

PERSICON@night am 19. März 2009

Der Datenschutzbeauftragte

Anforderungen, Aufgaben, Ausbildung und Zertifizierung

Vorstellung Referent

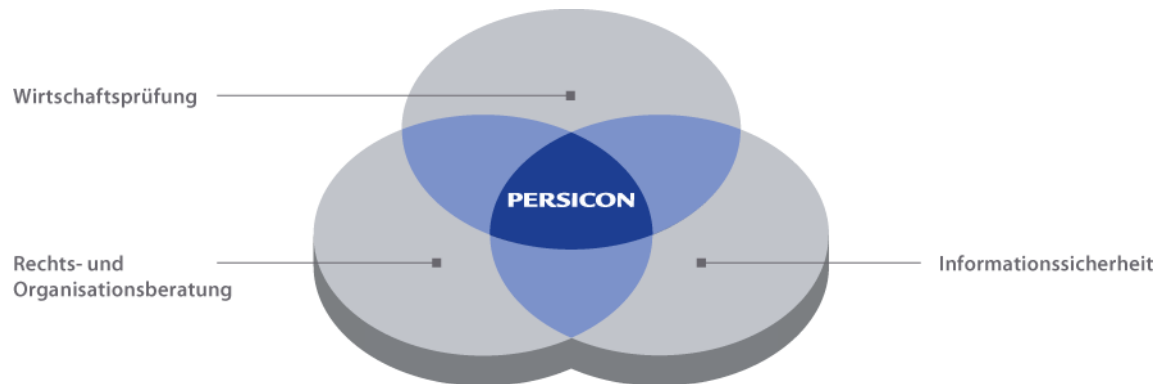
Haiko Ferber

- Rechtsanwalt
- Fachanwaltskurs Steuerrecht
- Ausbildung zum IT-Sicherheitsbeauftragten



PERSICON

- Führender Anbieter von spezialisierten Beratungs- und Prüfungsleistungen in den – auf Informationssysteme fokussierten – Bereichen:
Governance, Compliance, Security
- Schnittmenge zwischen Wirtschaftsprüfung, Rechts- und Organisationsberatung sowie Informationssicherheit



- Hauptsitz in Berlin, Niederlassungen in Düsseldorf, Frankfurt am Main, München

Leistungsschwerpunkte

Governance

- Strategie-, Prozess- und Organisationsberatung für Informationssysteme
- Design, Dokumentation und Prüfung interner Kontrollsysteme (IKS)
- Prüfung ausgelagerter Geschäftsprozesse nach SAS 70/IDW PS 951
- Co- und Outsourcing der internen Revision
- Forensische Untersuchungen/Betrugsprävention
- IT-Systemprüfung im Rahmen der Jahresabschlussprüfung
- Testierung der Ordnungsmäßigkeit rechnungslegungsrelevanter Software
- Risiko- und Business-Impact-Analyse (BIA)
- Risikomanagement (Beratung und Prüfung)
- Implementierung und Schulung von IT-Governance
- Reifegradbestimmung der IT-Managementprozesse
- CobiT-Workshops und -Schulungen

Compliance

- Gesetzeskonformität gemäß den Anforderungen aus dem Steuer- und Handelsrecht (KonTraG, GDPdU, GoBS, Sarbanes-Oxley Act, GxP/FDA ...)
- Compliance nach Basel II, Solvency II, KWG und MaRisk
- Schulung, Beratung und Prüfung zur Einhaltung der Datenschutzbestimmungen sowie Stellung des externen Datenschutzbeauftragten
- Erstellung von Richtlinien, Verfahrensverzeichnissen, IT-Regelwerken, Betriebs- und Sicherheitskonzepten
- Compliance-Audits, z.B. für das Outsourcing bei Kreditinstituten
- Gestaltung ordnungsgemäßer IT-Change- und Configuration-Management-Prozesse

Leistungsschwerpunkte

Security

- IT-Sicherheitsberatung, Auditierung und Zertifizierung nach IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder ISO 27001
- Zertifizierung von Rechenzentren
- SAP-Sicherheitsaudits und Testierungen
- Implementierung von Informationssicherheitsmanagementsystemen (ISMS)
- Stellung des externen IT-Sicherheitsbeauftragten
- Durchführung von IT-Strukturanalysen und Erstellung von IT-Dokumentationen
- Kontinuitäts- und Notfallmanagement
- Schulung zur Anwendung des GSTOOLs des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- Ausbildung von IT-Sicherheitsbeauftragten und Risikomanagern
- CISA- und CISM-Ausbildungskurse

Referenzen

- Deutsche Post
- Pfizer Deutschland
- E.ON edis, E.ON BKB
- RWE enviaM
- Bertelsmann/arvato
- ThyssenKrupp
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Staatskanzlei des Landes Sachsen-Anhalt
- Ministerium für Jugend, Bildung und Sport des Landes Brandenburg
- Ministerium für Ländliche Entwicklung, Umwelt und Verbraucherschutz des Landes Brandenburg
- Thüringer Ministeriums für Landwirtschaft, Naturschutz und Umwelt
- Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau des Landes Rheinland-Pfalz

- Landesrechnungshof Berlin
- Landesamt für Gebäudebewirtschaftung Berlin
- Landesinformationszentrum Sachsen-Anhalt
- Landesamt für Datenverarbeitung und IT-Serviceaufgaben des Landes Brandenburg
- Landesamt für Verbraucherschutz, Landwirtschaft und Flurneuordnung des Landes Brandenburg
- Bundesdruckerei
- Berliner Verkehrsbetriebe (BVG)/BT Berlin Transport
- Rundfunk Berlin-Brandenburg (IVZ/RBB)
- Stadtwerke Dresden, Münster, Neubrandenburg
- Berliner Wasserbetriebe, Kommunale Wasserwerke Leipzig
- Sparkasse KölnBonn, Nassauische Sparkasse, Kölner Kreissparkasse

Agenda

1. Anforderungen
2. Aufgaben
3. Ausbildung
4. Zertifizierung

PERSICON@night am 19. März 2009

Der Datenschutzbeauftragte: Anforderungen

Erforderliche Fachkunde des Datenschutzbeauftragten

- Erfolgreiche Qualifizierung (Ausbildung) im Datenschutz
- Praxiserfahrungen im Datenschutz
- Kenntnisse in unter anderem folgenden Bereichen:
 - Betriebliche Organisation
 - Recht
 - Technik
 - Informationssicherheit
- Aktualität der Fachkunde → z. B. Weiterbildung, Lektüre von Fachzeitschriften und Fachliteratur

Erforderliche Zuverlässigkeit des Datenschutzbeauftragten (1)

- Unabhängigkeit, d. h. wenn er
 - frei von Interessenkonflikten ist und
 - über ausreichende Ressourcen verfügt.
- Interessenkonflikte liegen vor, wenn die Tätigkeit des Datenschutzbeauftragten mit anderen Aufgaben in einem zeitlichen oder fachlichen Widerspruch steht.
- Für eine unabhängige Ausführung der Funktion des Datenschutzbeauftragten sind die Datenschutzaufgaben vorrangig vor anderen Verpflichtungen zu erfüllen.
 - Die anderen Verpflichtungen treten in den Hintergrund.
 - Kann die andere Verpflichtung nicht in den Hintergrund treten, ist eine Bestellung zum Datenschutzbeauftragten nicht möglich.

Erforderliche Zuverlässigkeit des Datenschutzbeauftragten (2)

Fachlicher Interessenkonflikt:

- Schwerpunktmäßige Verarbeitung oder Nutzung personenbezogener Daten, wie z.B. administrative Aufgaben im IT-Bereich, Personalsachbearbeitung, Kundendatenbearbeitung
- Konzeptionelle und strategische Tätigkeiten im IT-Bereich
- Operative Tätigkeiten zur Gewährleistung der IT-Sicherheit
- Unternehmens- bzw. Behördenleitung, Mitarbeiterführung und deren Assistenz
- Rechtliche Beratungen als Justiziar, Rechtsabteilungsleiter, Rechtsanwälte und anderer Berater, die das Unternehmen bzw. die Behörde (nach außen) vertreten.
- Leitungsfunktionen der Mitarbeitervertretung
- Wirtschaftsprüfer

Erforderliche Zuverlässigkeit des Datenschutzbeauftragten (3)

Persönliche Voraussetzungen:

- Persönliche Integrität
- Durchsetzungsfähigkeit des eigenen Status
- Verschwiegenheit
- Haftungsfähigkeit, d. h. der Datenschutzbeauftragte muss rechtlich und wirtschaftlich in der Lage sein, die Verantwortung für die Richtigkeit seiner Tätigkeit zu gewährleisten.

PERSICON@night am 19. März 2009

Der Datenschutzbeauftragte: Aufgaben

Aufgaben des Datenschutzbeauftragten

Beispiele:

- Beratende Mitwirkung in Prozessen und Projekten
- Prüfungsaufgaben
- Schulungs- und Sensibilisierungsaufgaben
- Berichts- und Informationspflichten
- Erstellung datenschutzrelevanter Unterlagen
- Erfüllung von Meldepflichten
- Abbildung der Schnittstelle zu:
 - Aufsichtsbehörden
 - Betroffenen
 - Management und Fachabteilungen (z. B. Revision, IT-Sicherheit, Qualitätsmanagement, Arbeitssicherheit)
 - etc.

Aufgaben des Datenschutzbeauftragten (2)

Organisation der Arbeit des Datenschutzbeauftragten:

- Planung → Schriftlichen Aktivitätenplan aufstellen und fortführen bzgl. Aufgaben, Maßnahmen, Audits und Termine
- Dokumentationsaufgaben → z. B. Aktivitätenplan, Schulungen, Sensibilisierungsmaßnahmen, Prüfungen, Tätigkeitsbericht, Beratungen, Stellungnahmen, Vorabkontrollen, Vorfälle und Beschwerden, Mitwirkung bei Richtlinien oder Betriebs- bzw. Dienstvereinbarungen, Gespräche und Schriftverkehr mit der Aufsichtsbehörde, sonstige Gesprächsergebnisse
- Personelle und sachliche Unterstützung → Die vom Datenschutzbeauftragten benötigte sachliche und personelle Unterstützung fordert er von der Unternehmens- bzw. Behördenleitung ein. Er steuert das ihm zugeordnete Personal fachlich.

Aufgaben des Datenschutzbeauftragten (3)

Prüfungsaufgaben:

- Ein wichtiges Hilfsmittel der Prüfung ist die interne Verarbeitungsübersicht.
- Umfang und Tiefe der Prüfungen unterliegen der Weisungsfreiheit des Datenschutzbeauftragten. Dabei hat er sich am geltenden Datenschutzrecht und dem aktuellen Stand der Technik zu orientieren.
- Die Prüfungsergebnisse werden strukturiert dokumentiert und der Unternehmens- bzw. Behördenleitung berichtet. Hierbei ist auf festgestellte Risiken gesondert hinzuweisen.

Aufgaben des Datenschutzbeauftragten (4)

Gestaltungsaufgaben:

- Erstellung datenschutzrelevanter Unterlagen wie z. B. Datenschutzkonzept, Arbeitsanweisungen
- Sicherung der Betroffenenrechte (insbesondere zeitnahe Verwirklichung der Rechte)
- Aufklärungspflichten → auf umfassende Transparenz der Datenverarbeitung in der verantwortlichen Stelle und eine weit reichende Aufklärung über die Erhebung und Verarbeitung personenbezogener hinwirken

Mitwirkung in Prozessen und Projekten der verantwortlichen Stelle:

- Beteiligungen - als unabhängiger Sachverständiger zu Datenschutzfragen an Beratungen aller relevanten internen und einschlägigen externen Gremien
- Stellungnahmen
- Projektmitarbeit

Aufgaben des Datenschutzbeauftragten (5)

Schulungs- und Sensibilisierungsaufgaben:

- Basiswissen
- Vertiefungswissen

Beratung:

- Erkennen, welche Risiken von den Einzelphasen ausgehen.
- Wirksamkeit, Wirtschaftlichkeit, Praktikabilität, Angemessenheit sowie Akzeptanz organisatorischer und technischer Maßnahmen.

PERSICON@night am 19. März 2009

Der Datenschutzbeauftragte: Ausbildung

Ausbildung

- Das Landgericht Ulm hat in einem Beschluss Grundsätze zu Eigenschaften, Fachkunde und Befähigung des Datenschutzbeauftragten aufgestellt.
- Danach ist die Tätigkeit eines Datenschutzbeauftragte als ein Beruf anzusehen.
- Ein betrieblicher Datenschutzbeauftragter muss
 - die Vorschriften der Datenschutzgesetze des Bundes und der Länder und andere, den Datenschutz betreffende Rechtsvorschriften anwenden können,
 - über Kenntnisse der betrieblichen Organisation verfügen und
 - Computerexperte sein.

Ausbildung

Dem Ulmer Modell und dem Bundesdatenschutzgesetz entsprechend sollte die Ausbildung umfassen:

- Anwendung der Vorschriften der Datenschutzgesetze des Bundes und der Länder und aller anderen, den Datenschutz betreffenden, Rechtsvorschriften
- Kenntnisse der betrieblichen Organisation
- Didaktische Fähigkeiten
- Psychologisches Einfühlungsvermögen
- Organisationstalent
- Angemessener Umgang in Konflikten um seine Person, seine Funktion und seine Aufgabe

Weiterbildung

- Die fundierten fachlichen Kenntnisse aus der Ausbildung sind ständig aufzufrischen.
- Es empfiehlt sich die stetige Lektüre von Fachzeitschriften und Fachliteratur.
- Regelmäßiger Erfahrungsaustausch mit anderen Datenschutzbeauftragten unterstützt die eigene Tätigkeit als Datenschutzbeauftragter → ERFA-Kreise
- Der Besuch von Aufbauseminaren hilft, die eigene Fachkunde zu verbessern und bietet zudem eine Plattform für Erfahrungsaustausch.

PERSICON academy

- Die PERSICON academy bietet eine vollumfängliche Ausbildung an.
- Die Aus- und Weiterbildung entspricht dem Leitbild des Ulmer Modells.
- Die Schulungsinhalte werden ständig an aktuelle Tendenzen und Entwicklungen angepasst.
- Dozenten sind Praktiker, die in unterschiedlichen Branchen, Unternehmensformen und -größen die Funktion des externen Datenschutzbeauftragten wahrnehmen oder sonst beratend tätig sind.

PERSICON@night am 19. März 2009

Der Datenschutzbeauftragte: Zertifizierungen

Zertifizierungen

- Es gibt keine offizielle, bundesweit anerkannte Zertifizierung.
- Es fehlen objektive Bewertungskriterien einer übergeordneten Stelle.
- Die ausbildende Stellen attestieren die Teilnahme an Weiterbildungsmaßnahmen.
- Die regelmäßige (bescheinigte) Weiterbildung dient neben der Vertiefung der Fachkunde auch als Qualitätsnachweis gegenüber der Aufsichtsbehörde.

Welche Fragen haben Sie?



Vielen Dank für Ihre Aufmerksamkeit

Haiko Ferber

hferber@persicon.com

www.persicon.com

PERSICON@night am 19. März 2009

Der Datenschutzbeauftragte

Praxisteil

Vorstellung des Referenten

Michael Rautert

- staatlich geprüfter Informatiker (Fachrichtung Wirtschaft)
 - geprüfter, fachkundiger Datenschutzbeauftragter
-
- seit 2006 bei PERSICON
 - Einsatzbereiche bei PERSICON
 - Business Continuity Management/IT-Notfallvorsorge,
 - IT-Sicherheit gemäß BSI IT-Grundschutz und gemäß ISO 27001 IT-Sicherheit Fachkonzeption sowie
 - Datenschutz



Agenda - Praxisteil

1. Der Datenschutzbeauftragte in der Praxis
2. Kooperation mit dem IT-Sicherheitsbeauftragten
3. Schulung und Sensibilisierung der Mitarbeiter

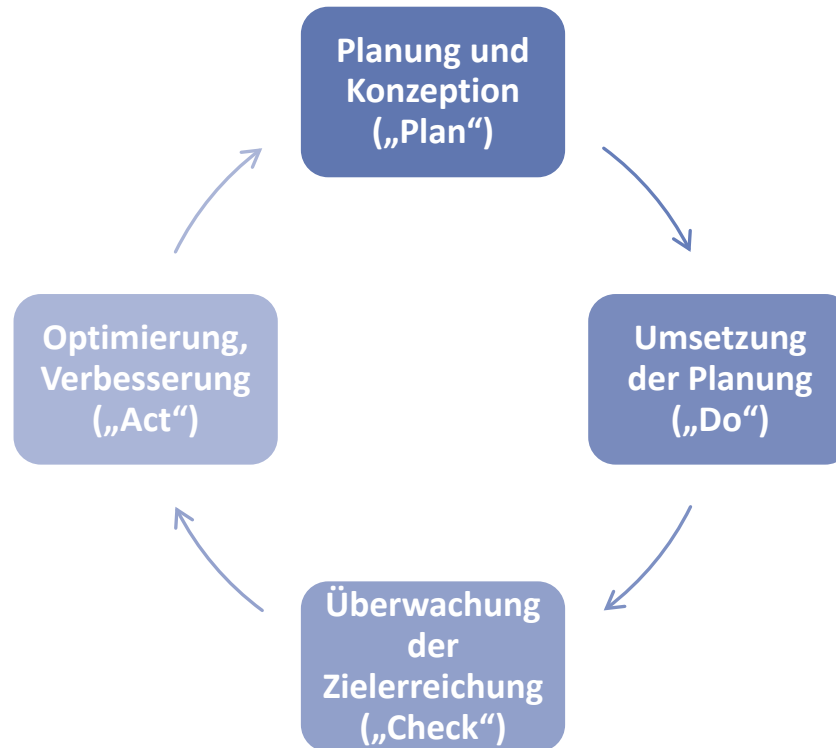
PERSICON@night am 19. März 2009

Der Datenschutzbeauftragte in der Praxis

Die Rolle des Datenschutzbeauftragten in der Praxis

- Wirksame Bestellung des Datenschutzbeauftragten
 - Rollenbeschreibung
 - Definition von Ressourcen
- Bekanntmachung gegenüber Management und Mitarbeitern
 - Vertrauen schaffen
 - Sensibilisierung
- Datenschutzorganisation
 - Allein
 - Datenschutzkoordinatoren

Datenschutz als Prozess: PDCA-Modell



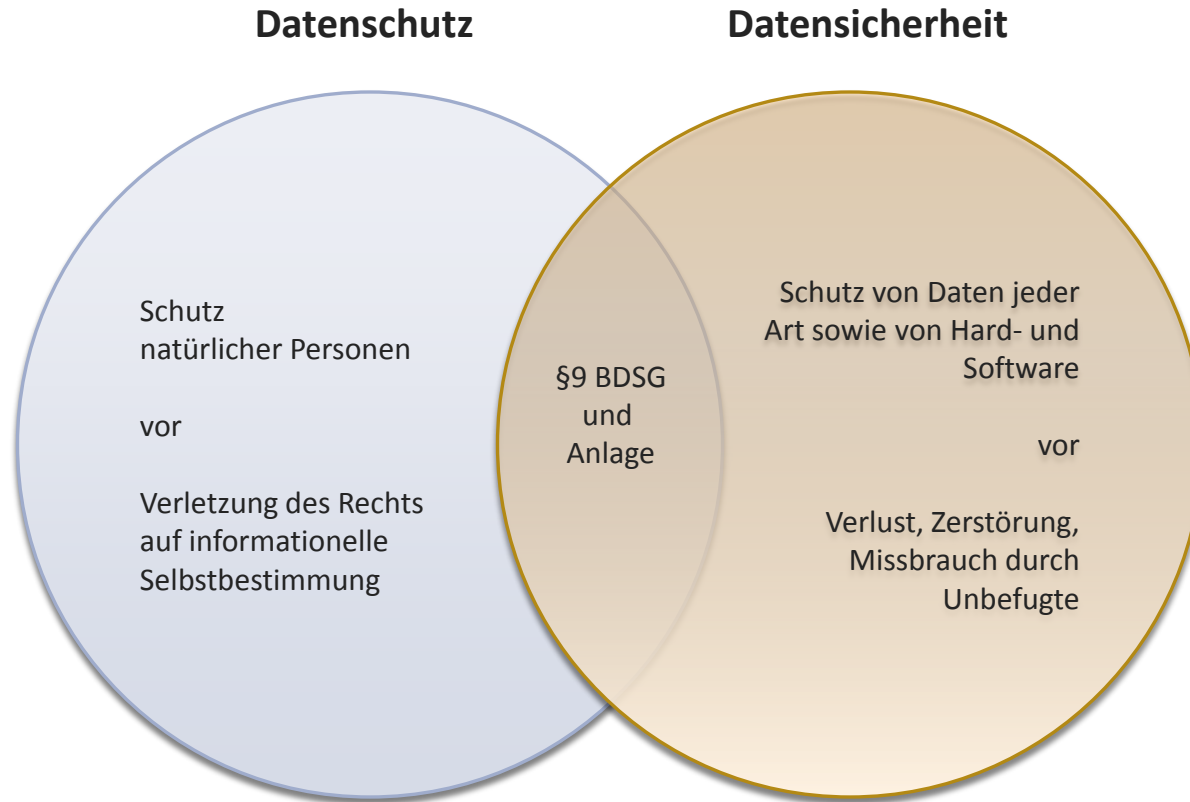
Lebenszyklus nach William Edwards Deming

Quelle: BSI 100-1

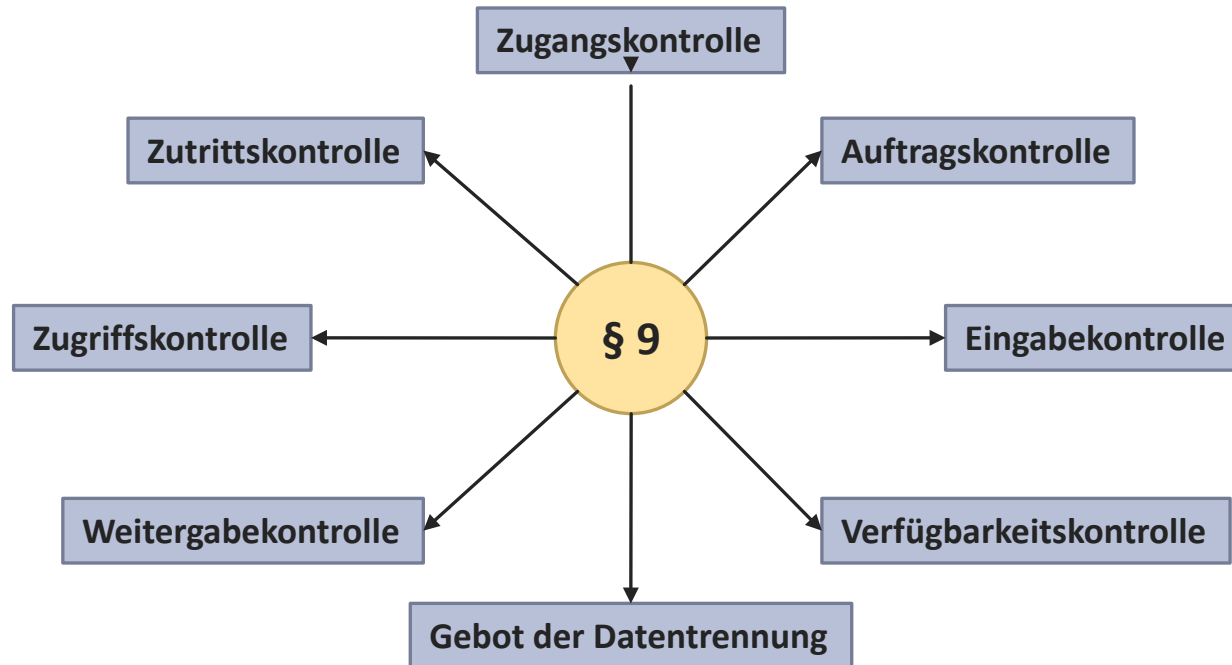
PERSICON@night am 19. März 2009

Kooperation mit dem IT-Sicherheitsbeauftragten

Datenschutz: Abgrenzung zwischen Datenschutz und Datensicherheit

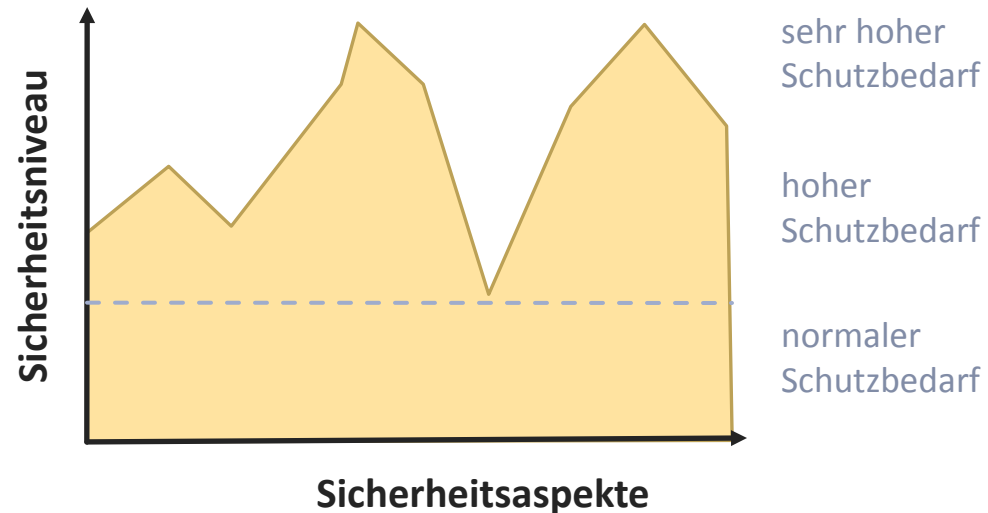


Datenschutz: Maßnahmen gemäß Anlage zu § 9 Satz 1 BDSG

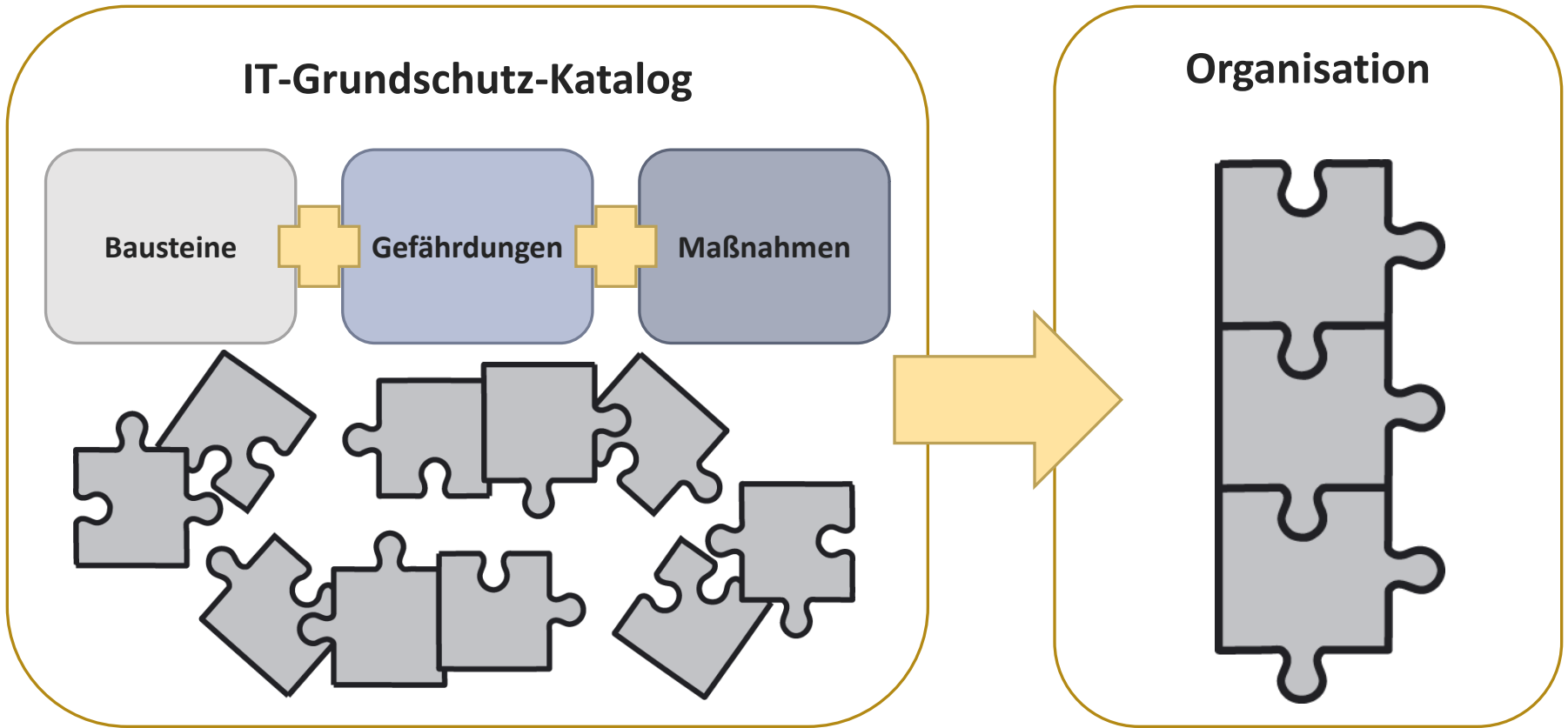


Das Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz

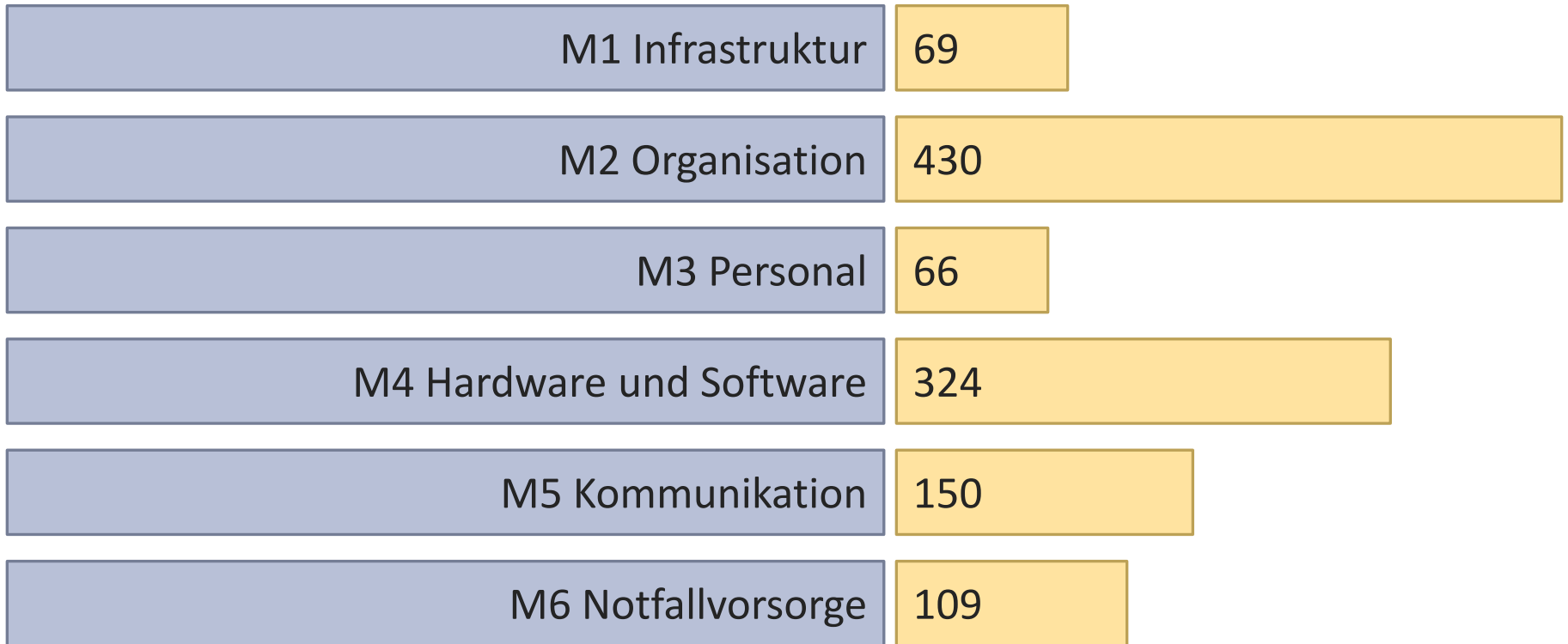
- Standardsicherheitsmaßnahmen für typische IT-Umgebungen
- Personelle, technische, organisatorische und infrastrukturelle Aspekte
- Initialer Verzicht auf eine detaillierte Risikoanalyse
- Drei Schutzbedarfskategorien:
 - normal
 - hoch
 - sehr hoch



Baukastenprinzip



Maßnahmenkataloge (1148 Maßnahmen)



Kreuzreferenztablelle

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				
M1.32	x	x	x					
M1.33		x	x				x	
M1.34		x	x				x	

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

PERSICON@night am 19. März 2009

Schulung und Sensibilisierung der Mitarbeiter

Schulungsprozess

Prozessschritt 1

- Eruiieren des Schulungs- und Sensibilisierungsbedarfes

Prozessschritt 2

- Planung und Erstellung eines Sensibilisierungs- und Schulungskonzeptes

Prozessschritt 3

- Durchführung von Sensibilisierungsschulungen zur Informationssicherheit

Prozessschritt 4

- Messung der Wirksamkeit von Sensibilisierungsschulungen

Prozessschritt 1 – Eruiieren des Schulungs- und Sensibilisierungsbedarfes

- Erstellung von Fragebögen
 - Fragen erstellen
 - Kommunikationsform auswählen (Papier/elektronisch)
 - Abstimmung mit Datenschutzbeauftragten/Personalvertretung
- Ausgabe/Überwachung
- Anonymisierte Auswertung

Prozessschritt 2 – Planung und Erstellung eines Sensibilisierungs- und Schulungskonzeptes

- Zeitplanung
- Wahl der Kommunikationskanäle/Medien
- Kreation/Ideenfindung

Prozessschritt 3 – Durchführung von Sensibilisierungsschulungen zur Informationssicherheit

- Form der Präsenzveranstaltung
 - Umfang (z.B. vier Stunden)
 - Art und Umfang der Gruppe
 - Terminfindung
- Darstellung des Themas
 - Vortragsstil
 - Motivation und Führung der Teilnehmer
- Feedback-Bogen

Prozessschritt 4 – Messung der Wirksamkeit von Sensibilisierungsschulungen

- Vorgehensweise
 - Soll/Ist Vergleich
 - Stand vor/nach Schulung
- Beispiel:
 - Vorab:
 - Verteilung von Testbögen/Durchführung von Interviews
 - Auswertung der Bögen (ggf. nach Abteilungen)
 - Durchschnittspunktzahl ermitteln
 - Anschließend:
 - Auswertung der Bögen, Ermittlung einer Durchschnittspunktzahl für den jeweiligen Kurs
 - Vergleich zum Durchschnitt (und ggf. der zugehörigen Abteilung)

Welche Fragen haben Sie?



Vielen Dank für Ihre Aufmerksamkeit

Michael Rautert
mrautert@persicon.com
www.persicon.com