IT-Sicherheit

Handbuch zum Datenschutz

[11.02.2016] Das Standard-Datenschutzmodell unterstützt Kommunen dabei, personenbezogene Verfahren datenschutzkonform einzurichten und zu betreiben. Erste Orientierung bietet ein jüngst veröffentlichtes Handbuch der Datenschutzbehörden des Bundes und der Länder.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder haben jetzt ein 40 Seiten umfassendes Handbuch zum Standard-Datenschutzmodell (SDM) veröffentlicht. Das SDM gibt Organisationen wie Behörden, Unternehmen oder Wissenschaftsinstituten ein Instrument an die Hand, mit dem sie personenbezogene Verfahren datenschutzkonform einrichten und betreiben können. Außerdem soll das Modell zu bundesweit abgestimmten, transparenten und nachvollziehbaren Beratungs- und Prüftätigkeiten auch der Datenschutzbehörden führen. Die Bedeutung des SDM wird vermutlich dann ihre volle Wirkung entfalten, wenn die europäische Datenschutzgrundverordnung in Kraft tritt. Die Kommunen müssen ihre Verwaltungsverfahren technisch und organisatorisch entsprechend ihren Landesdatenschutzgesetzen umsetzen. Die deutschen Datenschutzgesetze sind ausdrücklich in den Artikeln eins und zwei des Grundgesetzes verankert. Demzufolge sollen technische und organisatorische Schutzmaßnahmen den Grundrechteschutz der Bürger operationalisieren. Ein Problem bei Datenschutzprüfungen im Alltag ist, dass es häufig Spielraum für die Interpretation der Wirksamkeit technischer Schutzmaßnahmen gibt. Dies hat bei notorisch knappen Kassen in der Vergangenheit häufig dazu geführt, dass Schutzmaßnahmen allein mit dem Blick auf geringe Kosten ausgewählt und umgesetzt wurden und nicht nach der real zu erzielenden Wirksamkeit. Zudem ist unklar, ob die etwa aus dem Maßnahmenkatalog des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI) ausgewählten Schutzmaßnahmen, den Geschäftsprozessen einer Behörden oder den grundrechtlich verbürgten Datenschutzrechten der Bürger dienen. IT-Grundschutz hat die Sicherung von Geschäftsprozessen zum Ziel. Diese können allerdings den rechtlich gesicherten Schutzinteressen von Bürgern entgegenstehen. Das SDM nimmt hier entschieden die Schutzperspektive des Bürgers ein, sucht aber über das Konzept der Schutzziele auch die Nähe zum IT-Grundschutz.

Elementare Schutzziele

In den vergangenen 30 Jahren hat man mit der Verwendung von Schutzzielen im Kontext der IT-Sicherheit gute Erfahrungen gemacht. Die Schutzziele sind sowohl für Juristen und Techniker als auch für Organisations- und Systemplaner im Grundsatz verständlich. Das Konzept der Schutzziele bietet zudem eine Systematik, mittels derer technische und organisatorische Schutzmaßnahmen aufeinander abgestimmt und vollständig berücksichtigt werden können. Sobald für ein Verfahren die umzusetzenden Schutzmaßnahmen ausgewiesen sind, kann der Betriebswirt kalkulieren. Viele der neueren Landesdatenschutzgesetze, insbesondere in den neuen Bundesländern, enthalten bereits Schutzziele. Etwa die Hälfte der deutschen Landesdatenschutzgesetze (LDSG) sowie das Bundesdatenschutzgesetz (BDSG) kennen sie hingegen nicht. Die Autoren des SDM haben deshalb viel Mühe darauf verwendet, die LDSGe sowie das BDSG mit den sechs elementaren Schutzzielen abzugleichen. Ziel ist es, ein deutschlandweit einheitliches Niveau an Schutzmaßnahmen zu erreichen.
Die drei weithin bekannten Schutzziele der IT-Sicherheit sind Verfügbarkeit, Integrität und Vertraulichkeit. Das SDM weist daneben die weniger bekannten Schutzziele Transparenz, Intervenierbarkeit und Nichtverkettbarkeit aus. Diese werden im Modell als Gewährleistungsziele bezeichnet. Außerdem betont

das SDM die besondere Bedeutung von Datenvermeidung und Datensparsamkeit. So sollen bevorzugt gar keine Daten oder, falls unabdingbar, Daten nur im geringstmöglichen Umfang verarbeitet werden.
Das Gewährleistungsziel Transparenz umfasst im Wesentlichen zwei Schutzmaßnahmen, mit denen die Prüffähigkeit von Kommunen hergestellt wird. Dazu zählt die Dokumentation von Verfahren und die Protokollierung von Prozessen. Die Transparenz ist eine notwendige Voraussetzung für Kommunen, um personenbezogene Verfahren nachweisbar rechtskonform zu beherrschen und zu steuern. Je stärker Kommunen mit ihren Aktivitäten Personen fremdbestimmen, desto zugriffsfester, aktueller, hochauflösender, fälschungssicherer und revisionsfester muss die Prüfbarkeit der Organisationstätigkeiten sein.

Verschiedene Stufen

Um das Gewährleistungsziel Intervenierbarkeit zu erfüllen, müssen Kommunen ihre Datenverarbeitung so einrichten, dass sie jederzeit die Rechte der Bürger an ihren Daten – wie Beauskunftung, Korrektur, Löschung nachweisbar umsetzen. Des Weiteren sind Prozesse notwendig, mit denen die Datenverarbeitung jederzeit geändert und an neue Verhältnisse angepasst werden kann. In Analogie zum IT-Grundschutz unterscheidet das SDM drei Stufen an Schutzbedarfen: Bei einem normalen Schutzbedarf kann die Schutzmaßnahme Löschen etwa so umgesetzt werden, dass ein Datum mit großem technischen Aufwand für eine gewisse Zeit noch rekonstruierbar bleibt. Für die gleiche Schutzmaßnahme Löschen muss bei hohem Schutzbedarf hingegen ein sehr viel höherer Aufwand an Know-how, Geld und Zeit in die Rekonstruktion investiert werden. Es gilt die Regel: Je höher der Schutzbedarf einer Person ist, desto wirkungsvoller müssen die Schutzmaßnahmen zugunsten der Personen ausgebildet sein. Das Schutzziel Nichtverkettbarkeit besagt, dass Kommunen ihre personenbezogene Datenverarbeitung sehr eng am Zweck des Verfahrens ausrichten müssen. Umgesetzt wird dieses Schutzziel durch ein Rollen- und Rechtekonzept, durch die Trennung von Datenbeständen, IT-Systemen und Prozessen sowie durch Pseudonymisierung und Anonymisierung von Daten und Kommunikationsbeziehungen. Das Schutzziel soll etwa verhindern, dass bei der Nutzung von Landesrechenzentren oder von Clouds die Trennung der drei Gewalten operativ unterlaufen wird. Schließlich ist es die Gewaltentrennung, die den Bürgern den strukturellen Schutz vor staatlicher Willkür bietet. Derzeit arbeiten die Datenschutzbehörden an einem deutschlandweit abgestimmten Katalog mit Details zu Referenzschutzmaßnahmen. Ein solcher könnte dann analog zum Maßnahmenkatalog des IT-Grundschutzes von den verantwortlichen Stellen einfach abgearbeitet werden.

()

Dieser Beitrag ist in der Februar-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, ULD, SDM, LDSG, BDSG, BSI