

Aufbau und Zertifizierung

Im Rahmen der Diskussion über die Aufgaben der beabsichtigten Stiftung Datenschutz wird auch das Datenschutzaudit diskutiert. Dieses ist zwar seit langem in § 9a BDSG vorgesehen, die Regelung der Anforderungen, die in einem separaten Gesetz erfolgen sollte, steht aber immer noch aus. Das hat eine Reihe von Unternehmen, die in diesen Bereichen als Dienstleister tätig werden möchten, veranlasst, über die Zertifizierung von Datenschutzmanagementsystemen einerseits und Produkte und Anwendungsverfahren andererseits nachzudenken. Der Beitrag stellt grundsätzliche Überlegungen zu Datenschutzmanagementsystemen vor, beschreibt eine sinnvolle Vorgehensweise und will Missverständnisse ausräumen.

1 Grundsätzliche Überlegungen

1.1 Datenschutz, IT-Sicherheit und IT-Grundschutz

Der Datenschutz legt fest, unter welchen Voraussetzungen (Rechtsgrundlage, Erforderlichkeit, Zweckbindung, Datenvermeidung etc.) personenbezogene Daten unter Einhaltung bestimmter technischer und organisatorischer Maßnahmen verarbeitet werden dürfen. Für nicht-öffentliche Stellen und für öffentliche Stellen, soweit sie am Wettbewerb teilnehmen, geschieht dies auf der Basis des Bundesdatenschutzgesetz (BDSG) [1]; für hessische öffentliche Stellen im Hessischen Datenschutzgesetz (HDSG) [2]; Für öffentliche Stellen anderer Bundesländer im jeweiligen Landesdatenschutzgesetz. Viele dieser Maßnahmen dienen auch der IT-Sicherheit.

Die IT-Sicherheit trifft technische und organisatorische Maßnahmen, um das von einer Organisation (Unternehmen, Behörde) benötigte Maß an Vertraulichkeit, Verfügbarkeit und Integrität der zu verarbeitenden Daten – unabhängig vom Personenbezug – sicherzustellen.

Der Datenschutz betrachtet die Maßnahmen der IT-Sicherheit als wesentliches Werkzeug, um die Datenschutzziele zu erreichen.

Dr. rer. nat. Gisela Quiring-Kock

Referatsleiterin Informatik beim Hessischen Datenschutzbeauftragten.

E-Mail: G.Quiring-Kock@datenschutz.hessen.de

Zwar sind in den Datenschutzgesetzen unterschiedliche Formulierungen für diese Ziele gewählt (z. B. in der Anlage zu § 9 BDSG und in § 10 Abs. 2 HDSG Zutritts-, Benutzer-, Zugriffs-, Datenverarbeitungs-, Verantwortlichkeits-, Auftrags-, Dokumentations- und Organisationskontrolle; in § 9 des Thüringer Datenschutzgesetzes (ThürDSG) oder § 10 des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität, Revisionsfähigkeit und Transparenz), für das Ergebnis spielt dies jedoch keine Rolle.

Die Betrachtung der Datenschutzziele macht deutlich, dass es trotz unterschiedlichem Fokus im Zeitalter der automatisierten bzw. elektronischen Datenverarbeitung Datenschutz ohne IT-Sicherheit nicht geben kann. Vielmehr umfassen die Maßnahmen für den Datenschutz im Wesentlichen diejenigen für die IT-Sicherheit. Als mögliche Ausnahmen seien hier Blitzschutz und Handfeuerlöscher genannt, die man aber durchaus auch als Maßnahmen zur Datenverarbeitungskontrolle bzw. zur Verfügbarkeit sehen kann.

Zur Umsetzung der IT-Sicherheit für Daten mit normalem Schutzbedarf dient der IT-Grundschutz. Hier hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die IT-Grundschutz-Kataloge [3] entwickelt, in denen Gefährdungen und zugehörige Maßnahmen für verschiedene Bausteine aufgelistet sind. Diese Kataloge werden ständig aktualisiert und ergänzt.

Es herrscht zumindest unter Datenschützern Einigkeit, dass Datenschutz die Umsetzung des IT-Grundschutzes bei der für die Datenverarbeitung verantwortlichen Stelle und ggf. bei deren Auftragnehmer erfordert bzw. voraussetzt. Denn ein Angreifer wird alle Schwachstellen in der IT einer Organisation für seine Zwecke nutzen, nicht nur jene, die evtl. ausschließlich personenbezogene Daten betreffen.

Es gibt einige Bereiche, in denen Anforderungen und Maßnahmen des Datenschutzes und solche der IT-Sicherheit nicht von

vornherein übereinstimmen, sondern erst in Einklang gebracht werden müssen: beispielsweise bei der Protokollierung von externen Angriffen oder Benutzer- und Systemverhalten. Für die IT-Sicherheit wäre eine vollständige Protokollierung aller Aktivitäten über große Zeiträume unbedenklich, datenschutzgerecht ist eine aussagefähige, aber datensparsame Gestaltung der Protokollierung unter Beachtung der Grundsätze der Erforderlichkeit und der Zweckbindung.

Diese gestalterische Aufgabe kann nur gelöst werden, wenn man beide Aspekte gleichzeitig betrachtet. Aus diesem Grund hat der Arbeitskreis Technische und organisatorische Fragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder das IT-Grundschutzhandbuch bzw. die Grundschutzkataloge um den Baustein „B1.5 Datenschutz" ergänzt [4], der 13 typische zusätzliche Gefährdungen im Umfeld des Datenschutzes betrachtet und für diesen Bereich ein ergänzendes Maßnahmenbündel von 16 Maßnahmen benennt und ausführlich erläutert, das für alle IT-Systeme und IT-Verfahren anzuwenden ist, mit deren Hilfe personenbezogene Daten verarbeitet werden [5, 6].

Wegen der oft schwierigen Rechtslage bei Datenschutzfragen in allgemeinen oder spezialrechtlichen Regelungen sollte zur Beurteilung der gesetzlichen Anforderungen und der daraus folgenden Maßnahmen für das IT-Sicherheits- und das Datenschutzkonzept fachkundige Unterstützung in Anspruch genommen werden.

Der Datenschutzbaustein ist in der Zertifizierung nach IT-Grundschutz nicht enthalten, kann aber ggf. von entsprechend qualifizierten Auditoren mit einbezogen werden. Dies ändert allerdings nichts daran, dass die Einhaltung der datenschutzrechtlichen Bestimmungen durch unabhängige Datenschutz-Kontrollinstanzen überprüft wird:

Die betrieblichen und behördlichen Datenschutzbeauftragten haben die Aufgabe der internen Datenschutzkontrolle. Der Hessische Datenschutzbeauftragte ist zuständig für die Beratung und Kontrolle der Dienststellen der hessischen Gebietskörperschaften sowie derjenigen Stellen, die deren Aufsicht unterliegenden und Aufgaben der öffentlichen Verwaltung wahrnehmen. Seit dem 1. Juli 2011 ist ihm auch die Aufgabe der Datenschutzaufsichtsbehörde nach § 38 BDSG für die nicht-öffentlichen Stellen (z. B. Unternehmen) mit Sitz in Hessen übertragen. Analoges gilt für die anderen Bundesländer; für die Bundesbehörden ist der Bundesbeauftragte für Datenschutz zuständig.

Wenn eine Zertifizierung vorliegt, die die Maßnahmen zum Datenschutz einbezogen hat, kann sie den Aufsichtsbehörden ihre Tätigkeit erleichtern. Das führt – darauf sei an dieser Stelle ausdrücklich hingewiesen – nicht dazu, dass die Datenschutzbeauftragten an das Ergebnis der Zertifizierung gebunden sind; sie können eigene Wertungen treffen.

1.2 Datenschutz- und Informationssicherheitsmanagementsysteme

Die internationale Norm ISO/IEC 27001 *Information technology – Security techniques – Information Security Management Systems – Requirements* spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Hierbei werden sämtliche Arten von Organisationen (z. B. Handelsunternehmen, staatliche Organisationen, Non-Profit Organisationen) berücksichtigt. Sie beschreibt unter Verwendung des so genannten „Plan-Do-Check-Act (PDCA)"-Modells einen prozessorientierten Ansatz zum Aufbau eines Informations-Sicherheits-Management-Systems (ISMS).

Ein Spezialfall von ISO 27001 ist der BSI-Standard „ISO 27001 auf der Basis von IT-Grundschutz". Das BSI (Bundesamt für Sicherheit in der Informationstechnik) ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit. Es ist zur Erteilung von Sicherheitszertifikaten für informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile ermächtigt gemäß §§ 3 und 9 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG).

Bei der Zertifizierung nach „ISO 27001 auf der Basis IT-Grundschutz" hält sich das BSI an die dafür vorgegebenen internationalen Standards. Dies betrifft neben der Zertifizierung von ISMS gemäß ISO 27001 auch die Akkreditierung der für das BSI in diesem Bereich als Auditoren tätigen Personen gemäß ISO 27006 *Information technology – Security techniques. Requirements for bodies providing audit and certification of information security management systems*. Zusätzlich bindet es die Grundschutzkataloge in das Verfahren ein und erreicht damit eine starke Strukturierung, die bei der Durchführung hilfreich sein kann.

Die vom BSI in diesem Bereich vergebenen Zertifikate sind allerdings – im Gegensatz zu den genuinen ISO 27001-Zertifizierungen – nicht international anerkannt. Das hat folgenden Grund: In Deutschland wird die Akkreditierung von Konformitätsbewertungsstellen für ISMS gemäß ISO 27001 als hoheitliche Aufgabe des Bundes durch die Akkreditierungsstelle gemäß § 1 des Gesetzes über die Akkreditierungsstelle (Akkreditierungsstellengesetz – AKKStelleG) durchgeführt. Die deutsche Akkreditierungsstelle führt ein Verzeichnis der akkreditierten Konformitätsbewertungsstellen mit Angabe des fachlichen Umfangs und hält es gemäß § 2 Satz 2 AKKStelleG auf dem neuesten Stand. Das BSI als nationale Zertifizierungsbehörde im Bereich der IT hat sich nicht selbst dem Verfahren zur Akkreditierung als Konformitätsbewertungsstelle unterworfen.

Der Begriff „ISO 27001 auf der Basis IT-Grundschutz" sollte nicht missverstanden werden. Hier werden die Grundschutzkataloge als „Basis" verwendet. Das bedeutet aber nicht, dass die Zertifizierung nach ISO 27001 auf den Bereich des normalen Schutzbedarfs beschränkt ist oder reduziert wird. Vielmehr ist hier, genauso wie bei der genuinen ISO 27001-Zertifizierung, in jedem Fall eine Risikoanalyse erforderlich. Diese Risikoanalyse ist die Grundlage für die Erstellung der beiden für die Durchführung der Zertifizierung zentralen Dokumente, nämlich des Sicherheitskonzepts und des Risikobehandlungsplans.

Im Falle der Verarbeitung von Daten mit hohem oder sehr hohem Schutzbedarf muss eine „erweiterte" Risikoanalyse vorgenommen und festgestellt werden, ob und ggf. wie diesen Risiken mit zusätzlichen Maßnahmen so weit begegnet werden kann, dass das Restrisiko tragbar ist. Das gilt zunächst unabhängig davon, ob es sich um personenbezogene Daten oder andere für die Organisation wichtige Informationen im Sinne von Unternehmenswerten handelt.

ISO 27001 fordert, dass das verbleibende Risiko von einem Mitglied der Leitung der Organisation (Geschäftsführer, Behördenleiter) persönlich verantwortet werden muss; dies ist in einem handschriftlich unterschriebenen Dokument zu bestätigen. Insbesondere bei personenbezogenen Daten mit hohem oder sehr hohem Schutzbedarf kann die automatisierte Verarbeitung der

Daten aber auch unzulässig sein, wenn der Schutz der Daten in dem betreffenden Verfahren nicht sichergestellt werden kann.

Im Anhang A, der zum normativen Teil von ISO 27001 gehört, ist der Datenschutz unter der Ziffer A.15.1.4 *Data protection and privacy of personal information* enthalten, aber nicht weiter differenziert. Eine ISO 27001-Zertifizierung, auch eine genuine, ist also ohne Datenschutz nicht zu haben.

Der Datenschutzbaustein B 1.5 der Grundschutzkataloge mit seinen konkreten Listen und Erläuterungen datenschutzspezifischer Gefährdungslagen und Maßnahmenbündel (s. o.) ist kein Pflichtbaustein für die Zertifizierung nach ISO 27001, auch nicht für die des BSI auf der Basis von IT-Grundschutz. Es steht aber selbstverständlich jeder Organisation frei, ihn nicht nur beim Aufbau ihres ISMS zu verwenden, sondern ihn auch zusätzlich in die ISO 27001-Zertifizierung mit einzubeziehen.

Beim Aufbau eines Datenschutzmanagementsystems sind Checklisten sinnvoll, an denen sich die für die Datenverarbeitung verantwortlichen Stellen sowie deren Auftragnehmer beim Aufbau eines Datenschutzmanagementsystems orientieren können, sowie Werkzeuge zur technischen Unterstützung des Datenschutzmanagement-Prozesses.

2 Datenschutzmanagementsysteme

2.1 Aufbau eines Datenschutzmanagementsystems

Hier stellt sich zunächst die Frage, ob ein Datenschutzmanagementsystem autonom aufgebaut oder in ein Informationssicherheitsmanagementsystem (ISMS) integriert werden sollte. Aus den bisherigen Ausführungen ergibt sich eine Reihe von Argumenten für die Integration des Datenschutzmanagementsystems in das ISMS:

- Datenschutz setzt den IT-Grundschutz voraus.
- Zumindest im Bereich der Protokollierung gibt es eine gemeinsame Gestaltungsaufgabe.
- Der Datenschutz ist in der Norm ISO 27001 enthalten (Anhang A, Ziffer A.15.1.4).
- Es gibt den Baustein B 1.5 Datenschutz in den Grundschutzkatalogen des BSI.

Umgekehrt müssten in ein autonomes Datenschutzmanagementsystem fast alle Anforderungen an die IT-Sicherheit mit aufgenommen werden.

Ein Datenschutzmanagementsystem sollte daher sinnvoller Weise auf einem normierten bzw. standardisierten ISMS aufsetzen. Es bietet sich an, nach ISO 27001 zu verfahren und zusätzlich den Datenschutzbaustein der Grundschutzkataloge zu verwenden und verbindlich in die Zertifizierung mit einzubeziehen. Falls sich zukünftig wichtige zusätzliche Datenschutzthemen ergeben, die damit nicht abgedeckt sind, kann man sich an eine der deutschen Datenschutzkontrollinstanzen wenden, damit der Autor des Bausteins, der Arbeitskreis Technische und organisatorische Fragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, den Baustein ggf. entsprechend anpasst oder erweitert.

Die Vorteile einer Integration des Datenschutzmanagementsystems in das ISMS sind:

- Es gibt bereits einen internationalen Standard mit klaren Vorgaben.
- Es gibt zwei auf diesem Standard beruhende Zertifizierungsverfahren: ein internationales sowie ein weiter differenziertes nationales auf der Basis von IT-Grundschutz.
- Die Auditoren werden jeweils nach der Norm ISO 27006, also nach den gleichen Kriterien, akkreditiert.
- Der vorhandene Datenschutzbaustein kann bei Bedarf erweitert werden.
- ISO 27001 fordert eine Koordinierung der Informationssicherheit durch Repräsentanten von verschiedenen Teilen der Organisation mit relevanten Rollen und Funktionen. Es ist sinnvoll, hieran sowohl den IT-Sicherheitsbeauftragten als auch den betrieblichen bzw. behördlichen Datenschutzbeauftragten zu beteiligen. Die IT-Sicherheitsleitlinie für die Hessische Landesverwaltung schreibt genau das für die IT-Sicherheitsmanagementteams der Dienststellen vor. Dieses Gremium kann und sollte gleichzeitig die Koordination im Bereich des Datenschutzes übernehmen. Nur so wird die gestalterische Aufgabe gelöst und gleichzeitig Doppelarbeit vermieden.

Die am Markt befindlichen Versuche von Unternehmen, eigene Datenschutzmanagementsysteme zu definieren, reichen von einer unvollständigen Zusammenstellung der datenschutzrechtlichen Regelungen des BDSG bis hin zu einer weitgehenden Übernahme des Datenschutzbausteins der Grundschutzkataloge des BSI ergänzt durch Teile anderer Normen und Standards.

Aus meiner Sicht erscheint es nicht sinnvoll, weitere Datenschutzmanagementsysteme zu kreieren und damit von Nutzern in Wirtschaft und Verwaltung zusätzlich noch eine zeit- und kostenaufwändige Auswahl eines geeigneten proprietären Systems zu verlangen. Vielmehr ist es empfehlenswert, als Standard die Norm ISO 27001 zusammen mit dem Datenschutzbaustein zu nutzen.

2.2 Zertifizierung von Datenschutzmanagementsystemen

Eine Zertifizierung von Datenschutzmanagementsystemen sollte wie die von ISMS stets nach umfassenden, sinnvollen und objektiven Kriterien erfolgen und auf abweichende Definitionen üblicher Begriffe verzichten. Weder eine Zertifizierung anhand eines lückenhaften Systems noch eine „Auditierung mit Augenmaß", wie sie am Markt derzeit bereits angeboten werden, erscheint daher zielführend. Organisationen können nur dann von einem Audit profitieren, wenn alle Fakten klar benannt werden, unabhängig davon, ob es sich um Stärken oder um Schwächen handelt. Letztere können dann im Verlaufe des Managementprozesses gezielt in Angriff genommen werden.

Unternehmen, die im Bereich Datenschutzmanagementsysteme ihre Dienste anbieten wollen, sollten sich vielmehr als Auditoren nach der Norm ISO 27006 akkreditieren lassen und darüber hinaus die erforderliche Fachkunde im Datenschutzrecht sowie seiner technischen und organisatorischen Umsetzung erwerben.

Eine Zertifizierung eines ISMS nach ISO 27001 und demzufolge auch die eines Datenschutzmanagementsystems gemäß dem hier vorgeschlagenen Verfahren setzt immer eine – ggf. erweiterte – Risikoanalyse voraus. Insbesondere die Dokumente „Statement of Application", das einem Sicherheitskonzept entspricht, und der „Risiko-Behandlungsplan", die im Rahmen der ISO 27001-Zertifizierung erstellt werden, sind zentrale Dokumente auch für die Prüfung durch Datenschutzbeauftragte bzw. Aufsichtsbehörden. Dies gilt selbst dann, wenn nicht auf der Basis IT-Grundschutz

zertifiziert wird, und selbstverständlich auch, wenn der Datenschutzbaustein nicht in die Zertifizierung einbezogen wurde.

3 Grenzen und Missverständnisse

3.1 Datenschutzrechtliche Grenzen

In den Rechtsvorschriften zum Datenschutz sind unbestimmte Rechtsbegriffe enthalten, die der Auslegung bedürfen. Dazu gehören u. a. die Begriffe Angemessenheit und Erforderlichkeit.

Eine Zertifizierung in Bezug auf die Umsetzung des Datenschutzes und die Einführung eines Datenschutzmanagements wird bei unbestimmten Rechtsbegriffen auf dokumentierten rechtlichen Wertungen aufsetzen.

Es ist nicht Zweck oder Inhalt der Zertifizierung, die von der Daten verarbeitenden Stelle selbst oder von Beratern oder anderen von ihr beauftragten Dritten getroffenen Wertungen und Auslegungen im Einzelnen zu überprüfen. Die Auditoren legen sie Ihrer Tätigkeit zu Grunde und setzen sie damit als richtig bzw. zutreffend voraus. Sie müssen aber über die erforderliche rechtliche und technische Fachkunde verfügen, um die Umsetzung der datenschutzrechtlichen Ziele beurteilen zu können. Und selbstverständlich müssen sie in der Lage sein, offenkundige Mängel zu erkennen und diese dann im Audit darstellen.

Dazu gehört beispielsweise die Verarbeitung von personenbezogenen Daten mit hohem Schutzbedarf, insbesondere der „besonderen Arten" nach § 3 Abs. 9 BDSG wie Religionszugehörigkeit, Gesundheit etc., wenn eine erweiterte Risikoanalyse fehlt oder die erforderlichen Maßnahmen nicht umgesetzt sind.

Behördlichen bzw. betrieblichen Datenschutzbeauftragten wie auch Datenschutzaufsichtsbehörden gegenüber entfalten die getroffenen Wertungen aber keinerlei Bindungswirkung. Ihre Aufgabe ist eine unabhängige Prüfung der vorgenommenen Wertungen und Auslegungen im Hinblick darauf, ob sie rechtlich in Ordnung sind. Die Zertifizierung kann hier Hilfestellung sein, weil sie die für die Datenverarbeitung verantwortliche Stelle zwingt, überhaupt Überlegungen hierzu anzustellen und die getroffenen Wertungen und Auslegungen zu dokumentieren, und so die Prüfung erleichtert.

§ 9a BDSG befasst sich mit dem Datenschutzaudit. Dort heißt es in Satz 2: „Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt." Dieses Gesetz gibt es noch nicht. Demzufolge kann auch kein Datenschutzaudit auf dieser Basis durchgeführt werden. Dennoch gibt es Unternehmen, die Zertifikate „gemäß § 9a BDSG" ausstellen. Solange das Verfahren nach § 9a BDSG nicht geregelt ist, ist eine solche Zertifizierung unzulässig und irreführend.

3.2 Inhaltliche Grenzen

Ein Informationssicherheitsmanagementsystem nach ISO 27001 zertifiziert nicht den IT-Grundschutz selbst, insbesondere nicht auf der Ebene von Produkten und Anwendungsverfahren. Vielmehr geht es hier darum, im Sinne des Plan-Do-Check-Act-Verfahrens eine dauerhafte Aktualität von Unterlagen und ständige Verbesserungen des Prozesses zu erreichen. Dieser Management-Prozess erlaubt bzw. befähigt, die Anforderungen an die IT-Sicherheit umzusetzen. Gegenstand ist hier also nicht die Informationssicherheit selbst, sondern die ständige Überprüfung und Verbesserung derselben. Analoges gilt für ein Datenschutzmanagementsystem.

Für konkrete Produkte oder Verfahren, die beschafft werden sollen oder die beim Auftragnehmer eingesetzt werden, kann und sollte die Umsetzung der Anforderungen der IT-Sicherheit durch eine Zertifizierung nach den *Common Criteria* (CC), den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik", nachgewiesen und so das erforderliche Vertrauen geschaffen werden. Auch eine Zertifizierung nach einem speziellen Protection Profile (PP), das auf der Basis der Common Criteria für bestimmte Produkte oder Verfahren als Anforderungskatalog für Lösungen konkreter Aufgaben definiert wurde, ist möglich. Solche Protection Profiles werden zunehmend auch für Ausschreibungen beispielsweise im öffentlichen Bereich, verwendet; die Erfüllung der Anforderungen kann dann mit der Zertifizierung nach dem PP nachgewiesen werden.

Gleichwohl umfasst nach Aussagen des BSI eine Zertifizierung nach ISO 27001 auf der Basis IT-Grundschutz auch eine Zertifizierung der Umsetzung des IT-Grundschutzes. Obwohl hier die Grundschutzkataloge zugrunde gelegt werden, halte ich diese Aussage in mehrfacher Hinsicht für problematisch:

- Die ISO 27001-Zertifizierung eines ISMS durch das BSI basiert auf einem Stichprobenverfahren, bei dem je Bausteingruppe nur ein Baustein zufällig ausgewählt und geprüft wird. Das bedeutet, dass viele Bausteine gar nicht in die Prüfung einbezogen werden.
- In vielen Bereichen wird nur geprüft, ob erforderliche Unterlagen wie Passwortrichtlinien, IT-Sicherheitskonzept etc. vorhanden sind, ohne dass diese Unterlagen inhaltlich geprüft werden.
- Die Ebene der Anwendungsverfahren wird nicht bzw. nicht im erforderlichen Umfang einbezogen.
- Maßnahmen können häufig auf verschiedenen Ebenen des ISO-OSI-Modells umgesetzt werden; in vielen Fällen ist sogar eine bestimmte Kombination von Maßnahmen auf verschiedenen Ebenen erforderlich. Daher ist bei der Zertifizierung des IT-Grundschutzes die vollständige Einbeziehung aller Ebenen erforderlich, um sicherzustellen, dass das Gesamtsystem wirklich die erforderliche Sicherheit gewährleistet. Dies ist aber offensichtlich nicht der Fall.

Bestenfalls ergibt sich bei diesem Vorgehen eine gewisse Wahrscheinlichkeit bzw. ein gewisser Anschein dafür, dass der IT-Grundschutz bezüglich der RZ- oder Netzwerkinfrastruktur umgesetzt ist. Das ist aber im Vergleich mit der Aussage des BSI eine starke Einschränkung.

Ein Beispiel soll das erläutern: Ein Rechenzentrum, das seine Dienste einschließlich Anwendungsverfahren vielen anderen Stellen im Rahmen der Auftragsdatenverarbeitung zur Verfügung stellt, hatte personenbezogene Daten in vielen Fällen weder auf der Anwendungs- noch auf der Netzwerk- bzw. Leitungsebene verschlüsselt übertragen noch eigene Leitungen genutzt. Damit ist die erforderliche Vertraulichkeit nicht gegeben. Dieses RZ ist aber vom BSI nach ISO 27001 auf der Basis IT-Grundschutz zertifiziert. Bei der erforderlichen ebenenübergreifenden, ggf. auch erweiterten Risikoanalyse hätte das diesem Auftragnehmer und dem Auditor auffallen müssen.

Dieses Beispiel zeigt, dass weder Auftraggeber noch Auftragnehmer sich auf Zertifizierungen allein verlassen können. Vielmehr müssen sie sich der Aussagen und Grenzen der Zertifikate

bewusst sein und die erforderlichen weiteren Schritte und Maßnahmen dem entsprechend festlegen.

3.3 Missverständnisse

In diesem Abschnitt sollen noch einige Missverständnisse ausgeräumt werden, mit denen ich im Rahmen meiner Tätigkeit beim Hessischen Datenschutzbeauftragten immer wieder konfrontiert werde.

Die für die Datenverarbeitung verantwortliche Stelle ist verpflichtet, die ihr anvertrauten Daten zu schützen. Sie kann dazu ein Datenschutzmanagementsystem aufbauen, muss das aber nicht. Das Gleiche gilt für einen Auftragnehmer, der nicht die für die Datenverarbeitung verantwortliche Stelle ist (Auftragsdatenverarbeitung). Er kann aber den verantwortlichen Stellen ihre Pflicht zur Auftragskontrolle mit einer Zertifizierung nach ISO 27001 erleichtern und bei potenziellen Auftraggebern Vertrauen in die Sicherheit seines RZ-Betriebes schaffen. Entsprechendes gilt für eine Zertifizierung nach den CC oder einem PP.

Jede Zertifizierung kann Aufwand an anderen Stellen einsparen und Vertrauen schaffen. Sie kostet aber auch Zeit und Geld. Deshalb sollte sie nur nach allgemeinen Normen und Standards erfolgen, um eine Vergleichbarkeit der Zertifikate und der mit ihnen getroffenen Aussagen und Wertungen zu ermöglichen. Und sie sollte möglichst gut softwaretechnisch, organisatorisch und personell unterstützt werden, um den Gesamtaufwand in Grenzen zu halten. Der Begriff „Standard" wird hier im Sinne der klaren Definition der British Standards (früher British Standards Institute) verstanden:

Ein Standard ist ein öffentlich zugängliches technisches Dokument, das unter Beteiligung aller interessierten Parteien entwickelt wird und deren Zustimmung findet. Der Standard beruht auf Ergebnissen aus Wissenschaft und Technik und zielt darauf ab, das Gemeinwohl zu fördern.

4 Fazit

Beide Zertifizierungen, die nach ISO 27001 für Managementsysteme und die nach den CC für Produkte, können den Aufsichtsbehörden für den Datenschutz die Arbeit erleichtern ohne deren Kontrollen zu ersetzen oder vorwegzunehmen.

Datenschutz-Zertifikate greifen zu kurz, wenn sie einzelne Datenschutzanforderungen herausgreifen und zu einer positiven Gesamtbewertung kommen, ohne dass der IT-Grundschutz durchgängig gewährleistet ist. Denn ein Angreifer nutzt die Schwächen, nicht die Stärken von Systemen. Erst nach Umsetzung des IT-Grundschutzes und aller einschlägigen Datenschutzanforderungen können für besonders gute Lösungen in bestimmten Teilbereichen Pluspunkte vergeben werden.

Unternehmen, die im Bereich Auditierung und Zertifizierung von Datenschutzmanagementsystemen tätig werden wollen, sollten darauf verzichten, eigene Datenschutzmanagementsysteme zu entwerfen und sich stattdessen als Auditoren für ISO 27001 akkreditieren. Selbstverständlich erfordert dies zusätzlich Fachkunde sowohl im Datenschutzrecht selbst als auch im Bereich der Ziele des technischen und organisatorischen Datenschutzes sowie deren Umsetzung.

Verweise

[1] *Bundesdatenschutzgesetz (BDSG)* in der Fassung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814): http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/BDSG/BDSG_node.html

[2] *Hessisches Datenschutzgesetz (HDSG)* vom 20. Mai 2011 (GVBL. I S. 208): http://www.datenschutz.hessen.de/hdsg99.htm

[3] *IT-Grundschutz-Kataloge des BSI:* https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[4] *Baustein B 1.5 Datenschutz*. Quelle BSI https://www.bsi.bund.de/ContentBSI/grundschutz/baustein-datenschutz/html/index_htm.html

[5] Simon, Claus: *Neuer Baustein Datenschutz im IT-Grundschutz*. Datenschutz und Datensicherheit (DuD), 2/2007, S. 87-90.

[6] Simon, Claus: *Arbeiten zum Datenschutz im IT-Grundschutz vorläufig abgeschlossen*. Datenschutz und Datensicherheit (DuD), 7/2007, S. 486.

[7] Karper, Irene; Maseberg, Sönke: *Zertifikat für Datenschutz-Management*. Datenschutz und Datensicherheit (DuD), 10/2010, S. 704-708

[8] Prietz, Christian: *Musterprozesse zum Datenschutzmanagement*. Datenschutz und Datensicherheit (DuD), 1/2012, S. 14-19