Vorlesung

Inf-DatSchutz:Datenschutz

SS 2025

Durchführung:

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

Ansprechpartner:

Benjamin Bremert

Organisatorisches

- Verantwortlich: Benjamin Bremert, ab dem 05.05.2025
- Dozentenmix: (Ex)Beschäftigte des ULD
- Themenmix:
  Rechtlich und technische Aspekte des Datenschutzes
- heute/nächste Woche:
  Thomas Probst: Datenschutz durch Technik

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.

Brainstorming: Was ist Datenschutz?

Kennen Sie rechtliche Regelungen zum Datenschutz?

Beispiele

- Datenschutzgrundverordnung (DSGVO)
- Richtlinie Datenschutz Polizei + Sicherheit + Justiz (JI-Richtlinie)

- Bundesdatenschutzgesetz (BDSG)
- Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

- Landesdatenschutzgesetze (LDSG XX)

Abgrenzung zu anderen rechtlichen Regelungen im Bereich „Daten"

- Welche kennen Sie?

Beispiele

- Informationssicherheit
  - BSI-Gesetz, Cyberresiliance-Act, NIS2, KRITIS
  - Regelungen der BaFin im Bereich Banken und Versicherungen (BAIT, VAIT); DORA
- Urheberrecht
- KI (AI-Act)
- Wettbewerbsrecht, Digital Market Act

Kennen Sie andere Regelwerke außer Rechtsnormen?

Begriffsklärung: Informationssicherheit

Begriffe

- Informationssicherheit = ?
- Datensicherheit = ?
- 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 Personen** auf informationelle Selbstbestimmung (Grundrechtsschutz)

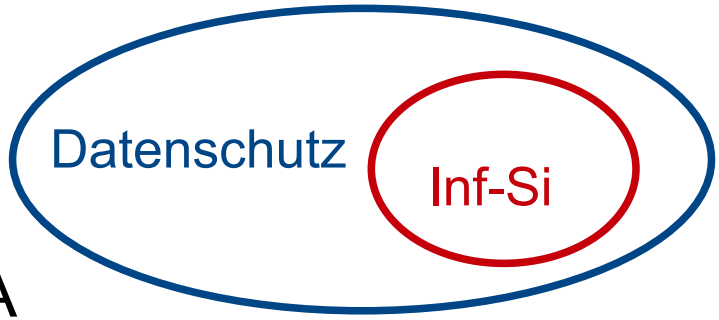
- [in Publikationen wird manchmal „Datenschutz“ anstelle von „Informationssicherheit“ verwendet. Manchmal werden im Englischen mit „data protection″ auch Backupmechanismen bezeichnet.]

Datenschutz und Informationssicherheit

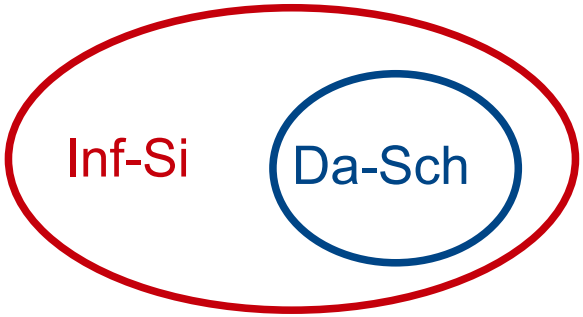
- Datenschutz:
  Schutz der Menschen vor Missbrauch ihrer personenbezogenen Daten

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

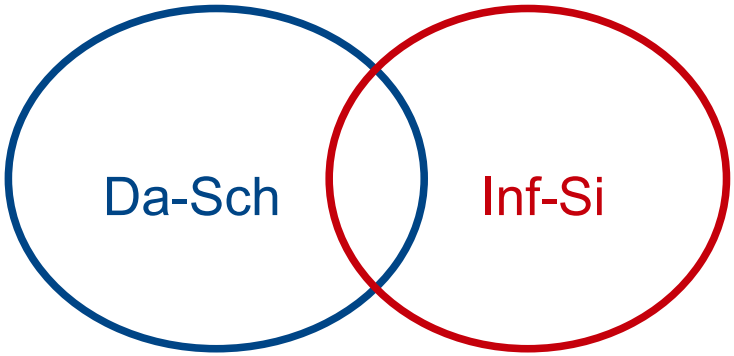
Verhältnis Datenschutz – Informationssicherheit ?



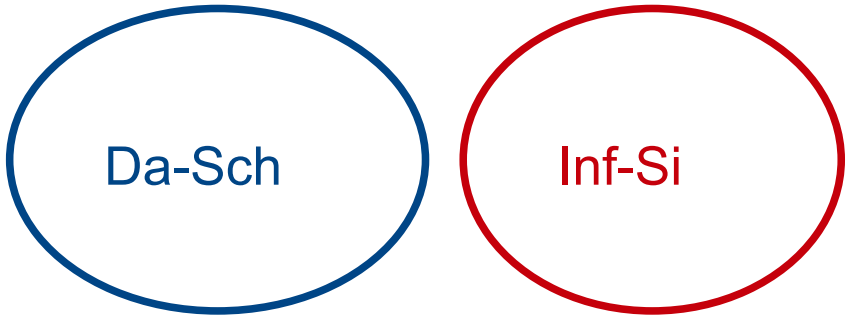
A



B



C

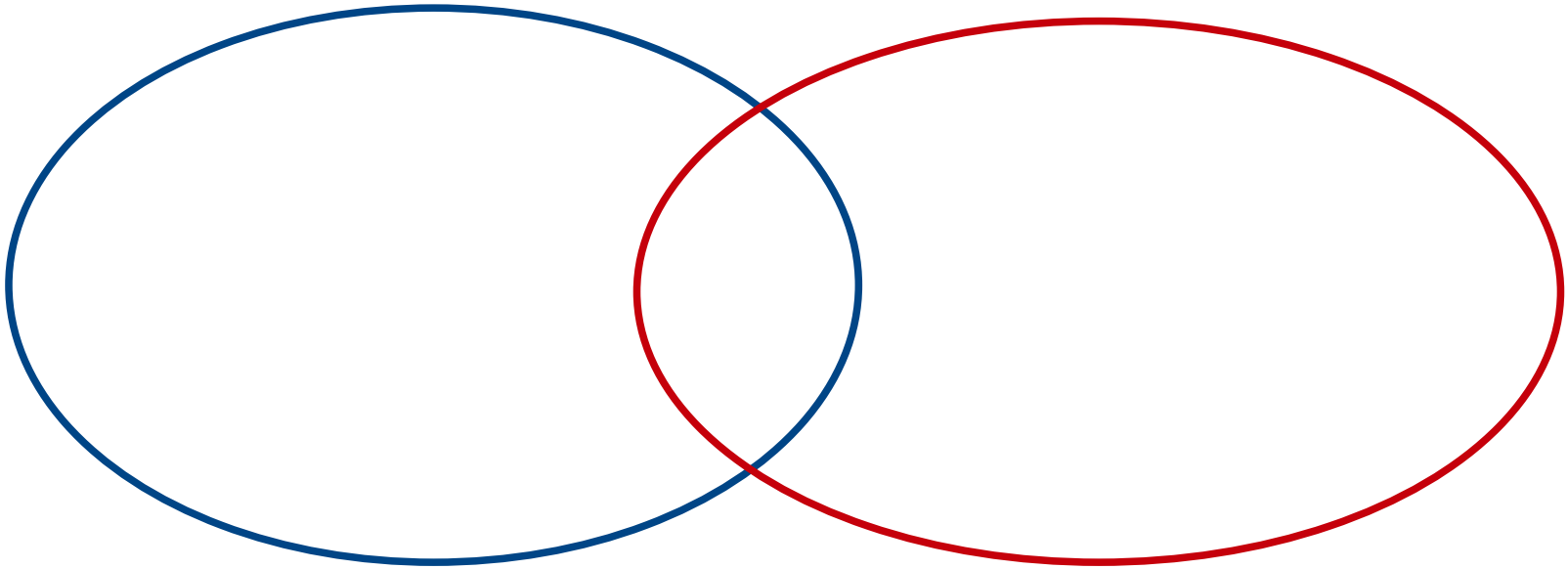


D

Abstimmung

- A
- B
- C
- D

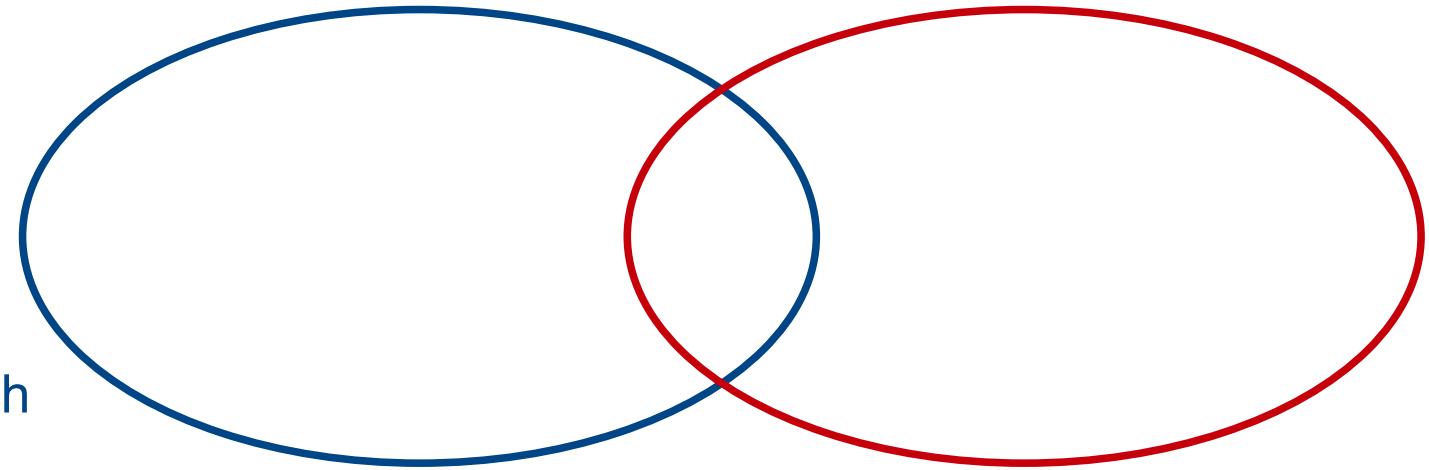
Verhältnis Datenschutz – Informationssicherheit ?



Da-Sch

Inf-Si

Verhältnis Datenschutz – Informationsicherheit ?



- Rechtsvorschriften zur Zulässigkeit der DV
- Meldepflichten
- Auskunftspflichten

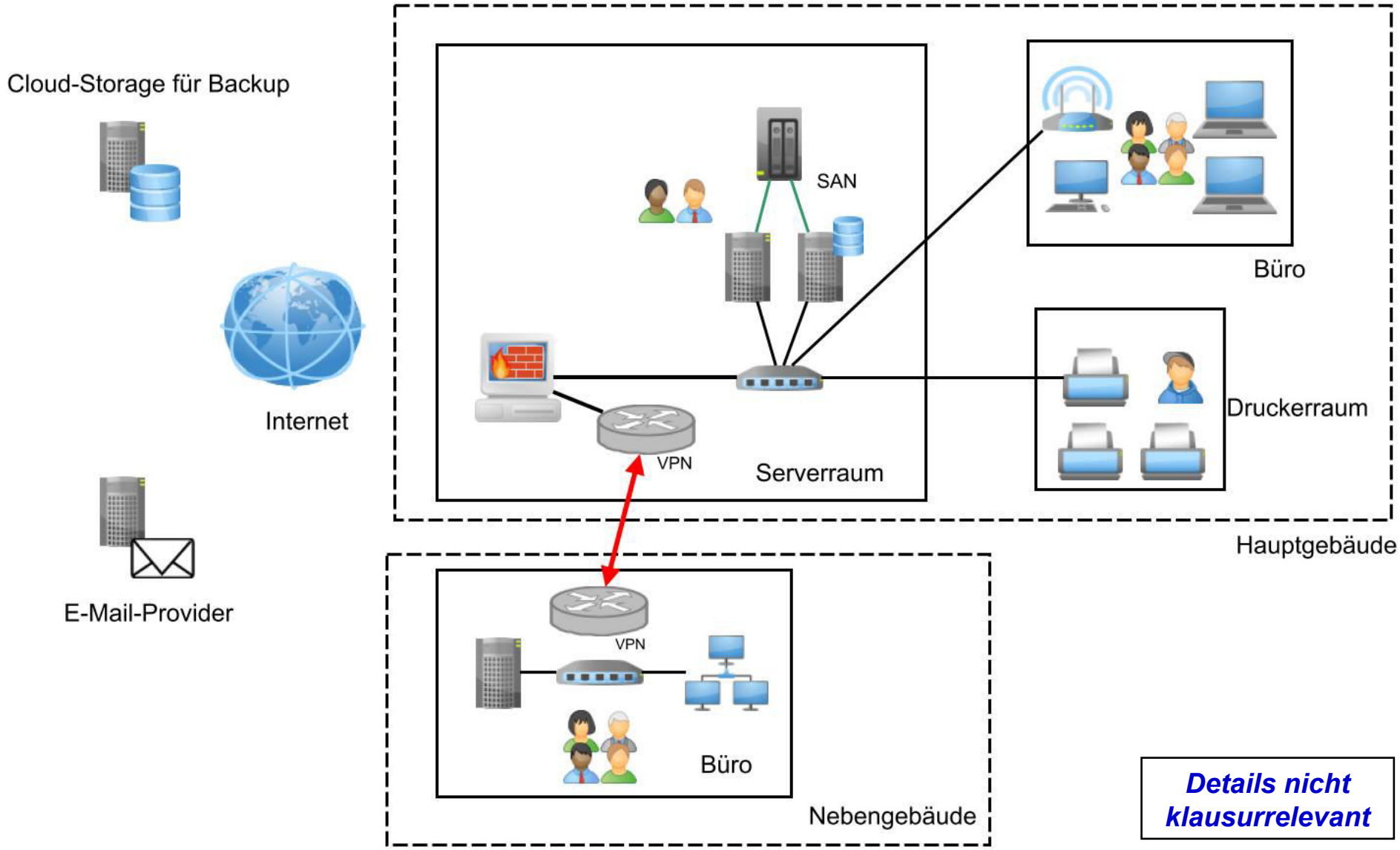
- Sicherheit personenbezogener Daten
- Protokollierungs-pflichten

- 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“)

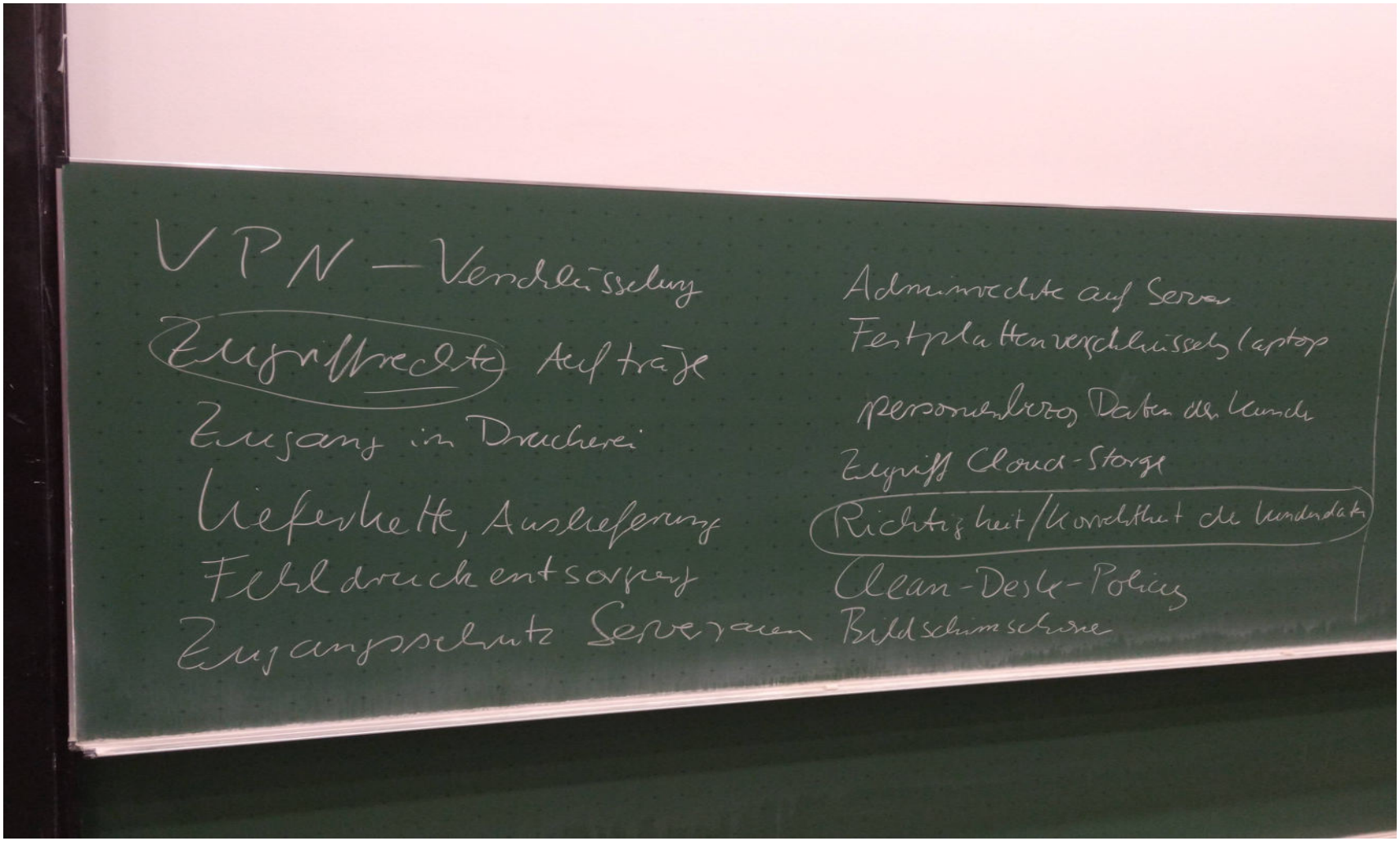
- Risikobegriff

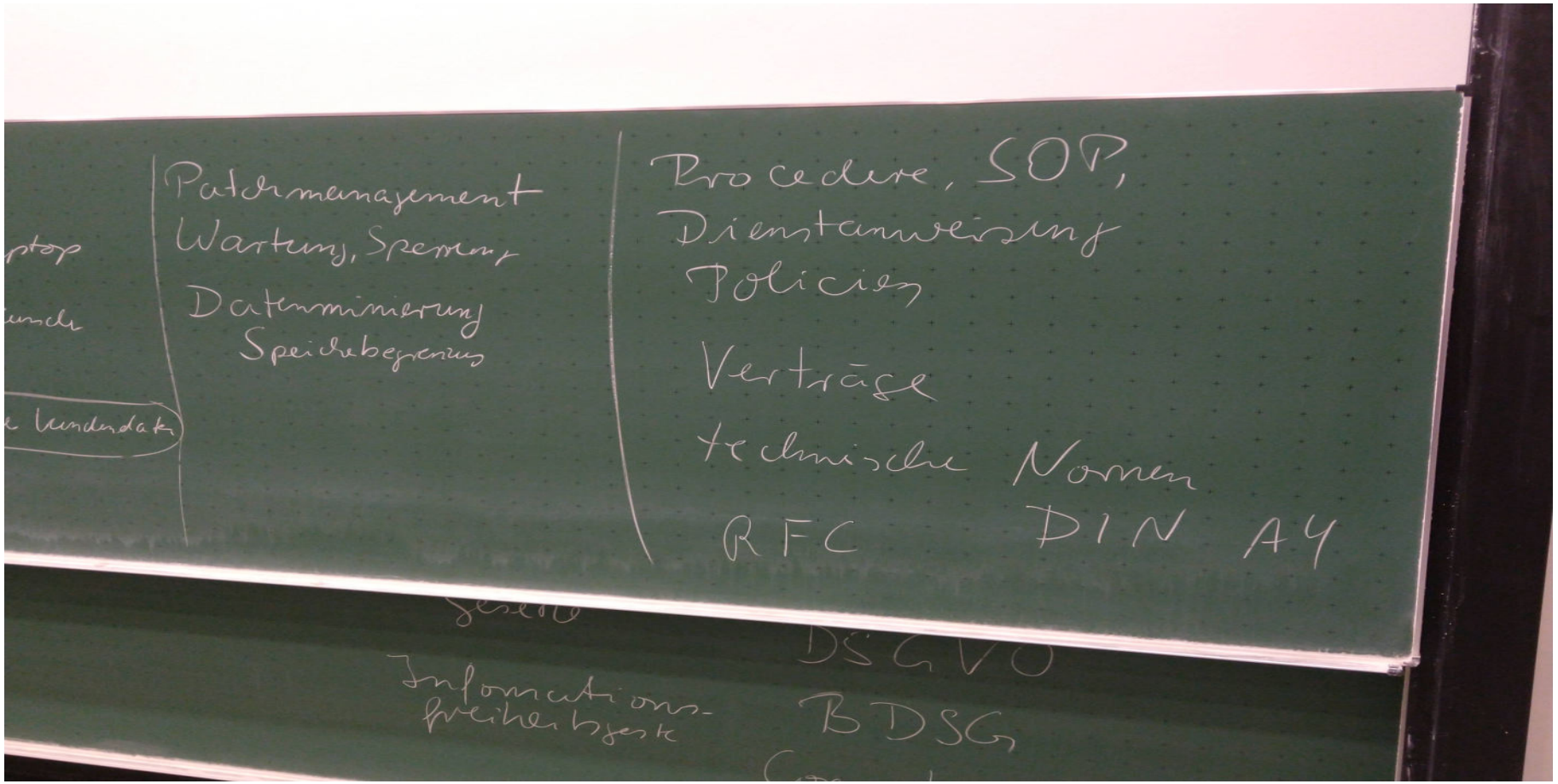


Details nicht klausurrelevant

Aufgabe

Legen Sie geeignete Datenschutzmaßnahmen fest.
Legen Sie geeignete Sicherheitsmaßnahmen fest.


VPN – Verschlüsselung
Zugriffsrechte Aufträge
Einsang 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

Diskussion: Was soll geschützt werden?

- Was soll Informationssicherheit erreichen?
- Schutz in Bezug auf was?
  (Richtigkeit der Daten? Finanzen? ...)

Systematik Zielvorgaben vs. Sicherheitsmaßnahmen

Unterschiedliche Detaillierungsgrade von Vorgaben

- in Gesetzen häufig sehr abstrakt
  - teilweise Zielvorgaben: „ Vertraulichkeit“
  - teilweise abstrakte Maßnahmenvorgaben „Eingabekontrolle“
  - teilweise konkrete Maßnahmenvorgaben: „Verschlüsselung“

- in Branchen/Industriestandards häufig sehr ausführlich und konkret (z. B. „ TLS 1.3 -Verschlüsselung zwischen Clients und Server“)

Klassische Schutzziele (CIA)

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

Vertraulichkeit

Vertraulichkeit: Informationen dürfen nur Berechtigten bekannt werden.

- Schutz von Vertraulichkeit:
  Verhindern von unberechtigter Kenntnisnahme,
- z.B. durch
  - Verschlüsselung von Daten (Kryptographie)
  - Verstecken von Daten (Steganographie)
  - Verhindern des Zugriffs auf Daten (Zugriffskontrolle)

```
-----BEGIN PGP-----
0IxWZHhKYoECwCBeIweKU+0Ed
m068SB4ADeGGCtd+eacjDT5Ig
TdwAypl8+WOFYxTVEXbqOqjoW
mY4T9zuoSC5e
=lu9g
-----END PGP-----
```

Wer darf unter welchen Bedingungen welche Daten lesen?

Grundsatz:

Die Verletzung der Vertraulichkeit personenbezogener Daten kann nicht ungeschehen gemacht werden.

Ein verratenes Geheimnis ist keines mehr und wird nie wieder eines!

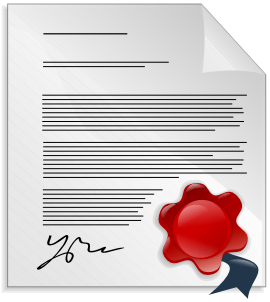
Integrität

Integrität: Informationen sind richtig, vollständig und aktuell
oder aber dies ist erkennbar nicht der Fall.

Schutz von Integrität:

Verhindern von unberechtigter Manipulation oder Datenverlust , z.B. durch

- Prüfsummen, fehlerkorrigierende Codes
- Einschränkung von Schreibrechten
- Erkennen von Manipulationen durch
  - Zeitstempel
  - Protokolle
  - Signaturen und Prüfsummen



www.openclipart.org

Wer darf unter welchen Bedingungen welche Daten oder IT-Systeme ändern?

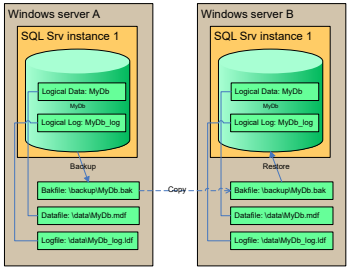
Verfügbarkeit

Verfügbarkeit: Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

Schutz von Verfügbarkeit:

Gewährleisten von Funktionalität gegen vorsätzliche oder versehentliche Einschränkung, z.B. durch

- Redundanz (Daten, Hardware)
- Wartung
- Sicherheitsmaßnahmen (z. B. Firewall)



www.openclipart.org

Bedrohungen der Verfügbarkeit

Beispiele:

- E-Mail-SPAM
- DDOS (Distributed Denial of Service)
- Sabotage: **Ransomware**
- Feuer
- Hardware-Versagen (z.B. Speicher, Switches, Netzteil, interne Kühlung)
- Infrastrukturausfall: Strom, Kühlung, Netze
- Infrastrukturausfall: Gebäudeschäden, Wasserschaden, Erdbeben

Sicherheitsvorfälle

Finden Sie Beispiele für

- (IT-)Sicherheitsvorfälle
- Datenschutzvorfälle

Heise 06.03.2021
https://www.heise.de/-5073716.html

Exchange-Lücken: BSI sieht hierzulande zehntausende Server betroffen

….

Allen Betreibern von betroffenen Exchange-Servern rät das BSI, sofort die von Microsoft in der Nacht zum Mittwoch bereitgestellten Sicherheitsupdates einzuspielen. Die damit geschlossenen Schwachstellen würden derzeit "aktiv von einer Angreifergruppe" per Fernzugriff ausgenutzt ...

Heise 10.12.2021
https://www.heise.de/-6291653.html

Über eine kritische **Zero-Day-Sicherheitslücke namens Log4Shell** in der weitverbreiteten Java-Logging-Bibliothek Log4j können Angreifer beliebigen Code ausführen lassen. Betroffen sind etwa Dienste von Apple, Twitter, Steam, Amazon und vermutlich sehr viele kleinere Angebote. Es gibt Proof-of-Concept-Code, der das Ausnutzen der Lücke demonstriert und auch bereits erste Angriffe. Seit Kurzem steht ein Quellcode-Update des Apache-Projekts bereit; Admins sollten dringend aktiv werden….

Heise 21.10.2023
https://heise.de/-9318038

Vor einigen Monaten ist es der Ransomware-Gang Clop gelungen, eine **Zero-Day-Lücke** in der **Datenaustauschsoftware MOVEit** auszunutzen. So konnten sie Daten aus dem Zugriffsbereich der Software-Nutzer stehlen. MOVEit wird weltweit von vielen Organisationen, Unternehmen und Dienstleistern zum Datenaustausch genutzt – dabei werden auch Daten **anderer Stellen und (Privat-)Personen** verarbeitet, die nicht in direktem Zusammenhang mit den Nutzern der Software stehen müssen.

Heise 23.3.2024
https://www.heise.de/-9662578.html

Datenleck bei beliebter KiTa-App XXX

Bei der App "XXX", die in über **11.000 Kitas**, Horten & Schulen zum Einsatz kommt, gab es ein Datenleck. Potenziell betroffen sind über **800.000 Nutzer**. …

Der Server ... lieferte direkt ein "**Directory Listing**" seines Inhalts. ... liegen auf einem Server Dateien, die nicht für die Öffentlichkeit bestimmt sind, offenbart Directory Listing sie gnadenlos. Das eigentliche Problem im konkreten Fall ist aber der **fehlende Zugriffsschutz** auf die Dateien…..

Unter den ungeschützten Daten befanden sich fast 1500 CSV-Dateien, die jeweils persönliche Daten einer Vielzahl von Personen enthielten, insbesondere von Minderjährigen. In Verbindung mit **Namen, Geburtsdaten und Anschriften** fanden sich teilweise auch **Herkunftsländer, Informationen über Impfungen, Konfessionen, Erziehungsberechtigte, Notfallkontakte**, Klassenlehrer und vieles mehr.

https://en.wikipedia.org/wiki/Heartbleed
(Abruf 13.04.2025)

Implementierungsfehler in Open SSL (2012-2014)

Heartbleed is a security bug in some outdated versions of the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014.