Vorlesung Datenschutz

SS 2024

Durchführung:

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

Ansprechpartner:

Benjamin Bremert

Vorlesung Datenschutz CAU SS 2024

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.

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)

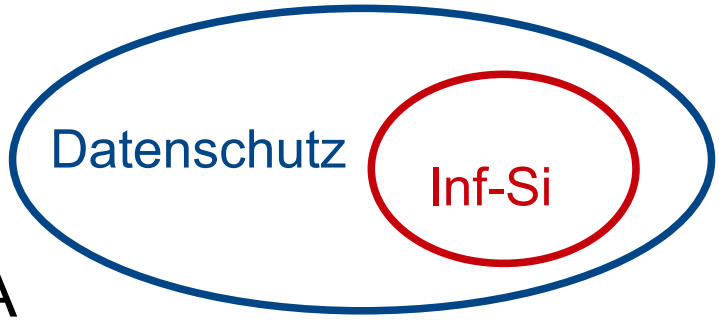
- [in Publikationen wird manchmal „Datenschutz“ anstelle von „Informationssicherheit“ verwendet. Manchmal werden im Englischen mit „data protection″ auch Backupmechanismen bezeichnet.]

Datenschutz und Informationssicherheit

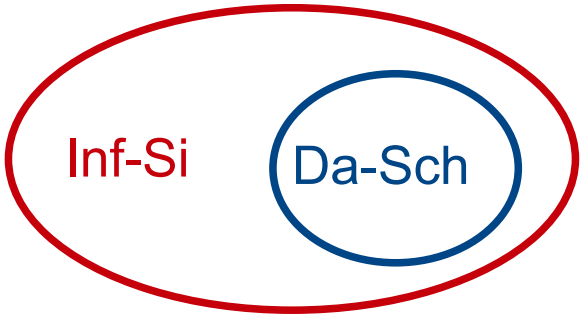
- Datenschutz:
  Schutz der Menschen vor Missbrauch ihrer personenbezogenen Daten

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

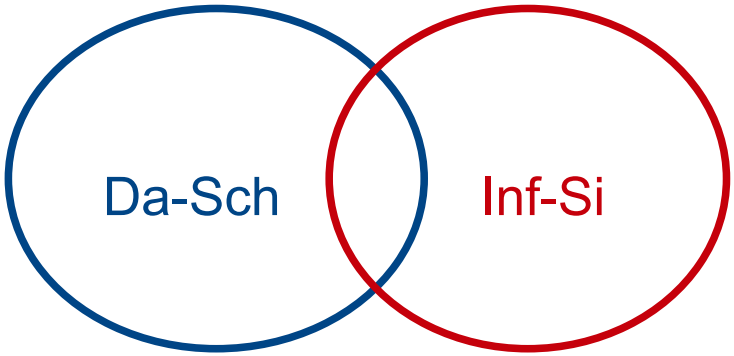
Verhältnis Datenschutz – Informationssicherheit ?



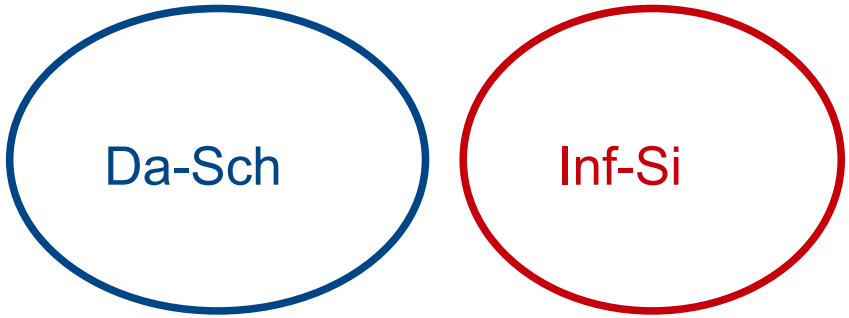
A



B



C

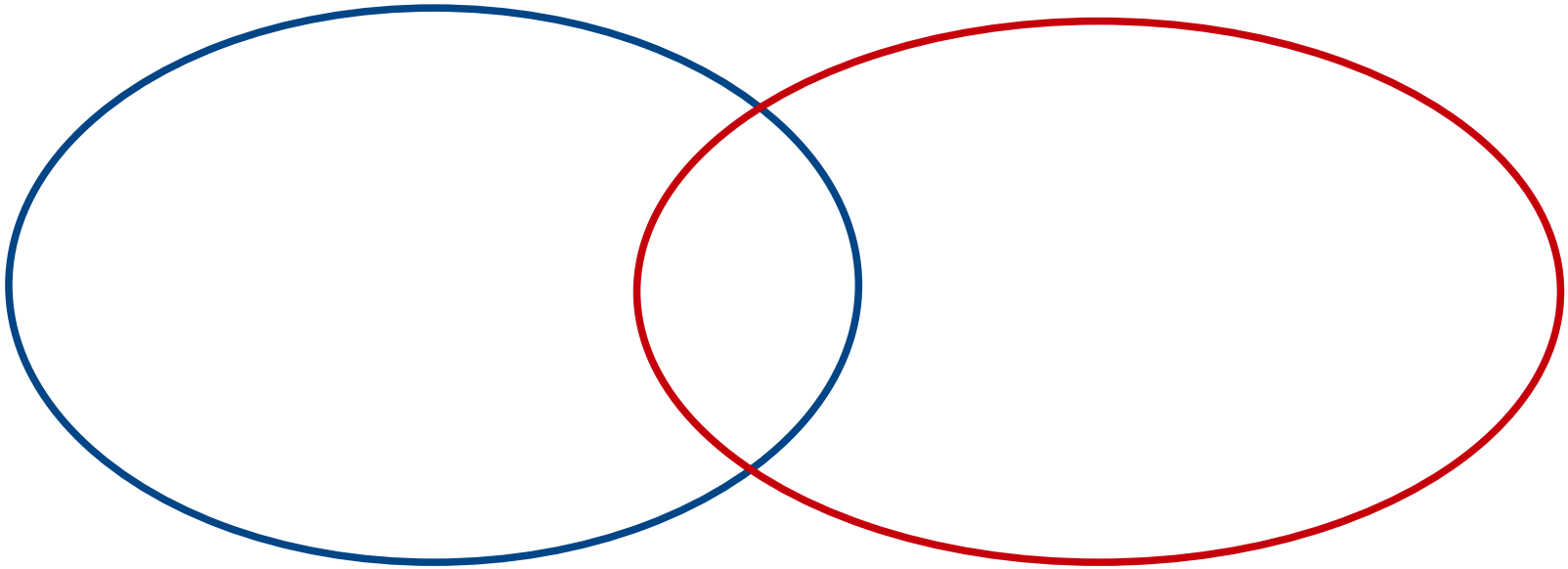


D

Abstimmung

- A
- B
- C
- D

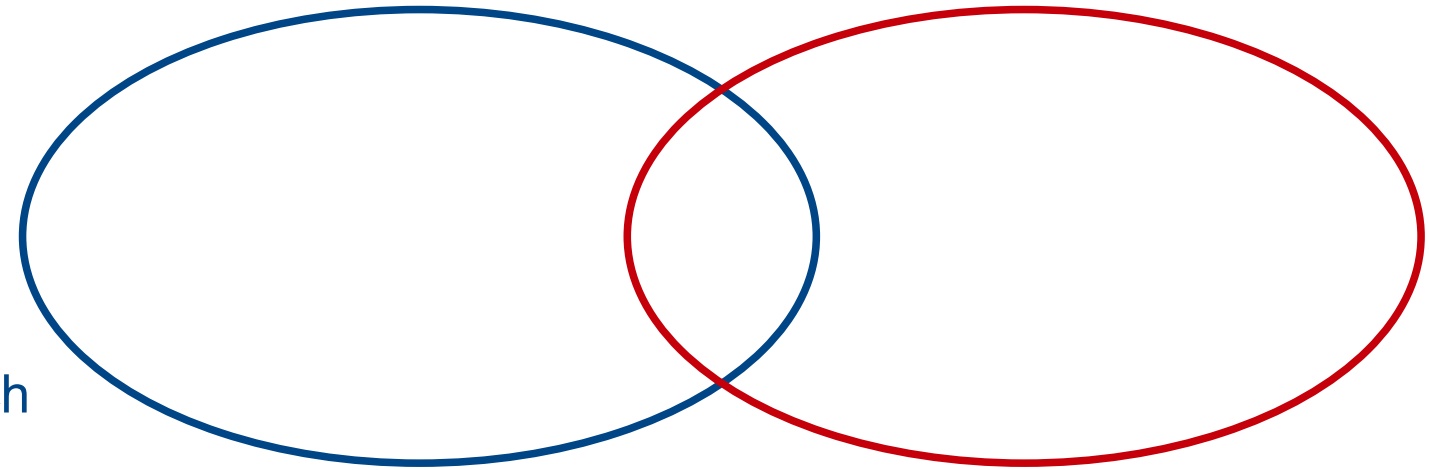
Verhältnis Datenschutz – Informationssicherheit ?



Da-Sch

Inf-Si

Verhältnis Datenschutz – Informationsicherheit ?



Da-Sch

Inf-Si

- Rechtsvorschriften zur Zulässigkeit der DV
- Meldepflichten
- Auskunftspflichten

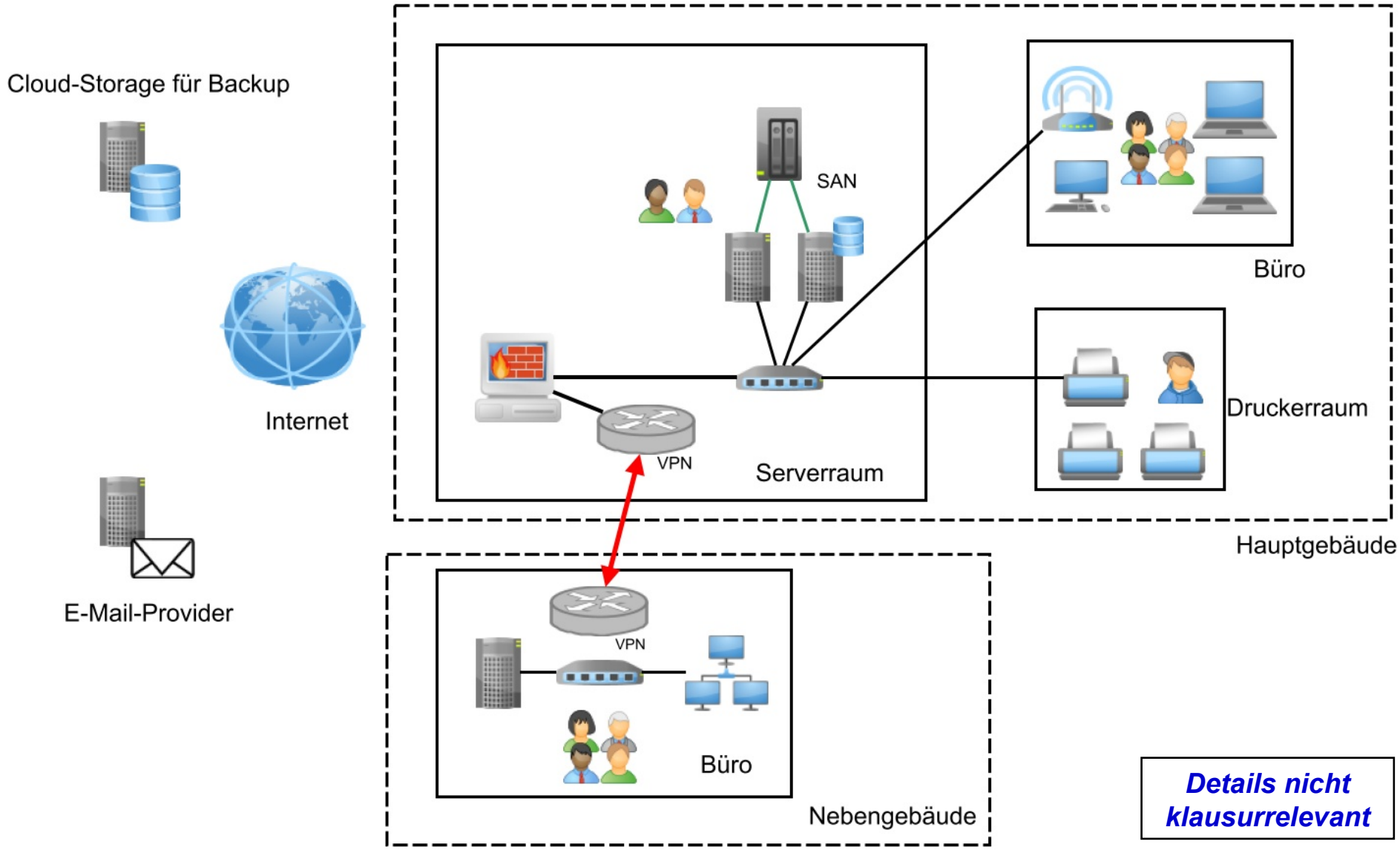
- Sicherheit personenbezogener Daten
- Protokollierungs-pflichten

- 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.

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!

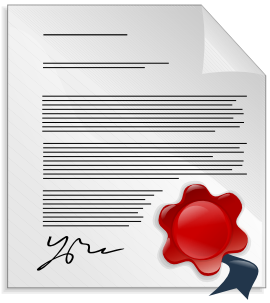
Integrität

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?

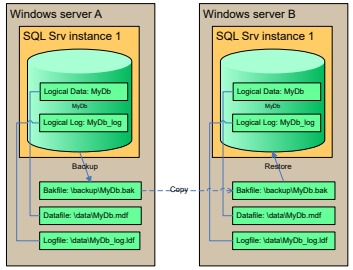
Verfügbarkeit

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. Festplatten, 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 25.04.2024)

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.

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. Dieses so genannte "Greyballing" soll Strafen und die Beschlagnahme von Fahrzeugen reduzieren. ....

Zu den ausgewerteten Metadaten gehören unter anderem Bewegungsmuster, Kreditkartennummern und Handy-Seriennummern. XXX stellte den Bericht gegenüber heise online nicht in Abrede. "[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."

Heise 26.04.2018
https://heise.de/-4035950.html

… hatte vor wenigen Wochen bekannt gemacht, dass Cambridge Analytica unter Zuhilfenahme von Dutzenden Millionen Facebook-Nutzerdaten Einfluss auf Abstimmungen wie ... genommen haben soll. …. Die dafür genutzten Daten waren vorgeblich für Forschungszwecke abgegriffen worden, weswegen Facebook das erlaubt habe, aber dann widerrechtlich weitergegeben worden. Durch dieses Detail und die anschließende Debatte über Facebook massive Datensammelei ….

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

https://lfd.niedersachsen.de/startseite/infothek/tatigkeitsberichte/2022/28-tatigkeitsbericht-2022-223047.html (Abschnitt 1.3. S. 101)

Datenbankabruf

„Der Polizist hatte Informationen zu einem Kollegen aus ComVor und POLAS, zwei polizeilichen Informationssystemen, abgefragt. Ein dienstlicher Bezug hatte nicht bestanden. Vielmehr war der Bußgeldempfänger aufgrund von Gerüchten zu einem Strafverfahren neugierig geworden."

https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-besch%C3%A4ftigter-der-polizei-2022-06-08-DE-2058.php

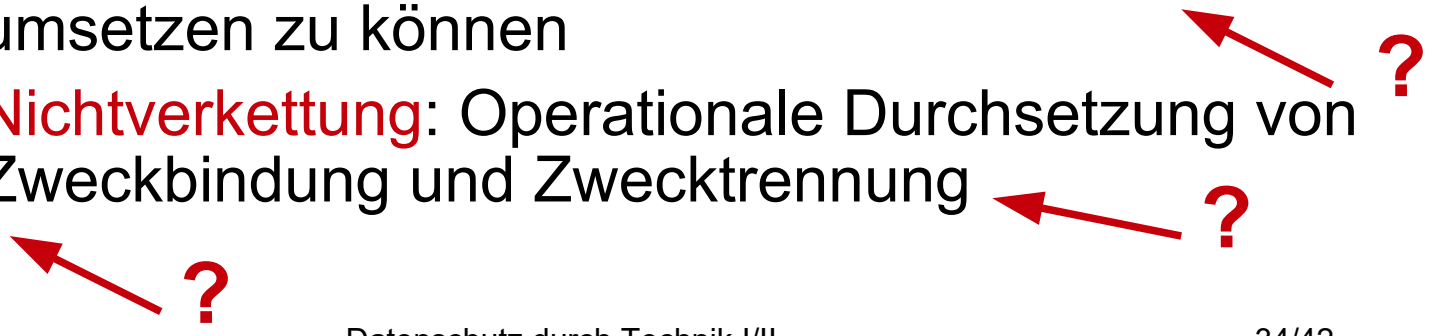
Datenschutzziele

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

Spezifische Datenschutzschutzziele:

Ergänzung in einigen LDSGen vor 2018 (andere Form) und teilweise in der EU-Datenschutzgrundverordnung:

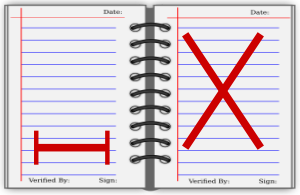
- Datenminimierung: dem Zweck angemessen, beschränkt
- Transparenz: nachvollziehbare und aktuelle Dokumentation von Verfahren (einschließlich methodischer Planung), insbesondere für betroffene Personen
- Intervenierbarkeit: Fähigkeit, Betroffenenrechte wirksam umsetzen zu können
- Nichtverkettung: Operationale Durchsetzung von Zweckbindung und Zwecktrennung



Datenminierung

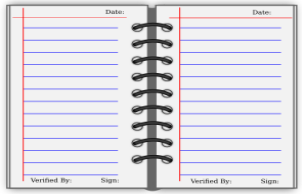
Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

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



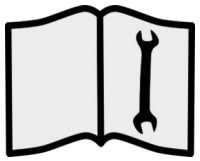
Transparenz

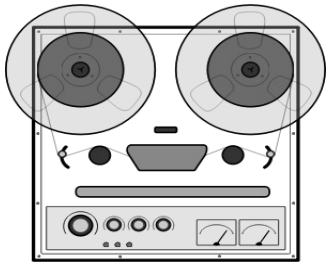
Die Datenverarbeitung ist für Betroffene nachvollziehbar und erfüllt prüfbar die datenschutzrechtlich bestehenden Anforderungen.



Sicherung von Transparenz:

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

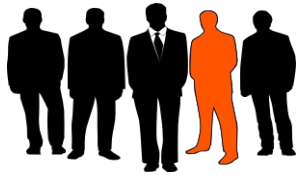




www.openclipart.org

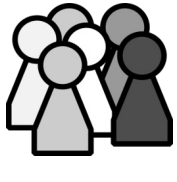
Nicht-Verkettung

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



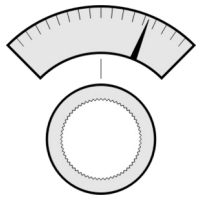
www.openclipart.org

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