Tabelle: „Maßnahmen und Datenschutz-Kontrollziele“ zu Baustein 1.5 „Datenschutz“

(Verweis aus Maßnahme M 7.5)

Basierend auf den IT-Grundschutz-Katalogen Version 2006 Stand: November 2006, Stand der Tabelle: 22.08.07

Einleitung: Das Verhältnis zwischen Datenschutz und IT-Sicherheit

Datenschutz und **IT-Sicherheit** weisen in der Umsetzung eine große Schnittmenge auf, haben aber zunächst unterschiedliche Ziele.

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. Datenschutz und IT-Sicherheit weisen eine bedeutende Schnittmenge auf.

Die sich aus Datenschutz und IT-Sicherheit ergebenden, teilweise unterschiedlichen Anforderungen und Mittel in Einklang zu bringen, ist eine gestalterische Aufgabe. Dies wird am Beispiel „Firewallsysteme“ deutlich. Aus Sicht des Datenschutzes sollen einerseits so wenig personenbezogene Daten (und dazu gehören unter anderem auch IP-Adressen) wie möglich erhoben und gespeichert werden. Andererseits sollen externe Angriffe oder unerlaubtes Benutzer- bzw. Systemverhalten unterbunden und analysiert werden. Tatsächlich werden in der Praxis, häufig unter einem pauschalen Verweis auf die IT-Sicherheit, Protokolldaten unbegrenzt personenbezogen erhoben und längerfristig gespeichert, um potentielle Angriffe erkennen, analysieren und unterbinden zu können.

Die Lösung liegt in einer datensparsamen Gestaltung der Protokollierung unter Beachtung der Grundsätze der Erforderlichkeit und der Zweckbindung: Eine Protokollierung ist nach Art der Daten und ihrer Speicherdauer nur soweit notwendig und legitim, wie personenbezogene Datensätze zur Datenschutz- und IT-Sicherheitskontrolle tatsächlich benötigt werden. Vielfach reicht eine anonymisierte Zusammenfassung der Datensätze aus. Protokolldaten, die aussagelos sind oder tatsächlich nicht ausgewertet werden, sind grundsätzlich zu löschen.

Die folgende Abbildung stellt das Verhältnis zwischen Datenschutz und IT-Sicherheit schematisch dar.

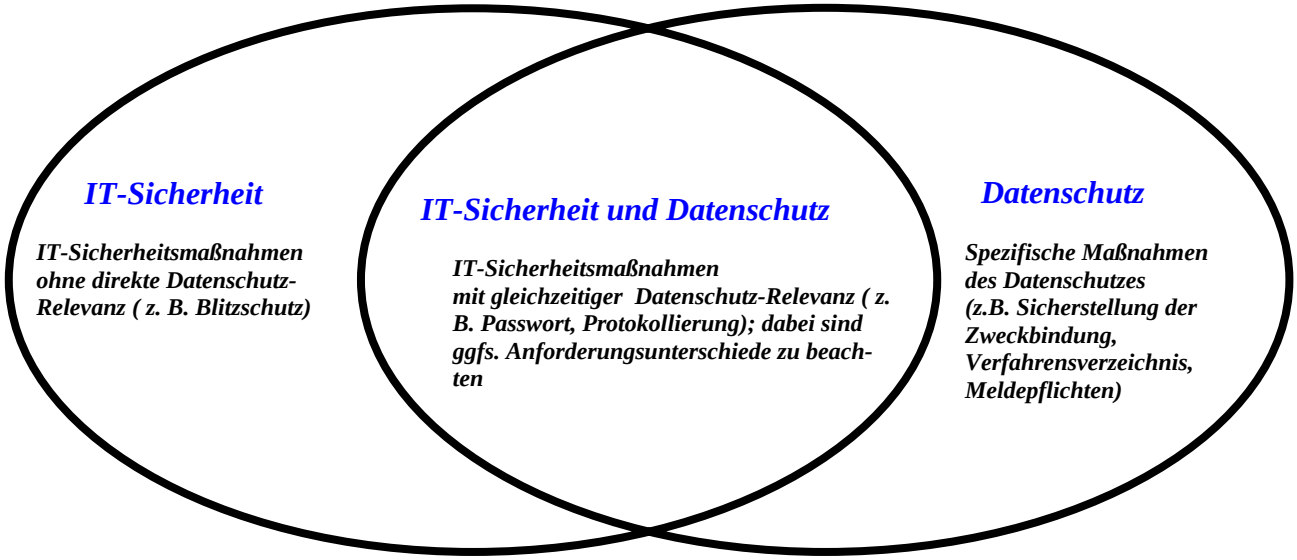

Abbildung: Das Verhältnis zwischen Datenschutz und IT-Sicherheit

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)

In der folgenden Tabelle sind alle Maßnahmen der IT-Grundschutz-Kataloge unter Berücksichtigung der Zielsetzungen des Datenschutzes auf ihre Relevanz hin bewertet worden. Dargestellt werden die Maßnahmen, die dem gemeinsamen Bereich „IT-Sicherheit und Datenschutz“ und dem spezifischen Bereich „Datenschutz“ zuzuordnen sind. Wie die Auflistung zeigt, sind nicht alle Maßnahmen der IT-Grundschutz-Kataloge erfasst. Es gibt Lücken, deren Maßnahmen dem Bereich „IT-Sicherheit“ zuzuordnen sind und die keine direkte Datenschutz-Relevanz haben.

Zuordnung der Maßnahmen der IT-Grundschutz-Kataloge zu den datenschutzrechtlichen Kontrollzielen des Bundesdatenschutzgesetzes BDSG:

Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
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**				
M1.32	**x**	**x**	**x**					
M1.33		**x**	**x**				**x**	
M1.34		**x**	**x**				**x**	
M1.36			**x**	**X**			**x**	
M1.37	**x**	**x**	**X**					
M1.42	**x**	**x**	**x**				**x**	
M1.43	**x**	**x**	**x**				**x**	
M1.44	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M1.45	**x**	**x**	**x**				**x**	**x**
M1.46			**x**				**x**	
M1.49	**x**	**x**	**x**	**X**			**x**	**x**
M1.53	**x**	**x**					**x**	
M1.58	**x**	**x**	**x**	**X**			**x**	**x**
M1.59	**x**	**x**	**x**				**x**	
M1.60	**x**	**x**	**x**				**x**	
M1.61		**x**	**x**				**x**	
M1.63	**x**	**x**	**x**					
Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M2.1	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**

Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M2.3			x				x	
M2.4			x	X		x	x	
M2.5		x	X	X	x			x
M2.6	x							
M2.7		x						
M2.8			X					
M2.11		x	X		x			
M2.13			x	X		x		
M2.14	x		x				x	
M2.16	x						x	
M2.17	x						x	
M2.19			X				x	
M2.22							x	
M2.23	x	x	x	X	x	x		
M2.27		x	x	X		x	x	
M2.30		x	X					
M2.32		x	X					
M2.35			x				x	
M2.41							x	
M2.42				X				
M2.43			x	X		x		
M2.44			x	X		x	x	
M2.45			x	X		x	x	
M2.46			x	X		x	x	
M2.50			x	X				
M2.53		x	x	X				
M2.60		x	X	X				
M2.61		x	X	X				
M2.63			X					
M2.64			x	X	x	x		
M2.69	x	x	x	X	x	x	x	x
M2.91	x	x	x	X	x	x	x	x
M2.92	x	x	x	X	x	x	x	x
M2.93	x	x	x	X	x	x	x	x

Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M2.94			**x**				**x**	
M2.98 – M101	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M2.102		**x**	**x**				**x**	
M2.110			**x**	**X**	**x**			
M2.112			**x**	**X**			**x**	
M2.113	**x**	**x**	**x**	**X**		**x**	**x**	**x**
M2.114				**X**				
M2.115			**x**	**X**	**x**	**x**	**x**	
M2.117			**x**	**X**	**x**		**x**	**x**
M2.118			**x**	**X**			**x**	**x**
M2.119			**x**	**X**			**x**	**x**
M2.120			**x**	**X**			**x**	**x**
M2.124 - M2.135		**x**	**x**	**X**	**x**		**x**	**x**
M2.137							**x**	
M2.138							**x**	**x**
M2.139- M2.153		**x**	**x**	**X**			**x**	
M2.154 - M2.160		**x**	**x**				**x**	
M2.161 - M2.166			**x**	**X**			**x**	
M2.167			**x**					
M2.168 - M2.171	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M2.177				**X**			**x**	
M2.178 - M2.181		**x**	**x**	**X**			**x**	**x**
M2.204		**x**	**x**	**X**				
M2.205			**x**	**X**				
M2.214	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M2.217	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M2.218				**X**				

Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M2.220		x	x					
M2.223		x	x	X	x	x	x	x
M2.224		x	x	X	x		x	x
M2.225	x	x	x	X	x	x	x	x
M2.226	x	x	x	X		x		x
M2.242-M2.246	x	x	x			x	x	x
M2.250-M2.256			x	X		x	x	X
M2.259			x		x		x	x
M2.262	x	x	x			x	x	x
M2.265			x	X	x			
M2.279		x	x				x	
M2.300			x					
M2.309		x	x	X	x		x	x
M2.315-M2.322	x	x	x	X	x	x	x	x
M2.324-M2.330	x	x	x	X	x	x	x	x
M2.342			x					
M2.344		x	x					
M2.345						x		
M2.356						x		
M2.357		x	x					
M2.363		x	x				x	
M2.370		x	x	x	x			
M2.371			x					
M2.384		x	x	x				
M2.387						x		
M2.388		x	x	x				
M2.389		x	x	x				

Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M3.14			x	X			x	

M3.21	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M3.22	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M3.26-M3.32							**x**	
Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M4.1		**x**	**X**	**X**	**x**		**x**	
M4.2		**x**	**X**	**X**	**x**		**x**	
M4.3							**x**	
M4.4		**x**	**x**				**x**	
M4.7		**x**	**X**	**X**	**x**		**x**	
M4.13 bis M4.24		**x**	**X**	**X**	**x**		**x**	
M4.27		**x**	**x**	**X**	**x**		**x**	
M4.29		**x**	**x**	**X**			**x**	
M4.32			**x**	**X**				
M4.33				**X**			**x**	
M4.48			**x**		**x**		**x**	**x**
M4.51			**x**				**x**	
M4.53			**x**		**x**		**x**	**x**
M4.63	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**X**
M4.64			**x**	**X**				
M4.72			**x**					
M4.79			**x**				**x**	
M4.80			**x**				**x**	
M4.84		**x**						
M4.91 – M4.92		**x**	**x**				**x**	
M4.99			**x**		**x**		**x**	
M4.133		**x**	**x**					
M4.135		**x**	**x**					**x**
Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M4.146		**x**	**x**	**X**	**x**	**x**	**x**	**x**
M4.149			**x**					
M4.168			**x**				**x**	

M4.171 M2.200			**x x**	**X**			**x**	
M4.201			**x**					
M4.202			**x**					
M4.204			**x**					
M4.228-M2.231		**x**	**x**	**X**				
M4.237		**x**	**x**	**X**	**x**	**x**	**x**	**x**
M4.239		**x**	**x**	**X**	**x**	**x**	**x**	**x**
M4.241		**x**	**x**	**X**	**x**	**x**	**x**	**x**
M4.243-M4.249		**x**	**x**	**X**	**x**	**x**	**x**	**x**
M4.254-M4.273		**x**	**x**		**x**			
M4.276-M2.286		**x**	**x**	**x**	**x**			
M4.293-M4.297		**x**	**x**	**x**	**x**			
Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M5.6 bis M5.12		**x**	**x**	**X**	**x**		**x**	
M5.14 bis M5.22				**X**			**x**	
M5.23				**X**				
Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M5.26 bis M5.28		**x**	**x**	**X**				
M5.32				**X**				
M5.37-M5.43		**x**	**x**	**X**			**x**	

M5.51-M5.52				**X**				
M5.56 – M5.67			**x**	**X**				
M5.63 – M5.68			**x**	**X**				
M5.81				**X**				
M5.88				**X**		**x**		
M5.108				**X**	**x**			
M5.121-M5.122		**x**	**x**	**X**				
M5.123-M5.132		**x**	**x**	**x**	**x**			
M5.139		**x**	**x**	**x**				
Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M6.1 - M6.71			**x**				**x**	
M6.78-M6.84							**x**	
M6.90-M6.91		**x**						
M6.95					**x**	**x**	**x**	**x**
M6.99							**x**	
M6.102								
Maß-nahme aus GSK	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-Kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfüg-barkeits-kontrolle	(Zweck-bindung)
M7.2						**x**		
M7.3	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M7.5	**x**	**x**	**x**	**X**	**x**	**x**	**x**	**x**
M7.6		**x**	**x**	**X**				
M7.12								**x**
M7.15			**x**	**X**			**x**	**x**

Erläuterung der datenschutzrechtlichen Kontrollziele:

Anlage zu § 9 Satz 1 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren **(Zutrittskontrolle),**

2) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können **(Zugangskontrolle)**,

3) zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle)**,

4) zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist **(Weitergabekontrolle),**

5) zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle),**

6) zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle),**

7) zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind **(Verfügbarkeitskontrolle),**

8) zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können ***(redaktionelle Ergänzung: Zweckbestimmung).***