Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Anstalt des öffentlichen Rechts

Digitale Woche 2018

Datensicherheit

Meine Daten sind sicher, ich trage die Verantwortung!

Heiko Behrendt
ISO 27001 Auditor
Fon: 0431 988 1212
Mail: hbehrendt@datenschutzzentrum.de
Web: https://www.datenschutzzentrum.de/

Themen

- Hat Ihr Unternehmen eine Strategie zur Umsetzung von Datenschutz und Informationssicherheit?
- Welche Anforderungen sind zu erfüllen und welche Aufgaben sind zu bewältigen?
- Wie sicher ist mein Unternehmen (Selbstcheck)?

Informationen

- Spionage, Sabotage und Datendiebstahl
  https://www.bitkom.org
- BSI-Standards
  https://www.bsi.bund.de

Fakten

- Viele Unternehmen schützen ihre materiellen und immateriellen Werte nicht ausreichend!
- Systemausfälle und Datenverluste treffen jedes Unternehmen!
- Der Diebstahl von Daten und Datenträgern nimmt aufgrund der Digitalisierung zu und wird immer einfacher!
- Bei Eintritt eines Notfalls liegt der finanzielle Schaden häufig im fünfstelligen Bereich (>10.000 Euro)!

Hat Ihr Unternehmen eine Strategie zur Umsetzung von

Datenschutz und Informationssicherheit

?

10 Indikatoren

Sind Ihre Daten sicher?

1. Hat das Unternehmen / die Behörde eine Leitlinie, die die Ziele und die Datenschutz- und Sicherheitsstrategie verbindlich vorschreibt?
2. Ist ein Datenschutz- und Informationssicherheitsmanagement (DISM) eingerichtet?
3. Wurden dem DISM ausreichende Ressourcen zur Verfügung gestellt?
4. Besteht eine aktuelle Dokumentation über die eingesetzte Hard- und Software, über die Netzstrukturen und die Anwendungen?
5. Sind die Datenkommunikationsprozesse transparent?
6. Ist der Schutzbedarf für die zu schützenden Werte im Unternehmen festgelegt?
7. **Gibt es Vorgaben über umzusetzende Schutzmaßnahmen?**
8. Ist ein Plan für die Durchführung von Kontrollen und Audits vorhanden?
9. Sind Datenschutz- und Informationssicherheitsvorfälle definiert und werden sie bearbeitet?
10. Ist ein Schulungskonzept vorhanden und werden Beschäftigte über Datenschutz und Informationssicherheit regelmäßig sensibilisiert und geschult?

Datenschutzstandard
Datenschutz-Grundverordnung

- 11 Kapitel, 99 Artikel, 173 Erwägungsgründe (Veranschaulichung, Begründung)

- **Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten**

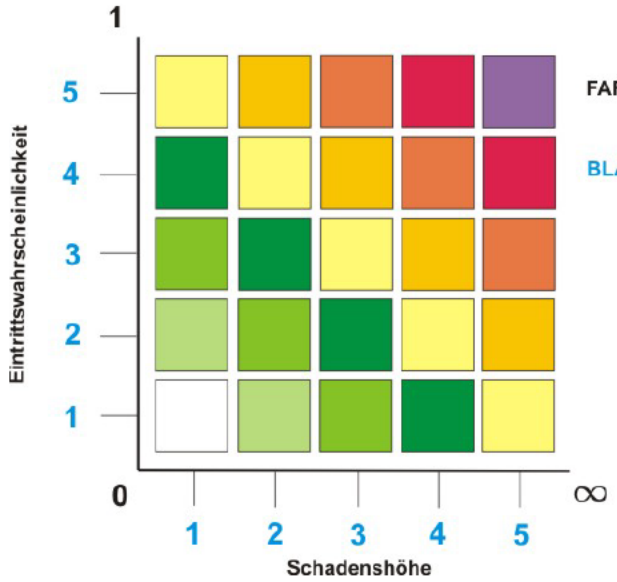
  Für personenbezogene Daten müssen folgende **Grundsätze** beachtet werden:
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (→ Rechtsgrundlagen, Nachvollziehbarkeit)
  - Zweckbindung (→ festgelegte, eindeutige und legitime Zwecke)
  - Datenminimierung (→ Begrenzung durch Zwecksetzung)
  - Richtigkeit (→ Berichtigung/Löschung personenbezogener Daten)
  - Speicherbegrenzung (→ Erforderlichkeit)
  - Integrität und Vertraulichkeit (→ technisch-organisatorische Maßnahmen)
    Rechenschaftspflicht (→ Dokumentationspflicht)

  Der Verantwortliche ist für die Einhaltung verantwortlich und muss dessen Einhaltung nachweisen können

Risiko-orientierter Ansatz

- Was sind die schützenswerten Güter (**Kronjuwelen**) des Unternehmens?
- Welche Risiken bestehen für **Verantwortliche** und für **Betroffene**?
- Wie **hoch** darf ein (finanzieller) Schaden maximal sein?

RISIKOMATRIX



Risiko = Eintrittswahrscheinlichkeit X Schadenshöhe

Risikoreduzierung = Umsetzung von Schutzmaßnahmen

Quelle: https://de.wikipedia.org/wiki/Risikomatrix

Geschäftsprozesse und betroffene Personen

	Datenschutz		IT-Grundschutz
	Datenschutzrecht	**Datensicherheit**	**Grundschutzstandard**
KERNELEMENTE	- Zulässigkeit der Datenverarbeitung - Zweckbindung - Transparenz - Verhältnismäßigkeit - Datenminimierung - Verzeichnis der Verarbeitungstätigkeiten - Datenweitergabe - Rechte der betroffenen Personen - Datenschutzbeauftragte(r) - Datenschutz-Folgenabschätzung - Ordnungswidrigkeiten - Haftung	- Gefährdungs- und Risikoanalyse - Schutzbedürftigkeit - Technische und organisatorische Sicherheitsmaßnahmen - Überwachung und Audits	- Sicherheitsmanagement - IT-Sicherheitsbeauftragte(r) - Abgrenzung der Datenverarbeitung (IT-Verbund) - Schutzbedarfsfestlegung - Grundschutzmaßnahmen - Risikoanalyse - Überwachung und Audits
ZWECK	- Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten - Schutz der Rechte und Freiheiten der betroffenen Personen		- Schutz der Informationen des Unternehmens bzw. der Behörde, keine Differenzierung zwischen personenbezogenen und nicht personenbezogenen Daten
§	- Rechtliche Vorschrift		- Keine rechtliche Vorschrift

Datenschutz auf der Basis von IT-Grundschutz

Welcher Standard ist für

Datenschutz und Informationssicherheit

geeignet

?

Informationssicherheitsstandard für Informationssicherheit
ISO 27001

- Regelwerke zum Informationssicherheitsmanagement – ISMS

  - ISO/IEC 27000 – Übersicht
  - ISO/IEC 27001 – ISMS Anforderungen
  - ISO/IEC 27002 – Leitfaden - Code of practice
  - ISO/IEC 27003 – Implementierungsrichtlinie ISMS
  - ISO/IEC 27004 – Kennzahlen, Messmethoden für das ISMS
  - ISO/IEC 27005 – Risikomanagement
  - IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI)
  - BSI-Standard 200-1 – Managementsysteme für Informationssicherheit
  - BSI-Standard 200-2 – IT-Grundschutzvorgehensweise
  - BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz
  - BSI-Standard 100-4 – Notfallmanagement
  - ISIS12 für kleine und mittelständige Unternehmen!?
  - Standard-Datenschutzmodell in Erprobung
  - …

Wie erstelle ich eine

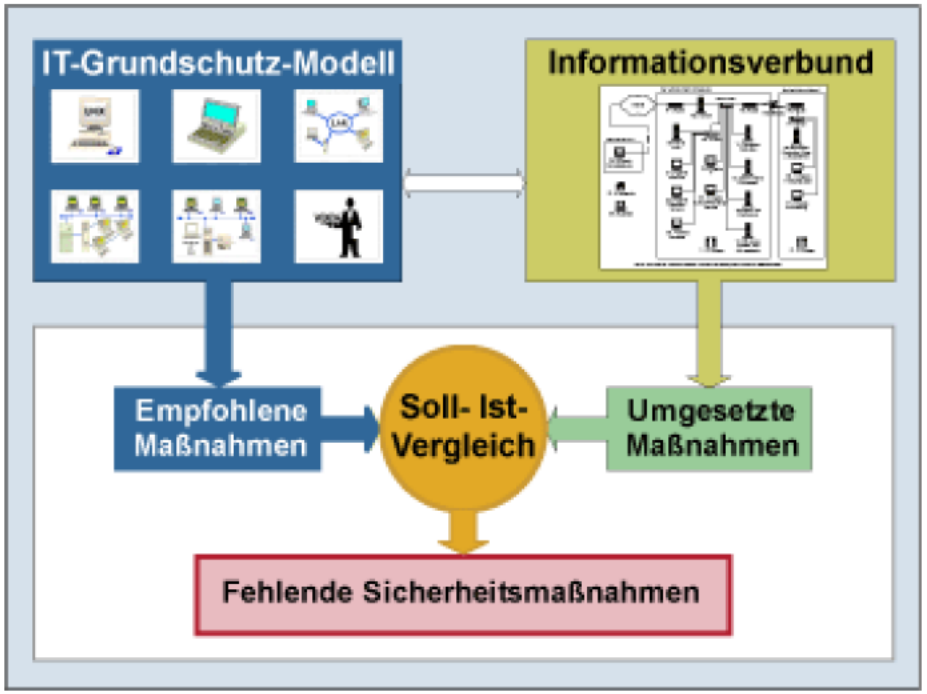
Datenschutz- und Informationssicherheitskonzeption

?

Datenschutz auf der Basis von IT-Grundschutz

Datenschutz- und Informationssicherheitsmanagement (DISM)

- Der IT-Grundschutz des BSI ist eine bewährte Methodik, um das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen.
- Die Anforderungen des IT-Grundschutzes gelten in Verwaltung und Wirtschaft als Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit (ISMS) geht.
- Der IT-Grundschutz ist durch seine Kompatibilität zu ISO 27001 ein anerkannter Standard.



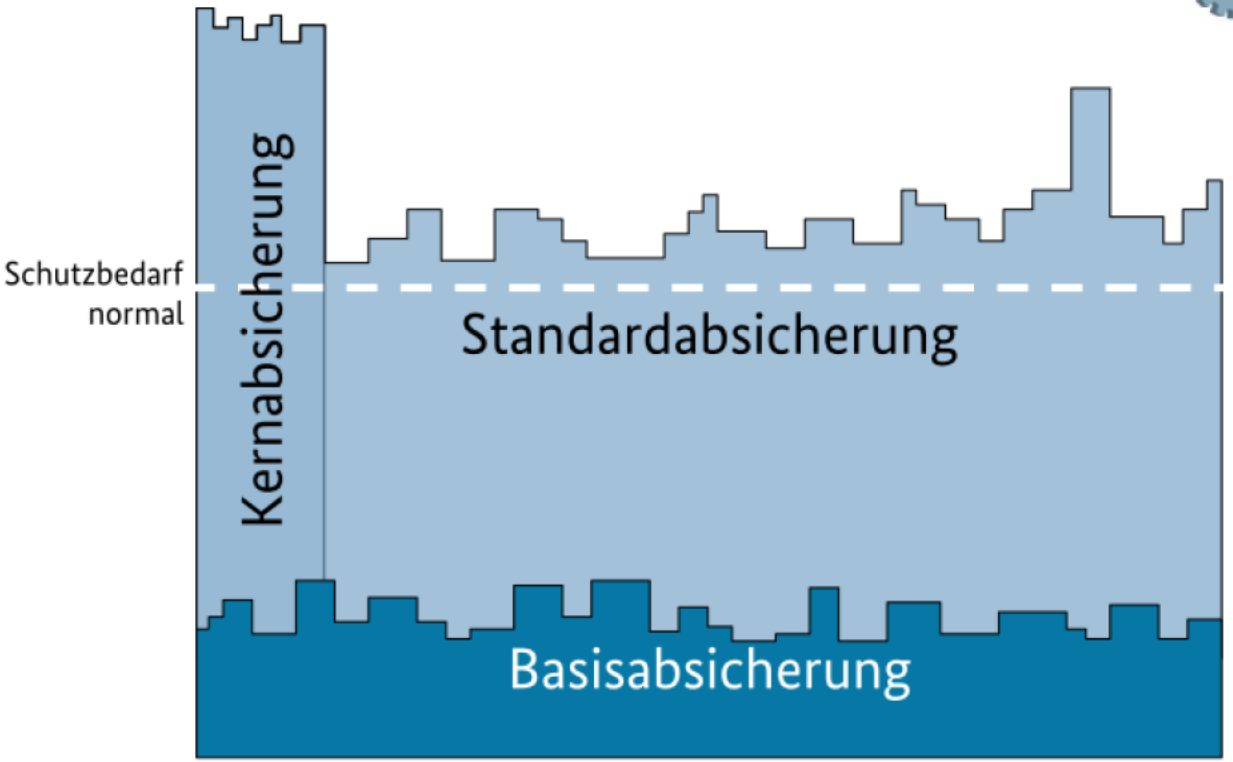
https://www.bsi.bund.de

Datenschutz auf der Basis von IT-Grundschutz

Stufenmodell

Vorgehensweisen

Überblick



Bundesamt für Sicherheit in der Informationstechnik

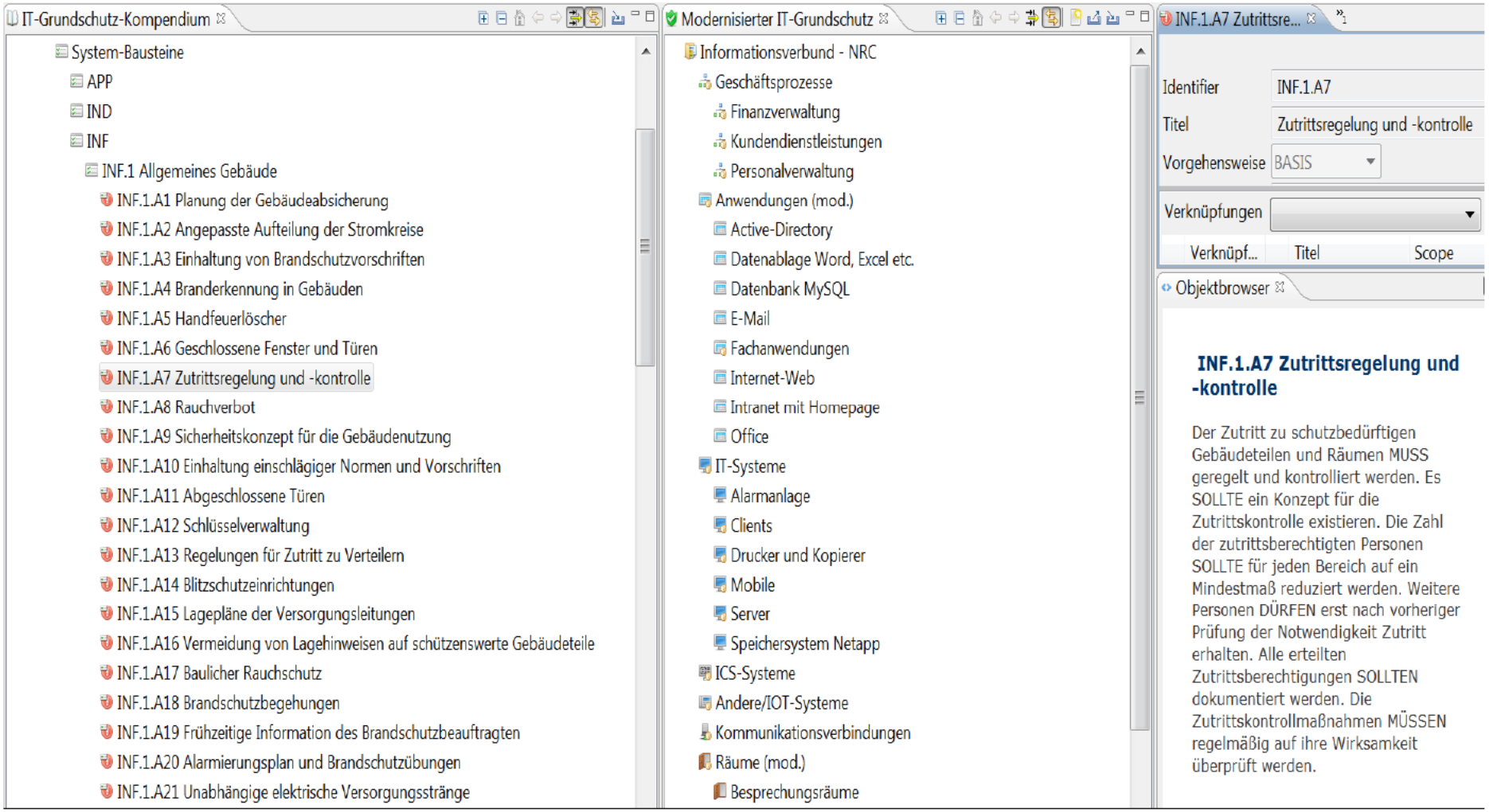
I. Münch & H. Schildt | CeBIT 2016 | Seite 10

Mit Methode implementieren
„Roter Faden"

- Implementierung des Datenschutz- und Informationssicherheitsmanagements (DISM)
- Initiierung des Sicherheitsprozesses
- **Erstellung einer Datenschutz- und Sicherheitskonzeption**
  - Geltungsbereich
  - Strukturanalyse
  - Schutzbedarfsfeststellung (Perspektive Geschäftsprozesse und Betroffene)
  - Bausteine Grundschutzkompendium + benutzerdefinierte Datenschutzbausteine
  - Basischeck
  - Risikoanalyse bei hohem Schutzbedarf
- Aufrechterhaltung der Datenschutz- und Sicherheitskonzeption
- Audits zur Verbesserung der Datenschutz- und Sicherheitsprozesse

Einsatz eines Tools für die Transparenz

Verinice



Datenschutz- und Informationssicherheitskonzept

Dokumentation

Technische Dokumentation

- Inventarisierung
- Aufnahme und Abgrenzung des Informationsverbunds
- Konzepte für den Einsatz der IT
  - Netzkonzept
  - Virenschutz
  - Datensicherung
  - Schulung und Sensibilisierung
  - Patchmanagement
- Richtlinien für IT-Komponenten
- Anweisungen für Administratoren und Nutzer
- Konfigurationsbeschreibungen
- Benutzer- und Rechteverwaltung
- Protokolle
- …

Datenschutz und Informationssicherheit

- Leitlinie zum Datenschutz und zur Informationssicherheit
- Beschreibung der Datenschutz- und Informationssicherheitsorganisation
- Schutzbedarfsfeststellung
- Risikoanalyse
- **Technische und organisatorische Maßnahmen**
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Datenschutz- und Sicherheitsvorfälle
- Revision und Audits
- Verträge mit Auftragsverarbeiter
- …

Checkliste

10 Schritte für Datenschutz und Informationssicherheit

1. Datenschutz- und Informationssicherheitsanforderungen verifizieren
2. Datenschutz und Informationssicherheitsmanagement (DISM) integrieren
3. Bestandsaufnahme der Geschäftsprozesse für die Bereiche Infrastruktur, IT-Systeme, Netz und Anwendungen/Daten durchführen
4. Schutzbedarfe bzw. Sicherheitsniveau aus der Betroffenenperspektive und nach Geschäftsprozessen, Daten und zugehörigen Objekten (Gebäude, Server, Clients etc.) bestimmen
5. Personal schulen und sensibilisieren
6. Technische Dokumentation verbessern
7. Technische und organisatorische Maßnahmen unter Einsatz eines Tools festlegen, dokumentieren und umsetzen
8. Richtlinien und Anweisungen erstellen
9. Restrisiken analysieren und dokumentieren
10. Datenschutz und Informationssicherheit durch Audits intensivieren und aufrechterhalten

Vielen Dank für Ihre Aufmerksamkeit!

Heiko Behrendt
ISO 27001 Auditor
Fon: 0431 988 1212
Mail: hbehrendt@datenschutzzentrum.de
Web: https://www.datenschutzzentrum.de/