Vorgehen beim Datenschutzaudit mit SAVe®

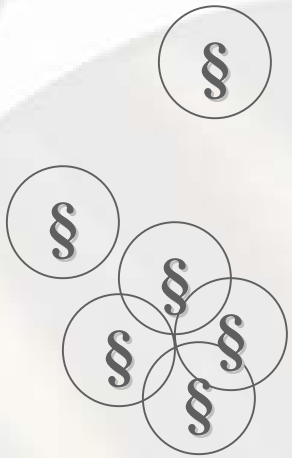
Frank Reiländer, Berater IT-Sicherheit
Infodas GmbH, Rhonestr. 2, 50765 Köln
f.reilaender@infodas.de
www.save-infodas.de

Prinzipien des modernen Datenschutzes

- Fokussierung auf elektronische Speicherung und Nutzung
- Aspekte der IT-gestützten Übermittlung
- Auftrags-DV und Outsourcing
  - technische/organisatorische Schutzmaßnahmen
- Prozesssicht
  - Dateiregister -> Verfahrensübersicht
- Systemdatenschutz
  - Datenvermeidung und -Sparsamkeit

Novellierung des BDSG 2001
Erweiterte Anforderungen

- Erweiterte Transparenz gegenüber dem Betroffenen
  - Erstellen einer öffentlichen Verfahrensübersicht
- Erweiterte Verarbeitungsbeschränkungen
  - Allgemeines Widerspruchsrecht
  - „Besondere Arten“ personenbezogener Daten
- Erweiterte Datenschutzkontrolle
  - Vorabkontrolle bei risikoreichen Verarbeitungen
- Einführung des Datenschutzaudits
  - Qualitätsmerkmal und –Kontrolle (freiwillig)



Stellenwert der IT-Sicherheits-Aspekte im Datenschutz

- Technische und organisatorische Maßnahmen (§9, Anlage zu §9 BDSG)
  - Datensicherungsmaßnahmen (BDSG 1990) -> Datensicherheitsmaßnahmen (BDSG 2001)
  - „Terminologie der IT-Sicherheit“ (Aussage BMI)
- Prozesssicht der Verarbeitung
  - Datei-Register -> Verfahrensübersicht
  - Widerspruchsrecht des Betroffenen
- Datenschutzkontrolle
  - Kontrolle der DV-Programme, Vorabkontrolle

Thesen zur Konvergenz von Datenschutz und IT-Sicherheit

infodas
Software and Services made in Cologne

- „Datenschutz stützt sich zu zwei Dritteln auf Datensicherheit“
  - allg. Betrachtung der Datenschutz-Fachpresse
- „Datensicherheit identifiziert sich mit den Grundwerten der IT-Sicherheit“
  - Kommentierung BDSG-Novelle
- Praxistest „Datenschutzaudit und IT-Gütesiegel“ des ULD, Schleswig-Holstein
  - Datenschutz und -sicherheit als Qualitätsmerkmal
  - Einführung datenschutzfreundlicher Technik

Argumente zum Datenschutz-Audit

- Datenschutzaudit zur Stärkung der Selbstkontrolle des betrieblichen Datenschutzbeauftragten
- Effizientes, wettbewerbsgerechtes Verfahren statt staatlicher Kontrolle
- „Wildwuchs“ an Datenschutz-Gütesiegeln sollte verhindert werden
- Etablierte Standards fördern Synergie-Effekte und eine schnelle Etablierung im Sinne eines Qualitätsmerkmals

Datenschutz-Audit mit SAVe®
Methodischer Ansatz

- IT-Grundschutzhandbuch, Baustein 3.5
  - Bundesbeauftragter für den Datenschutz 1999, wurde nicht offiziell ins IT-GSHB übernommen
  - siehe www.bfd.bund.de/technik/DS-KAP/35.htm
- Zuordnungstabelle der „Gebote“ (Anl. zu §9 BDSG) – Grundschutzmaßnahmen
- Konsolidieren der Maßnahmen-Empfehlungen anhand aktueller Datenschutz-Ziele (Prüffragen)
- Aktualisierung der Datensicherheits-Maßnahmen gemäß BDSG 2001

Datenschutz-Audit mit SAVe® Umsetzung der Methodik

- Datenschutzorganisation und Aufgaben des betrieblichen Datenschutz-beauftragten (Datenschutz-Aspekte)
  - Prüfung der Datenschutzorganisation anhand der Maßnahmenempfehlungen des BfD
- Prüfung der Umsetzung der technischen und organisatorischen Maßnahmen (Datensicherheits-Aspekte)
  - Prüfung des Umsetzungsstands der Maßnahmen durch Abbildung auf relevante Grundschutz-Maßnahmen

Datenschutz-Audit mit SAVe®
Datenschutzorganisation

infodas®
Software and Services made in Cologne

- Konsolidieren der Maßnahmen-Empfehlungen M 7.0 – M 7.17 (BfD)
- Aktualisierung gemäß Veränderungen BDSG-Novelle 2001
- Kategorisierung der „neuen“ Datenschutzaspekte
- Modellierung anhand von Prüffragen
- Erfassen und Bewerten der Prüffragen mittels SAVe®

Einbinden bestehender Audit-Prüflistenlisten

infodas
Software and Services made in Cologne

1. Strukturieren der Auditlisten als Excel-Tabellen
2. Übernahme in die Datenbank über die Import-/ Export-Schnittstelle
3. Erweitern der Umsetzungstabelle

Anforderungen nach dem Bundesdatenschutzgesetz (BDSG)

Prüfansätze	ja	nein
Allgemeine Datenschutzerfordernisse (§§ 1, 27 ff. BDSG)		
Werden im Unternehmen personenbezogene Daten automatisiert verarbeitet?		
Gibt es eine Jobverarbeitung?		
Findet die Verarbeitung interaktiv statt?		
Werden APC eingesetzt?		
Unterliegt das Unternehmen den Vorschriften des BDSG?		

Checks.xls

	A	B	
1	CheckID	CheckShort	CheckDescription
2	700001	Q 7.0.1	Finden die Vorschriften des Bundesdatenschutzgesetzes (BDSG) im Unternehmen Anwendung?
3	700002	Q 7.0.2	Finden die Vorschriften des Landesdatenschutzgesetzes (LDSG) Anwendung?
4	700003	Q 7.0.3	Findet das Telekommunikationsgesetz (TKG) Anwendung?
5	700004	Q 7.0.4	Findet das Teledienstegesetz (TDG) Anwendung?
6	700005	Q 7.0.5	Wird das Teledienstedatenschutzgesetz (TDDSG) beachtet?
7	700006	Q 7.0.6	Wird der Mediendienstestaatsvertrag (MDSV) beachtet?
8	700007	Q 7.0.7	Sind der Unternehmensleitung die Anforderungen des BDSG im wesentlichen bekannt?
9	700008	Q 7.0.8	Kommt die Unternehmensleitung uneingeschränkt ihren gesetzlichen Verpflichtungen nach?
10	700009	Q 7.0.9	Werden freiwillige Maßnahmen zur Umsetzung der Datenschutzziele gemäß BDSG ergriffen?
11	700010	Q 7.0.10	Hat der Datenschutz einen angemessenen Stellenwert im Unternehmen?
12	700011	Q 7.0.11	Stellt Verarbeitung und Nutzung personenbezogener Daten einen wesentlichen Teil der Geschäfts
13	700012	Q 7.0.12	Entspricht der Stellenwert des Datenschutzes dieser Geschäftstätigkeit?
14	700013	Q 7.0.13	Sind mehr als vier Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt?
15	700014	Q 7.0.14	Wurde ein betrieblicher Datenschutzbeauftragter bestellt?
16	700101	Q 7.1.1	Werden im Unternehmen personenbezogene Daten automatisiert verarbeitet?
17	700102	Q 7.1.2	Wird der Datenschutzbeauftragte hinreichend in die Geschäftsprozesse einbezogen?
18	700103	Q 7.1.3	Wird der betriebliche Datenschutzbeauftragte frühzeitig über die Einführung neuer Verfahren inform
19	700104	Q 7.1.4	Findet eine Abstimmung mit den jeweiligen Fachverantwortlichen statt?
20	700105	Q 7.1.5	Findet eine Abstimmung mit dem IT-Verfahrensverantwortlichen statt?
21	700106	Q 7.1.6	Wird dem Datenschutzbeauftragten ausreichend Zeit zur Prüfung der Zulässigkeit eingeräumt?
22	700107	Q 7.1.7	Sind aktuelle Gesetzestexte verfügbar, um die wesentlichen Normen nachlesen zu können?
23	700108	Q 7.1.8	Sind die notwendigen bereichsspezifischen Gesetze vorhanden?

Maßnahmen Datenschutz (Baustein 3.5)

- Regelung der Verantwortlichkeiten im Bereich Datenschutz (M 7.0)
- Prüfung der Zulässigkeit der Datenverarbeitung (M 7.1)
- Prüfung der Erforderlichkeit (M 7.2)
- Prüfung der Verwendung von Daten hinsichtlich der Zweckbindung (M 7.3)
- Prüfung der Verwendung der Daten hinsichtlich der besonderen Zweckbindung (M 7.4)
- Bestellung eines Datenschutzbeauftragten (M 7.5)
- Verpflichtung/Unterrichtung der Mitarbeiter (M 7.6)
- Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen (M 7.7)
- Führung von Dateien- und Geräteverzeichnissen und Erfüllung der Meldepflichten (M 7.8)

Maßnahmen Datenschutz (Baustein 3.5)

- Ergreifen von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik (M 7.9)
- Dokumentation der datenschutzrechtlichen Zulässigkeit (M 7.10)
- Datenschutzaspekte bei der Protokollierung (M 7.11)
- IT- und Datenschutz-Regelungen (M 7.12)
- Datenschutzrechtliche Freigabe (M 7.13)
- Meldung und Regelung von Abrufverfahren (M 7.14)
- Regelung der Auftragsdatenverarbeitung (M 7.15)
- Regelung der Verknüpfung und Verwendung von Daten (M 7.16)
- Einrichtung einer internen IT-Revision und Datenschutzkontrolle (M 7.17)

Eröffnen der Datensicherheits-Sicht auf den Grundschutz

- Konsolidieren, Aktualisieren und Erweitern der Verknüpfungen
- Zuordnen der neuen Datensicherheits-„Gebote“
- Modellieren der Referenzbeziehungen in SAVe®
- Regelmäßiger Expertenworkshop zur Bewertung der Maßnahmen-Empfehlungen

SAVe® – Erweiterung durch Erstellen neuer Bausteine

infodas
Software and Services made in Cologne

1. Erstellen der Bausteine als Excel-Tabelle
2. Übernahme in die Datenbank über die Import-/ Export-Schnittstelle
3. Aktivieren der neuen Bausteine in SAVe

Module.xls

	A	B	C	D	E	F	G
1	ModuleID	ModuleShort	ModuleDescription	ModuleText	ModuleLevel	ModuleClassID	Module
2	3050	B 3.5	Datenschutz	B 3.5	1	3	
3	3051	B 3.5.1	Zutrittskontrolle (BDSG)	B 3.5.1	1	3	
4	3052	B 3.5.2	Zugangskontrolle (BDSG)	B 3.5.2	1	3	
5	3053	B 3.5.3	Zugriffskontrolle (BDSG)	B 3.5.3	1	3	
6	3054	B 3.5.4	Weitergabekontrolle (BDSG)	B 3.5.4	1	3	
7	3055	B 3.5.5	Eingabekontrolle (BDSG)	B 3.5.5	1	3	
8	3056	B 3.5.6	Auftragskontrolle (BDSG)	B 3.5.6	1	3	
9	3057	B 3.5.7	Verfügbarkeitsgebot (BDSG)	B 3.5.7	1	3	
10	3058	B 3.5.8	Trennungsgebot (BDSG)	B 3.5.8	1	3	
11	3059	B 3.5.9	Organisationskontrolle (BDSG)	B 3.5.9	1	3	

Datenimport aus Microsoft Excel

Liste aller Tabellen

Tabellenname: Module

Beschreibung: Grundschutzbausteine

Funktion

Importieren aus Excel

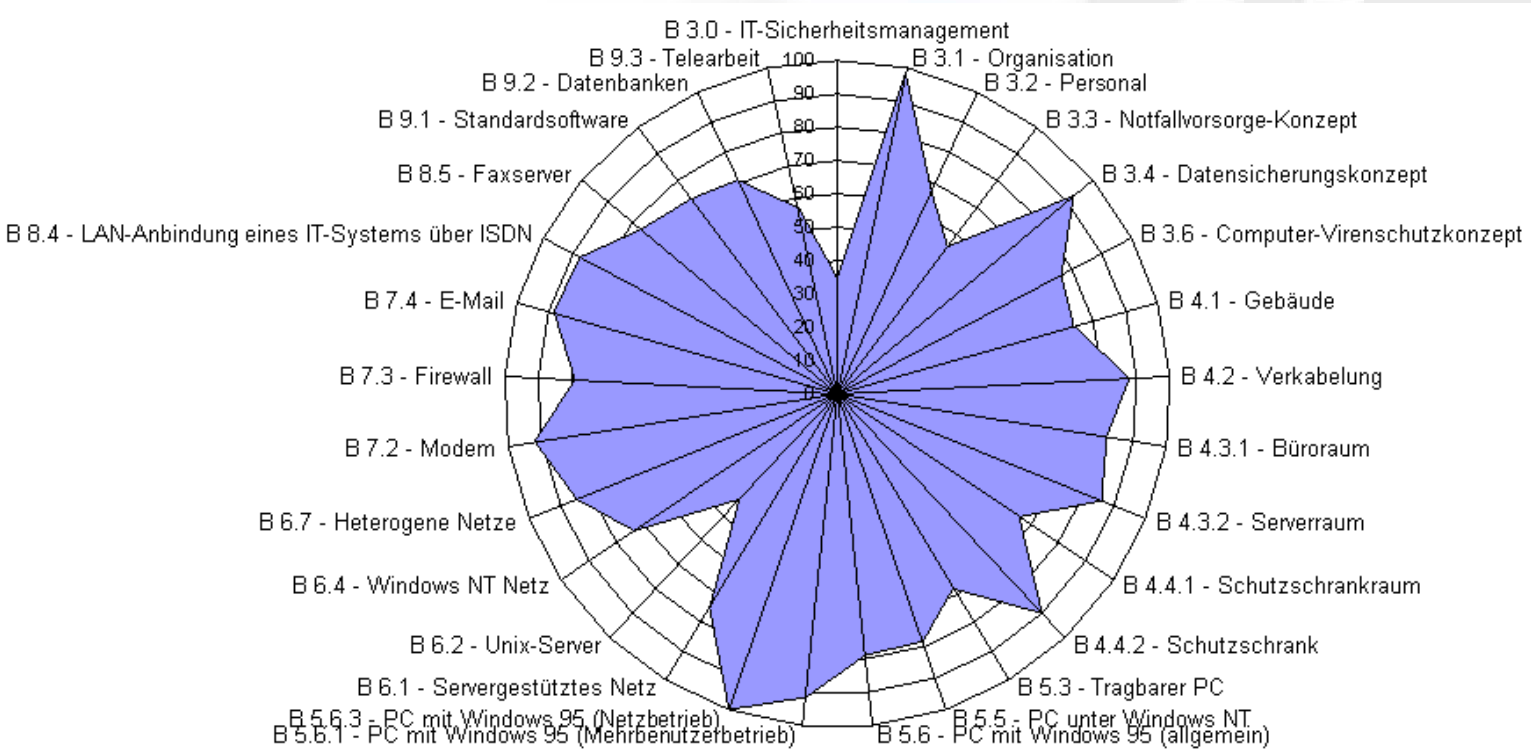
Übersicht Bausteine

Kennung	Aktiv	Beschreibung	Klasse
B 3.0	☐	IT-Sicherheitsmanagement	Übergeordnete Komponenten
B 3.1	☑	Organisation	Übergeordnete Komponenten
B 3.2	☑	Personal	Übergeordnete Komponenten
B 3.3	☐	Notfallvorsorge-Konzept	Übergeordnete Komponenten
B 3.4	☐	Datensicherungskonzept	Übergeordnete Komponenten
B 3.5	☑	Datenschutz	Übergeordnete Komponenten
B 3.5.1	☑	Zutrittskontrolle (BDSG)	Übergeordnete Komponenten
B 3.5.2	☑	Zugangskontrolle (BDSG)	Übergeordnete Komponenten
B 3.5.3	☑	Zugriffskontrolle (BDSG)	Übergeordnete Komponenten
B 3.5.4	☑	Weitergabekontrolle (BDSG)	Übergeordnete Komponenten
B 3.5.5	☑	Eingabekontrolle (BDSG)	Übergeordnete Komponenten
B 3.5.6	☑	Auftragskontrolle (BDSG)	Übergeordnete Komponenten
B 3.5.7	☑	Verfügbarkeitsgebot (BDSG)	Übergeordnete Komponenten
B 3.5.8	☑	Trennungsgebot (BDSG)	Übergeordnete Komponenten
B 3.5.9	☑	Organisationskontrolle (BDSG)	Übergeordnete Komponenten
B 3.6	☐	Computer-Virenschutzkonzept	Übergeordnete Komponenten

Bausteine Datensicherheit

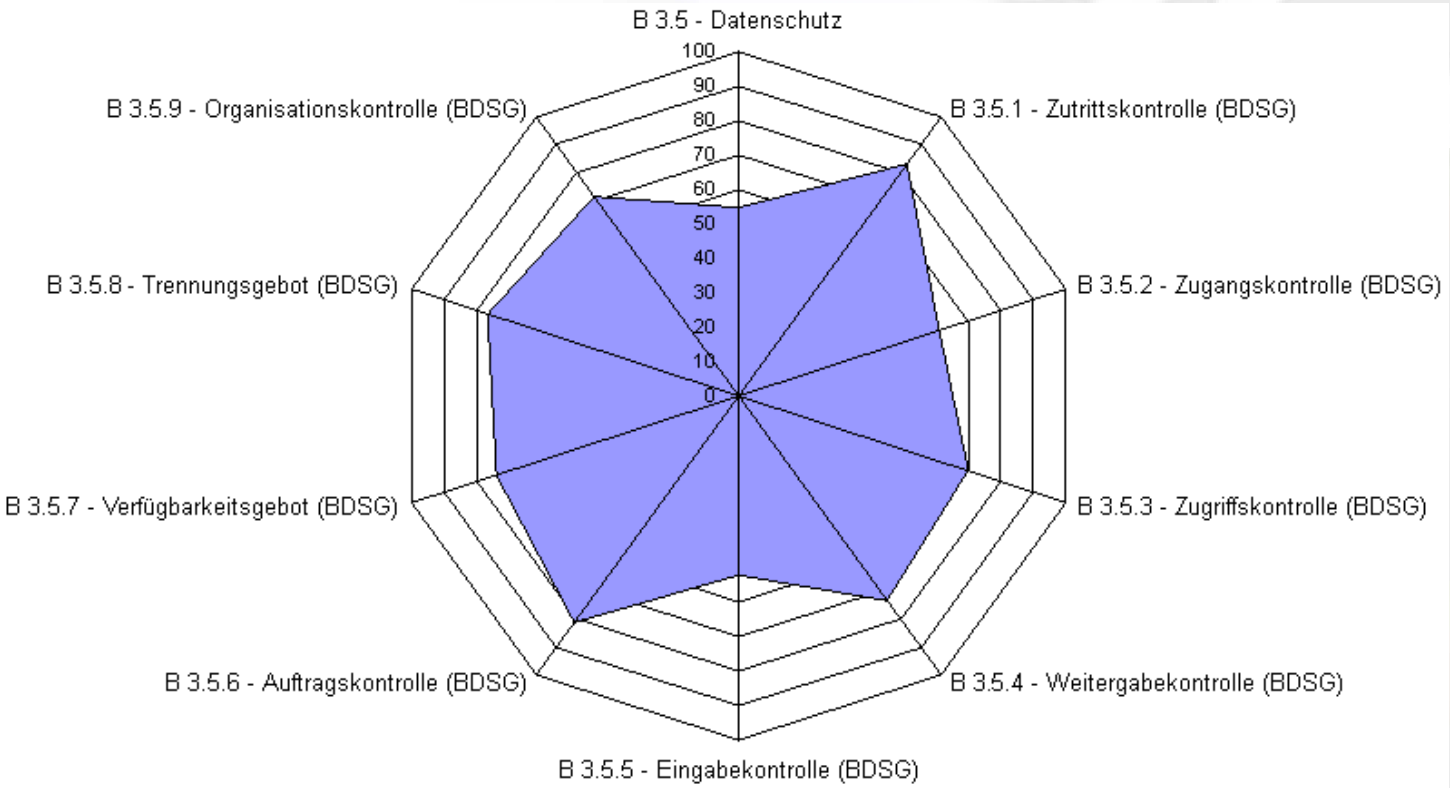
- Zutrittskontrolle (Baustein 3.5.1)
- Zugangskontrolle (Baustein 3.5.2)
- Zugriffskontrolle (Baustein 3.5.3)
- Weitergabekontrolle (Baustein 3.5.4)
- Eingabekontrolle (Baustein 3.5.5)
- Auftragskontrolle (Baustein 3.5.6)
- Verfügbarkeitsgebot (Baustein 3.5.7)
- Trennungsgebot (Baustein 3.5.8)
- Organisationsgebot (Baustein 3.5.9)

Umsetzungsstand von IT-Grundschutzmaßnahmen



- Ergebnis eines Basis-Sicherheitschecks nach IT-Grundschutz-Handbuch (Praxisbeispiel)

Datenschutz-Audit – Ergänzung des Basis-Sicherheitschecks



- Datensicherheitssicht auf den den Ergebnisse dieser Grundschutzerhebung (Praxisbeispiel)

Vorgehen beim Datenschutzaudit mit SAVe®

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf Ihre Fragen und Anforderungen:

INFODAS GmbH, Rhonestraße 2, D-50765 Köln
info@save-infodas.de oder www.save-infodas.de