Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 9. Übung im SoSe 2014:
Vergleich Datenschutz und IT-Sicherheit

9.1 Vergleich Sicherheitsziele & Kontrollbereiche

Aufgabe:

- Ordnen Sie die im BDSG genannten **Kontrollbereiche** inhaltlich den **Sicherheitszielen** der mehrseitigen IT-Sicherheit zu (Mehrfach-Zuordnungen sind erlaubt)!

9.1 Vergleich Sicherheitsziele & Kontrollbereiche

	Verfügbarkeit	Integrität	Vertraulichkeit	Zurechenbarkeit	Rechtsverbindlichkeit
Organisationskontrolle	X	X	X	X	X
Zutrittskontrolle	X		X		
Zugangskontrolle	X	X	X		
Zugriffskontrolle	X	X	X	X	X
Weitergabekontrolle	X	X	X	X	X
Eingabekontrolle		X		X	
Auftragskontrolle					X
Verfügbarkeitskontrolle	X				
Datentrennungskontrolle		X	X	X	X

9.2 Gegensätze Datenschutz & IT-Sicherheit

Aufgabe:

- Welche **Gegensätze** sehen Sie zwischen den Anforderungen zum Datenschutz und zur IT-Sicherheit? Begründen Sie Ihre Antwort.

9.2 Gegensätze Datenschutz & IT-Sicherheit

- **Datenschutz**: Grundsatz der Datensparsamkeit
  IT-Sicherheit: Redundante Datensicherung zur Ausfallsicherheit
- **Datenschutz**: Informationelles Selbstbestimmungsrecht
  IT-Sicherheit: Nachvollziehbarkeit und Überwachung von Aktionen
- **Datenschutz**: Transparenz der Verfahren
  IT-Sicherheit: Verschleierung von Sicherheitsmechanismen
- **Datenschutz**: Inhaltsebene der Daten im Vordergrund
  IT-Sicherheit: Transportebene der Daten im Vordergrund
- **Datenschutz**: Schutzbereich personenbezogene Daten
  IT-Sicherheit: Schutzbereich alle (Unternehmens-)Daten
- **Datenschutz**: Vertraulichkeit zentral
  IT-Sicherheit: Vertraulichkeit nur ein Ziel unter vielen
- **Datenschutz**: Ausgangspunkt = Interesse von Betroffenen
  IT-Sicherheit: Ausgangspunkt = Interesse von Systembetreibern

9.3 Vergleich DSB & IT-SB

Aufgabe:

- Vergleichen Sie die **Aufgaben** eines **Datenschutzbeauftragten** mit den Aufgaben eines **IT-Sicherheitsbeauftragten**.
  a) Welche Gemeinsamkeiten gibt es?
  b) Welche Unterschiede gibt es?

9.3 Vergleich DSB & IT-SB (1)

Gemeinsamkeiten:

- Da sich ein erheblicher Teil der Datenverarbeitung auf die automatisierte Verarbeitung personenbezogener Daten erstreckt, haben beide Beauftragte oftmals die gleichen IT-Systeme im Blick.
- Beide Beauftragte kümmern sich im Wesentlichen darum, welche technischen und organisatorischen Maßnahmen zum Schutz der Daten zu ergreifen sind, und prüfen regelmäßig deren Wirksamkeit.
- Beide Beauftragte beschäftigen sich mit Sicherheitsvorfällen: Der IT-Sicherheitsbeauftragte mit den Ursachen, der Datenschutzbeauftragte mit den Folgen (Datenpanne?)

9.3 Vergleich DSB & IT-SB (2)

Gemeinsamkeiten: (Fortsetzung)

- Beide Beauftragte beschäftigen sich mit der Awareness der Beschäftigten und führen Schulungen / Unterweisungen durch.
- Beide Beauftragte sind zu beteiligen an Planungen zur Einführung von neuen IT-Systemen.
- Wird im Rahmen von Outsourcing dem Auftragnehmer ein Zugriff auf Daten der verantwortlichen Stelle gewährt, sind beide Beauftragte einzubinden.

9.3 Vergleich DSB & IT-SB (3)

Unterschiede:

- Die Aufgaben des Datenschutzbeauftragten sind im BDSG (bzw. in den LDSG, soweit Landesrecht ausschlaggebend ist) definiert, die Aufgaben des IT-Sicherheitsbeauftragten werden dagegen von der verantwortlichen Stelle selbst festgelegt, soweit es sich nicht um einen TK-Provider handelt, für den § 109 Abs. 4 TKG zumindest dessen Benennung vorschreibt. In erster Linie fußt der Einsatz eines IT-Sicherheitsbeauftragten insoweit eher auf internationalen Best Practice Standards.
- Durch die gesetzliche Festlegung der Aufgaben, genießt der Datenschutzbeauftragte Schutzrechte im Gegensatz zum IT-Sicherheitsbeauftragten.

9.3 Vergleich DSB & IT-SB (4)

Unterschiede: (Fortsetzung)

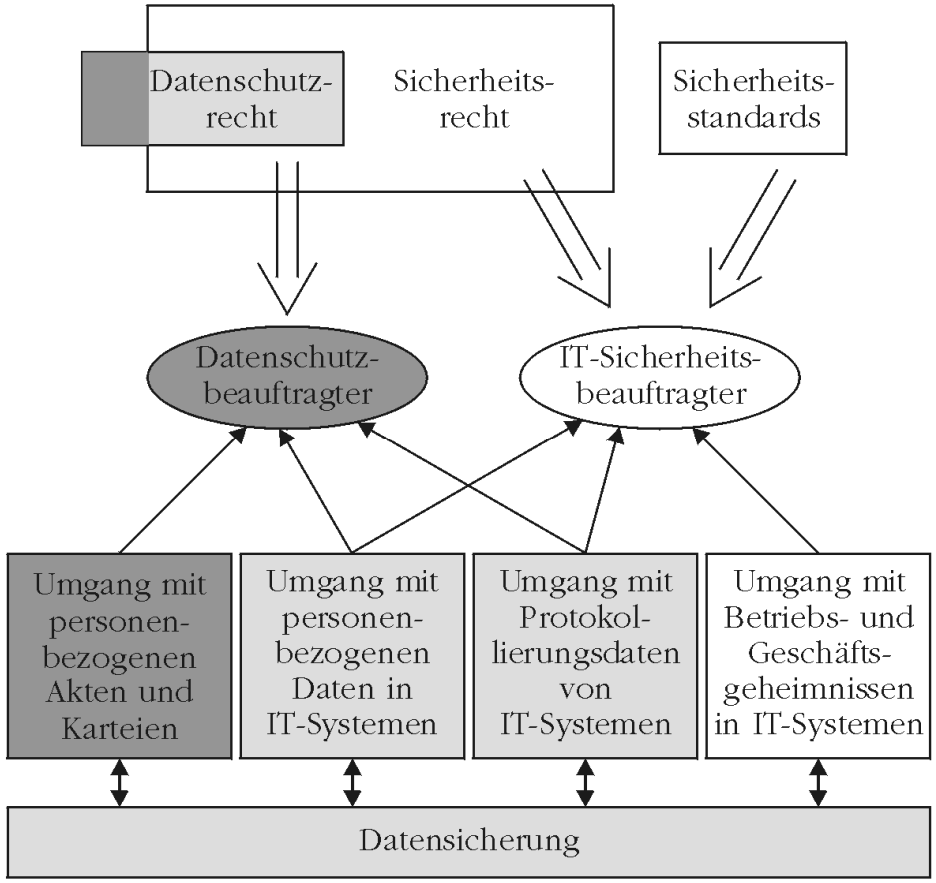
- Der Datenschutzbeauftragte ist nur beratend tätig, während der IT-Sicherheitsbeauftragte auch eine sog. „Garantenstellung“ einnehmen kann: Wenn der IT-Sicherheitsbeauftragte eine Sonderverantwortlichkeit zur Beanstandung und Unterbindung von Rechtsverstößen übernimmt, macht er sich sogar strafbar, wenn er derartige Vorgänge nicht angeht (nach einem BGH-Urteil vom 17.07.2009). Das ist aber nur der Fall, wenn der IT-Sicherheitsbeauftragte der Führungsebene (C-Level) angehört.
- Der IT-Sicherheitsbeauftragte kann oftmals Regelungen selbst in Kraft setzen, der Datenschutzbeauftragte nicht.

9.3 Vergleich DSB & IT-SB (5)

Unterschiede: (2. Fortsetzung)

- Der Datenschutzbeauftragte adressiert auch Akten und Unterlagen, während der IT-Sicherheitsbeauftragte sich ausschließlich um IT-Systeme kümmert (im Gegensatz zum Informationssicherheitsbeauftragten).

9.3 Vergleich DSB & IT-SB (6)



9.4 Interessenausgleich zwischen Betroffene & Systemnutzer

Aufgabe:

- Nennen Sie Beispiele, in denen sich die **Interessen** der **Betroffenen** von den Interessen der **Systemnutzer** deutlich unterscheiden! Welcher Ausgleich wäre in diesen Beispielen ein möglicher Kompromiss?

9.4 Interessenausgleich zwischen Betroffene & Systemnutzer

Beispiele für abweichende Interessen:

- Systemnutzer möchten möglichst detaillierte Daten angezeigt bekommen, um sicher gehen zu können, dass sie keine fehlerhaften Daten eingeben bzw. bearbeiten. Betroffene möchten, dass verantwortliche Stellen nur so viel Daten über sich haben, wie unbedingt nötig. Der Ausgleich erfolgt daher durch das **Berechtigungskonzept**, in dem festgelegt ist, welcher Nutzer welche Daten (zu welchem Zweck) einsehen und bearbeiten darf.
- Systemnutzer wünschen eine umfassende Datensicherung, damit im Falle eines ungewollten Datenverlustes oder bei einem zeitlich späteren Vorgang noch die Historie berücksichtigt werden kann. Betroffene möchten, dass ihre Daten nur für die vorgeschriebene Dauer abrufbar sind. Der Ausgleich erfolgt daher über die Regelungen zur **Sperrung** von Daten.

9.5 Vergleich Risikomanagement

Aufgabe:

- Vergleichen Sie die **Methoden** zum **Risikomanagement** bei Datenschutz und IT-Sicherheit miteinander! An welchen Punkten unterscheiden sich diese grundlegend voneinander?

9.5 Vergleich Risikomanagement (1)

- Beim Datenschutzrisikomanagement werden nur automatisierte Verarbeitungen von personenbezogenen Daten betrachtet, beim IT-Risikomanagement dagegen alle automatisierten Verarbeitungen.
- Beim Datenschutzrisikomanagement werden auch manuelle Vorgänge betrachtet, beim IT-Risikomanagement nicht.
- Beim Datenschutzrisikomanagement wird betrachtet, mit welcher Wahrscheinlichkeit ein Datenschutzverstoß begangen wird oder Daten kompromittiert werden können. Beim IT-Risikomanagement wird dagegen betrachtet, mit welcher Wahrscheinlichkeit eine Bedrohung eine Verwundbarkeit eines IT-Systems erfolgreich ausnutzen kann. Die Auswirkung wird stattdessen in der Business Impact Analysis betrachtet.
- Der Schaden beim Datenschutzrisikomanagement hängt davon ab, wie schwerwiegender ein Verstoß gegen datenschutzrechtliche Vorschriften wiegt (Bußgeldhöhe, Gefahr der Datenpanne) oder wie hoch der Schutzbedarf der Daten ist, beim IT-Risikomanagement dagegen, welchen Wert das gefährdete Asset hat.

9.5 Vergleich Risikomanagement (2)

- Datenschutzrisikomanagement ist ein Instrument zur Vorabkontrolle, d.h. zur systematischen Analyse bei Einführung bzw. grundlegenden Änderung einer automatisierten Verarbeitung. Das IT-Risikomanagement ist dagegen ein Instrument zur fortwährenden Steuerung, welche Maßnahmen zu ergreifen sind und welche nicht.