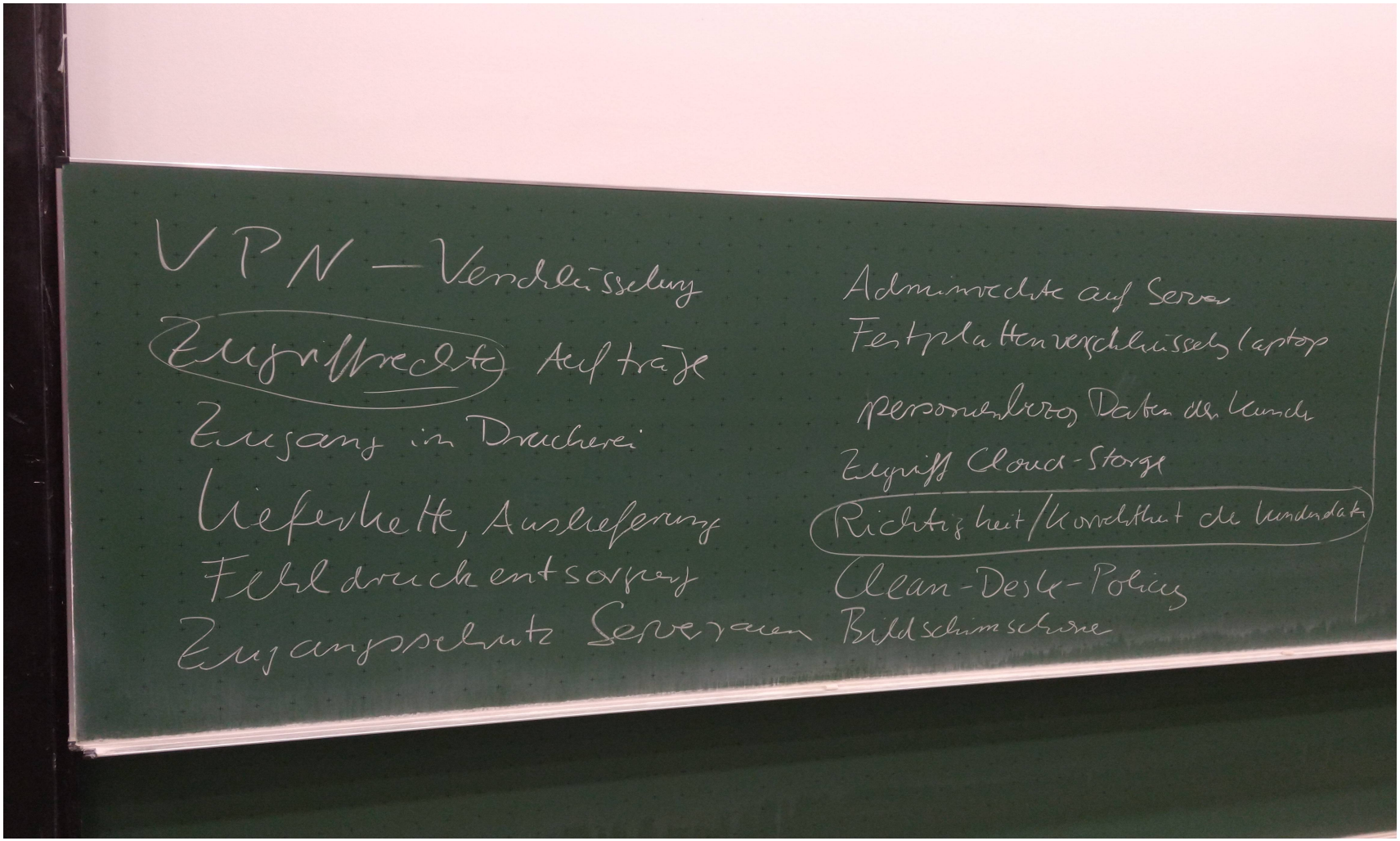
Vorlesung Datenschutz CAU SS 2025

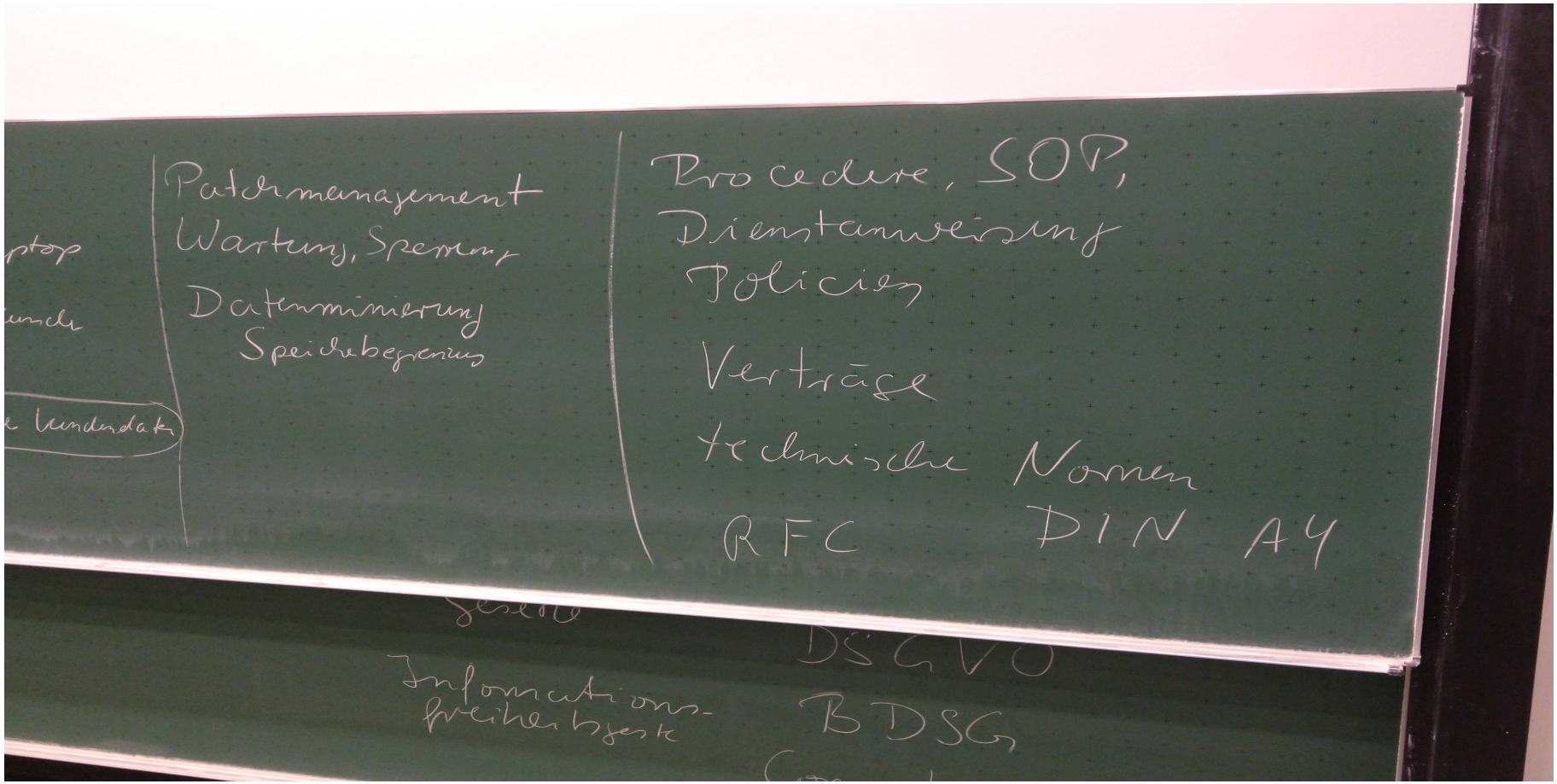
Datenschutz durch Technik I/II

Schutz- und Gewährleistungsziele Datenschutz- und Sicherheitsmanagement, BSI-Grundschutz

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

Hinweis: Diese Folien wurden von dem Dozenten für die Vorlesung erstellt und nicht mit dem ULD abschließend abgestimmt.


VPN – Verschlüsselung
Zugriffsrechte Aufträge
Zugang in Druckerei
Lieferkette, Auslieferung
Fehldruck entsorgen
Zugangsschutz Server
Adminrechte auf Server
Festplattenverschlüsselung Laptop
personenbezog. Daten der Kunden
Zugriff Cloud-Storage
Richtigkeit/Korrektheit der Kundendaten
Clean-Desk-Policy
Bildschirmschoner


Patchmanagement
Wartung, Sperren
Datenminimierung
Speicherbegrenzung
Procedere, SOP,
Dienstanweisung
Policies
Verträge
technische Normen
RFC
DIN A4
DSGVO
BDSG

Klassische Schutzziele (CIA)

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availability)

Heise 4.3.2017
https://heise.de/-3644268

XXXX sammelt über seine App Metadaten von Mobiltelefonen, um daran Polizisten und andere Beamte zu erkennen, die gegen illegale XXX-Dienste vorgehen könnten. In jenen Städten, in denen XXX-Chauffeure ohne Genehmigung tätig sind, werden die Ordnungshüter dann nicht von XXX befördert.

Zu den ausgewerteten Metadaten gehören unter anderem Bewegungsmuster, Kreditkartennummern und Handy-Seriennummern.

…. "[Das Greyball]-Programm lehnt Bestellungen von betrügerischen Nutzern ab, die unsere Geschäftsbedingungen verletzen", sagte ein Firmensprecher, "Ob das Personen sind, die unsere Fahrer körperlich attackieren wollen, oder Mitbewerber, die unseren Betrieb stören möchten, oder Gegner, die mit Beamten kollaborieren, um Fahrer in die Falle zu locken."

Bewertungsportal

„... hat eine vierstellige Geldbuße gegen einen Arzt verhängt. Der Patient einer Arztpraxis hatte sich über diese auf einem Bewertungsportal im Internet kritisch geäußert. Der Arzt reagierte darauf mit einem Gegenkommentar, wobei er personenbezogene Daten des Patienten - wie Diagnosen und Behandlungsergebnisse – veröffentlichte."

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-arzt-2023-12-31-DE-3753.php

Zweckentfremdung Grundbuch

Der Bußgeldempfänger hatte im Rahmen seiner beruflichen Befugnis Einsichtnahme in das elektronische Grundbuch im automatisierten Abrufverfahren genommen und in zwei Fällen mehrere Hundert Grundstückseigentümer ohne deren Kenntnis identifiziert und die entsprechenden Informationen an einen ebenfalls nicht namentlich genannten Bauunternehmer weitergegeben. Dieser hatte anschließend den Grundstückseigentümern Kaufangebote für ihre Grundstücke unterbreitet.

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-vermessungsingenieur-2022-09-21-DE-2286.php

https://www.baden-wuerttemberg.datenschutz.de/bussgeld-daten-aus-dem-grundbuch-stehen-nicht-zur-freien-verfuegung/

Krankheitstage im Betrieb

Der Personalbereich eines Unternehmen hatte bezüglich einer jährlichen Beurteilung eine Liste erstellt, in der Name und Krankheitstage von Beschäftigten vermerkt wurden. Diese Liste wurde per E-Mail an einen Verteiler mit **allen** höherrangigen Führungskräften geschickt. Letzteres verstoße gegen den Beschäftigtendatenschutz.

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-textilunternehmen-2023-06-15-DE-2972.php

fehlende Vereinbarung für gemeinsame Datenverantwortlichkeit, unrechtmäßige Datenverarbeitung, keine Löschung

Der … erließ eine Strafe gegen ein Immobilienunternehmen. Dieses hatte

- keine Vereinbarungen über gemeinsame Datenverantwortlichkeit getroffen und hatte zudem
- Daten erhoben und verarbeitet, ohne dass es dafür eine rechtliche Grundlage gab.
- Löschungsanfragen von drei Betroffenen wurde nicht rechtzeitig nachgekommen.

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-unternehmen-2024-06-06-DE-3847.php

Datenbankabruf

Der Polizeibedienstete war während einer krankheitsbedingten Dienstabwesenheit mehrfach in sein Büro gegangen und hatte über seinen Arbeits-PC personenbezogene Informationen von Familienmitgliedern und Freunden aus den Polizeiakten abgerufen, aber auch von sich selbst.
Vor Gericht behauptete er, in seiner Freizeit gegen eine Gruppe gewaltbereiter Fußballfans ermittelt zu haben, doch … das Gericht stuften dies als unglaubwürdig ein.

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-polizeimitarbeiter-2025-03-25-DE-4280.php

Datenschutzziele

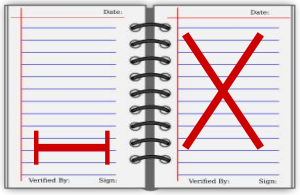
Sind diese Problemlagen durch die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität abgedeckt?

Formulierung weiterer Gewährleistungsziele

Datenminierung

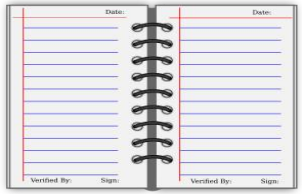
Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

- direkte Anforderung aus der DSGVO (Artikel 5)
- im Hinblick auf
  - Umfang,
  - Detaillierungsgrad,
  - Verarbeitungsdauer,
  - Speicherdauer,
  - Identifizierbarkeit



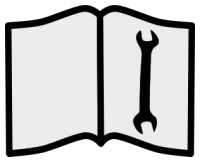
Transparenz

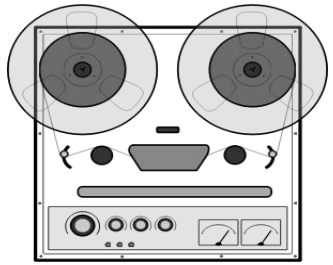
Die Datenverarbeitung ist für Betroffene nachvollziehbar und erfüllt prüfbar die datenschutzrechtlich bestehenden Anforderungen.



Sicherung von Transparenz:

- Dokumentation von Verfahren (Daten, IT-Systemen, technische Funktionen, organisatorischen Regelungen)
- (Teil-)Veröffentlichung gegenüber Betroffenen
- Protokollierung





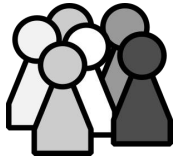
www.openclipart.org

Nicht-Verkettung

Keine Zusammenführung personenbezogener Daten, die für verschiedene Zwecke verarbeitet werden.

Sicherung von Nicht-Verkettung z.B. durch

- Festlegung der Verfahrenszwecke
- Rollenkonzepte für Lesen/Schreiben/Löschen
- Trennung von Verfahren durch Trennung der Daten-bestände, IT-Systeme und Prozesse



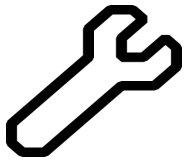
www.openclipart.org

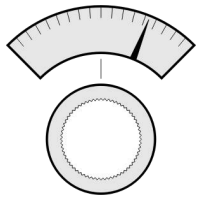
Intervenierbarkeit

Betroffenenrechte müssen umsetzt werden können.
=> Verarbeitungen müssen verändert werden können.

Sicherung von Intervenierbarkeit:

- Changemanagement für Störungen, Problembearbeitungen und Änderungen einer Organisation
- Single Point of Contact für Betroffene
- Ausnahmebehandlung





www.openclipart.org

Spezifische Datenschutzschutzziele:

keine „neuen“ Anforderungen, sondern

- Konkretisierung/Detaillierung von Anforderungen
- Formulierung als Gewährleistungsziele:

  „Baue die Datenverarbeitung so, dass die gesetzlichen Vorgaben erfüllt werden (können).“

Gegensätzliche Schutzziele

Schutzziele können im Widerspruch stehen

- Vertraulichkeit vs. Verfügbarkeit
- Transparenz vs. Nichtverkettung
- Integrität vs. Intervenierbarkeit

Diskussion:

- Blockchain
- Cloud-Backup

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

Details nicht klausurrelevant

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)

Details nicht klausurrelevant

Risikoanalyse für die 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)
- können auch durch regelhafte (=geplante) Datenverarbeitung entstehen

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: Quantitativer Ansatz

Methode 1: Quantitativer Ansatz

Loss type	Amount	Incidence/year	ALE
SWIFT fraud	$ 50.000.000	0.005	$ 250,000
ATM fraud (large)	$ 250.000	0,02	$ 100,000
ATM fraud (small)	$ 20.000	0.5	$ 10,000
Teller takes cash	$ 3,240	200	$ 648,000

(ALE = Annual loss expectancy).

Quelle: Anderson, Ross: Security Engineering, Chapter 27.1, 3rd Edition, 2020, Wiley; **https://www.cl.cam.ac.uk/~rja14/book.html**

Risikoanalyse: Quantitativer Ansatz

Methode 1: Quantitativer Ansatz

Loss type	Amount	Incidence/year	ALE
SWIFT fraud	$ 50.000.000	0.005	$ 250,000
ATM fraud (large)	$ 250.000	0,02	$ 100,000
ATM fraud (small)	$ 20.000	0.5	$ 10,000
Teller takes cash	$ 3,240	200	$ 648,000

(ALE = Annual loss expectancy).

Quelle: Anderson, Ross: Security Engineering, Chapter 27.1, 3rd Edition, 2020, Wiley; **https://www.cl.cam.ac.uk/~rja14/book.html**

Pro & Cons einer quantitativen Analyse

- Gute Methode zur Priorisierung, wenn statistische Daten verfügbar (Bsp.: Festplattenausfall eines Clouddienstleister, Betrug durch Bankbeschäftigte).
- Häufig nur Schätzwerte verfügbar.
- Kann nur finanzielle Auswirkungen betrachten. Andere Auswirkungen müssen monitarisiert 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 €")

Qualitative Risikoanalyse: Impact Rating

Methode 2: Qualitativer, szenarienbasierter Ansatz

- Kategorisierung, z. B. „normal", „hoch", „sehr hoch"
  - Schadenspotentialen und
  - Eintrittswahrscheinlichkeiten,

Zuordnung:

- Beschreibung von Schadensszenarien für die Analyse der Auswirkungen

Meist besser geeignet, weil „Zahlen" nicht zur Verfügung stehen

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
2. Beeinträchtigung des	Fehlverhalten ... Datenschutz

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

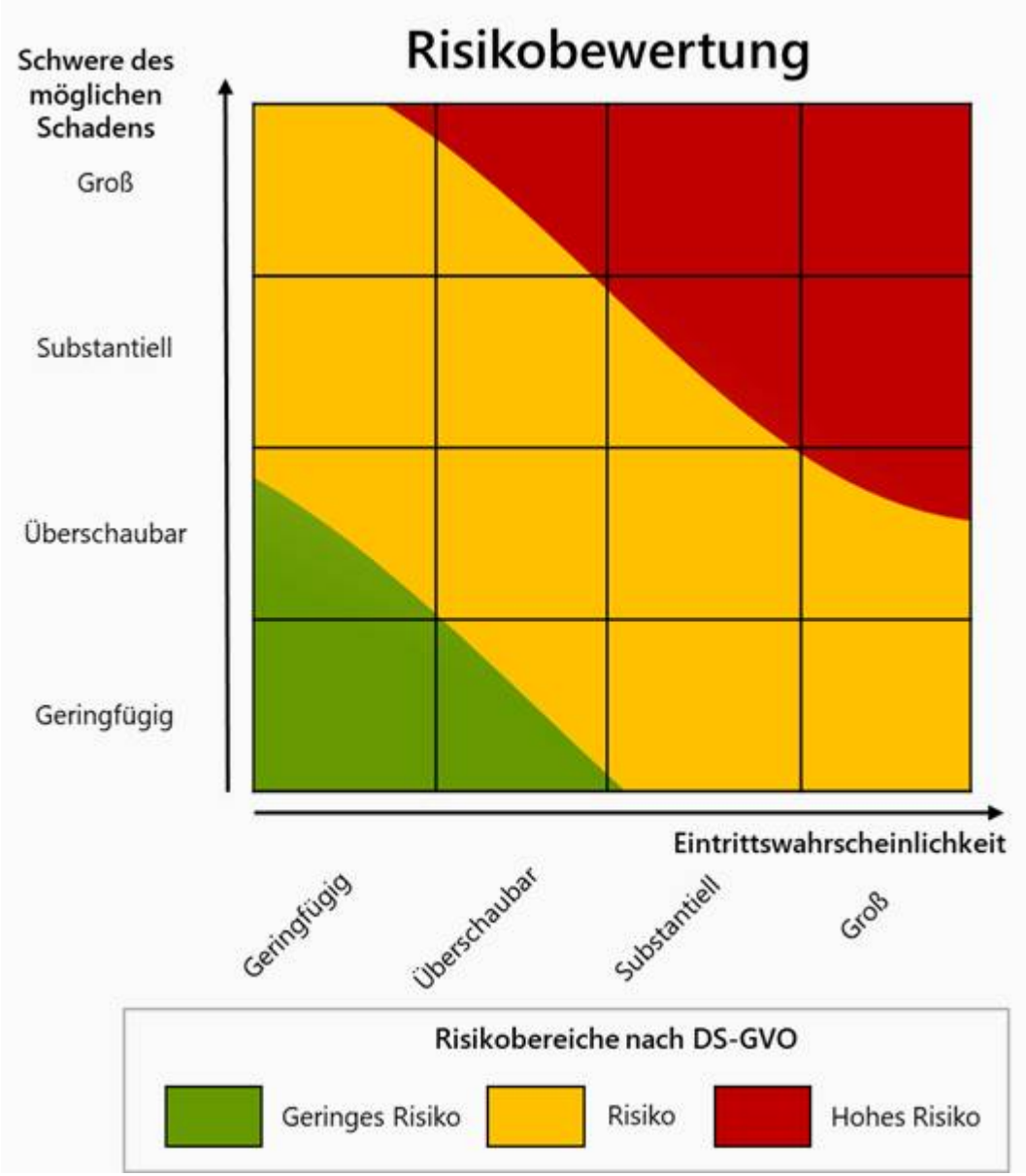
Schutzbedarfskategorie "sehr hoch"	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit 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)
- Angreifermodell:
  kann bei Datenschutzrisiken auch die Organisation sein



Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen

https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_18_Risiko.pdf

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®
- NIST Cybersecurity Framework
- ISO 27001 und ISO 27002
- BSI Standards und IT-Grundschutz
- *Standard-Datenschutzmodell*
- Common Criteria (ISO 15408)
- FIPS-140

COBIT

“Control Objectives for Information and related Technology“

- Fokus: IT-Management für Geschäftsprozesse anhand von „business objectives″
- kein spezifisches IT-Sicherheitsmanagement
- aber: zahlreiche Überschneidungen
- Guidelines „Implementing the NIST Cybersecurity Framework Using COBIT 2019″

Details nicht klausurrelevant

ITIL®

- IT Infrastructure Library® I - "ITIL® is a Registered Trade Mark of AXELOS Limited."
- „Good Practice" für Service Management
- Ziel: bestmöglicher Support von Geschäftsprozessen durch IT
- Autor: Office of Government Commerce (OGC)
  - 2019: ITIL 4
- Zahlreiche Verbindungen zwischen ITILv3 und ISO 20000
- Verbindungen von ITIL-Prozessen und IT-Sicherheitsprozessen (z. B. Change Mgt, Incident Mgt.)
- In ITIL 4: Übergang von Prozessen zu „Practices"
- **keine Zertifizierung**

Details nicht klausurrelevant

NIST Cybersecurity Framework

- freiwillige anzuwendendes Framework für „kritische Infrastrukturen″ und andere Bereiche
- derzeit: 2.0 (Stand 2/2024)
- 22 (abstrakte) Kernaktivitäten in 6 funktionalen Gruppen
- Verweise auf bestehende Standards und weitere Dokumente
- Bereitstellung von „Profilen″, die die Kernaktivitäten für bestimmte Problemlagen genauer fokussieren.
  Bsp:
  - CSF Profile for Ransomware Risk Management
  - Draft CSF Profile for Semiconductor Manufacturing
- https://www.nist.gov/cyberframework

Details nicht klausurrelevant

NIST Cybersecurity Framework

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Quelle:
NIST Cybersecurity Framework (CSF) 2.0, S. 15
https://doi.org/10.6028/NIST.CSWP.29

IT (Sicherheits-) Standards

- COBIT
- ITIL®
- NIST Cybersecurity Framework
- ISO 27001 und ISO 27002
- BSI Standards und IT-Grundschutz
- *Standard-Datenschutzmodell*
- Common Criteria (ISO 15408)
- FIPS-140

ISO 27001:2022

- „Information security, cybersecurity and privacy protection — Information security management systems — Requirements" (Stand 10/2022)
- 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 (Auszug)

5 Organizational controls (37 controls)
6 People controls (8 controls)
7 Physical controls (14 controls)
8 Technological controls (34 controls)

https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

Details nicht klausurrelevant

Controls/Sicherheitsmaßnahmen (Auszug)

….

7.4 Physical security monitoring

7.5 Protecting against physical and environmental threats

7.6 Working in secure areas

7.7 Clear desk and clear screen

7.8 Equipment siting and protection

7.9 Security of assets off-premises

7.10 Storage media

7.11 Supporting utilities

7.12 Cabling security

7.13 Equipment maintenance

7.14 Secure disposal or re-use of equipment

https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

Details nicht klausurrelevant

Controls/Sicherheitsmaßnahmen (Auszug)

8 Technological controls
8.1 User endpoint devices
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.6 Capacity management
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.13 Information backup
8.14 Redundancy of information processing facilities

Details nicht klausurrelevant

https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

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

IT (Sicherheits-) Standards

- COBIT
- ITIL®
- NIST Cybersecurity Framework
- ISO 27001 und ISO 27002
- BSI Standards und IT-Grundschutz
- *Standard-Datenschutzmodell*
- Common Criteria (ISO 15408)
- FIPS-140

Abstraktionsgrade

Anforderungen können unterschiedlich abstrakt formuliert werden:

- Sind die gesetzlichen Vorgaben eingehalten worden?
- Wird Verschlüsselung eingesetzt?
- Sind die Schlüssel für die verschlüsselte Dateiübertragung sicher verwaltet?
- Wird der AES Verschlüsselungsalgorithmus im CBC-Modus verwendet?

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. 110 Bausteinen
- teilweise Risikoanalyse durch „Pauschalisierung" ersetzt und Vorauswahl von Maßnahmen getroffen
- pro Baustein:
  - Gefährdungslagen
  - Anforderungen (Basis, Standard, erhöhter Schutzbedarf)
  - Umsetzungshinweise

Maßnah
men

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-Grundschutzkompendium (und Umsetzungshinweise)
- BSI 200-4 Business Continuity Management (3/2023)

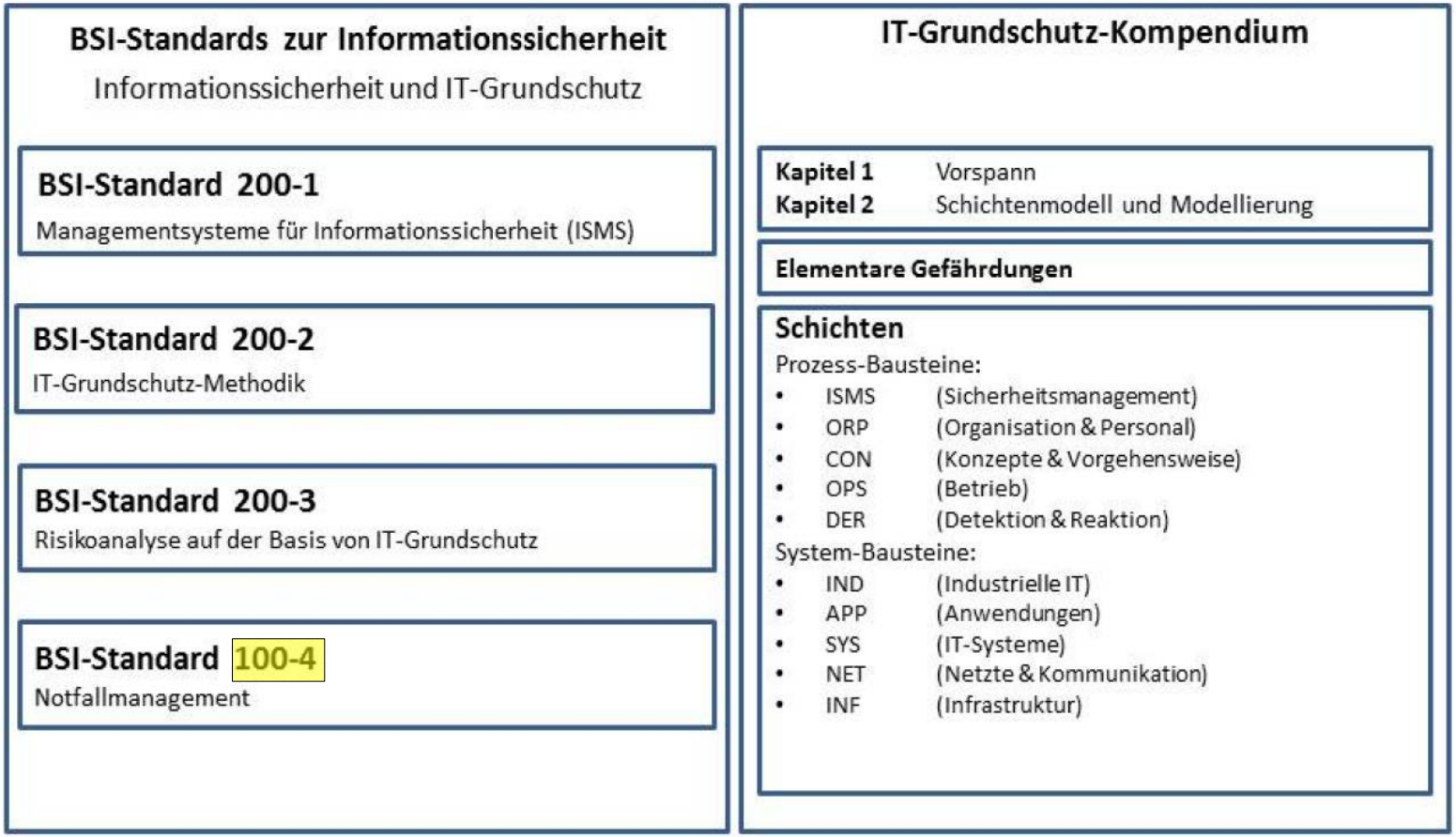


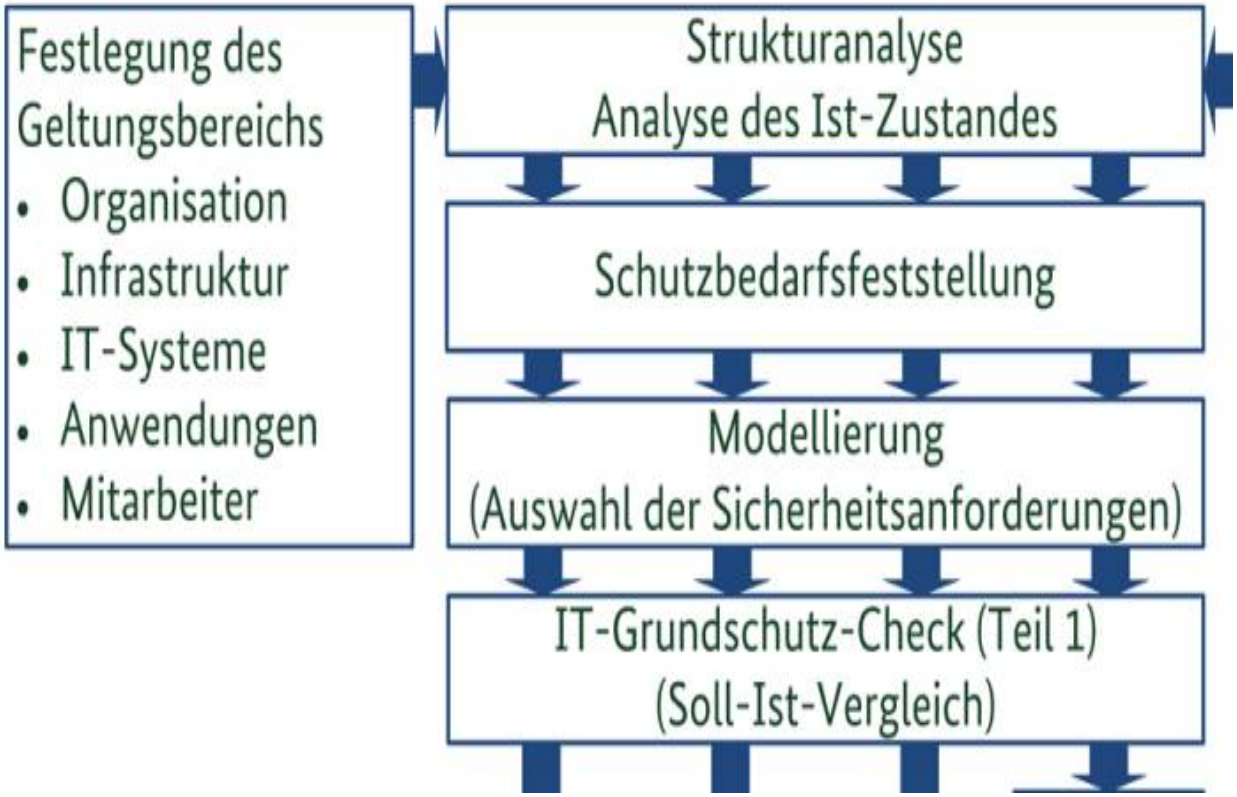
Abbildung 1: Übersicht über BSI-Publikationen zum Sicherheitsmanagement

Bei ISMS steht das Management im Vordergrund

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

BSI 200-1, Abb. 1.

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

Modellierung des IT-Verbundes mit „Bausteinen“

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

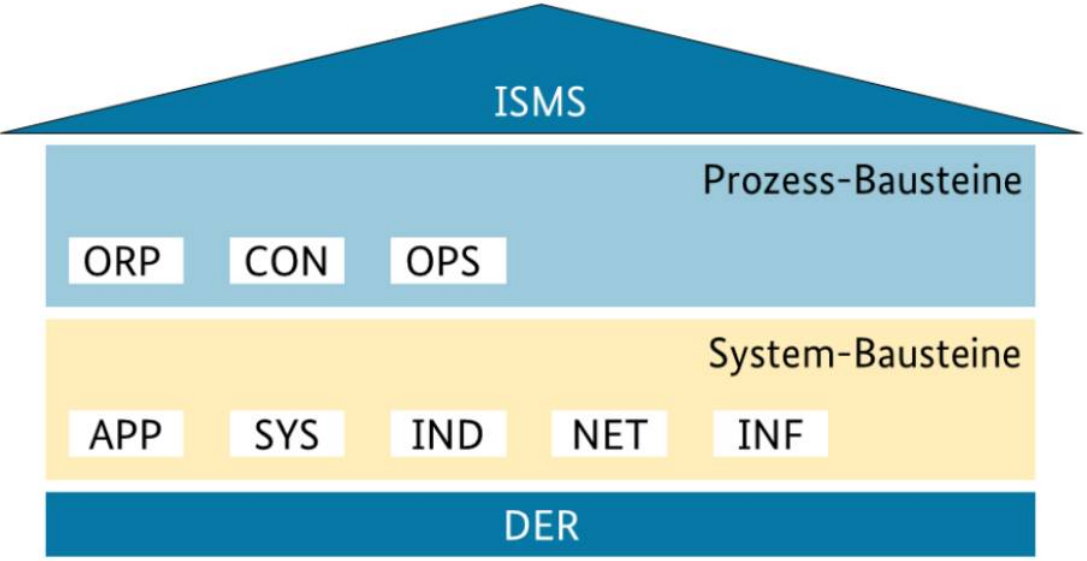
Sind die richtigen und relevanten Bausteine ausgewählt, ergeben sich die relevanten Anforderungen „automatisch“. Die Umsetzungshinweise unterstützen bei der Umsetzung der Anforderungen.

Vorgehen:

- Bausteinauswahl
- Gefährdungsanalyse
- Anforderungen und Umsetzungshinweise

Schichtenmodell

Details nicht klausurrelevant



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

Modellierung

Bausteinauswahl (Auswahl)
ISMS.1 Sicherheitsmanagement
OPS.1.1.2 Ordnungsgemäße IT-Administration
OPS 2.2. Cloud-Nutzung

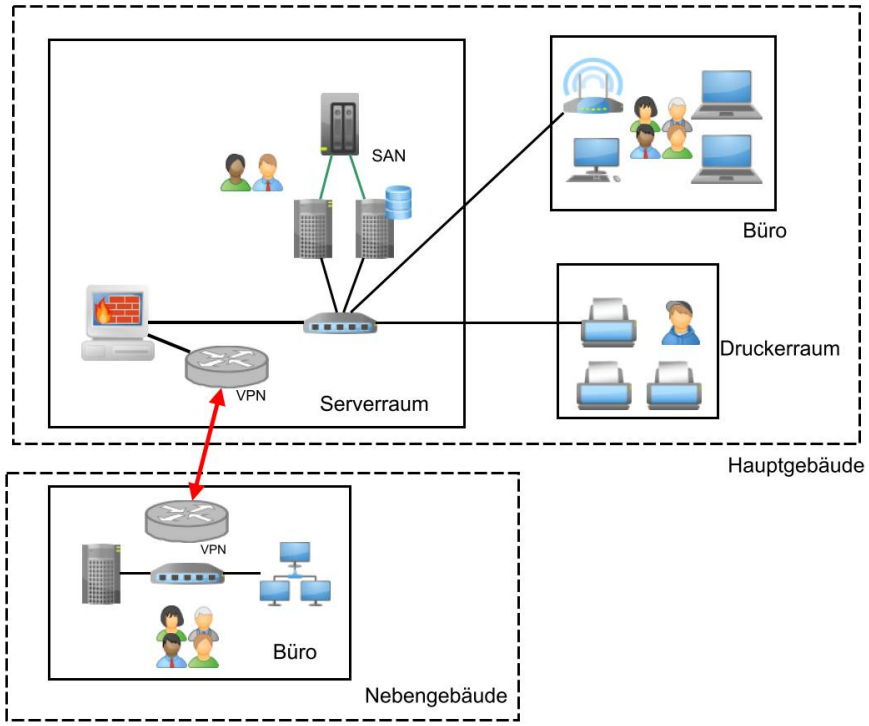
INF.1 Allgemeines Gebäude
INF.2 Rechenzentrum sowie Serverraum
INF.7 Büroarbeitsplatz
INF.12 Verkabelung

SYS.1.1 Allgemeiner Server
SYS.1.2.3 Windows Server
SYS.2.1 Allgemeiner Client
SYS.2.2.3 Clients unter Windows
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

IND.1 Prozessleit- und Automatisierungstechnik

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

APP.3.3 Fileserver
APP.4.3 Relationale Datenbanksysteme
(APP.5.3 Allgemeiner E-Mail-Client und Server)



Details nicht klausurrelevant

Anforderungen

Maßnahmen sind als „Anforderungen“ formuliert:

SYS.3.1.A3 Einsatz von Personal Firewalls (B)

Auf Laptops MUSS eine Personal Firewall aktiv sein, wenn sie außerhalb von Netzen der Institution eingesetzt werden. Die Filterregeln der Firewall MÜSSEN so restriktiv wie möglich sein. Die Filterregeln MÜSSEN regelmäßig getestet werden. Die Personal Firewall MUSS so konfiguriert werden, dass die Benutzenden nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können.

Drei Gruppen von Anforderungen:

Basis => MÜSSEN

Standard => SOLLTEN

erhöhter Schutzbedarf =>SOLLTEN

Beispiel: SYS.2.1 Allgemeiner Client spezifische Gefährdungen

2.1 Schadprogramme
2.2 Datenverlust durch lokale Datenhaltung
2.3 Hardware-Defekte bei Clientsystemen
2.4 Unberechtigte IT-Nutzung
2.5 Installation nichtbenötigter Betriebssystemkomponenten
2.6 Abhören von Räumen mittels Mikrofon und Kamera
2.7 Fehlerhafte Administration oder Nutzung von Geräten und Systemen

Details nicht klausurrelevant

Beispiel: SYS.3.1 Laptop Anforderungen

Anforderung: (**Standard**)

SYS.3.1.A13 Verschlüsselung von Laptops (S)

In Laptops verbaute Datenträger wie Festplatten oder SSDs SOLLTEN verschlüsselt werden

Details nicht klausurrelevant

Beispiel: SYS.3.1 Laptop Umsetzungshinweise (2022)

Umsetzungshinweis:

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. ….

Eine Verschlüsselung kann online oder offline vorgenommen werden. Online bedeutet, dass sämtliche Daten der Festplatte (bzw. einer Partition) verschlüsselt werden, ohne dass der Benutzer dies aktiv veranlassen muss. …..

Details nicht klausurrelevant

Grundschutz-Profile

IT-Grundschutz-Profilen als **Musterszenarien**

In einem IT-Grundschutz-Profil werden die einzelnen Schritte eines Sicherheitsprozesses für einen definierten Anwendungsbereich dokumentiert, dazu gehören:

- Festlegung des **Anwendungsbereichs**
- Durchführung einer **verallgemeinerten** Strukturanalyse, Schutzbedarfsfeststellung und Modellierung für diesen Bereich
- **Auswahl und Anpassung** von umzusetzenden IT-Grundschutz-**Bausteinen** sowie
- Beschreibung **spezifischer Sicherheitsanforderungen** und -maßnahmen.

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/it-grundschutz-profile_node.html

Details nicht klausurrelevant

Grundschutz-Profile (Auswahl)

- für Leitstellen
- zur Absicherung von 5G-Campusnetzen Eigenbetrieb/ Fremdbetrieb
- für oberste Bundesbehörden/ obersten Landesbehörden
- Basis-Absicherung Kommunalverwaltung
- für Bundesgerichte
- für den Betrieb von UAS (Unmanned Aircraft Systems)
- "Chemie"
- für Hochschulen
- für Weltrauminfrastrukturen
- für die Verkehrssteuerungs- und Leitsysteme der Bundesautobahn
- für Papierfabriken
- "i-Kfz"
- für Reedereien - Landbetrieb / für Reedereien - Schiffsbetrieb
- für Handwerkskammern

Details nicht klausurrelevant

IT (Sicherheits-) Standards

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

Standard-Datenschutzmodell (SDM)

- „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
- https://www.datenschutzzentrum.de/sdm/
- spezifische Datenschutz-Maßnahmen (teilweise Überdeckung mit IT-Sicherheit, teilweise spezifisch wie Einschränkung, Auskunftserteilung, Pseudonymisierung) verfügbar und in Arbeit (https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/)

SDM: Gewährleistungsziele

- Verfügbarkeit
- Vertraulichkeit
- Integrität

} klassische Ziele der Informationssicherheit

- Datenminimierung
- Nichtverkettung
- Transparenz
- Intervenierbarkeit

} datenschutzspezifische Ziele

SDM: Beispiele generische Maßnahmen

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit sind:

- Sicherheitskopien
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
- Redundanz von Hard- und Software + Infrastruktur
- Vertretungsregelungen für abwesende Mitarbeitende
- ….

SDM: Beispiele generische Maßnahmen

Typische Maßnahmen zur Gewährleistung der Transparenz:

- Inventarisierung alle Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO
- Dokumentation von Tests, der Freigabe und ggf. der Datenschutz-Folgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten
- Dokumentation der Faktoren, die für eine Profilierung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden
- Protokollierung von Zugriffen auf und Änderungen von Daten
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept

IT (Sicherheits-) Standards

- COBIT
- ITIL®
- NIST Cybersecurity Framework
- ISO 27001 und ISO 27002
- BSI Standards und IT-Grundschutz
- *Standard-Datenschutzmodell*
- 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
- Formelle **Zertifizierung** der Vertrauenswürdigkeit von Produkten
- International anerkannt (gegenseitige Anerkennung der Zertifizierung bis EAL 4)
- TOE: Target of Evaluation

Ansatz: Wasserfallmodell

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

IT (Sicherheits) Standards

- COBIT
- ITIL®
- NIST Cybersecurity Framework
- ISO 27001 und ISO 27002
- BSI Standards und IT-Grundschutz
- *Standard-Datenschutzmodell*
- Common Criteria (ISO 15408)
- FIPS-140

FIPS 140

- Ziel: Koordination von Anforderungen und Standards von Kryptomodulen (Hardware und Software)
- Zertifizierung verfügbar
- FIPS 140-2: seit Mai 2001
- Annexes:
  - Annex A: Approved Security Functions [2021]
  - Annex B: Approved Protection Profiles [2019]
  - Annex C: Approved Random Number Generators [2021]
  - Annex D: Approved Key Establishment Techniques [2021]

- derzeit: Übergang zu FIPS 140-3 mit Verweis auf ISO-Normen (bis 2026)

Details nicht klausurrelevant

Literatur/Links

Standards:

- CobiT:
  - www.isaca.org
  - Asprion, P. M., Burda, D.: Cobit https://wi-lex.de/index.php/lexikon/informations-daten-und-wissensmanagement/grundlagen-der-informationsversorgung/cobit/
- Common Criteria: www.commoncriteriaportal.org
- https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/zertifizierung-nach-cc_node.html
- BSI Standards/ IT Grundschutz: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
- SDM: https://www.datenschutzzentrum.de/sdm/

Literatur:

- Anderson, Ross: Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition, 2020, Wiley, ISBN: 978-1-119-64281-7 1232 pages, https://www.cl.cam.ac.uk/~rja14/book.html
- Kersten, H., Schröder, K.-W.:ISO 27001: 2022/2023, 2023, Springer Vieweg. ISBN 978-3-658-42243-1