Datenbanken und Informationssysteme

VL 06, Sicherheit

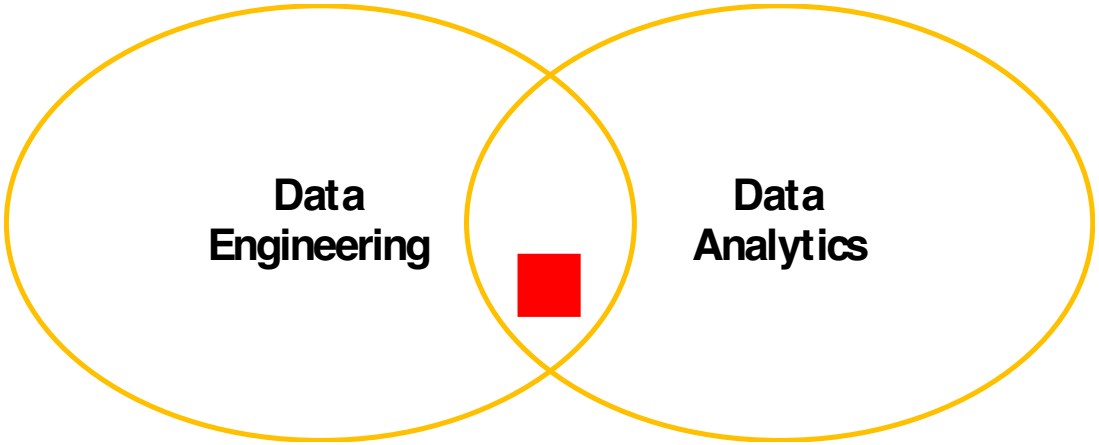
SoSe 2022

Univ.-Prof. Dr.–Ing. habil. Norbert Gronau
Lehrstuhlinhaber | Chairholder

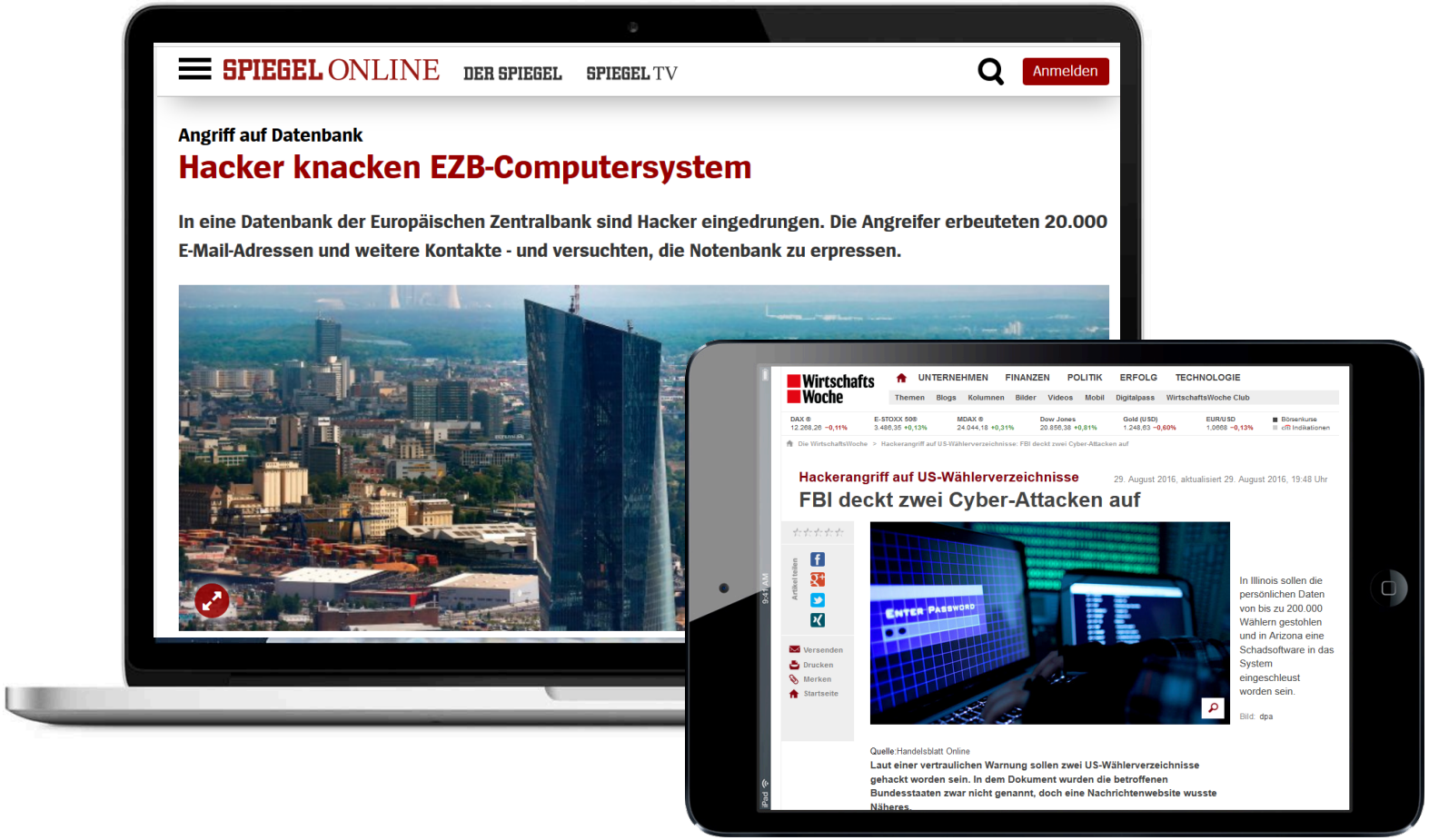
Mail August-Bebel-Str. 89 | 14482 Potsdam | Germany
Visitors Digitalvilla am Hedy-Lamarr-Platz, 14482 Potsdam
Tel +49 331 977 3322

E-Mail ngronau@lswi.de
Web lswi.de

Kapitel 6: Sicherheit



Sicherheitsvorfälle bei Datenbanken



Folgen eines Sicherheitsvorfalls

- Betriebswirtschaftliche Folgen
  - > Schaden durch Angriffe Dritter oder Betrug des Kunden
  - > Kunden nehmen wegen Sicherheitsbedenken das Angebot nicht wahr
- Schäden
  - > Unmittelbar
    - » eigene materielle Verluste
    - » Schadenersatzforderungen von Nutzern
  - > Mittelbar
    - » Öffentlichkeitswirkung, Vertrauensverlust, Umsatzausfall
    - » Erfordernis höherer Marketing- und Kundenservice-Ausgaben
- Implikation: Risikomanagement muss integraler Bestandteil der Geschäftstätigkeit sein!

Risikomanagement

- Aufgaben
  - > Identifizierung und Bewertung spezifischer Risiken
  - > Abwägung zwischen Nutzen und Aufwand der Maßnahmen
- Stufen der Risikoanalyse
  - > Prüfung der Datenvermeidung
    - » Kann der Umfang personenbezogener Daten reduziert werden?
  - > Schutzbedarfsfeststellung
    - » Wie schützenswert sind die erhobenen Daten?
  - > Bedrohungsanalyse
    - » Welche Objekte werden bedroht, welchen Bedrohungen sind sie ausgesetzt?
  - > Risikobewertung
    - » Wie hoch ist die Eintrittswahrscheinlichkeit und der mögliche Schaden?
  - > Ableitung von Schutzmaßnahmen
    - » Auswahl geeigneter technischer und organisatorischer Maßnahmen

Perspektiven der Sicherheit

- Objektive Sicherheit
  - > Erreichung objektiver Sicherheitsziele
  - > Informationssicherheit, Funktionssicherheit, Datenschutz
- Subjektive Sicherheit
  - > Wahrgenommenes Sicherheitsniveau
  - > Abhängig vom Vertrauen des Nutzers in den Anbieter
  - > Vertragsgemäße Leistungserbringung des Anbieters glaubhaft machen
    - » Aufbau und Nutzung von Marken
    - » Nutzung einer außerhalb der digital bestehenden Kundenbeziehung
    - » Bescheinigung bestimmter Eigenschaften (Attribute) durch Zertifikate

nicht Thema der DBIS

Objektive Sicherheitsziele

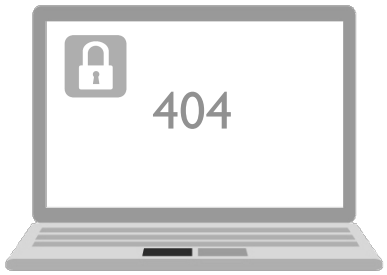
Funktions-sicherheit	Datenschutz	Informations-sicherheit
▪ Störungssicherheit ▪ Fehlertoleranz	▪ Anonymität ▪ Pseudonymität ▪ Unverknüpfbarkeit ▪ Unbeobachtbarkeit	▪ Verfügbarkeit ▪ Vertraulichkeit ▪ Integrität ▪ Authentizität ▪ Autorisierung ▪ Nicht-Abstreitbarkeit
> Schutz des Systems vor unkontrollierbaren Zuständen	> Schutz der System- und Nutzerdaten vor dem Missbrauch durch Dritte	> Schutz des Systems vor beabsichtigten Angriffen

Ziele der Funktionssicherheit

- Funktionssicherheit
  - > System darf nicht in einen unkontrollierten Zustand geraten
  - > erfordert risikomindernde Maßnahmen
  - > nicht dazu gehören Katastrophenschutzmaßnahmen

- Störungssicherheit
  - > Sicherheit des Systems vor/während Störungen

- Fehlertoleranz
  - > Sichere Nutzung des Systems trotz möglicher Fehler

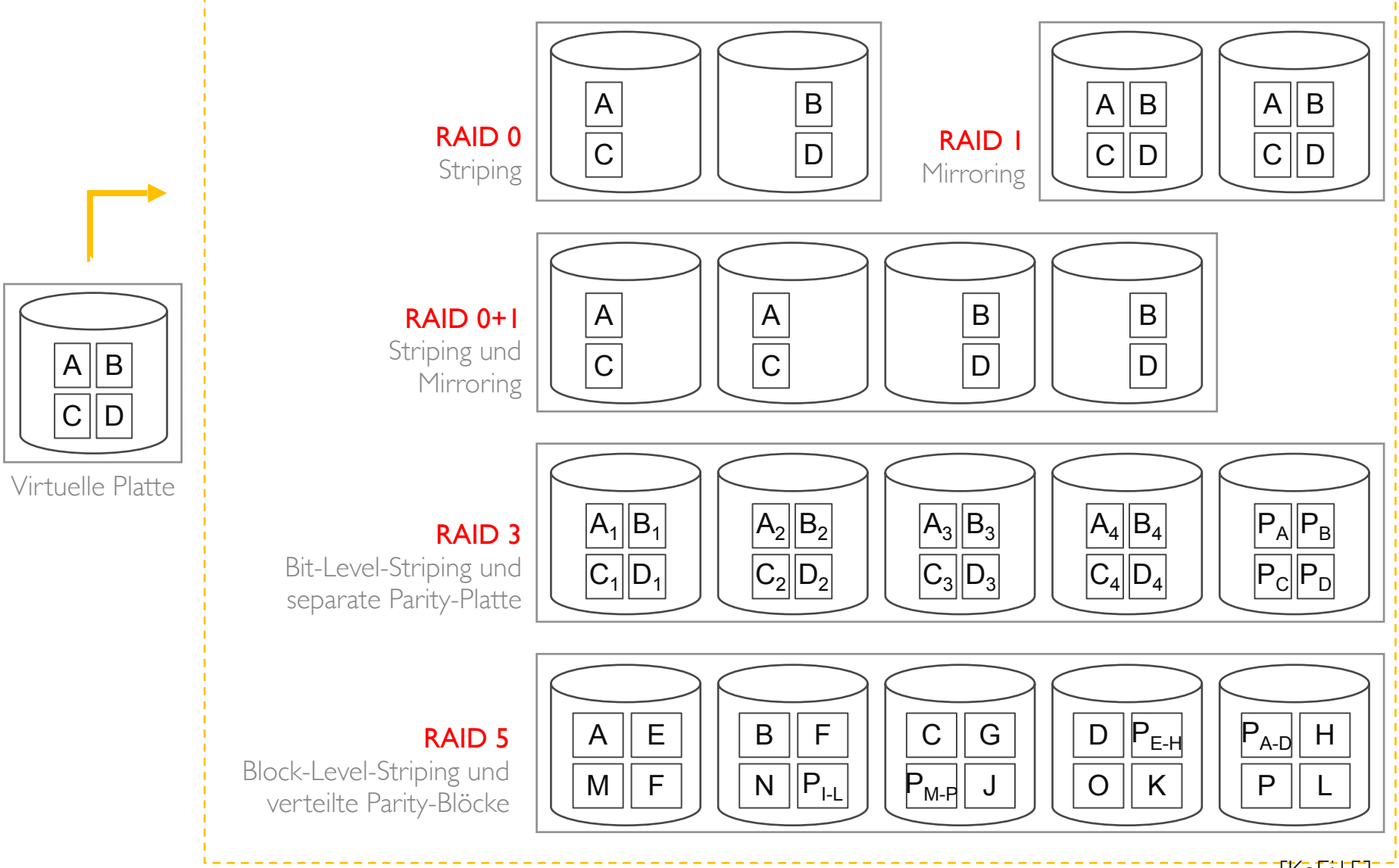


RAID: Sicherheit durch Speicherarrays

- RAID-Technologie
  - > RAID: Redundant Array on Inexpensive Disks
  - > Erzeugung von Datenredundanz und/oder -verteilung
- Funktionsweise
  - > effizienter Parallelbetrieb mehrerer kleiner, günstiger Laufwerke mit vielen unabhängigen Schreib- und Leseköpfen
  - > *ein* logisches (virtuelles) Laufwerk mittels RAID-Controller
  - > Unterscheidung in acht verschiedene *RAID-Levels*
    - » 0, 1, 2, 3, 4, 5, 6 sowie 0+1
- Nutzen
  - > Risikoverteilung zur Vermeidung von Datenverlust
  - > verbesserte Lastbalancierung der eingesetzten Platten
  - > Erhöhung der mittleren Zeitdauer bis zur nächsten DB-Recovery
    - » macht Archivierung und Protokollierung aber nicht obsolet

[KeEi15]

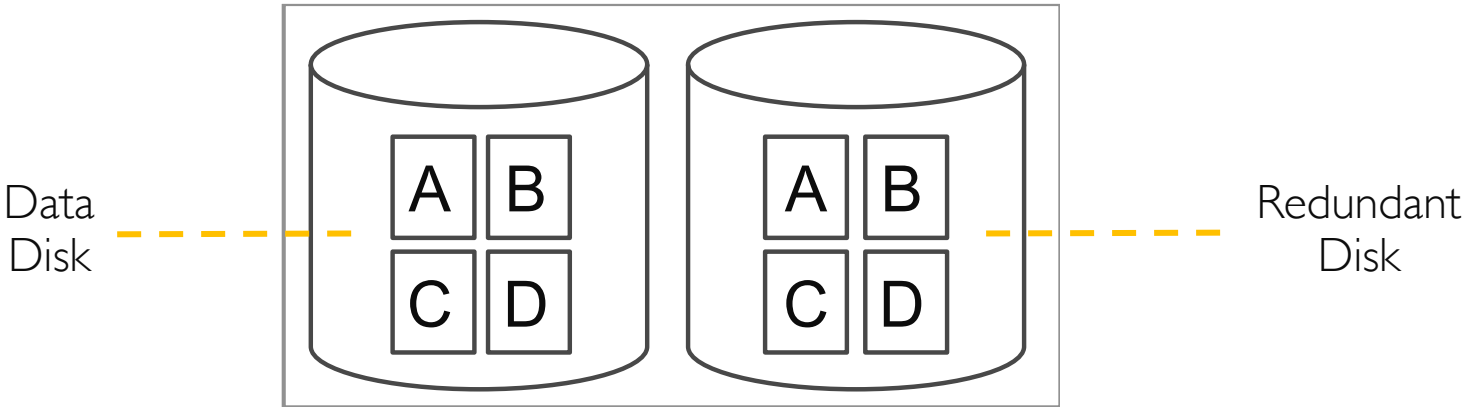
Datenverteilung bei verschiedenen RAID-Levels



[KeEi15]

RAID 1 (Mirroring)

- Eigenschaften
  - > Datensicherheit durch Redundanz *aller* Daten
  - > doppelter Speicherbedarf
  - > Lastbalancierung beim Lesen
  - > Möglichkeit des "konkurrierenden Lesens"



[Naum15]

Vergleich der RAID-Level

	Block-Striping	Bit-Striping	Kopie	Parität	Parität, dedizierte Disk	Verteilte Parität
RAID 0	x					
RAID 1			x			
RAID 0+1	x		x			
RAID 2		x				
RAID 3		x		x	x	
RAID 4	x			x	x	
RAID 5	x			x		x

- Insbesondere RAID 1 und RAID 5 sehr weit verbreitet
  - > RAID 1: einfach und schnell realisierbar, hohe Ausfallsicherheit, hohe Geschwindigkeit, doppelter Platzbedarf
  - > RAID 5: relativ schwierig realisierbar, hohe Ausfallsicherheit, hohe Geschwindigkeit, nur geringfügig erhöhter Platzbedarf, mindestens 3 Disks nötig

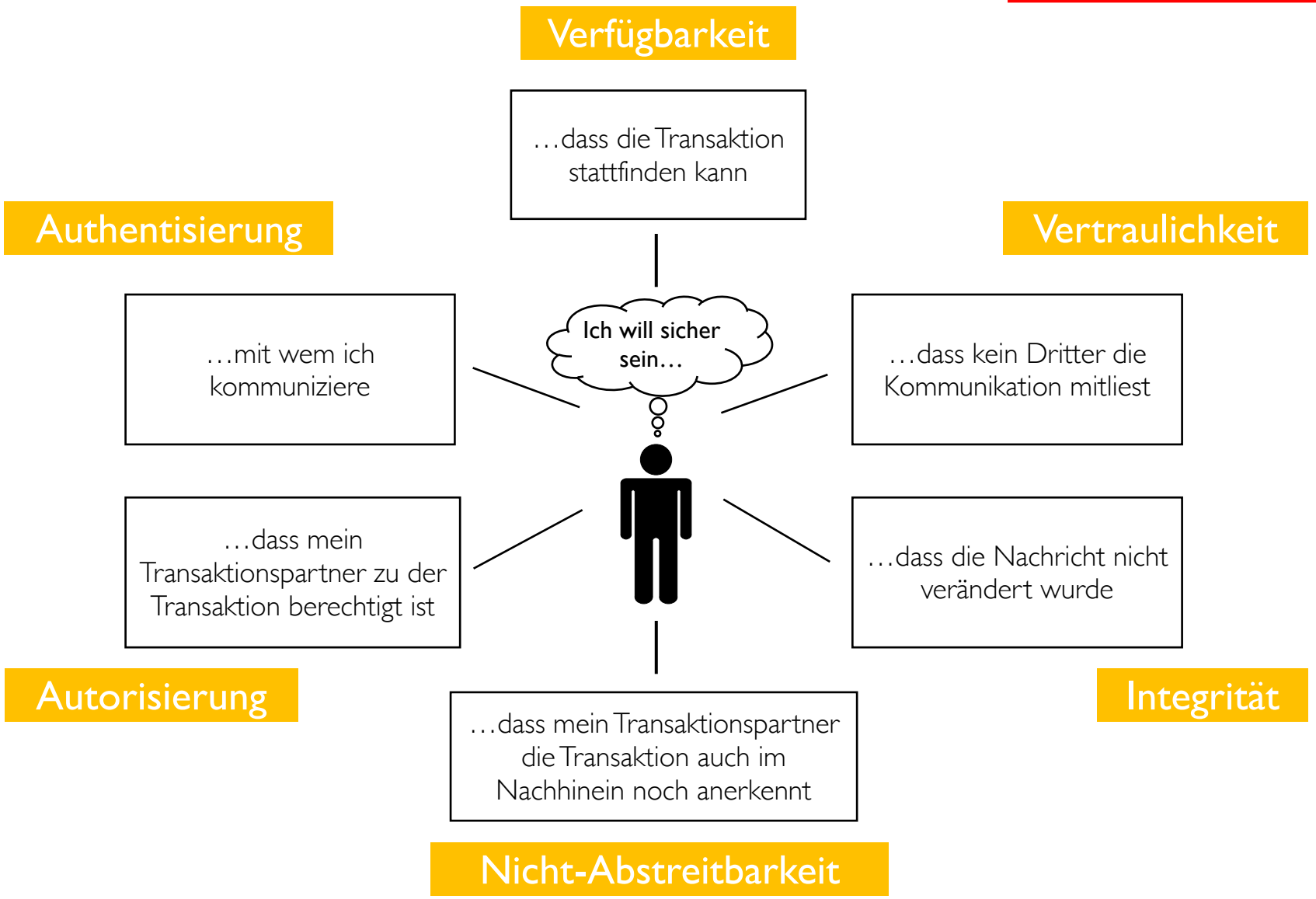
[Naum15]

Ziele des Datenschutzes

- Anonymität
  - > Verhinderung der Nutzeridentifikation durch externe Dritte
- Pseudonymität
  - > Systeminterne Verhinderung der Nutzeridentifikation
- Unverknüpfbarkeit
  - > Unabhängige Inanspruchnahme mehrerer Dienste
- Unbeobachtbarkeit
  - > Nichtfeststellbarkeit von Transaktionen

Ziele der Informationssicherheit

Informations-
sicherheit



Autorisierung

- Zweck
  - > Vergabe des Rechts, auf Ressourcen zuzugreifen
- Umsetzung
  - > Einrichtung von Zugriffsbarrieren auf Ressourcen
  - > Zugriff erfolgt erst nach Überwindung der Barrieren
- Unterscheidung nach Zugriffsform
  - > Berechtigungsbasiertes Zugriffskonzept
    - » Zugriff auf Objekte kann nur erfolgen, wenn explizit durch Autorisierungsregeln erlaubt
  - > Rollenbasiertes Zugriffskonzept
    - » Zugriff auf Objekte erfolgt implizit durch hierarchische Anordnung von Subjekten, Objekten und Operationen

Berechtigungsbasiertes Zugriffskonzept

- Zugriffsberechtigung
  - > erfolgt durch Erfüllung individueller Autorisierungsregeln
  - > erfordert Einzelfallprüfung
    - » zeitlich, sachlich, örtlich
  - > Sicherheitsstrategie: Discretionary Access Control (DAC)
- Autorisierungsregeln
  - > Regelung erlaubter Zugriffsarten auf Sicherheitsobjekte durch Sicherheitssubjekte
  - > Sicherheitsobjekt
    - » passive Entität, die Informationen enthält
    - » z.B. Tupel, Attribut
  - > Sicherheitssubjekt
    - » aktive Entität, die Informationsfluss bewirkt
    - » z.B. Benutzer(gruppe), DB-Prozess, Anwendungsprogramm

[KeEi15]

Discretionary Access Control (DAC)

- Konzept
  - > Angabe der Zugriffsarten *t* eines Subjektes *s* auf ein Objekt *o*
  - > Speicherung mithilfe von Zugriffsmatrizen
    - » Größe abhängig von Granularität der Autorisierung
  - > Durchsetzung der Regeln mittels *Sichten*
- Elemente und Regeln
  - > *o* : Objekt (z.B. Relation, Tupel, Attribut)
  - > *s* : Subjekt (z.B. Benutzer, Prozess)
  - > *t* : Zugriffsrecht (z.B. lesen, schreiben, löschen)
  - > *p* : Prädikat für *o* (z.B. *Rang* = "C4" für Relation *Professoren*)
  - > *f* : Weitergabe von Zugriffsrechten von *s* auf *s'*
- Nachteil
  - > Betrachtung des Datenerzeugers als Eigner bzw. Verantwortlichen für die Datensicherheit

[KeEi15]

Beispiel: Zugriffskontrolle in SQL

- Rechtevergabe
  - > GRANT
    - » SELECT, UPDATE, DELETE, INSERT, REFERENCES
  - > Beispiele:

```
GRANT SELECT
ON Studenten
TO Dehnert;
```

```
GRANT UPDATE (MatrNr, VorlNr, PersNr)
ON pruefen
TO Dehnert;
```

- Weitergabe von Rechten
  - > WITH GRANT OPTION

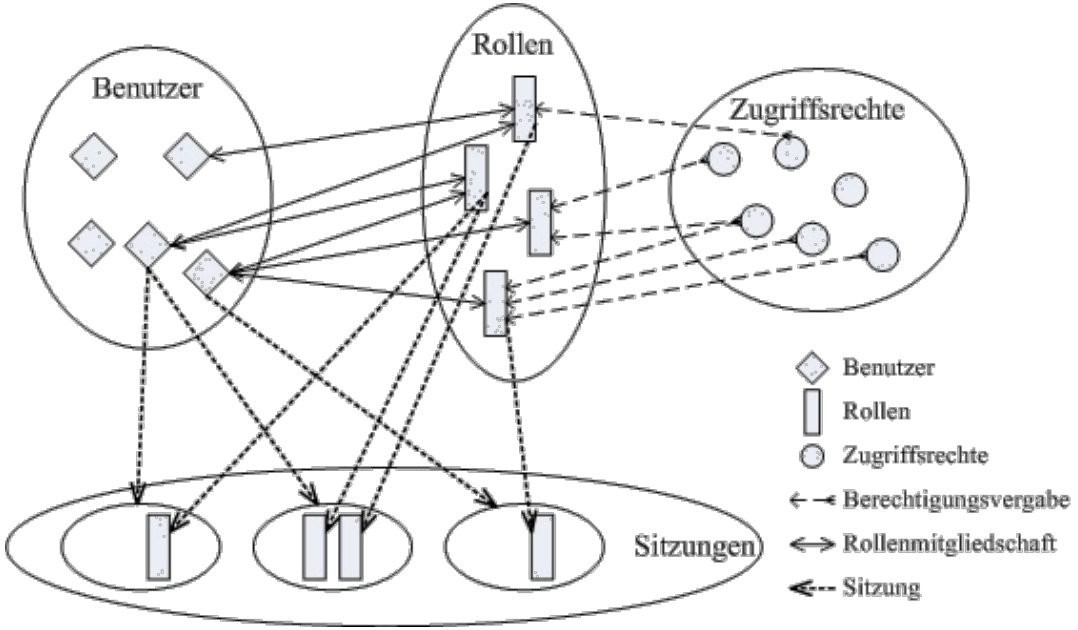
- Entzug von Rechten
  - > REVOKE
  - > Beispiel:

```
REVOKE UPDATE (MatrNr, VorlNr, PersNr)
ON pruefen
FROM Sekretariat CASCADE;
```

[KeEi15]

Rollenbasiertes Zugriffskonzept

- Zugriffsberechtigung
  - > erfolgt durch Zugehörigkeit zu einer berechtigten Gruppe
  - > erfordert Orchestrierung
    - » Zugriffsberechtigungsverwaltung bei der Zusammenarbeit von verschiedenen Mitarbeitern



[KeEi15]

Mandatory Access Control (MAC)

- Konzept
  - hierarchische Klassifizierung Sicherheitseinstufung von Subjekten *s* und Objekten *o*
    - Subjekte nach Rang oder Vertrauenswürdigkeit: *clear(s)*
    - Objekte nach Sicherheitsrelevanz oder Sensitivität: *class(o)*
- Elemente und Regeln
  - $class(0) \leq clear(s)$
    - ein Subjekt s darf ein Objekt o nur lesen, wenn das Objekt eine geringere Sicherheitseinstufung hat
  - $clear(s) \leq class(o)$
    - Ein Objekt o muss mit mindestens der Einstufung des Subjektes s geschrieben werden
- Nachteile
  - Zusammenarbeit von Nutzern unterschiedlicher Klassifizierung
  - Sicherheitseinstufung jedes Objektes erforderlich

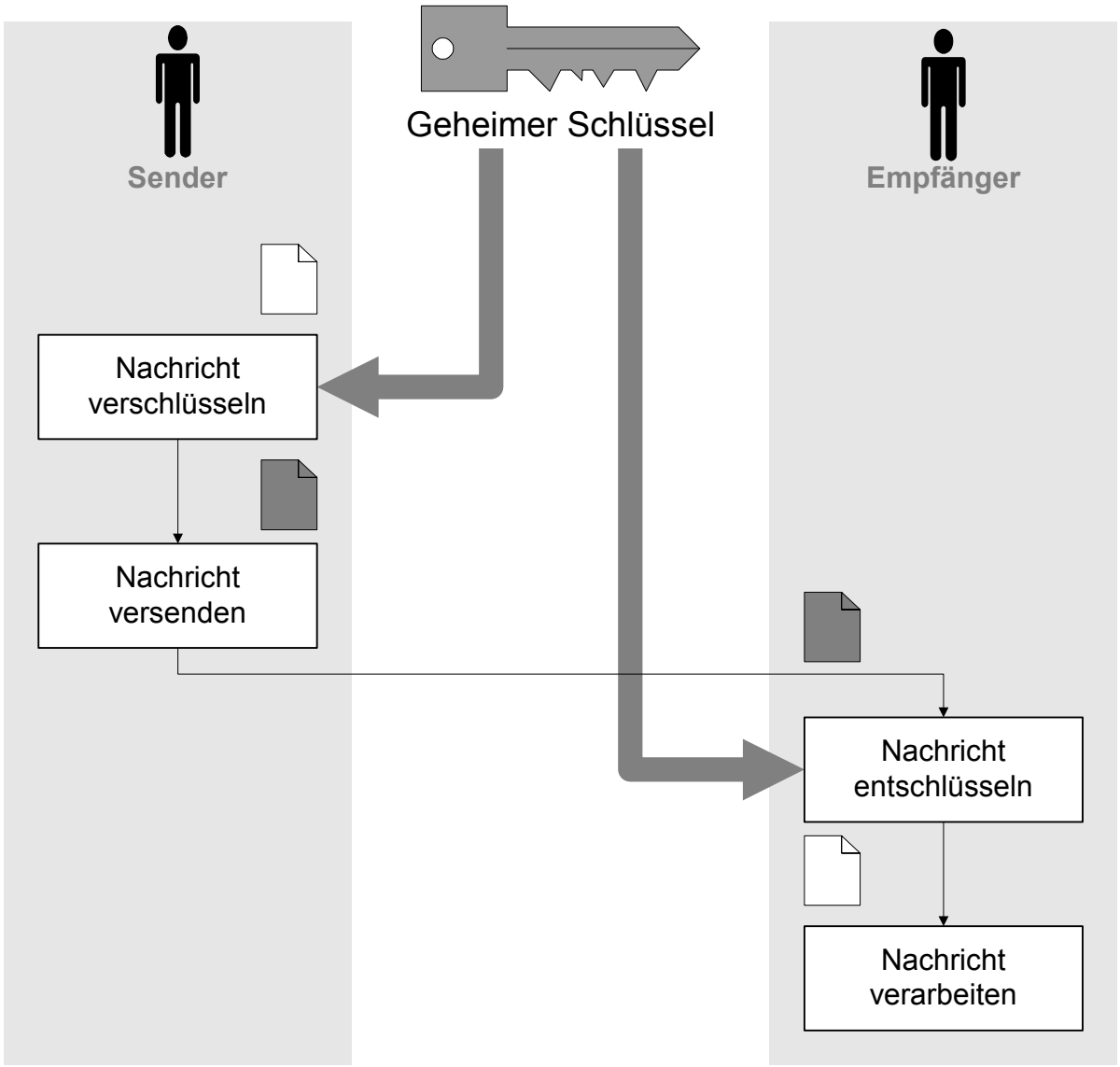
[KeEi15]

Vertraulichkeit

- Zweck
  - > Verhinderung eines nicht autorisierten Zugriffs auf Daten

- Techniken
  - > Virtual Private Network (VPN) für Übertragungssicherheit
  - > Verschlüsselung der zu übertragenden Nachrichten
  - > Kryptographische Methoden
    - » Symmetrische Verfahren
    - » Asymmetrische Verfahren

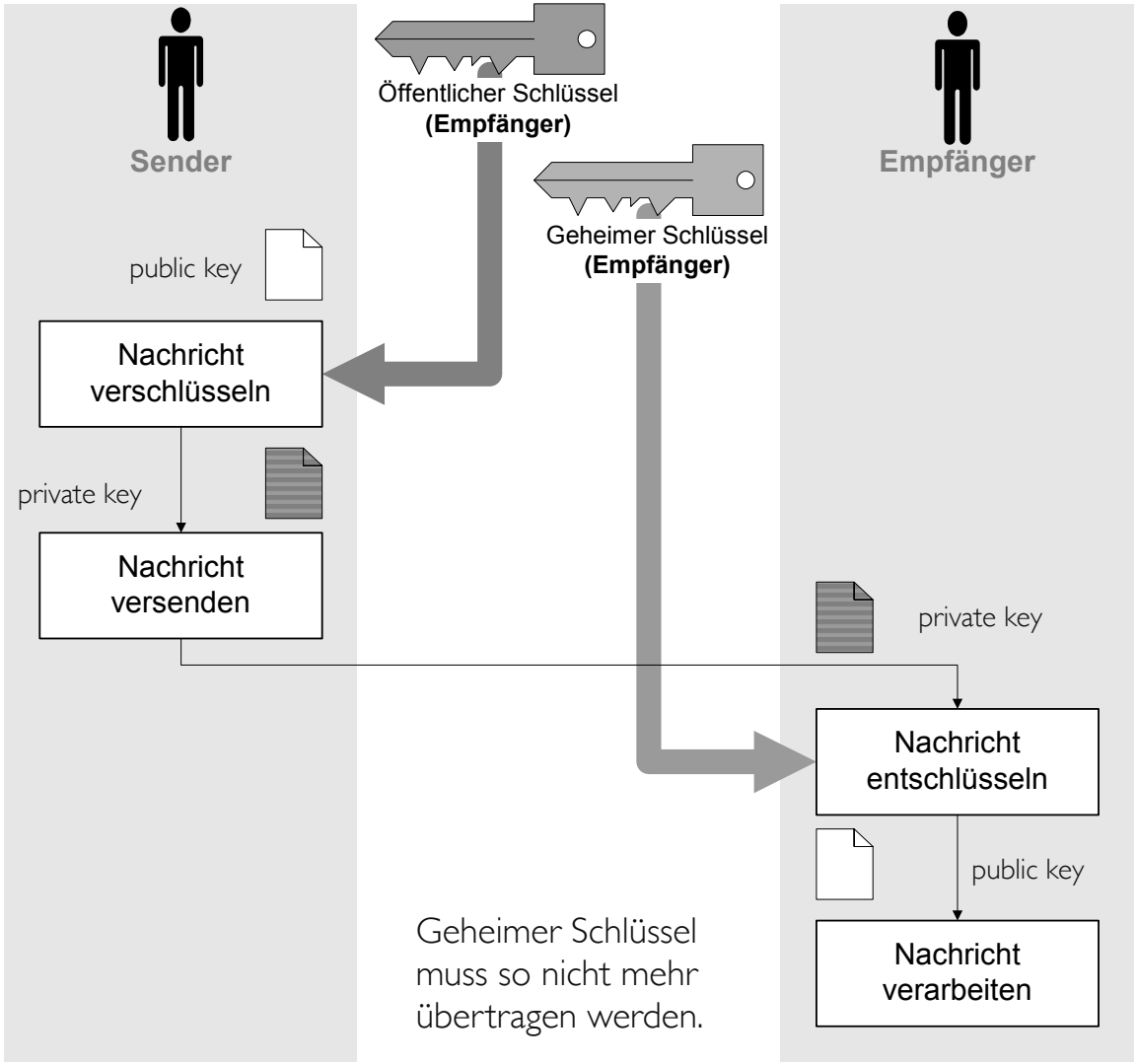
Kryptographie: Symmetrische Verfahren



Merkmale symmetrischer Verfahren

- Vor der Kommunikation
  - > Transport des Schlüssels notwendig
  - > Nutzung eines sicheren Kanals (z.B. USB-Stick)
- Gefahr, dass der Schlüssel in die Hände Dritter gelangt
- Benötigen gegenüber asymmetrischen Verfahren geringeren Rechenaufwand
- Sind leichter zu brechen (Kryptoanalyse)

Kryptographie: Asymmetrische Verfahren



Beispiel: Öffentlicher Schlüssel

- Zeitschrift c't (RSA, 1024 Bit (ASCII))

```
-----BEGIN PGP PUBLIC KEY BLOCK----- Version: PGP 6.0.2
mQCNAzMcNVcAAAEEAL3j6odz6MHhvCH2aGlSq31JVChaULaaWmzGGSE0QWKrA5wN
y6TqEwsOM26DkIAsCGXiFPe5rJSk3l/fiiRz/
KoJEV3himvCppW+rJUN8bVmjVdl /oaYKK2frFRQ+peZLWHVfPq0WMcK6/
KhyrQF1BZ2xbjvEjdvLES43da7HZ9tAAUR
tCtjdCBtYWdhemluZSBDRVJUSUZJQ0FURSA8cGdwQ0FAY3QuaGVpc2UuZGU+iQEV
AwUTNCrGBXtrpmPYdZxlAQFj3ggAruN469ENifRkK1qBAwYKF7t0SmA8C7YynoL+
HgTnpzfHXJLcACsCupHiJ59uKlB0Pib9NLHQi8zYowB50mZV+Bk+T253B4jmc8IM
3Su2x9sP/nA55TMrV/mjcFMosA+DqnwtCHXueioqiU2xRezBiXDyXHXdGtXHvGLA
nQK+G2kGPYg+wyi/hu3uC35a6Rc7pejg3km7pH/HRjy5jh+5XmQ5igz4ao1/v7N8
8t8G5YLprVQ9wJNvvxXnOOn5cgBqxp+V0D1CQRfvhLrhcHfgslaJYG2v481zPxoI
UBMp0HJFdLY+N5egk7oLMlRrAfv5Hrkrr3vsaWzbQDUOx0jJhYkAlQMFEDMdM9Y2
DLIHXGfJqQEBwsYEAMaXOLTtjYronfHxR8g3Pxg6lJ/6ivK2PvKfer031YHpoB6/
8RR/YDicdfwIOAMz/Cmzy9tMA7fC9Um1rYCmDTeQmOF95xGiQZ50AEZ8BTgf1I0F
2oYsgdkP79ZAqnctCgHEP+81M+I+BqVhyw7LrBJrzmSv96gqyL4wacJh2OKAiQCV
AwUQMxw1WkS43da7HZ9tAQFrDQQAglvoRTdjRzpz3aX6HcAMlFtQUJdwSV+D6KRO
nsMMJBF14dpEpfyNH+8g2smpLOrB3wu3xPZOCY4W0Gd5mmd4WNVRC7B7oQPqR4OL
r6pWJxMuwxUtPC8iD7ypC/GYHhzJ4PlhUZ9yTuV9UM3rCKP4m0P2Ivx5jWs/Af4v
2/sUdiCJARUDBRA1x0mQc893jFfBww0BAShdCADG6EyX3MBAC3o4vkvHEHmagAzn
ilHLg2pIA3rrVTRHGEruCv4Hnapg+H6rILucPlx52l29wY1/uLmrzNO3qbhfn+2n
u6Ji0KHpGYWIk097C/xTewaHq6wzlsOff2aiRpNvTLL/YUd+HWW4fQCvJkPDOsR9
LDgvBjrLYKjit5YsYAb/DSwt9jGRrh/nFp97NXPq1N8HbyXO/jXNE2HKQ0kAfgyX
NB/L25vlxB318MPaPBTWwA/SngbHsJ66k1ClxJMNHwI+c8lDcwtWEdYEZ/5t/5uY
bPGVkcovTp4jVfiVpyEYuynWB/9yqs/J8bbUGDP5/GpvRYXAUCKi4YelOy5CiQEV
AwUQNRt4rqHjr5012/VlAQFGNwf/V+cvpZgbpkroFyn7YyllRTBk4ivC5aUqzmYN
tR1e8lyv5Ts/ZgjjmJfCDjTojMVckbLJiY7TdCltJQzUEU0d4se/JxSp8vvljiZL
FQ9aohzcvz08+1nnIITaVnuTj9CO4niHtwSRasnGUtiDsPtqqHsOJ74GblONZ5eN
ZGTxvonkSFISP6CCHiB/aBadY0Kt50jI+g9Pe9J+Kk7sXH8XvCYlpTTZKu13wxDM
FkzqEqi7M951Uxu1wVQF1FXSnKVpk25f0OqXAMKOBg+l3EU/e+JdC6zAYApUMXhZ
YAe8QnrJaOzmKAs0C1bcSsZM52Xrf61xh6hEDRuJ3f/Gxau9ZYkASgQQEQIACgUC
Nzk0AAMFAXgACgkQ29JF/LOyoSxJsACfV3wiVlw/tibzc7vaeH7FSJANzOIAn006
cpoh0rT96Or3GvZVQTT/jtXA =1/zJ -----END PGP PUBLIC KEY BLOCK-----
```

Merkmale asymmetrischer Verfahren

- Gegenüber symmetrischen Verfahren höhere Sicherheit
- Kein Transport der geheimen Schlüssel notwendig
- Hoher Rechenaufwand für Ver- und Entschlüsselung
- Erfordert eine *Public Key Infrastructure (PKI)*
  - > Typisches Beispiel: *PGP (Pretty Good Privacy)*

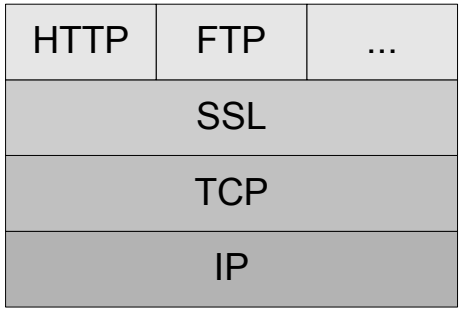
Hinweis:

Der Begriff "privater Schlüssel" existiert nicht, sondern ist eine Fehlübersetzung von "Private Key" (geheimer Schlüssel), die sich aber inzwischen vielfach verbreitet hat

Hybrid-Verfahren

- Beschreibung
  - > pragmatische Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren
- Umsetzung und Merkmale
  - > Verwendung eines asymmetrischen Verfahrens zum Transport eines Schlüssels für ein symmetrisches Verfahren
    - » erfordert häufiges Wechseln der Schlüssel
    - » Abstand wenige Minuten bis einige Stunden
  - > sicherer als symmetrisches Verfahren
  - > geringerer Rechenaufwand als asymmetrisches Verfahren
- Typisches Beispiel
  - > Secure Socket Layer (SSL) / Transaction Layer Security (TLS)

Secure Socket Layer (SSL)



- Entwickelt von Netscape
- Zweck
  - > Bereitstellung eines *sicheren* (verschlüsselten) Kanals auf der Basis von TCP
  - > sichere Ende-zu-Ende-Kommunikation möglich
- Vorgehensweise
  - > beim Verbindungsaufbau authentisieren sich Client (optional) und Web-Server und handeln mittels eines asymmetrischen Verschlüsselungsverfahrens einen Sitzungsschlüssel aus
- Erkennungszeichen (im Browser)
  - > Protokoll HTTPS, Port 443 an Stelle von HTTP, Port 80

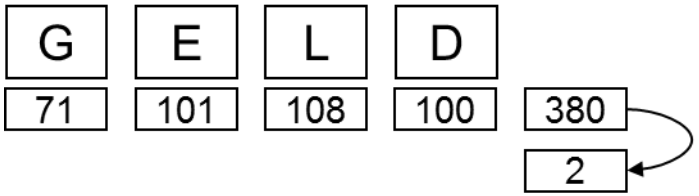
Integrität

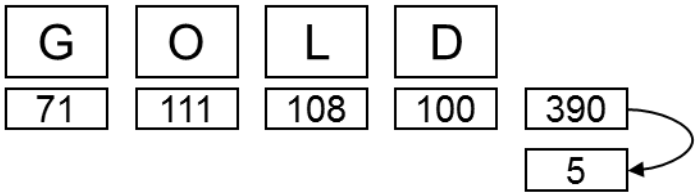
- Zweck
  - > Sicherstellen, dass eine Nachricht (auf ihrem Weg von Sender zu Empfänger) nicht verändert wurde
- Techniken
  - > Ermittlung des "Fingerabdrucks" einer Nachricht = Berechnung eines Hash-Werts (z.B. Quersumme)
  - > Transport des Hash-Werts auf einem sicheren Kanal
- Hash-Wert
  - > Zahl, die für eine Nachricht charakteristisch ist
    - » Veränderung der Nachricht führt (i.d.R.) zu anderem Hash-Wert
    - » Vermeidung von Kollisionen
      - zwei unterschiedliche Eingabewerte führen zu gleichem Hash-Wert

Beispiel für eine Hash-Funktion

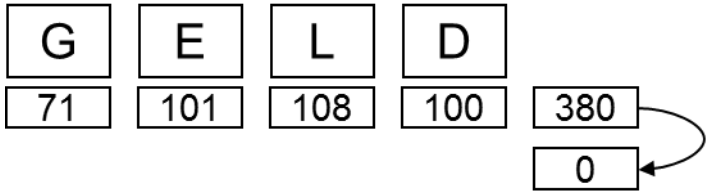
A	65	G	71	M	77	S	83	Y	89
B	66	H	72	N	78	T	84	Z	90
C	67	I	73	O	79	U	85		
D	68	J	74	P	80	V	86		
E	69	K	75	Q	81	W	87		
F	70	L	76	R	82	X	88		

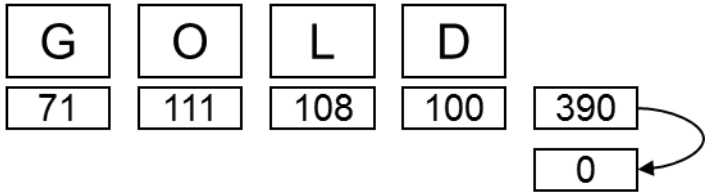
- Beispiel
  - > y mod x = Restwert, der bei ganzzahliger Division von y durch x entsteht
  - > Hashwert: (∑ ASCII(Buchstabe)) mod 7





  - > Kollision bei: (∑ ASCII(Buchstabe)) mod 10

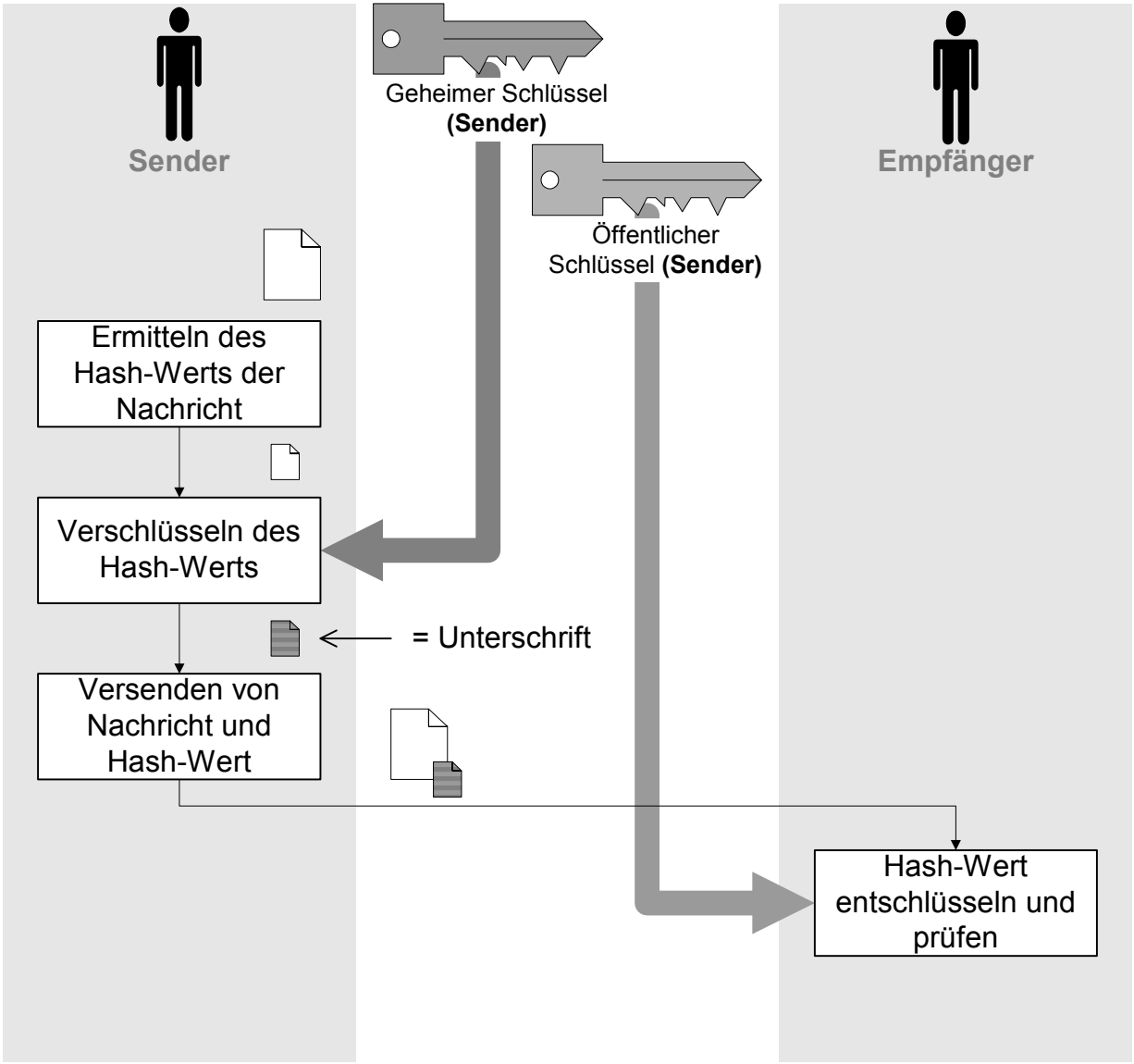




Authentisierung

- Zweck
  - > Zweifelsfreier Nachweis der Identität eines Transaktionspartners
- Nachweis der Identität durch
  - > Besitz, z.B. Magnetkarte, Schlüssel ...
  - > Wissen, z.B. Passwort, PIN-Code
  - > Eigenschaft, z.B. biometrische Merkmale

Elektronische Signatur: Nachweis der Authentizität



Zertifikate

- Deutsches Signaturgesetz
  - "Ein Zertifikat [...] ist eine mit einer digitalen Signatur versehene Bescheinigung über die Zuordnung eines öffentlichen Signatur-schlüssels zu einer natürlichen Person (Signaturschlüssel-Zertifikat) oder eine gesonderte digitale Bescheinigung, die unter eindeutiger Bezugnahme auf ein Signaturschlüssel-Zertifikat weitere Angaben enthält (Attribut-Zertifikat)."

- Haupteinsatzgebiet für Zertifikate
  - Authentizitätsnachweis für öffentliche Schlüssel
  - Ausstellung durch vertrauenswürdige, unabhängige Partei
  - Zertifizierungsstellen in Deutschland z.B.
    - Deutsches Forschungsnetz
    - Heise Verlag
    - TC TrustCenter

Aufgaben einer Zertifizierungsautorität

- Registrierung von Personen und deren öffentlicher Schlüssel
- Einrichtung eines (Online-)Dienstes zur automatischen Verifikation von Schlüsseln an Hand von Zertifikaten
- Verwaltung von Schwarzen Listen für ungültige Zertifikate
- Ansätze für gegenseitige Anerkennung von Zertifikaten
  - > Trust Network
    - » Teilnehmer zertifizieren sich gegenseitig
  - > Hierarchie
    - » weltweite Wurzel-Zertifizierungsstelle, darunter nationale Zertifizierungsstellen usw.
  - > Wald
    - » Beliebig viele Wurzel-Zertifizierungsstellen, die sich gegenseitig zertifizieren

Signaturgesetz: Angaben in einen Zertifikat

- Eindeutiger Name des Signaturschlüssel-Inhabers
- Der zugeordnete öffentliche Signaturschlüssel
- Bezeichnung der Algorithmen, mit denen die öffentlichen Schlüssel von Zertifizierungsstelle und Signaturschlüssel-Inhaber benutzt werden können
- Laufende Nummer des Zertifikats
- Gültigkeitszeitraum des Zertifikats
- Name der Zertifizierungsstelle
- Angaben zur Einschränkung des Signaturschlüssels auf bestimmte Anwendungen

Weitere Anwendungen für Zertifikate

- Rollenzertifikate
  - > Ausstellen von *Vollmachten* an Dritte
- Auszeichnungen
  - > beste Webseite, bestes Produkt, usw.
- Zusicherung von *Eigenschaften* bei Programmen
  - > bei Java Applets, Active-X-Komponenten usw.
- Einstufung
  - > Einstufung eines Angebots, z.B. hinsichtlich Eignung für Minderjährige
- Zeugnisse, Qualifikationsnachweise usw.

Zertifikate und Subjektive Sicherheit

- Beispiel: Gütesiegel aus Kundensicht

(963<n>981, Skala: 1 = stimme überhaupt nicht zu, 4 = stimme voll und ganz zu)

[ECC Handel, 2012]

Grundlegende Angriffstechniken

- Ziele eines Angreifers
  - unbefugtes Lesen von Daten (Ausspähen)
  - unbefugtes Verändern von Daten (Manipulieren)
  - unbefugte bzw. kostenlose Dienstnutzung
- Beispiele für Angriffstechniken
  - Klassisches Auskundschaften
  - Malware
  - Exploit
  - Brute-Force Attack
  - Man-in-the-Middle Attack
  - Denial-of-Service Attack
  - SQL-Injection

Konkrete Angriffstechniken (1)

- Malware
  - > Schadprogramme zur Veränderung oder zum Fernzugriff der System- oder Anwendungssoftware des Anwenders
  - > Virus: Änderung der System- oder Anwendungssoftware und Reproduktion mithilfe des Anwenders
  - > Wurm: Änderung der System- oder Anwendungssoftware und Reproduktion durch Ausnutzung von Schwachstellen
  - > Trojaner: Software, die unter falschem Vorwand vom Anwender installiert wird und unbemerkt Fernzugriff ermöglicht
- Exploit
  - > Ausnutzung von Schwachstellen in der Datenübertragung, im Betriebssystem, in der Middle- oder Anwendungssoftware
  - > Local Exploit zur Erlangung privilegierter Nutzerrollen z.B. zur Installation von Schadsoftware
  - > Remote Exploit zum irregulären Netzwerkzugang

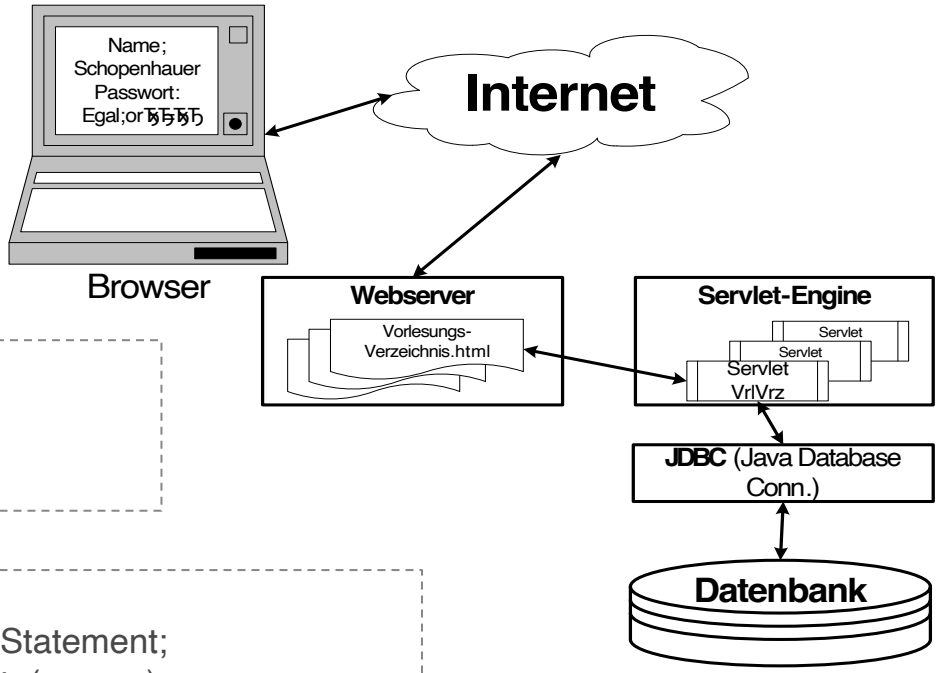
Konkrete Angriffstechniken (2)

- Brute-Force-Attack
  - > schnelles, automatisierte Wechseleingabe von Bitfolgen zur Dekodierung von Passwörtern und Zugangsschlüsseln
- Man-in-the-Middle Attack
  - > eine dritte Partei schiebt sich unbemerkt zwischen zwei Kommunikationspartner, fängt Daten ab und leitet (ggf. andere/ veränderte) Daten weiter
- Denial-of-Service Attack (DoS)
  - > Überlastung des angegriffenen Systems durch
    - » Senden von (absichtlich gewählten) ungültigen Pakten
    - » Senden von übermäßig vielen (sinnlosen) Paketen
  - > verteilter Angriff als Distributed DoS (DDoS) möglich

Konkrete Angriffstechniken (3)

- SQL-Injection
  - > Eintragung von SQL-Anfragen in das Benutzer-Eingabefeld
  - > bei fehlender Kontrolle erfolgt unbefugter Zugriff auf die DB
    - » Ausspähen, Manipulation oder größere Schäden möglich
  - > Beispiel: SQL-Injection über Webinterface:

```
String _name = ... Auslesen aus der Session
String _pwd =  ... Auslesen aus der Session
```




```
String _query =
 "SELECT * " + "FROM Studenten s JOIN prüfen p
  ON s.MatrNr = p.MatrNr" + "WHERE s.Name = '"
  + _name + "' AND s.Passwort = '" + _pwd +"';";
```

Initialisiere Connection c:

```
Statement stmt = c.createStatement;
ResultSet rs = stmt.execute(_query);
```

Beispiel: SQL-Injection-Attacke

Name: Schopenhauer

Passwort: Egal'; **update** pruefen **set** Note = 1 **where** MatrNr = 25403;

```
SELECT *
  FROM Studenten s JOIN prüfen p
  ON s.MatrNr = p.MatrNr
  WHERE s.Name = "Schopenhauer"
  AND s.Passwort = "Egal";
  UPDATE prüfen SET Note = "1"
  WHERE MatrNr = "25403";
```

pruefen

MatrNr	PersNr	VorlNr	Note
28106	5001	2126	1
25403	5041	2125	~~5~~ 1
27550	4630	2137	2

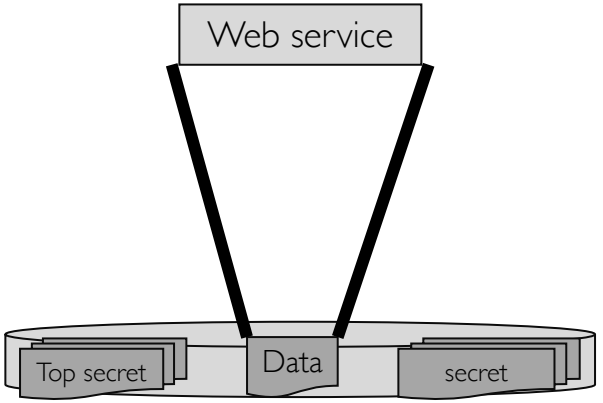
Schutz vor SQL-Injection-Attacken

- SQL-Verwendung über sog. *Prepared Statements*
  - > vorbereitete Anweisung für ein DBS
  - > Platzhalter an DBS übergeben
  - > DBS prüft die Gültigkeit von Parametern vor deren Verarbeitung

```
PreparedStatement
stmt = conn.prepareStatement(
 "SELECT * FROM Vorlesungen v JOIN Professoren p
 ON v.gelesenVon = p.PersNr
 WHERE v.Titel = ? AND p.Name = ? ");
String einzulesenderTitel = "Logik";
String einzulesenderName = "Sokrates";
 stmt.setString(1, einzulesenderTitel);
 stmt.setString(2, einzulesenderName);
 ResultSet rs = stmt.executeQuery();
```

- Filterung der Eingabe-Parameter

- Restriktive Autorisierungskorridore für den Datenzugriff durch Anwendungen



Literaturverzeichnis

Literaturverzeichnis

[Bapp14] Bappalige, O. (2014). Introduction to Apache Hadoop. URL: https://opensource.com/life/14/8/intro-apache-hadoop-big-data

[BEPW16] Backhaus, K., Erichson, B., Plinke, W., Weiber, R. (2015). Multivariate Analysemethoden: Eine anwendungsorientierte Einführung. Springer-Verlag.

[Dave14] Davenport, T. (2014). Big data at work: dispelling the myths, uncovering the opportunities. Harvard Business Review Press.

[EFH+11] Edlich, S., Friedland, A., Hampe, J., Brauer, B., Brückner, M. (2011). NoSQL: Einstieg in die Welt nichtrelationaler Web 2.0 Datenbanken. Hanser.

[FaEg05] Fassott, G., Eggert, A. (2005). Zur Verwendung formative und reflektiver Indikatoren in Strukturgleichungsmodellen, in: Handbuch PLS- Pfadmodellierung. Schäffer Poeschel.

[FaPS96] Fayyad, U. M., Piatetsky-Shapiro, G., Smyth, P. (1996, August). Knowledge Discovery and Data Mining: Towards a Unifying Framework. In KDD (Vol. 96, pp. 82-88).

[FHKo17] Fachhochschule Köln (2011). Datenbanken Online Lexikon. URL: http://wikis.gm.fh-koeln.de/wiki_db/Datenbanken

Literaturverzeichnis

[GaUW08] Garcia-Molina, H., Ullman, J. D., Widom, J. (2008). Database Systems: The Complete Book. Pearson International.

[GMPB+09] Ginsberg, J., Mohebbi, M. H., Patel, R. S., Brammer, L., Smolinski, M. S., & Brilliant, L. (2009). Detecting influenza epidemics using search engine query data. Nature, 457 (7232), 1012-1014.

[HaKa06] Han, J., Kamber, M. (2006). Data mining: concepts and techniques. Morgan Kaufmann.

[Harr15] Harrison, G. P. (2015). Next Generation Databases - NoSQL and Big Data. Apress.

[JZFF11] Jannach, D., Zanker, M., Felfernig, A., & Friedrich, G. (2010). Recommender Systems: An Introduction. Cambridge University Press.

[KeBM10] Kemper, H. G., Baars, H., Mehanna, W. (2010). Business Intelligence: Grundlagen und praktische Anwendungen. Vieweg.

Literaturverzeichnis

[KeEi15] Kemper, A., Eickler, A. (2015). Datenbanksysteme. Oldenbourg.

[KrGL05] Kraft, M., Götz, O., Liehr-Gobbers, K. (2005). Die Validierung von Strukturgleichungsmodellen mit Hilfe des Partial-Least-Squares-Ansatzes, in: Handbuch PLS-Pfadmodellierung. Schäffer Poeschel.

[KuJo13] Kuhn, M., Johnson, K. (2013): Applied Predictice Modeling. Springer.

[LKKV14] Lazer, D., Kennedy, R., King, G., Vespignani, A. (2014). The parable of Google Flu: traps in big data analysis. Science, 343 (6176), 1203-1205.

[MBK+12] Mertens, P., Bodendorf, F., König, W., Schumann, M., Hess, T. (2012). Grundzüge der Wirtschaftsinformatik. Springer.

[Muel15] Müller, E. (2015). Vorlesungsskript: Big Data Analytics. Hasso-Plattner- Institut Potsdam.

[Naum15] Naumann, F. (2015). Vorlesungsskript: Datenbanksysteme II. Hasso-Plattner-Institut Potsdam.

Literaturverzeichnis

[O'Nei16] O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown Books.

[PäPa15] Pääkkönen, P., Pakkala, D. (2015). Reference architecture and classification of technologies, products and services for big data systems. Big Data Research, 2 (4), 166-186.

[Plat13] Plattner, H. (2013). A Course in In-Memory Data Management. Springer.

[PoBe13] Becker, L., Pousttchi, K. (2013). Requirements for personalized m-commerce - what drives consumers' use of social networks?. In: Journal of Electronic Commerce in Organizations 11 (2013) 4, S. 19-36.

[RaSS15] Rahm, E., Saake, G., & Sattler, K. U. (2015). Verteiltes und paralleles Datenmanagement: von verteilten Datenbanken zu Big Data und Cloud. Springer.

[RePi91] Reichwald, R., Picot, A. (1991). Informationswirtschaft, in: Heinen, E. (Hrsg.). Industriebetriebslehre: Entscheidungen im Industriebetrieb. Springer.

[Rupa16] Ruparelia, N. B. (2016). Cloud Computing. MIT Press.

Literaturverzeichnis

[RuQZ07] Rupp, C., Queins, S., Zengler, B. (2007). UML 2 glasklar: Praxiswissen für die UML-Modellierung. Carl Hanser.

[SaSH11] Saake, G., Sattler, K. U., Heuer, A. (2011). Datenbanken: Implementierungstechniken. mitp.

[SaSH13] Saake, G., Sattler, K. U., Heuer, A. (2013). Datenbanken: Konzepte und Sprachen. mitp.

[Sche97] Scheer, A. W. (1997). ARIS—vom Geschäftsprozess zum Anwendungssystem. Springer.

[StHa04] Stahlknecht, P., Hasenkamp, U. (2004). Einführung in die Wirtschaftsinformatik. Springer.

[Sull15] Sullivan, D. (2015). NoSQL for mere mortals. Addison-Wesley Professional.

[Thor13] Thor, A. (2013). Vorlesungsskript: Datenmanagement. Universität Leipzig.

Literaturverzeichnis

[Vige16] Vigen, T. (2016). Spurious Correlations. Hachette Books.

[Voss08] Vossen, G. (2008). Datenmodelle, Datenbanksprachen und Datenbank-Management-Systeme. Oldenbourg.

[WeKa16] Wedel, M., Kannan, P. K. (2016). Marketing analytics for data-rich environments. Journal of Marketing, 80(6), 97-121.

[Wies15] Wiese, L. (2015). Advanced Data Management: For SQL, NoSQL, Cloud and Distributed Databases. de Gruyter.

[Zehn13] Zehnder, C. A. (2013). Informationssysteme und Datenbanken. Springer.

[Zoss15] Zoss, A. (2015). Practical Data Visualization. Lecture at Duke University.

Literaturverzeichnis

Literaturverzeichnis

[Bapp14] Bappalige, O. (2014). Introduction to Apache Hadoop. URL: https://opensource.com/life/14/8/intro-apache-hadoop-big-data

[BEPW16] Backhaus, K., Erichson, B., Plinke, W., Weiber, R. (2015). Multivariate Analysemethoden: Eine anwendungsorientierte Einführung. Springer-Verlag.

[Dave14] Davenport, T. (2014). Big data at work: dispelling the myths, uncovering the opportunities. Harvard Business Review Press.

[EFH+11] Edlich, S., Friedland, A., Hampe, J., Brauer, B., Brückner, M. (2011). NoSQL: Einstieg in die Welt nichtrelationaler Web 2.0 Datenbanken. Hanser.

[FaEg05] Fassott, G., Eggert, A. (2005). Zur Verwendung formative und reflektiver Indikatoren in Strukturgleichungsmodellen, in: Handbuch PLS- Pfadmodellierung. Schäffer Poeschel.

[FaPS96] Fayyad, U. M., Piatetsky-Shapiro, G., Smyth, P. (1996, August). Knowledge Discovery and Data Mining: Towards a Unifying Framework. In KDD (Vol. 96, pp. 82-88).

[FHKo17] Fachhochschule Köln (2011). Datenbanken Online Lexikon. URL: http://wikis.gm.fh-koeln.de/wiki_db/Datenbanken

Literaturverzeichnis

[GaUW08] Garcia-Molina, H., Ullman, J. D., Widom, J. (2008). Database Systems: The Complete Book. Pearson International.

[GMPB+09] Ginsberg, J., Mohebbi, M. H., Patel, R. S., Brammer, L., Smolinski, M. S., & Brilliant, L. (2009). Detecting influenza epidemics using search engine query data. Nature, 457 (7232), 1012-1014.

[HaKa06] Han, J., Kamber, M. (2006). Data mining: concepts and techniques. Morgan Kaufmann.

[Harr15] Harrison, G. P. (2015). Next Generation Databases - NoSQL and Big Data. Apress.

[JZFF11] Jannach, D., Zanker, M., Felfernig, A., & Friedrich, G. (2010). Recommender Systems: An Introduction. Cambridge University Press.

[KeBM10] Kemper, H. G., Baars, H., Mehanna, W. (2010). Business Intelligence: Grundlagen und praktische Anwendungen. Vieweg.

Literaturverzeichnis

[KeEi15] **Kemper, A., Eickler, A. (2015). Datenbanksysteme. Oldenbourg.**

[KrGL05] Kraft, M., Götz, O., Liehr-Gobbers, K. (2005). Die Validierung von Strukturgleichungsmodellen mit Hilfe des Partial-Least-Squares-Ansatzes, in: Handbuch PLS-Pfadmodellierung. Schäffer Poeschel.

[KuJo13] Kuhn, M., Johnson, K. (2013): Applied Predictice Modeling. Springer.

[LKKV14] Lazer, D., Kennedy, R., King, G., Vespignani, A. (2014). The parable of Google Flu: traps in big data analysis. Science, 343 (6176), 1203-1205.

[MBK+12] Mertens, P., Bodendorf, F., König, W., Schumann, M., Hess, T. (2012). Grundzüge der Wirtschaftsinformatik. Springer.

[Muel15] Müller, E. (2015). Vorlesungsskript: Big Data Analytics. Hasso-Plattner- Institut Potsdam.

[Naum15] Naumann, F. (2015). Vorlesungsskript: Datenbanksysteme II. Hasso-Plattner-Institut Potsdam.

Literaturverzeichnis

[O'Nei16] O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown Books.

[PäPa15] Pääkkönen, P., Pakkala, D. (2015). Reference architecture and classification of technologies, products and services for big data systems. Big Data Research, 2 (4), 166-186.

[Plat13] Plattner, H. (2013). A Course in In-Memory Data Management. Springer.

[PoBe13] Becker, L., Pousttchi, K. (2013). Requirements for personalized m-commerce - what drives consumers' use of social networks?. In: Journal of Electronic Commerce in Organizations 11 (2013) 4, S. 19-36.

[RaSS15] Rahm, E., Saake, G., & Sattler, K. U. (2015). Verteiltes und paralleles Datenmanagement: von verteilten Datenbanken zu Big Data und Cloud. Springer.

[RePi91] Reichwald, R., Picot, A. (1991). Informationswirtschaft, in: Heinen, E. (Hrsg.). Industriebetriebslehre: Entscheidungen im Industriebetrieb. Springer.

[Rupa16] Ruparelia, N. B. (2016). Cloud Computing. MIT Press.

Literaturverzeichnis

[RuQZ07] Rupp, C., Queins, S., Zengler, B. (2007). UML 2 glasklar: Praxiswissen für die UML-Modellierung. Carl Hanser.

[SaSH11] Saake, G., Sattler, K. U., Heuer, A. (2011). Datenbanken: Implementierungstechniken. mitp.

[SaSH13] Saake, G., Sattler, K. U., Heuer, A. (2013). Datenbanken: Konzepte und Sprachen. mitp.

[Sche97] Scheer, A. W. (1997). ARIS—vom Geschäftsprozess zum Anwendungssystem. Springer.

[StHa04] Stahlknecht, P., Hasenkamp, U. (2004). Einführung in die Wirtschaftsinformatik. Springer.

[Sull15] Sullivan, D. (2015). NoSQL for mere mortals. Addison-Wesley Professional.

[Thor13] Thor, A. (2013). Vorlesungsskript: Datenmanagement. Universität Leipzig.

Literaturverzeichnis

[Vige16] Vigen, T. (2016). Spurious Correlations. Hachette Books.

[Voss08] Vossen, G. (2008). Datenmodelle, Datenbanksprachen und Datenbank-Management-Systeme. Oldenbourg.

[WeKa16] Wedel, M., Kannan, P. K. (2016). Marketing analytics for data-rich environments. Journal of Marketing, 80(6), 97-121.

[Wies15] Wiese, L. (2015). Advanced Data Management: For SQL, NoSQL, Cloud and Distributed Databases. de Gruyter.

[Zehn13] Zehnder, C. A. (2013). Informationssysteme und Datenbanken. Springer.

[Zoss15] Zoss, A. (2015). Practical Data Visualization. Lecture at Duke University.