Vorlesung Datenschutz

WS 2018/2019

Durchführung:

Beschäftigte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Kiel

Ansprechpartner:

Henry Krasemann
ULD7@datenschutzzentrum.de
Tel. 0431-988 1398
www.datenschutzzentrum.de

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Organisatorisches I: Vorlesungsorganisation und Material

- **Datenschutz ist ein Querschnittsthema mit rechtlichen und technischen Fragestellungen.**
- **Die Vorlesung wird von verschiedenen Beschäftigten des ULD gehalten, die nach einer Einführung aus ihren jeweiligen Spezialgebieten berichten.**
- **Die Folien der Veranstaltungen werden auf der Seite https://www.datenschutzzentrum.de/vorlesungen/ zur Verfügung gestellt.**
- **Gesetzestexte auf www.datenschutzzentrum.de/gesetze/: Dürfen auch für die Klausur verwendet werden. Unterstreichungen und Hervorhebungen sind erlaubt. Ebenso Paragraphenverweise in der Form „=> § 3 VIII" nicht aber Anmerkungen mit Wörtern oder Text.**

Organisatorisches II

- **Prüfungsleistung: Klausur über alle Bestandteile der Veranstaltung**
- **Anteil Datenschutzrecht an der Gesamtleistung: ca. 2/3**
- **Üblicher Aufbau im Datenschutzrecht: Freitext-Fragen, Multiple Choice, evtl. ein kleiner Fall**
- **Es wird voraussichtlich eine Übungsklausur im Rahmen veröffentlicht und besprochen oder Musterlösungen bereitgestellt.**

Datenschutz durch Technik I

Datenschutz- und Sicherheitsmanagement, BSI-Grundschutz

Dr. Thomas Probst
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel
thomas.probst@datenschutzzentrum.de

Begriffe

Informationssicherheit = ?

Datenschutz = ?

Begriffe

Informationssicherheit ≈ Datensicherheit;

Teilgebiete:

- IT-Sicherheit
- Sicherheit von nicht-elektronischen Informationen

Die Informationssicherheit schützt Informationen (und zur deren Verarbeitung eingesetzter Infrastrukturen und Systeme) der Organisation.

Begriffe

Datenschutz

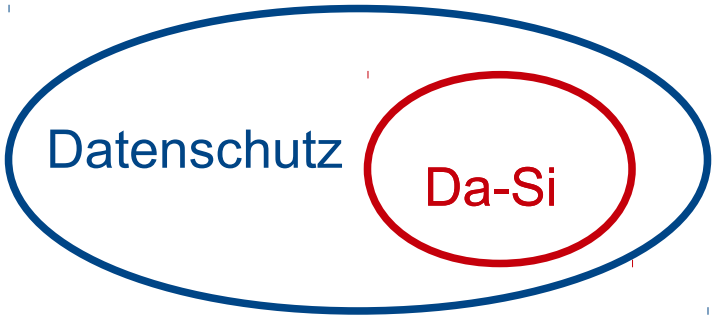
- Datenschutz schützt das Recht Betroffener (Bürger, Kunden, Mitarbeiter) auf informationelle Selbstbestimmung (Grundrechtsschutz)
- [in alten Publikationen wird manchmal „Datenschutz“ anstelle von „Informationssicherheit“ verwendet]

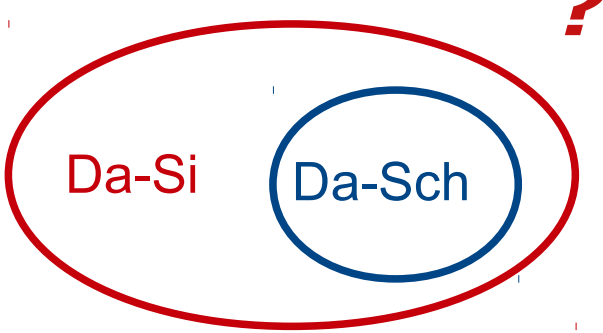
Datenschutz und Datensicherheit

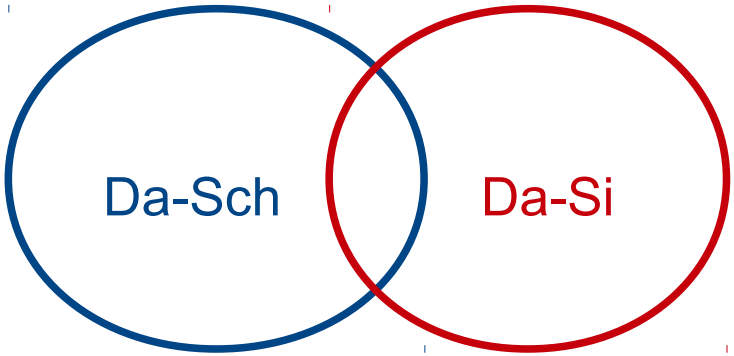
- Datenschutz:
  Schutz der Menschen vor Missbrauch ihrer personenbezogenen Daten

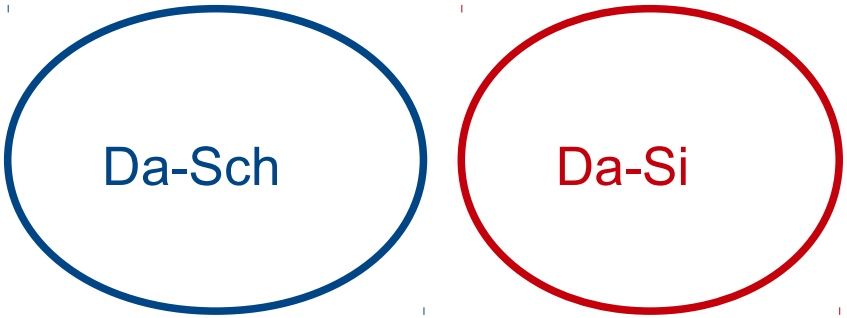
- Informationssicherheit/Datensicherheit:
  Schutz der Informationen/Daten(-verarbeitung) vor unberechtigten Zugriffen und vor Zerstörung

Verhältnis Datenschutz – Datensicherheit ?

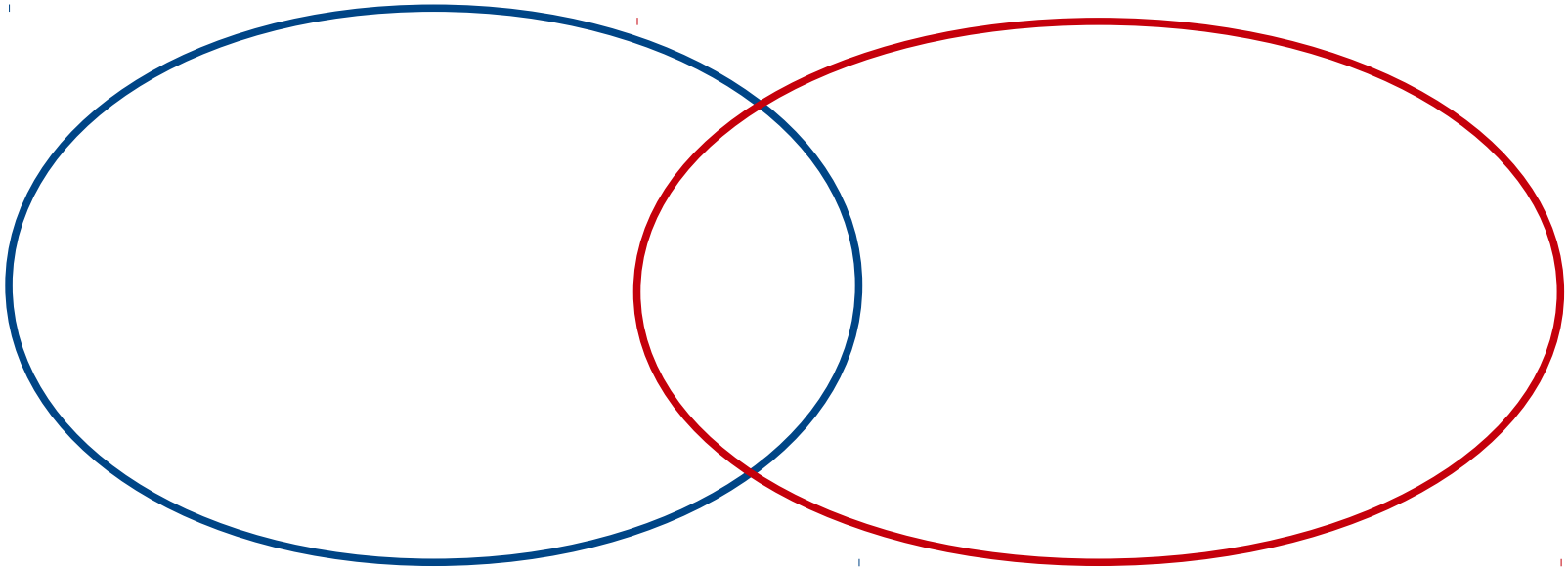








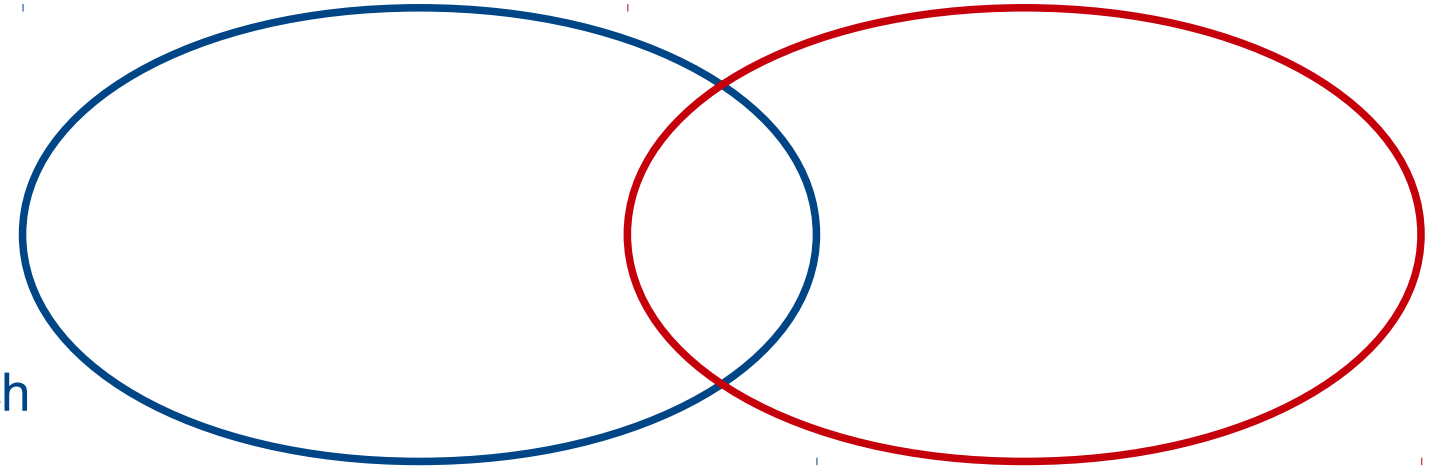
Verhältnis Datenschutz – Datensicherheit ?



Da-Sch

Da-Si

Verhältnis Datenschutz – Datensicherheit ?



- Rechtsvorschriften zur Zulässigkeit der DV
- Meldepflichten
- Auskunftspflichten

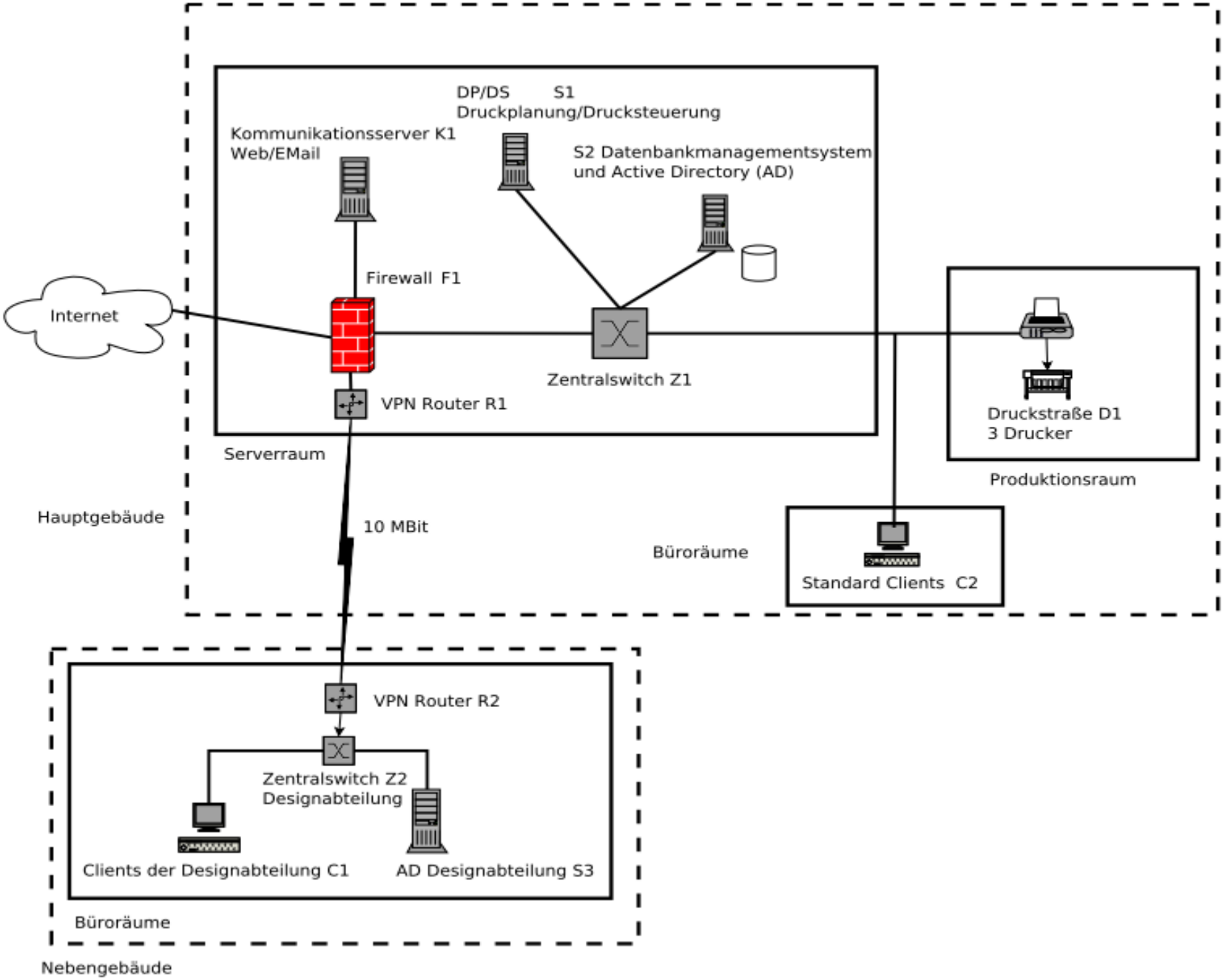
- Sicherheit personenbezogener Daten
- Protokollierungs-pflichten

- Sicherheit nicht-personenbezogener Daten (z. B. Betriebs-/Geschäftsgeheimnisse)
- häufig:Verfügbarkeit

Technisch-organsiatorische Maßnahmen

- Begriff des Bundesdatenschutzgesetzes/der DSGVO
- Maßnahmen, um die Ziele des Gesetzes zu erreichen
- Abwehrmaßnahmen („X soll nicht passieren“)
- Positive Maßnahmen („Y soll passieren“)

- Risikobegriff


DP/DS S1
Druckplanung/Drucksteuerung
Kommunikationsserver K1
Web/EMail
S2 Datenbankmanagementsystem
und Active Directory (AD)
Firewall F1
Internet
Zentralswitch Z1
VPN Router R1
Serverraum
Druckstraße D1
3 Drucker
Produktionsraum
Hauptgebäude
10 MBit
Büroräume
Standard Clients C2
VPN Router R2
Zentralswitch Z2
Designabteilung
Clients der Designabteilung C1
AD Designabteilung S3
Büroräume
Nebengebäude

Aufgabe

Legen Sie geeignete Sicherheitsmaßnahmen fest.

Sicherheitsmanagement

Management is that for which there is no algorithm. Where there is an algorithm, it's administration.

- Roger Needham -

Zwei Fragestellungen:

- Welche Risiken/Bedrohungen sollen angegangen werden?
- Wie können sie angegangen werden?

Antwort:

- Risikomanagement
- **T**echnische und **O**rganisatorische (Sicherheits-)**M**aßnahmen (**TOM**)

} Sicherheitsmanagement

ISO 27000:2018, Terms and Definitions:

3.61 risk: effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: **Uncertainty** is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Achtung: Beim Datenschutz geht es natürliche Personen

Risikomanagement

ISO 27000:2018, Terms and Definitions:

3.69 Risk Management:

coordinated activities to direct and control an organization with regard to risk ([SOURCE: ISO Guide 73:2009, 2.1])

3.70 Risk management process

systematic application of management policies (3.53), procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, **treating**, monitoring and reviewing risk (3.61)

Risikobewertung

Grundlegende Fragen des Risikomanagements:

1. Was kann passieren? (threat event)
2. Wenn es passiert: Wie schlimm kann es werden (threat impact)?
3. Wie häufig kann es passieren? (threat frequency, annualized)?
4. Wie verlässlich sind die Antworten auf diese Fragen? (recognition of uncertainty)

Risikoanalyse IT-Sicherheit

Bedrohungsanalyse (Threat Analysis):

Komplette Liste aller Bedrohungen, die technische und organisatorische Schwachstellen (auch Nutzer!) „ausnutzen“

Risikoanalyse (Risk Analysis):

Bewertung der Bedrohungen

- Wahrscheinlichkeit eines Ausfalls oder eines erfolgreichen Angriffs (wie schwierig? wie aufwändig? durch wen?)
- Größe des Schadens durch Ausfall/Angriff

Risikoanalyse für Datenschutz-Risiken

Bedrohungsanalyse (Threat Analysis):

Liste aller Bedrohungen für die Rechte und Freiheiten der Betroffenen (u.a. immaterielle Schäden, materielle Schäden, Diskriminierung, Einschüchterung)

Risikoanalyse (Risk Analysis):

Bewertung der Bedrohungen

- Wahrscheinlichkeit einer Beeinträchtigung von Rechten und Freiheiten oder eines daraus resultierenden Schadens
- Größe der Beeinträchtigung oder des Schadens

Umgang mit bewerteten Risiken (Treatment)

- Risiko **aus dem Weg gehen** (avoid)
- Risiko **eingehen** (accept)
- Etwas tun, um die Risiken auf ein akzeptables Maß zu **reduzieren** (risk mitigation or risk reduction)
- Risiko**verlagerung** (z. B. Versicherung) (transfer)

Aspekte für Entscheidung:

- Kosten-Nutzen-Analyse
- Vorschriften/Verträge/Policies

Risikoanalyse: Impact Rating

Methode 1: Quantitativer Ansatz

Loss type	Amount	Incidence	ALE
SWIFT fraud	$50,000,000	.005	$250,000
ATM fraud (large)	$250,000	.2	$100,000
ATM fraud (small)	$20,000	.5	$10,000
Teller takes cash	$3,240	200	$648,000

Figure 22.5 Example of Annual Loss Expectancies.**(=ALE).**

Quelle: Anderson, Ross: Security Engineering, Chapter 22, 1st Edition, 2001, Wiley.

Risikoanalyse: Impact Rating

Methode 1: Quantitativer Ansatz

Loss type	Amount	Incidence	ALE
SWIFT fraud	$50,000,000	.005	$250,000
ATM fraud (large)	$250,000	.2	$100,000
ATM fraud (small)	$20,000	.5	$10,000
Teller takes cash	$3,240	200	$648,000

Figure 22.5 Example of Annual Loss Expectancies.**(=ALE).**

Quelle: Anderson, Ross: Security Engineering, Chapter 22, 1st Edition, 2001, Wiley.

Risikoanalyse: Impact Rating

Methode 2: Qualitativer Ansatz

- Kategorisierung, z. B. „normal", „hoch", „sehr hoch"

Zuordnung:

- Beschreibung von Schadensszenarien für die Analyse der Auswirkungen

Pro & Cons

- ??

Pro & Cons

- Häufig nur Schätzwerte verfügbar.
- Gute Methode zur Priorisierung, wenn statistische Daten verfügbar (Bsp.: Festplattenausfall bei Google, Betrug durch Schaltermitarbeiter).
- Kann nur finanzielle Auswirkungen betrachten. Andere Auswirkungen müssen übersetzt werden. Was kostet ein Menschenleben? Wie bewertet man den Verlust des Wahlrechts?
- Gefahr: Katastrophale Auswirkungen könnten unterschätzt werden (wegen zu geringer Eintrittswahrscheinlichkeit; Bsp.: AKW)
- Lösung: Zusatzkriterien
  (z.B. „Keine Schadenshöhe über 1 Mio €")

Schadensszenarien

Mögliche Schadenskategorien (Beispiel aus BSI 200-2):

- Verstoß gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts („Datenschutzrecht")
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- negative Innen- und Außenwirkung
- finanzielle Auswirkungen

Häufig: ein Schaden, mehrere Schadenskategorien

Beispiele?

Beispiele

Details nicht klausurrelevant

Schutzbedarfskategorie "normal"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen

Schutzbedarfskategorie "hoch"	
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.

(aus BSI 200-2, V 1.0, 2017)

Beispiele

Details nicht klausurrelevant

Schutzbedarfskategorie "sehr hoch"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.

Dies sind Beispiele; sie sind individuell an die Situation vor Ort anzupassen!(z. B.: Was ist „ruinös”? 10 k€? 10 Mio €?)

(aus BSI 200-2, V 1.0, 2017)

Schadenssichten

- Organisationssicht (Schwerpunkt der IT-Sicherheit)
- Betroffenensicht (Schwerpunkt des Datenschutzes)

Sicherheitsmanagement

Management is that for which there is no algorithm. Where there is an algorithm, it's administration.

- **Roger Needham**

Zwei Fragestellungen:

- Welche Risiken/Bedrohungen sollen angegangen werden?
- Wie können sie angegangen werden? (Was ist zu tun? Wie ist es zu organisieren?)

Antwort:

- Risikomanagement
- **T**echnische und **O**rganisatorische (Sicherheits-)**M**aßnahmen (**TOM**)

IT (Sicherheits-) Standards

- Brainstorming: Welche kennen Sie?

IT (Sicherheits-) Standards

- COBIT
- ITIL®
- ISO 27001
- ISO 27002/17799
- BSI Standards/IT-Grundschutz
- Common Criteria (ISO 15408)
- FIPS-140

COBIT

- "Control Objectives for Information and related Technology"
- Best practices (framework) for IT management
- entwickelt von *Information Systems Audit and Control Association* (ISACA) und *IT Governance Institute* (ITGI)
- derzeit Version 5 (Mai 2012)
- 7 „Enabler" (=Ressorcen-Typen: Prozesse, Policies, Organisation, Personal ...)
- 37 Haupt-Prozesse in 5 Prozess-Domänen (Monitoring, Planung, Delivery...)
- nicht spezifisch IT-Sicherheitsmanagement
- aber: zahlreiche Überschneidungen

Literatur: https://www.isaca.org/COBIT/Documents/COBIT5-Introduction.ppt

Literatur: https://www.isaca.org/COBIT/Documents/COBIT5-and-InfoSec.ppt

Details nicht klausurrelevant

ITIL®

- IT Infrastructure Library®
- „Good Practice" für Service Management
- Ziel: bestmöglicher Support von Geschäftsprozessen durch IT
- Autor: Office of Government Commerce (OGC)
  - 1989 first development of manuals for processes
  - 1992 – 1998 ITILv1
  - seit 2000 ITILv2
  - Mai 2007 ITILv3
  - 2011: ITIL Edition 2011
- Zahlreiche Verbindungen zwischen ITILv3 und ISO20000
- Verbindungen von ITIL-Prozessen und IT-Sicherheitsprozessen (z. B. Change Mgt, Incident Mgt.)
- ITIL® - "ITIL® is a Registered Trade Mark of AXELOS Limited."

Details nicht klausurrelevant

IT (Security) Standards

- COBIT
- ITIL®
- ISO 27001 und ISO 27002/17799
- BSI Standards und IT-Grundschutz
- Common Criteria (ISO 15408)
- FIPS-140

ISO 27001:2018

- Prozess-basierter Ansatz für IT Sicherheit
- Konsequenz: Man braucht ein Management-System: ISMS (Information Security Management System)
- Anlehnung an QS-Systeme (ISO 9000-Serie)
- Ziel: „establishing, implementing, maintaining and continually improving an ISMS within the context of the organization“
- enthält auch Dokumentationsanforderungen für das ISMS

Vorgehensweise

- Risikoanalyse
- Risikobehandlung festlegen (u.a. Sicherheitsmaßnahmen, „controls“)
- Vollständigkeitscheck
- Sicherheitskonzept (Umsetzungsplan) erstellen
- o.k. des Managements einholen (einschließlich Restrisikoübernahme)

Controls/Sicherheitsmaßnahmen I

5 Sicherheitsleitlinien

6 Organisation der Informationssicherheit

7 Personalsicherheit

8 Management von organisationseigenen Werten

9 Zugriffskontrolle

10 Kryptographie

11 Schutz vor physikalischem Zugang und Umwelteinflüssen

Details nicht klausurrelevant

Controls/Sicherheitsmaßnahmen II

12 Betriebssicherheit

13 Sicherheit in der Kommunikation

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

15 Lieferantenbeziehungen

16 Management von Sicherheitsvorfällen

17 Betriebskontinuität

18 Richtlinienkonformität

Details nicht klausurrelevant

„Control objectives" und „Controls"

aus ISO 27000:2018:

3.14 control: **Maßnahme**

measure that is modifying risk (3.61)

Note 1 to entry: Controls include any process (3.54), policy (3.53), device, practice, or other actions which modify risk (3.61).

3.15 control objective **Zielsetzung**

statement describing what is to be achieved as a result of implementing controls (3.14)

Beispiele für „Control objectives" und „Controls"

Zielsetzung: Sicherstellung, dass Mitarbeiter und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Positionen geeignet sind.

Maßnahme:

Der Hintergrund von ... Bewerbern sollte im Einvernehmen mit einschlägigen Gesetzen, Verordnungen und ethischen Grundsätzen geprüft werden. Prüfungen sollten in einem angemessenen Verhältnis .... zum vermeintlichen Risiko stehen.

Details nicht klausurrelevant

Unterschied zwischen ISO 27001 und 27002

- ISO/IEC 27001: Standard
  - „normative Anforderungen" an ein ISMS
- ISO/IEC 27002: „Collection of Good Practice"
  - „Code of practice" und „implementation guidance" for selecting and implementing controls
  - keine „normativen Anforderungen"

Folge:

Zertifizierung nur „gegen" ISO/IEC 27001, aber nicht gegen ISO/IEC27002 möglich

Geschichte

Details nicht klausurrelevant

- Original: British Standard BS 7799-2
- Erste Version: 1999
- 2005 wurde BS 7799-2 zu ISO/IEC 27001:2005

- BS 7799-1: Code of Practice (Collection of Best-Practices)
- Erste Version: 1995
- Internationaler Standard ISO/IEC 17799:2005
- Umbenannt zu ISO/IEC 27002:2005 in 2007

- Neufassung 2013: ISO/IEC 27001/2:2013 (dt: 2015)
- Familie 27xxx: ISO/IEC-Standards für IT Sicherheit

Zusammenhang CobiT, ITIL, ISO 27001?

- Verschiedene Perspektiven:
  - „business perspective on IT"
  - „IT perspective on IT"
  - „IT Security perspective on IT"
- verschiedene Granularität
- starke Interaktionen einzelner Maßnahmen , Prozesse und Controls
- „Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit", http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Aligning-COBIT-4-1-ITIL-V3-and-ISO-IEC-27002-for-BusinessBenefit.aspx

IT (Security) Standards

- COBIT
- ITIL®
- ISO 27001 und ISO 27002/17799
- BSI Standards und IT-Grundschutz
- Common Criteria (ISO 15408)
- FIPS-140

Die IT-Grundschutzkataloge des BSI

- IT-Sicherheitsmaßnahmen für den öffentlichen und nicht-öffentlichen Bereich
- Umsetzung von ISO 27001 (aber detaillierter)
- Konzept für die Organisation von IT-Sicherheit (IT-Sicherheitsprozess) und konkrete Maßnahmen zur Reduktion von Gefährdungen
- Modellierung der IT-Struktur mit ca. 80 Bausteinen
- teilweise Risikoanalyse durch „Pauschalisierung" ersetzt und Vorauswahl von Maßnahmen getroffen
- pro Baustein:
  - Gefährdungslagen
  - Anforderungen (Basis, Standard, erhöhter Schutzbedarf)
  - Umsetzungshinweise

- BSI 200-1. Abb. 1.:

BSI-Standards zur Informationssicherheit

Informationssicherheit und IT-Grundschutz

BSI-Standard 200-1
Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-2
IT-Grundschutz-Methodik

BSI-Standard 200-3
Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 100-4
Notfallmanagement

IT-Grundschutz-Kompendium

Kapitel 1	Vorspann
Kapitel 2	Schichtenmodell und Modellierung

Elementare Gefährdungen

Schichten

Prozess-Bausteine:
- ISMS (Sicherheitsmanagement)
- ORP (Organisation & Personal)
- CON (Konzepte & Vorgehensweise)
- OPS (Betrieb)
- DER (Detektion & Reaktion)

System-Bausteine:
- IND (Industrielle IT)
- APP (Anwendungen)
- SYS (IT-Systeme)
- NET (Netzte & Kommunikation)
- INF (Infrastruktur)

Abbildung 1: Übersicht über BSI-Publikationen zum Sicherheitsmanagement

IT-Grundschutz

- Konkretisierung des Standards ISO 27001 durch BSI-Standards
  BSI 200-1 „Managementsysteme für Informationssicherheit”,
  BSI 200-2 „IT-Grundschutz-Vorgehensweise” und
  BSI 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz”
- Konkretisierung der Maßnahmen (ISO 27001 Anhang A, ISO 27002) durch IT-Grundschutz-Kataloge
- BSI 100-4 „Notfallvorsorge”

Gliederung der Aufgaben

Aspekte:

1) Organisation der IT-Sicherheitsaufgaben, Etablierung von Prozessen und Strukturen
2) Analyse der IT-Landschaft
3) Risikoanalyse
4) Maßnahmenauswahl
5) Priorisierung, Maßnahmenumsetzung
6) Überprüfung

Bei ISMS steht das *Management* im Vordergrund.

Beim IT-Grundschutz stehen auch die *Maßnahmen* und ihre Auswahl im Vordergrund.

IT-Sicherheitsprozess

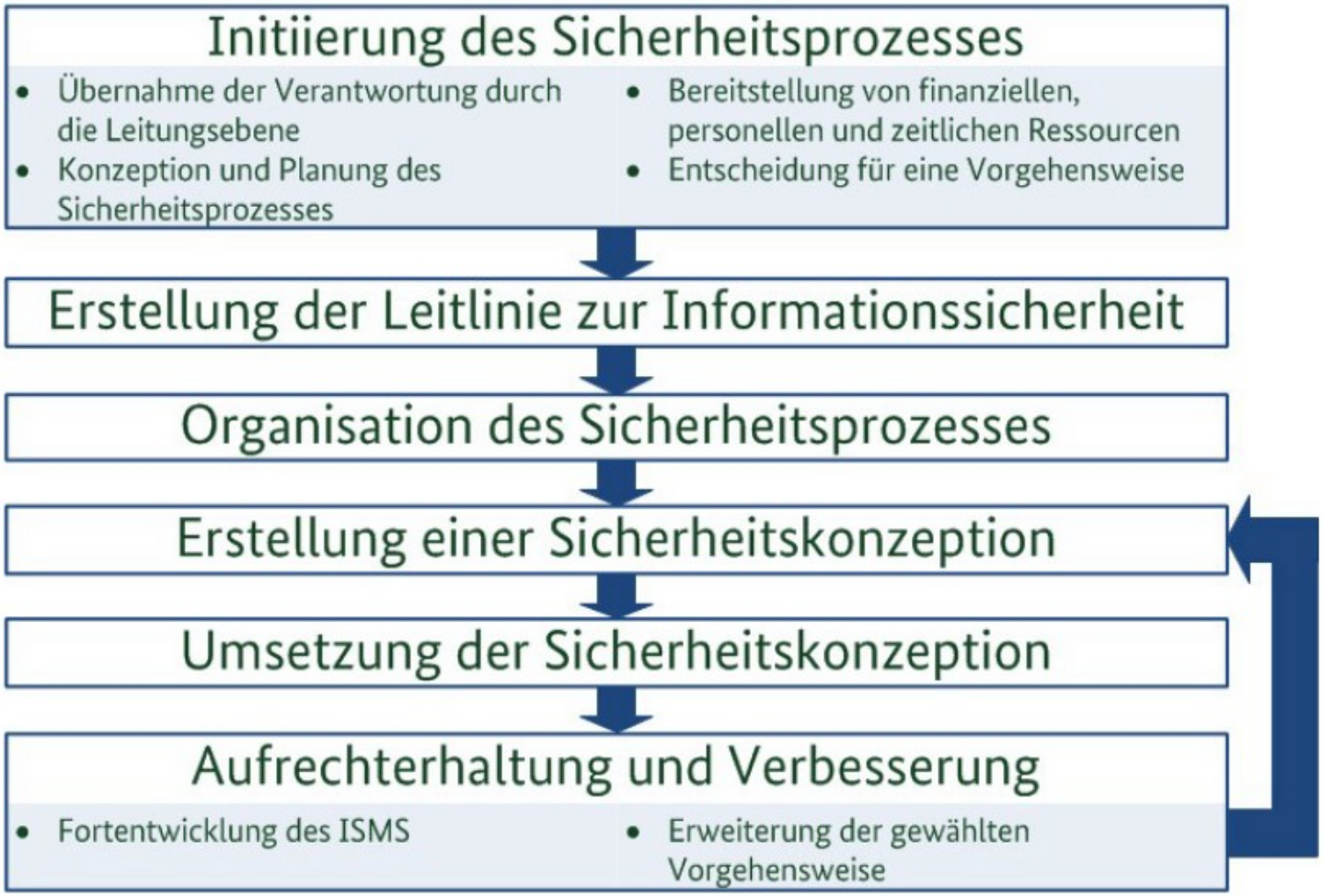
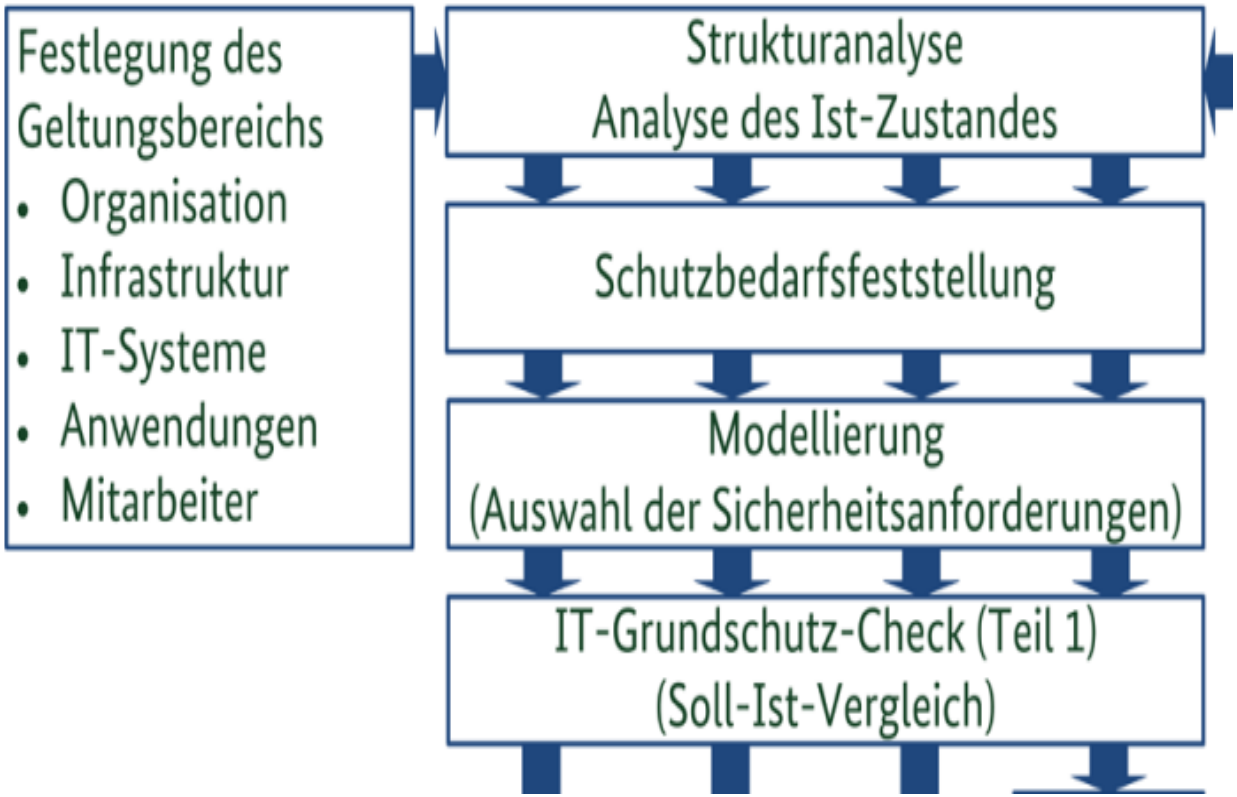


Abbildung 1: Phasen des Sicherheitsprozesses

Quelle: Abb. 1
BSI 200-2, V 1.0, 2017

Erstellen einer Sicherheitskonzeption



Was haben wir hier?

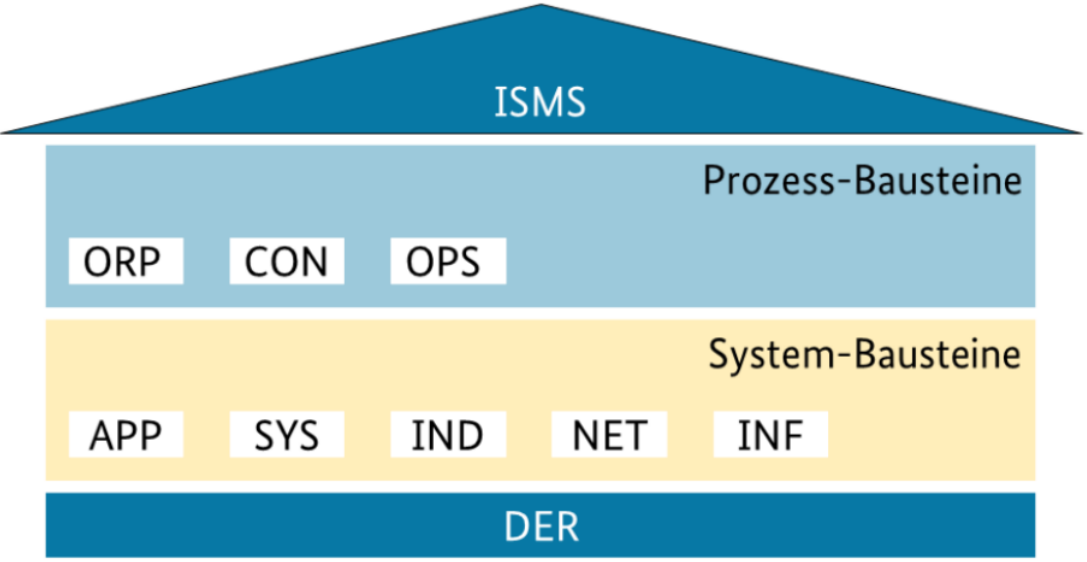
Wieviel Sicherheit brauchen wir?

Maßnahmenwahl (Soll)

Check: Umgesetzt? (Soll = Ist?)

Quelle: aus Abb.11, BSI 200-2, V 1.0, 2017

Schichtenmodell



Das Schichtenmodell des IT-Grundschutzes

- Prozess-Bausteine
  - ISMS (implementierte Anforderungen)
  - ORP (Organisation und Personal)
  - CON (Konzepte und Vorgehensweisen)
  - OPS (Betrieb)
  - DER (Detektion & Reaktion)
- System-Bausteine
  - APP (Anwendungen)
  - SYS (IT-Systeme)
  - IND (Industrielle IT)
  - NET (Netze und Kommunikation)
  - INF (Infrastruktur)

Quelle: IT-Grundschutzkompendium, Okt. 2017, Abschnitte 1.3 und 2.1

Details nicht klausurrelevant

Modellierung des IT-Verbundes mit „Bausteinen“

- Ziel: Herleitung von geeigneten Sicherheitsmaßnahmen
- diese ergeben sich aufgrund spezifischer Gefährdungen
- diese Gefährdungen sind für bestimmte Bausteine relevant

Vorgehen:

- Bausteinauswahl
- Gefährdungsanalyse
- Anforderungsbestimmung und Maßnahmenhinweise

Hilfe bei der Maßnahmenauswahl

Leistung der Grundschutzkataloge:

Zu einzelnen Bausteinen wurden spezifische Gefährdungen ermittelt und die relevanten Anforderungen beschrieben.

Sind die richtigen und relevanten Bausteine ausgewählt, ergeben sich die relevanten Anforderungen „automatisch". Die Umsetzungshinweise unterstützen bei der Umsetzung der Anforderungen.

Anforderungen

Maßnahmen sind als „Anforderungen“ formuliert:

SYS.3.1.A5 Datensicherung [Benutzer]

Alle Daten, die auf Laptops lokal gespeichert werden, MÜSSEN regelmäßig gesichert werden. Hierfür MÜSSEN abhängig vom Volumen des Datenbestands geeignete Verfahren zur Datensicherung ausgewählt werden. Die Datensicherung MUSS weitgehend automatisiert werden, sodass die Benutzer möglichst wenig Aktionen selbst durchführen müssen.

Drei Gruppen von Anforderungen:

Basis => MÜSSEN

Standard => SOLLTEN

erhöhter Schutzbedarf =>SOLLTEN

Details nicht klausurrelevant

Modellierung

Bausteinauswahl (Auszug)
ISMS.1 Sicherheitsmanagement
OPS.1.1.2 Ordnungsgemäße IT-Administration

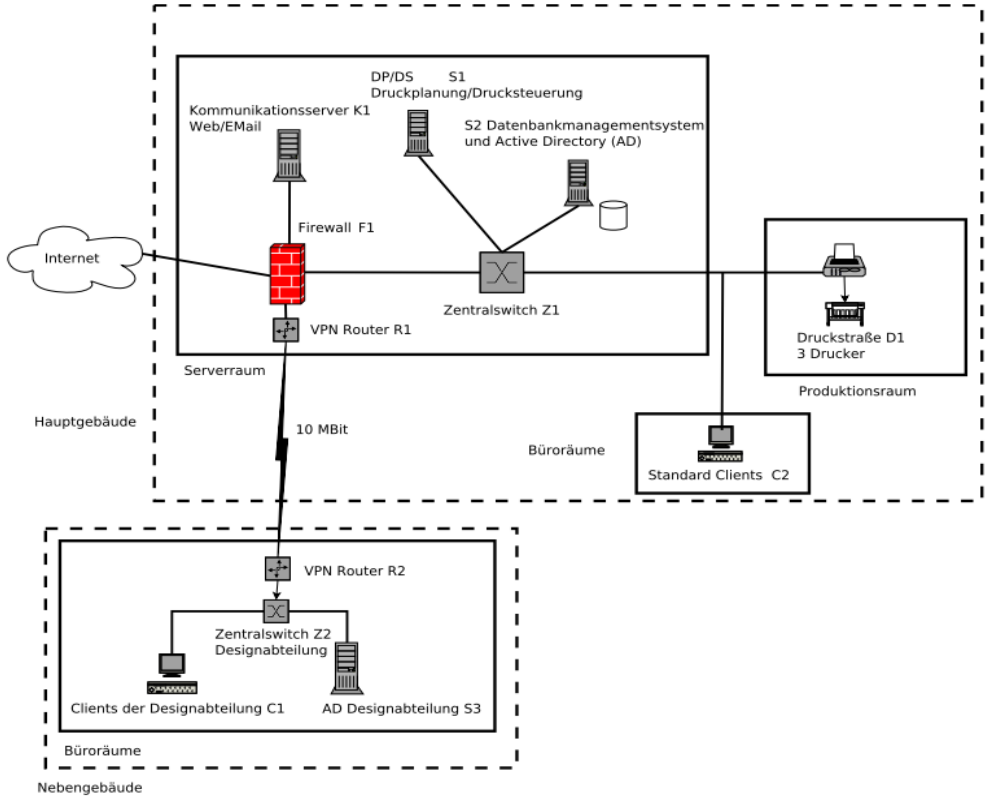
INF.1 Allgemeines Gebäude
INF.2 Rechenzentrum sowie Serverraum
INF.3 Elektrotechnische Verkabelung
INF.4 IT-Verkabelung
INF.7 Büroarbeitsplatz

SYS.1.1 Allgemeiner Server
SYS.1.2.2 Windows Server 2012
SYS.2.1 Allgemeiner Client
SYS.2.2.3 Clients unter Windows 10
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

IND.1 Betriebs- und Steuerungstechnik

NET.3.1 Router und Switches
NET.3.2 Firewall
NET.3.3 VPN

APP.3.1 Webanwendungen
APP.3.2 Webserver
APP.3.3 Fileserver
APP.4.3 Relationale Datenbanksysteme
APP.5.1 Allgemeine Groupware



Details nicht klausurrelevant

Beispiel: SYS.3.1 Laptops spezifische Gefährdungen

2.1 Beeinträchtigung durch wechselnde Einsatzumgebung
2.2 Diebstahl
2.3 Ungeordneter Benutzerwechsel bei Laptops
2.4 Fehler bei der Synchronisation
2.5 Datenverlust bei mobilem Einsatz
2.6 Datendiebstahl mithilfe von Laptops

Beispiel: SYS.3.1 Laptops
Auszug aus den Anforderungen

Basis:

SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops

SYS.3.1.A5 Datensicherung

Standard:

SYS.3.1.A8 Sicherer Anschluss von Laptops an Datennetze

SYS.3.1.A13 Verschlüsselung von Laptops

erhöhte Sicherheit:

SYS.3.1.A17 Sammelaufbewahrung(A)

SYS.3.1.A18 Einsatz von Diebstahl-Sicherungen(CIA)

Details nicht klausurrelevant

Beispiel: SYS.3.1 Laptops
Auszug aus den Umsetzungshinweisen

Standard:

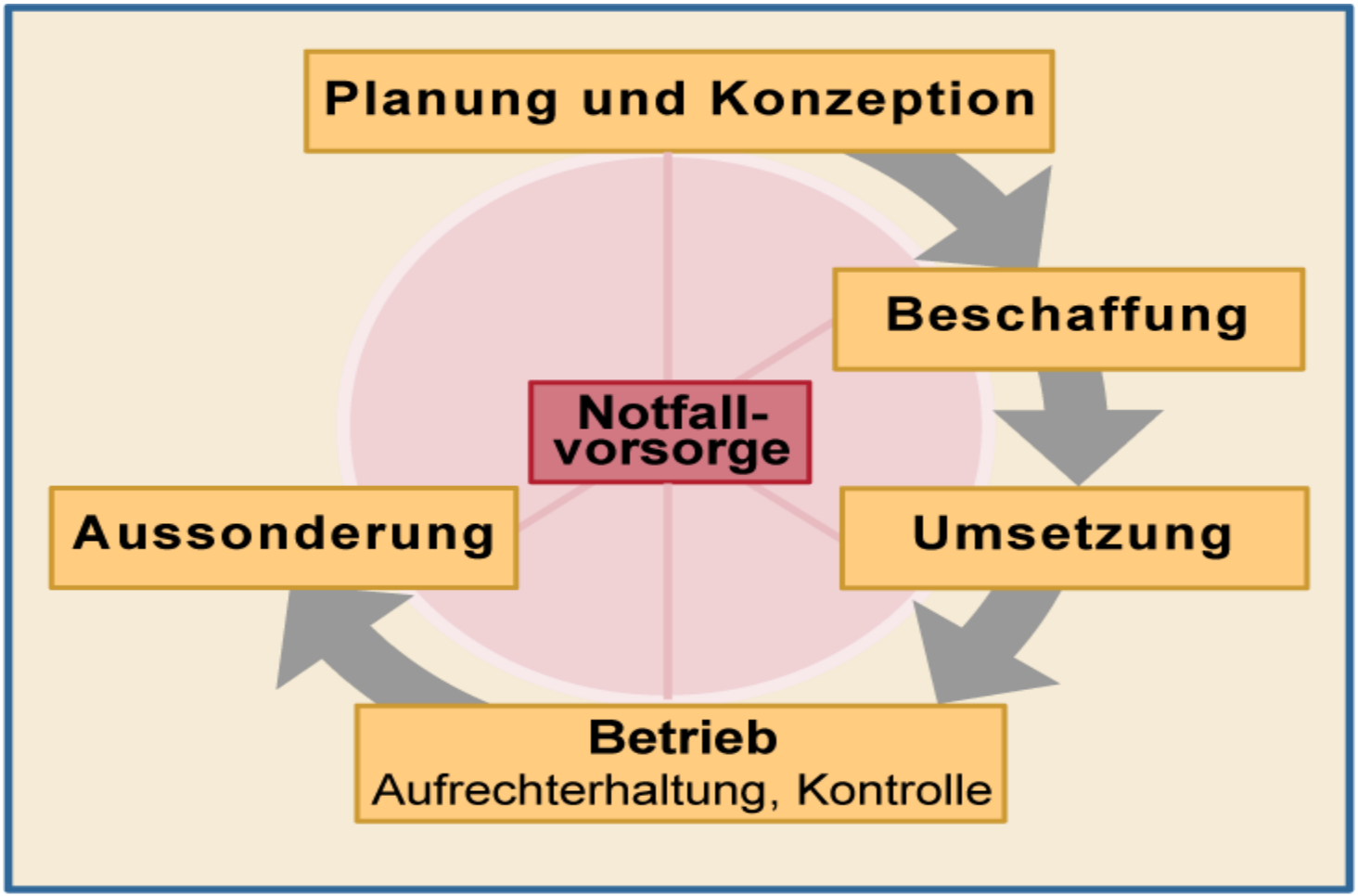
SYS.3.1.A13 Verschlüsselung von Laptops

Um zu verhindern, dass aus einem gestohlenen Laptop schutzbedürftige Daten ausgelesen werden können, sollte ein Verschlüsselungsprogramm eingesetzt werden. Mithilfe der marktgängigen Produkte ist es möglich, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so zu verschlüsseln, dass nur derjenige, der über den geheimen Schlüssel verfügt, die Daten lesen und bearbeiten kann.

Die Sicherheit der Verschlüsselung hängt dabei von drei verschiedenen Punkten zentral ab: . . .

Details nicht klausurrelevant

IT-Grundschutzkompendium
Lebenszyklus -Modell



IT (Security) Standards

- COBIT
- ITIL®
- ISO 27001 und ISO 27002/17799
- BSI Standards und IT-Grundschutz
- Standard-Datenschutzmodell
- Common Criteria (ISO 15408)
- FIPS-140

Standard-Datenschutzmodell

- „Mit dem SDM wird *eine* Methode bereitgestellt, mit dem die Risiken für das Recht auf informationelle Selbstbestimmung, die mit der Verarbeitung personenbezogener Daten zwangsläufig einhergehen, mit Hilfe von geeigneten technischen und organisatorischen Maßnahmen beseitigt oder wenigstens auf ein tragbares Maß reduziert werden können."
- weitergehender Risikobegriff als bei IT-Sicherheit
- spezifische Datenschutz-Maßnahmen (teilweise Überdeckung mit IT-Sicherheit, teilweise spezifisch wie Sperrung, Auskunftserteilung, Pseudonymisierung) in Arbeit
- https://www.datenschutzzentrum.de/sdm/

IT (Security) Standards

- COBIT
- ITIL®
- ISO 27001 und ISO 27002/17799
- BSI Standards und IT-Grundschutz
- Common Criteria (ISO 15408)
- FIPS-140

Common Criteria (ISO 15408)

- Internationaler IT-Sicherheitsstandard für die formale Spezifikation von IT-Sicherheits-Anforderungen und deren unabhängige Evaluation und Test
- Formelle Zertifizierung der Vertrauenswürdigkeit von Produkten
- 3-teiliger Standard, plus „evaluation methodology"
- International anerkannt (gegenseitige Anerkennung der Zertifizierung bis EAL 4)
- TOE: Target of Evaluation

Ansatz

Common Criteria

Security Problem Definition:

What's my security problem (e.g., protecting XYZ)?

Security Objectives:

Who (TOE? Environment?) is responsible to ensure what?

Security Requirements:

What security functions need the TOE to implement?

Security Specification:

How does the ToE implements the security functions?

Zahlreiche „Security functions" einschließlich Querverweisen und Prüfanweisungen in den CC spezifiziert

FIPS

- FIPS: Federal Information Processing Standards
- öffentliche US (Bundes-)Standards
- für alle nicht-militätrischen Regierungsstellen und ihre Vertragspartner
- Beispiele?
  - FIPS country codes and region codes (10-4)
  - FIPS Data Encryption Standard (46-3)
  - FIPS Advanced Encryption Standard (197)

FIPS 140

- Ziel: Koordination von Anforderungen und Standards von Kryptomodulen (Hardware und Software)
- Zertifizierung verfügbar
- FIPS 140-2: Aktuelle Version, seit Mai 2001
- Annexes:
  - Annex A: Approved Security Functions [2018]
  - Annex B: Approved Protection Profiles [2016]
  - Annex C: Approved Random Number Generators [2016]
  - Annex D: Approved Key Establishment Techniques [2017]

Details nicht klausurrelevant

Security Level 1	Security Level 2	Security Level 3	Security Level 4

- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Services, and Authentication
- Finite State Model
- Physical Security
- Operational Environment
- Cryptographic Key Management
- EMI/EMC
- Self-Tests
- Design Assurance
- Mitigation of Other Attacks

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Details nicht Klausurrelevant

Literatur/Links

Standards:

- CobiT: www.isaca.org
- COBIT® MAPPING: http://www.isaca.org/Knowledge-Center/Research/Pages/All-Deliverables.aspx
- CC: www.commoncriteriaportal.org
- BSI Standards/ IT Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- SDM: https://www.datenschutzzentrum.de/sdm/

Literatur:

Kersten, H., Klett, G., Reuter, J., Schröder, K.: IT-Sicherheitsmanagement nach der neuen ISO 27001. 2016, Springer-Vieweg-Verlag, ISBN 978-3-658-14694-8