

IT-Grundschutz und Datenschutz

Erstellt von Georg Osner, Datenschutzberater

Die Negativschlagzeilen zur „Lidl-Videoüberwachung“ oder zur „Telekom-Telefonüberwachung“ sind aktuelle Beispiele für gravierende Imageschäden aus einem mangelhaften Datenschutzbewusstsein.

Unter dem Begriff Compliance ist die Berücksichtigung und Einhaltung rechtlicher Rahmenbedingungen auch für die IT-Sicherheit schon seit geraumer Zeit ein nicht zu unterschätzendes Thema.

Ein gutes Hilfsmittel für eine datenschutz-, bzw rechtskonforme Umsetzung von IT-Sicherheitsmassnahmen ist der **Baustein Datenschutz aus dem IT-Grundschutzkatalog des BSI**. Die Inhalte des Bausteins B 1.5 Datenschutz wurden kürzlich aktualisiert (2007).

Inhalte und Einsetzbarkeit des Bausteins Datenschutz

Der IT-Grundschutz-Baustein "Datenschutz" wurde vom Bundesdatenschutzbeauftragten gemeinsam mit dem Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der - Länder erstellt.

Nach Angaben der Ersteller richtet sich der Baustein sowohl an die privaten wie auch öffentlichen Anwender für den IT-Grundschutz in Deutschland. Da er auf der deutschen Gesetzgebung basiert, kann er in dieser Form außerhalb Deutschlands jedoch nur sinngemäß umgesetzt werden und kann derzeit noch nicht als Bestandteil einer formalen IT-Grundschutz-Zertifizierung angesehen werden.

Aufgrund der engen Verflechtung von Datenschutz und IT-Sicherheit werden in diesem Datenschutz-Baustein einerseits die Rahmenbedingungen für den Datenschutz praxisgerecht aufbereitet und andererseits die Verbindung zur IT-Sicherheit im IT-Grundschutz aufgezeigt.

Dieser Baustein B 1.5 ist so formatiert, dass er nach Ausdruck problemlos in die Lose Blattsammlung der IT-Grundschutz-Kataloge einsortiert werden kann. Zusätzlich kann er als eigenständiges Modul in das GSTOOL geladen werden.

Der Baustein kann sowohl autonom, z.B. im Rahmen eines Datenschutzprojektes, wie auch im Rahmen eines umfassenden Gesamtprojektes zum IT-Grundschutz eingesetzt werden.

Entsprechend der Systematik des IT Grundschutz-Katalogs werden hierin die datenschutzrelevanten IT Sicherheits-Gefährdungen und IT Sicherheits-Massnahmen dargestellt.

Als zusätzliche Hilfsmittel werden mit angeboten:

- Formular zur IT-Grundschutzerhebung
- Kreuzreferenztafel (Zuordnung Gefährdungen zu Massnahmen)
- Tabelle der Sicherheits-Massnahmen der Kataloge zu den Kontrollzielen des BDSG

In der Tabelle der Sicherheits-Massnahmen werden aus datenschutzrechtlicher Sicht auch die Verbindung zwischen Datenschutz und IT-Sicherheit, aber auch die z. T. unterschiedlichen Zielsetzungen anschaulich dargestellt:

Das Verhältnis zwischen Datenschutz und IT-Sicherheit (Auszug)

Der **Datenschutz** legt auf Basis des jeweils gültigen Datenschutzrechts (z.B. Bundesdatenschutzgesetz, Landesdatenschutzgesetze oder spezielle Gesetzgebung wie das Telemediengesetz) fest, unter welchen Voraussetzungen personenbezogene Daten unter Einhaltung bestimmter organisatorischer und technischer Maßnahmen verarbeitet werden dürfen. Viele dieser Maßnahmen dienen auch der IT-Sicherheit.

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

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

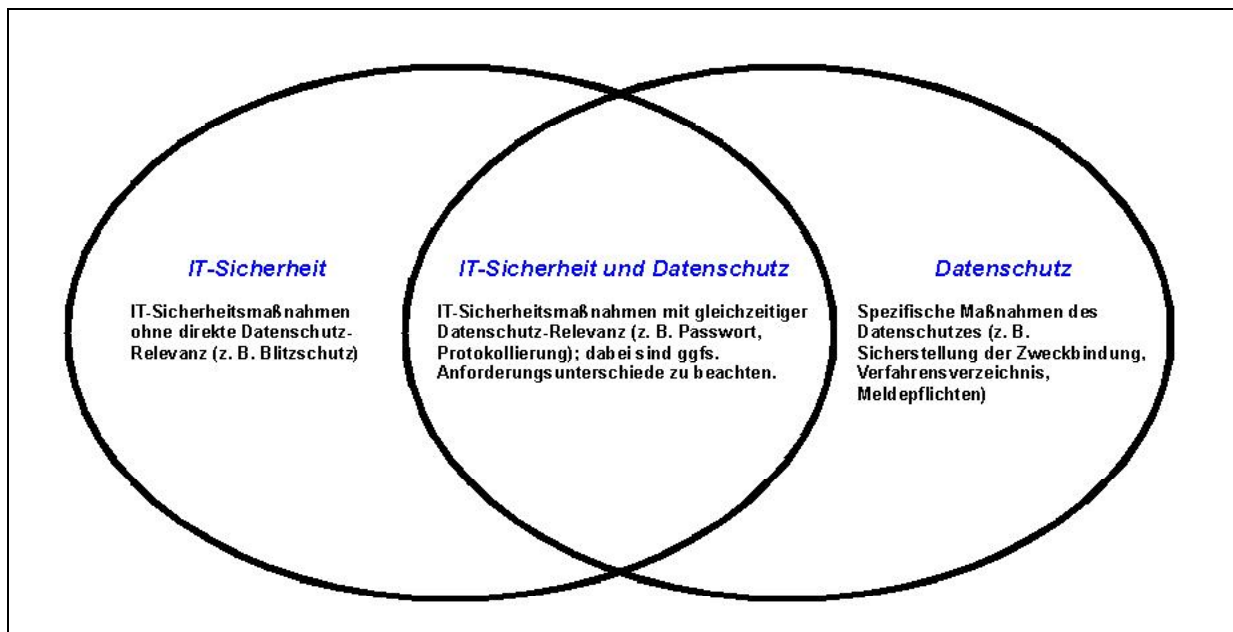
Umgekehrt betrachtet die IT-Sicherheit den Datenschutz bei Verfahren, in denen personenbezogene Daten verarbeitet werden, als eine wesentliche Quelle für Anforderungen, die sie umzusetzen hat.

Abbildung: Das Verhältnis zwischen Datenschutz und IT-Sicherheit (Auszug)

Aus Sicht des Datenschutzrechts lassen sich die Anforderungen an Verfahren und Systeme zur Verarbeitung personenbezogener Daten grundsätzlich in zwei Gruppen teilen:

Anforderungen an die Datensicherheit (Verfügbarkeit, Vertraulichkeit und Integrität, in Abbildung in der Schnittmenge dargestellt), die sich aus dem Datenschutz ergeben und

Datenschutzspezifische Anforderungen (unter anderem Zulässigkeit der Datenverarbeitung, Zweckbindung, Erforderlichkeit, Transparenz aber auch Vertraulichkeit und Integrität)



Zur Verfügung gestellte Hilfsmittel:

Neben den im **IT-Grundschutzkatalog Baustein B 1.5 Datenschutz** verfügbaren Beschreibungen von datenschutzrelevanten Gefährdungen und Massnahmen werden weitere Hilfsmittel für die Praxis zur Verfügung gestellt:

Formular zur IT-Grundschutzerhebung zu Baustein B 1.5 Datenschutz

Als Hilfsmittel zur IT-Grundschutzerhebung wird ein Erhebungsformular zur Verfügung gestellt. Enthalten sind u. a. Querverweise auf die Massnahmen im IT Grundschutzkatalog, eine Zuordnung zur Siegelstufe (A, B, C) und eine Prioritätsvergabe.

Eine Übersicht sehen Sie aus folgenden Auszug:

Maßnahme (Priorität) (Siegel)	Baustein B 1.5 Datenschutz	ent-behrlich	Ja	teil-weise	Nein	Umsetzung bis	verant-wortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kosten-schätzung
M 2.110 (1) [A]	Datenschutzaspekte bei der Protokollierung								
M 7.1 (1) [C]	Datenschutzmanagement								
M 7.2 (1) [B]	Regelung der Verantwortlichkeiten im Bereich Datenschutz								
M 7.3 (1) [A]	Aspekte eines Datenschutzkonzeptes								
M 7.4 (1) [A]	Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten								
M 7.5 (1) [A]	Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten								

Zuordnungsmatrix (Auszug)

Eine wertvolle Hilfe in der Praxis, insbesondere für Projekte mit Datenschutzbezug, z.B. Verarbeitung von Kundendaten oder Personaldaten, ist die angebotene Zuordnungsmatrix:

Hier werden Massnahmen aus dem IT-Grundschutzkatalog zu den in der Anlage § 9 Bundesdatenschutzgesetz aufgeführten datenschutzrechtlichen Kontrollzielen dargestellt.

Zuordnung der Maßnahmen der IT-Grundschutz-Kataloge zu den datenschutzrechtlichen Kontrollzielen des Bundesdatenschutzgesetzes BDSG:								
Maßnahme aus GSK	Zutrittskontrolle	Zugangskontrolle	Zugriffskontrolle	Weitergabekontrolle	Eingabekontrolle	Auftragskontrolle	Verfügbarkeitskontrolle	(Zweckbindung)
M1.2	x							
M1.10	X							
M1.12	x							
M1.15	x							
M1.17	x							
M1.19	x							
M1.23	x							
M1.29	x	X	x					
M1.30			x	X				

Kreuzreferenztafel

Zur Unterstützung einer projektmässigen Abwicklung nach IT-Grundschutz werden in einer Kreuzreferenztafel den speziellen Datenschutz-Gefährdungen die erforderlichen Massnahmen zugeordnet dargestellt.

Die beschriebenen Unterlagen und Hilfsmittel stehen als Download unter der Website des BSI oder des Bundesdatenschutzbeauftragten zur Verfügung:

www.bsi.bund.de/gshb/baustein-datenschutz

Die Darstellung dieser Übersicht erfolgte auf der Grundlage und teilweise mit Auszügen aus der Aufbereitung der Verfasser des Bausteins Datenschutz (2007) und den zugehörigen Hilfsmitteln durch:

Georg Osner, Datenschutzberater und IT-Revisor

7-08