Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

3. Regensburger Datenschutztag zum Themenschwerpunkt EU-Datenschutz-Grundverordnung, Regensburg, 6. Juli 2017

Folien unter:
http://tinyurl.com/pbd17fed

Soft- und Hardware-Entwicklung: Was verbirgt sich hinter Privacy-by-default und Privacy-by-design?

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Recht auf informationelle Selbstbestimmung

Mit dem Begriff Datenschutz wird das Recht des Einzelnen auf informationelle Selbstbestimmung umschrieben.

- Datenschutz

  = Schutz der Menschen

  ≠ (Schutz der Daten = Datensicherheit)

- Ab 2018 europaweit einheitlich geregelt über eine EU-Datenschutz-Grundverordnung

Recht auf informationelle Selbstbestimmung

Mit dem Begriff Datenschutz wird das Recht des Einzelnen auf informationelle Selbstbestimmung umschrieben.

- Recht auf informationelle Selbstbestimmung = Grundrecht

- Herleitung des Rechts auf informationelle Selbstbestimmung
  - aus dem Allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) durch das

    Bundesverfassungsgericht im Volkszählungsurteil

- «Volkszählungsurteil» des Bundesverfassungsgerichts vom 15.12.1983:
  - «Das Grundrecht gewährleistet [...] die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.»

Recht auf informationelle Selbstbestimmung

«Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den *Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten* voraus. …

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. *Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.»*

aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 1. BvR 209/83 Abschnitt C II.1, S. 43

Auszug aus Artikel 25 DSGVO

Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

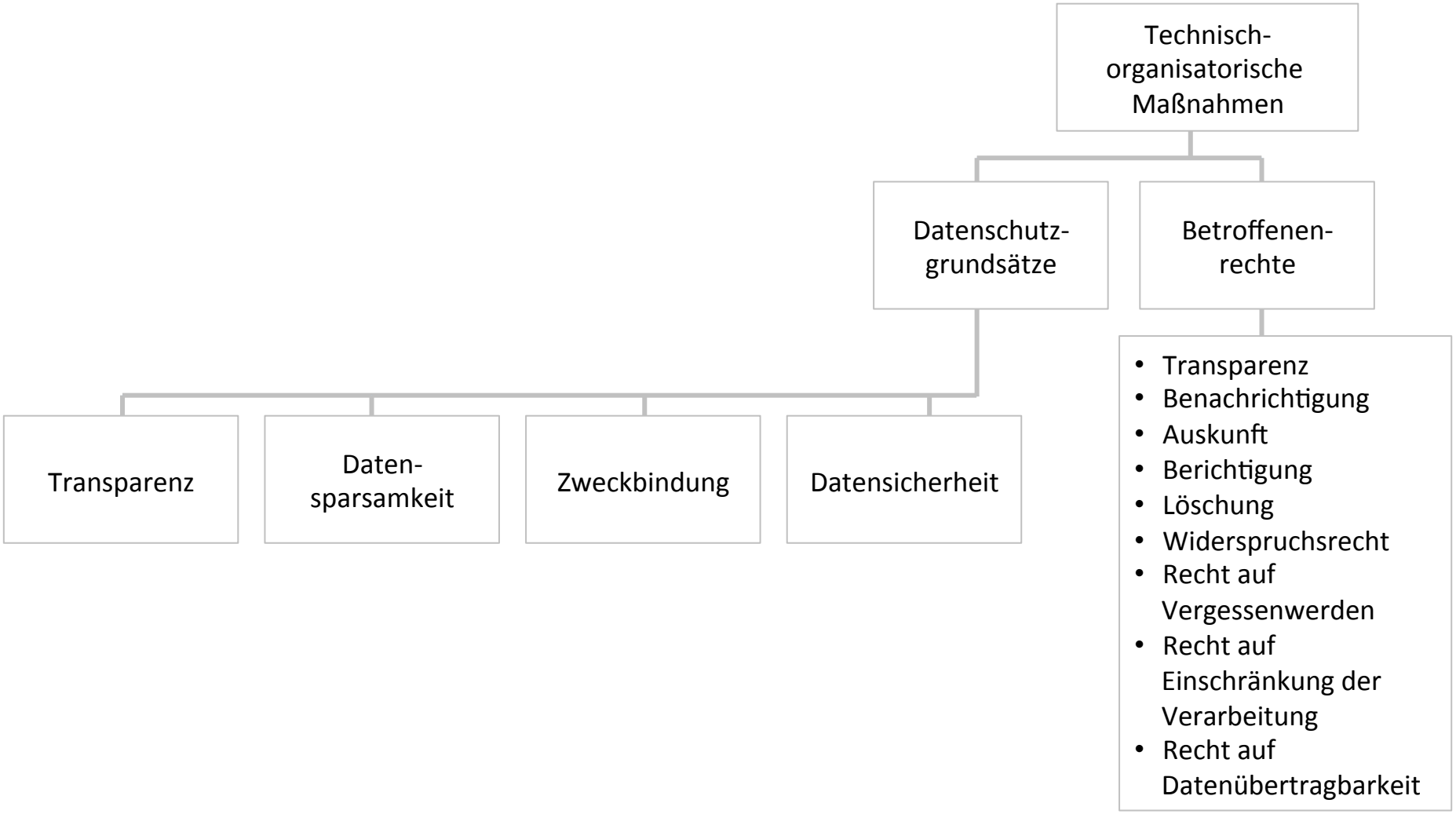
...

Begriffe

- Art. 25 (1) Privacy by Design – Datenschutz durch Technikgestaltung
  - Berücksichtigung
    - des Stands der Technik
    - der Implementierungskosten
    - der Umstände und Zwecke
    - der Eintrittswahrscheinlichkeiten und … Risiken
  - Geeignete technisch-organisatorische Maßnahmen
    - zur Umsetzung der Datenschutzgrundsätze
    - zur Durchsetzung der Betroffenenrechte

Begriffe

- Datenschutzgrundsätze
  - Rechtmäßigkeit und Transparenz
  - Datenminimierung und Datensparsamkeit
  - Zweckbindung
  - Datensicherheit
- Betroffenenrechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit


Technisch-organisatorische Maßnahmen
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Daten-sparsamkeit
Zweckbindung
Datensicherheit
• Transparenz
• Benachrichtigung
• Auskunft
• Berichtigung
• Löschung
• Widerspruchsrecht
• Recht auf Vergessenwerden
• Recht auf Einschränkung der Verarbeitung
• Recht auf Datenübertragbarkeit

Auszug aus Artikel 25 DSGVO

Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

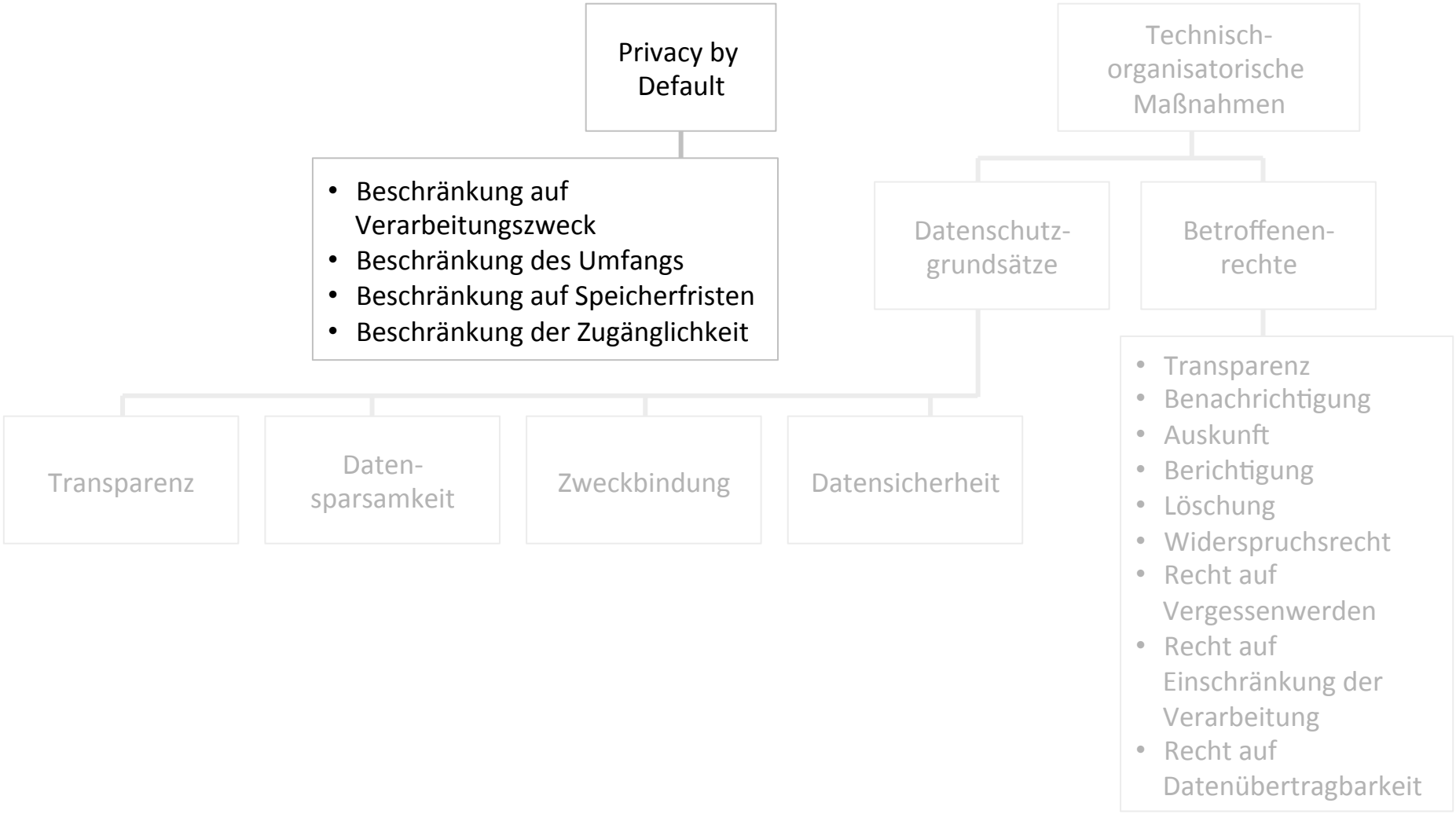
(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

...

Begriffe

- Art. 25 (2) Privacy by Default – datenschutzfreundliche Voreinstellungen
  - Beschränkung durch fest eingebaute Funktionalität
    - Beschränkung auf Verarbeitungszweck
    - Beschränkung des Umfangs
    - Beschränkung auf Speicherfristen
    - Beschränkung der Zugänglichkeit


Privacy by Default
Technisch-organisatorische Maßnahmen
• Beschränkung auf Verarbeitungszweck
• Beschränkung des Umfangs
• Beschränkung auf Speicherfristen
• Beschränkung der Zugänglichkeit
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Daten-sparsamkeit
Zweckbindung
Datensicherheit
• Transparenz
• Benachrichtigung
• Auskunft
• Berichtigung
• Löschung
• Widerspruchsrecht
• Recht auf Vergessenwerden
• Recht auf Einschränkung der Verarbeitung
• Recht auf Datenübertragbarkeit

Auszug aus Artikel 32 DSGVO

Art. 32 Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

...

Begriffe

- Art. 32 (1) Sicherheit der Verarbeitung
  - Geeignete technisch-organisatorische Maßnahmen
    - zur Pseudonymisierung und Verschlüsselung
    - zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit
    - zur Wiederherstellung der Verfügbarkeit nach Zwischenfällen
    - zur Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Maßnahmen


Privacy by Default
Technisch-organisatorische Maßnahmen
• Beschränkung auf Verarbeitungszweck
• Beschränkung des Umfangs
• Beschränkung auf Speicherfristen
• Beschränkung der Zugänglichkeit
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Daten-sparsamkeit
Zweckbindung
Datensicherheit
• Transparenz
• Benachrichtigung
• Auskunft
• Berichtigung
• Löschung
• Widerspruchsrecht
• Recht auf Vergessenwerden
• Recht auf Einschränkung der Verarbeitung
• Recht auf Datenübertragbarkeit
• Pseudonymisierung
• Verschlüsselung
• Vertraulichkeit
• Integrität
• Verfügbarkeit
• Belastbarkeit
• Wiederherstellbarkeit
• Notfallmanagement
• Überprüfbarkeit
• Bewertung
• Evaluierung

Unter Berücksichtigung …

Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitu… ilt für die Menge der erhobenen per… Speicherfrist und ihre Zugänglichk… personenbezogene Daten durch V… en Zahl von natürlichen Personen zu…

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände, Zwecke
- Risiko
- Technisch-organisatorische Maßnahmen

…

Unter Berücksichtigung …

Art. 32 Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

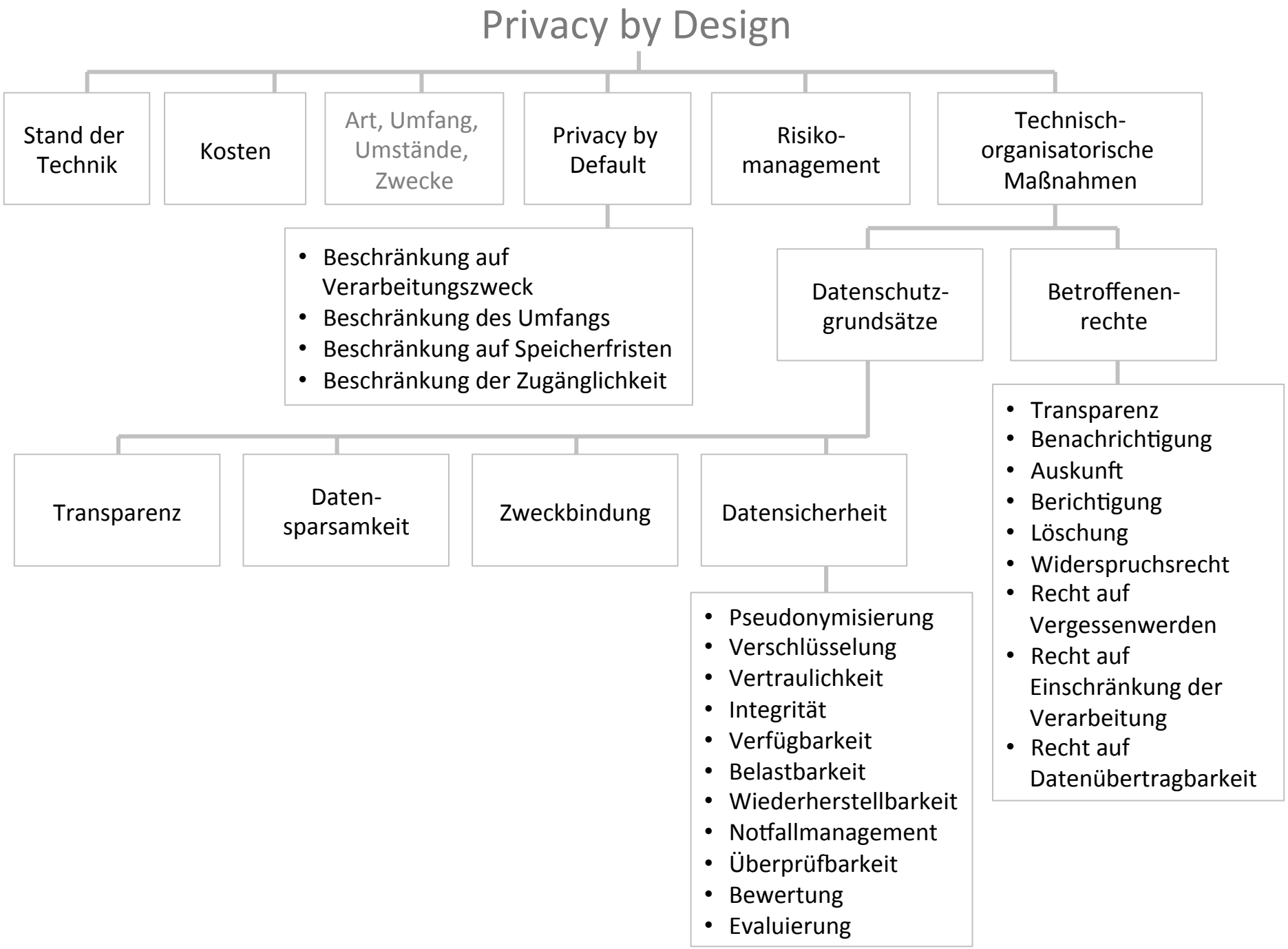
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwis

d) ein Verfahren zur regelmäßige
technischen und organisatorische

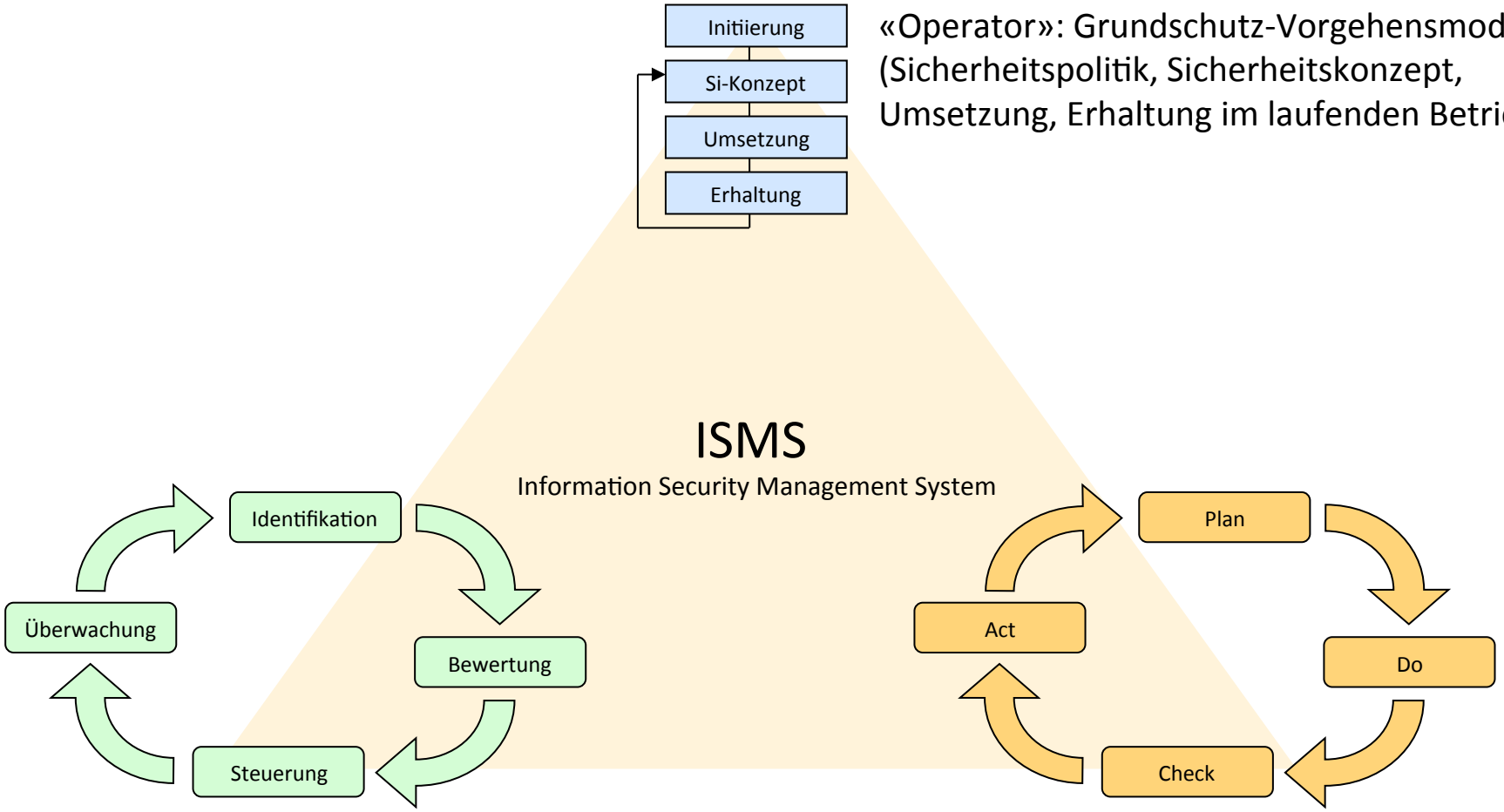
(2) Bei der Beurteilung des angem igen,
die mit der Verarbeitung verbund g —
Vernichtung, Verlust, Veränderun ang
zu personenbezogenen Daten, die .

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände, Zwecke
- Risiko
- Technisch-organisatorische Maßnahmen

…


Privacy by Design
Stand der Technik
Kosten
Art, Umfang, Umstände, Zwecke
Privacy by Default
Risiko-management
Technisch-organisatorische Maßnahmen
• Beschränkung auf Verarbeitungszweck
• Beschränkung des Umfangs
• Beschränkung auf Speicherfristen
• Beschränkung der Zugänglichkeit
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Daten-sparsamkeit
Zweckbindung
Datensicherheit
• Transparenz
• Benachrichtigung
• Auskunft
• Berichtigung
• Löschung
• Widerspruchsrecht
• Recht auf Vergessenwerden
• Recht auf Einschränkung der Verarbeitung
• Recht auf Datenübertragbarkeit
• Pseudonymisierung
• Verschlüsselung
• Vertraulichkeit
• Integrität
• Verfügbarkeit
• Belastbarkeit
• Wiederherstellbarkeit
• Notfallmanagement
• Überprüfbarkeit
• Bewertung
• Evaluierung

Information Security Management System — Views

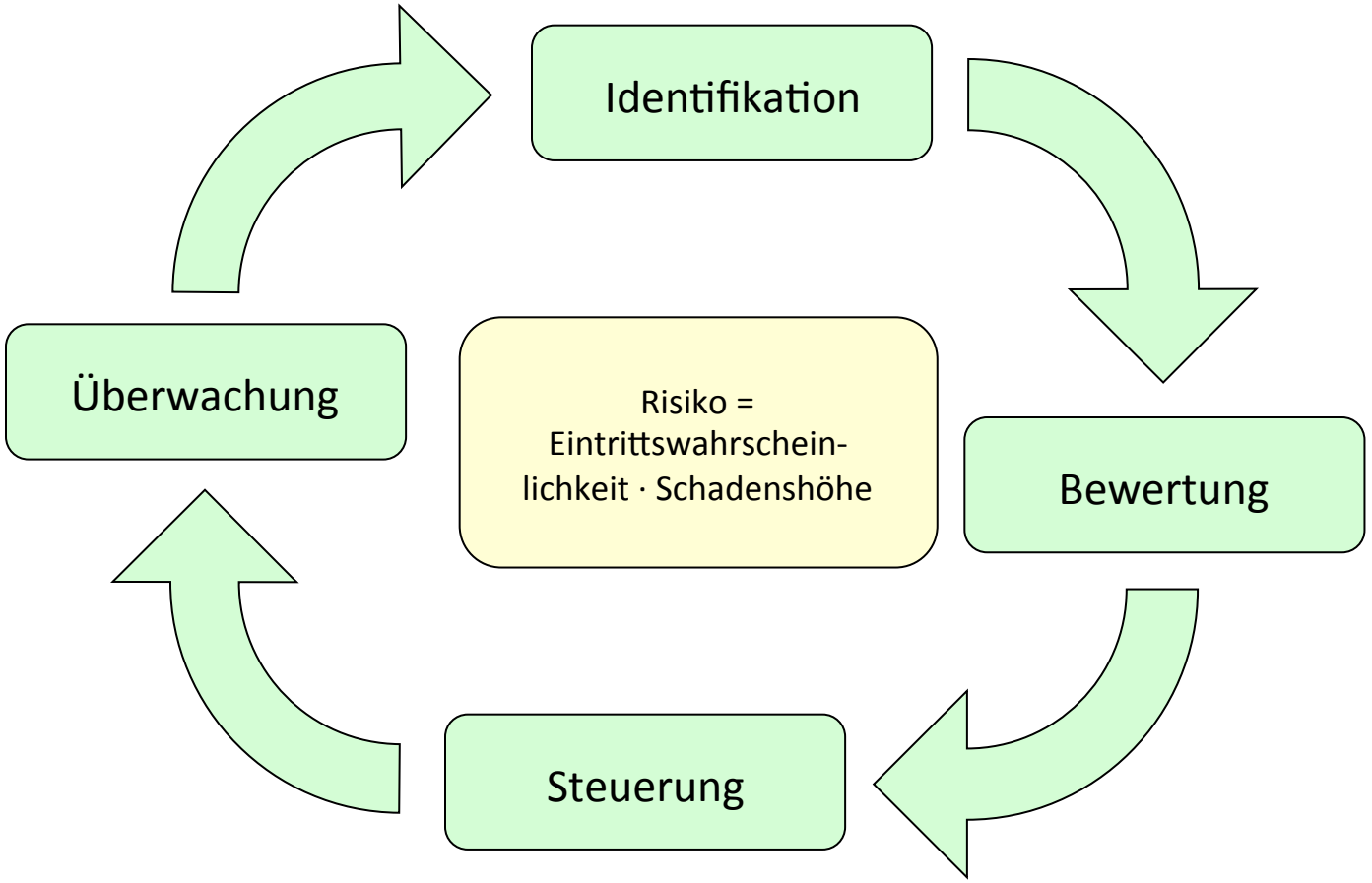


«Operator»: Grundschutz-Vorgehensmodell (Sicherheitspolitik, Sicherheitskonzept, Umsetzung, Erhaltung im laufenden Betrieb)

«Controller»: Risikomanagement (Identifikation, Bewertung, Steuerung, Überwachung)

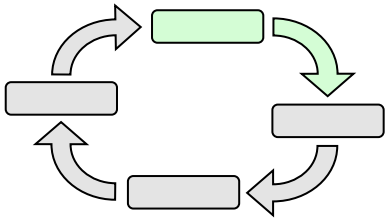
«Management»: Deming-Kreislauf (Plan, Do, Check, Act)

Risikomanagement Kreislauf

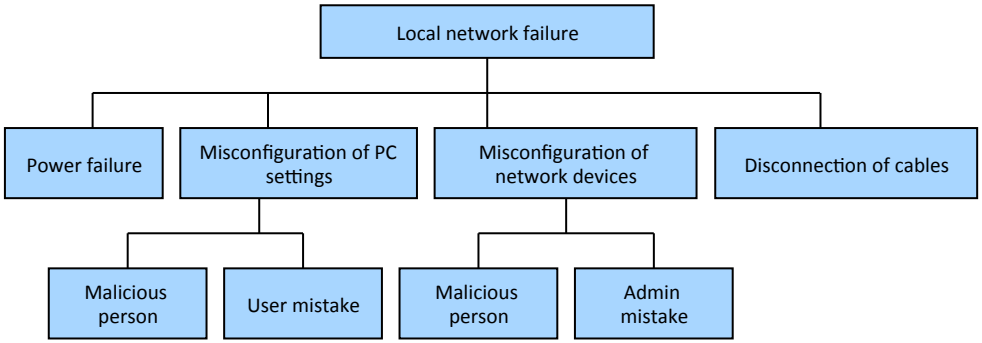


Identifikation von Bedrohungen

- Frage
  - Welche Bedrohungen sind für das jeweilige Schutzobjekt relevant?



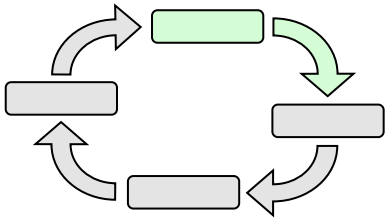
- Methoden & Werkzeuge
  - Checklisten und Workshops
  - Fehler- und Angriffsbäume
  - Szenarioanalysen
  - Historische Daten



- Herausforderungen
  - Vollständige Erfassung aller Bedrohungen

Identifikation von Bedrohungen

- Frage
  - Welche Bedrohungen sind für das jeweilige Schutzobjekt relevant?



- Beispiel Checklisten und Workshops

  Bedrohungskategorien des Security Development Lifecycle (SDL)

  STRIDE Threat Model:

  Spoofing: Fälschen der eigenen Identität

  Tampering: Fälschen oder Verändern von Daten

  Repudiation: Anwenden von Verschleierungstaktiken

  Information disclosure: Unbefugte Preisgabe vertraulicher Informationen

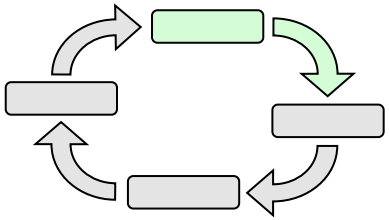
  Denial of service: Unbefugte Beeinträchtigung der Funktionalität

  Elevation of privilege: Unbefugtes Erlangen von Berechtigungen

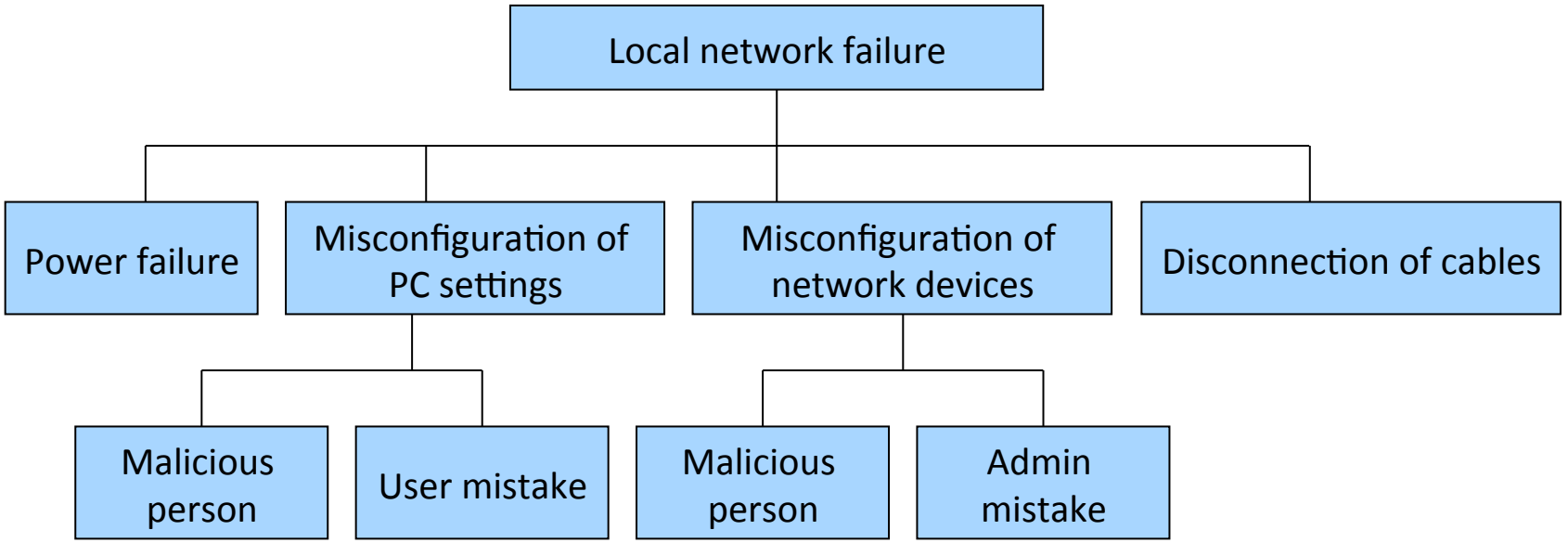
The STRIDE Threat Model. Microsoft, 2002
https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

Identifikation von Bedrohungen

- Frage
  - Welche Bedrohungen sind für das jeweilige Schutzobjekt relevant?

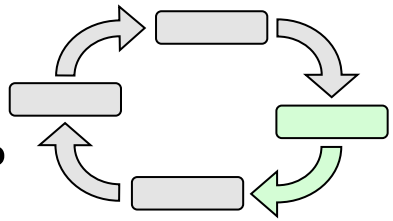


- Beispiel Fehler- und Angriffsbäume



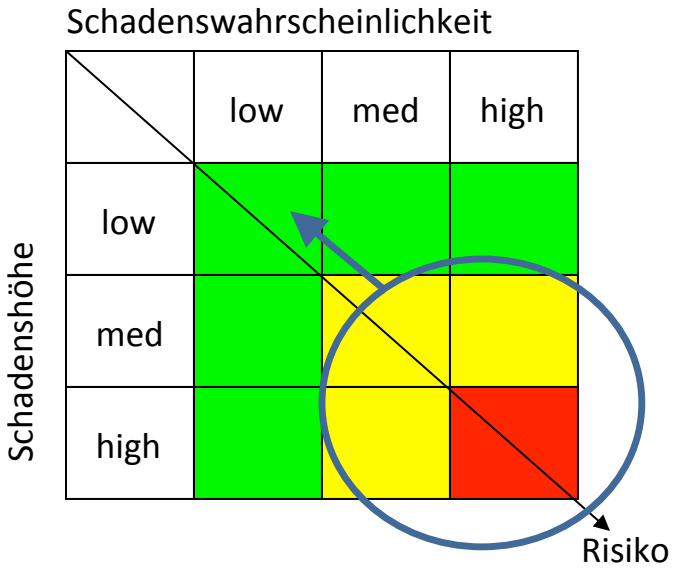
Bewertung von Risiken

- Frage
  - Wie groß sind Eintrittswahrscheinlichkeit und Schadenshöhe eines potentiellen Schadensereignisses?



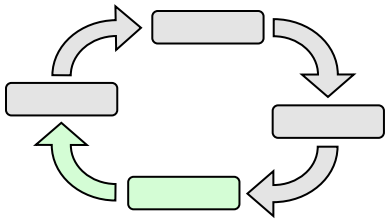
- Methoden & Werkzeuge
  - Qualitative Bewertung
  - Quantitative Bewertung
  - Spieltheorie
  - Maximalwirkungsanalyse

- Herausforderungen
  - Abhängigkeit von den Assets
  - Strategische Angreifer
  - Korrelationen
  - Quantifizierbarkeit



Steuerung der Risiken

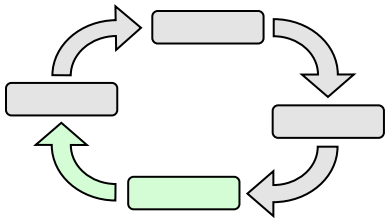
- Frage
  - Welche Risiken sollen wie behandelt werden?

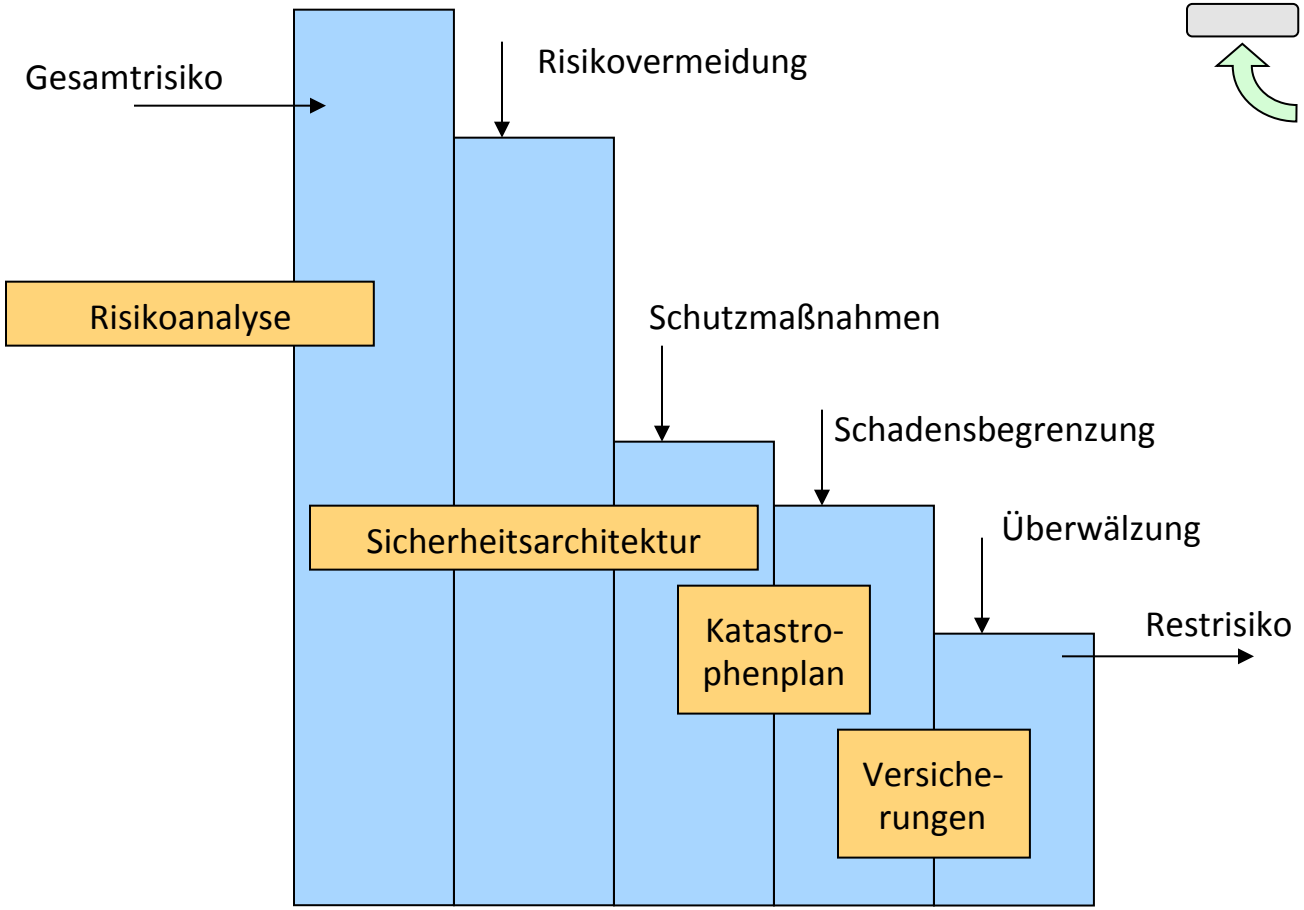


- Methoden
  - Risikovermeidung
  - Risikobehandlung (z.B. nach IT-Grundschutz und ISO 27002)
  - Risikoüberwälzung
  - Risikoakzeptanz

- Herausforderungen
  - Komplexität der Problemstellung
  - Finden von geeigneten Musterlösungen
  - Komposition eines sicheren Gesamtsystems aus sicheren Teillösungen

Risiko-Management für IT-Systeme

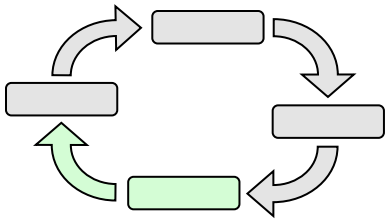




nach: Schaumüller-Bichl 1992

Risiko-Management für IT-Systeme

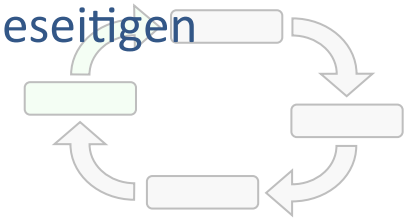
Typische Positionen für Vermeidung, Akzeptanz und Überwälzung:



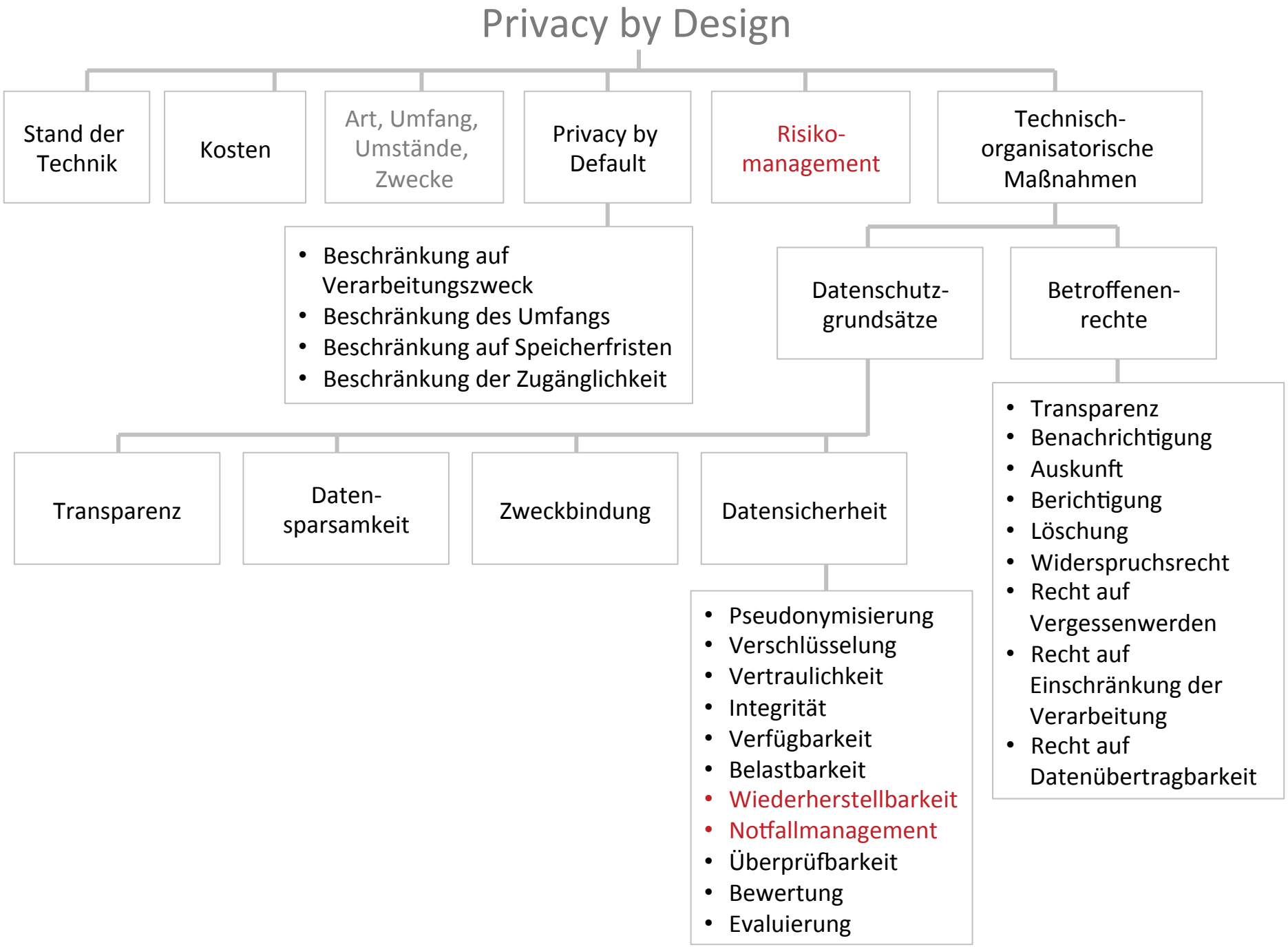
Schadenswahrscheinlichkeit

Schadenshöhe	low	med	high
low	Akzep-tanz	Vermeidung	Vermeidung
med		Schutzmaßnahmen	Schutzmaßnahmen
high	Über-wälzung	Schutzmaßnahmen	Schutzmaßnahmen

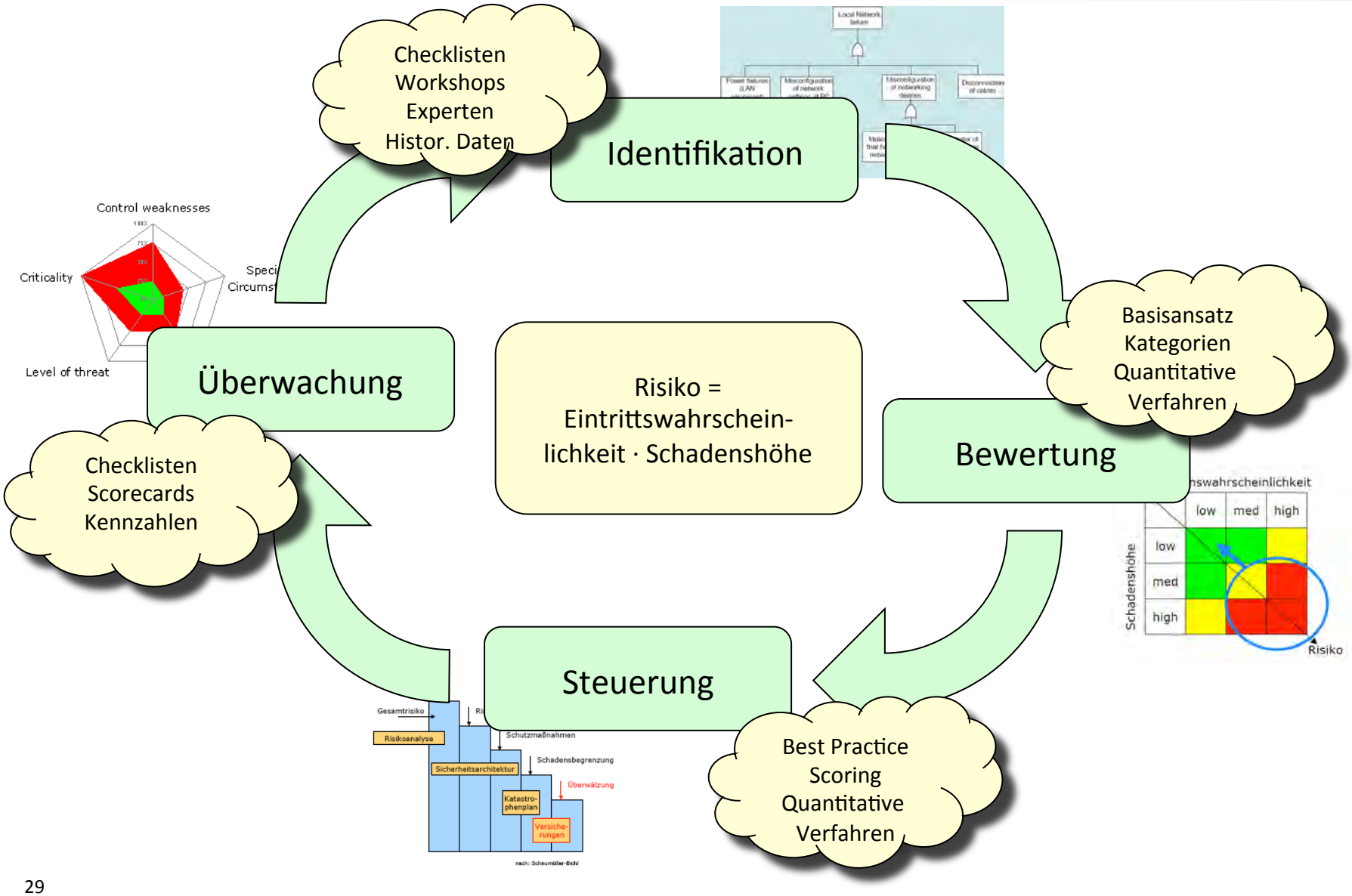
Notfall- bzw. Katastrophenplan zur Schadensbegrenzung



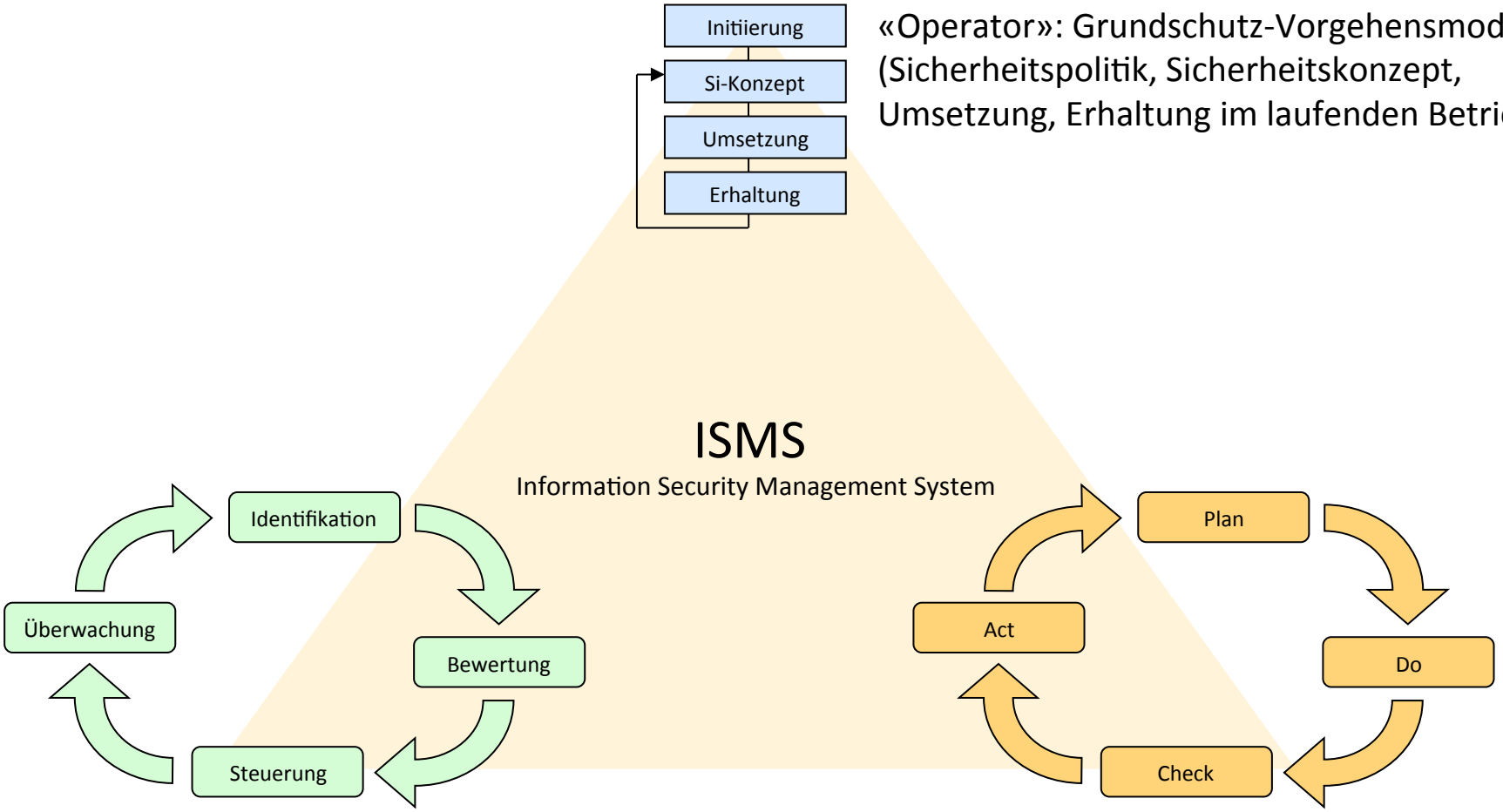
- IT-Sicherheitskonzept kann Risiko niemals 100-prozentig beseitigen
  - Notfallplan sollte Teil der Maßnahmenplanung sein
- Methoden
  - Back-Up-Planung (Rechenzentrum, Daten)
  - Notlaufkonzepte
  - Wiederbeschaffungs- und Wiederanlaufpläne
- Verlust von Verfügbarkeit
  - Notfallpläne sind primär ausgerichtet auf die schnelle Beseitigung von Verlusten der Verfügbarkeit.
- Verlust von Integrität
  - Schaden kann schleichend eintreten
  - schwer umkehrbar, Backup-Konzepte können helfen
- Verlust von Vertraulichkeit
  - Schaden kann schleichend eintreten
  - nahezu nicht umkehrbar, da Löschung aller Kopien kaum herbeiführbar


Privacy by Design
Stand der Technik
Kosten
Art, Umfang, Umstände, Zwecke
Privacy by Default
Risiko-management
Technisch-organisatorische Maßnahmen
Beschränkung auf Verarbeitungszweck
Beschränkung des Umfangs
Beschränkung auf Speicherfristen
Beschränkung der Zugänglichkeit
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Daten-sparsamkeit
Zweckbindung
Datensicherheit
Transparenz
Benachrichtigung
Auskunft
Berichtigung
Löschung
Widerspruchsrecht
Recht auf Vergessenwerden
Recht auf Einschränkung der Verarbeitung
Recht auf Datenübertragbarkeit
Pseudonymisierung
Verschlüsselung
Vertraulichkeit
Integrität
Verfügbarkeit
Belastbarkeit
Wiederherstellbarkeit
Notfallmanagement
Überprüfbarkeit
Bewertung
Evaluierung

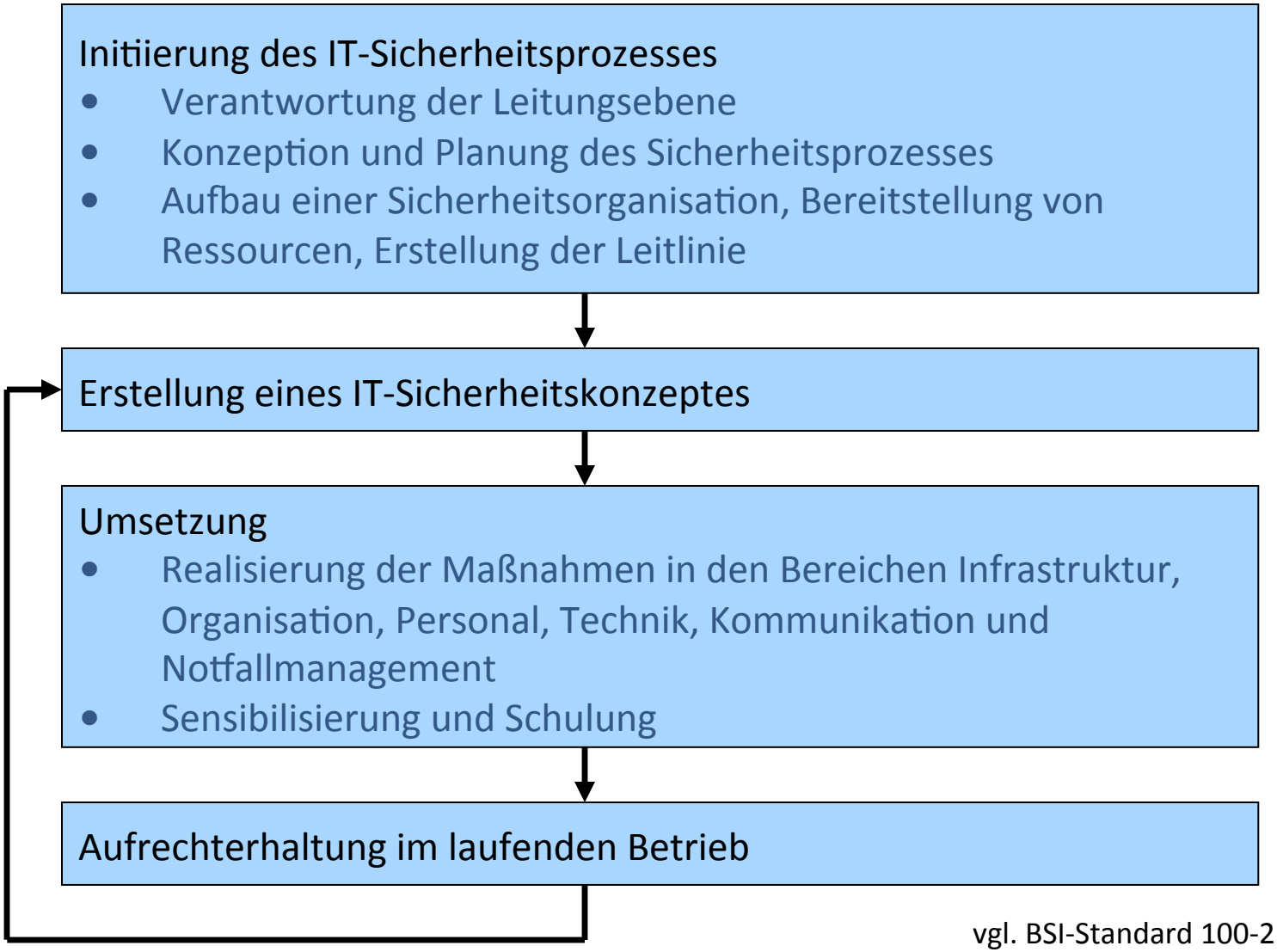
Risikomanagement Kreislauf



Information Security Management System — Views

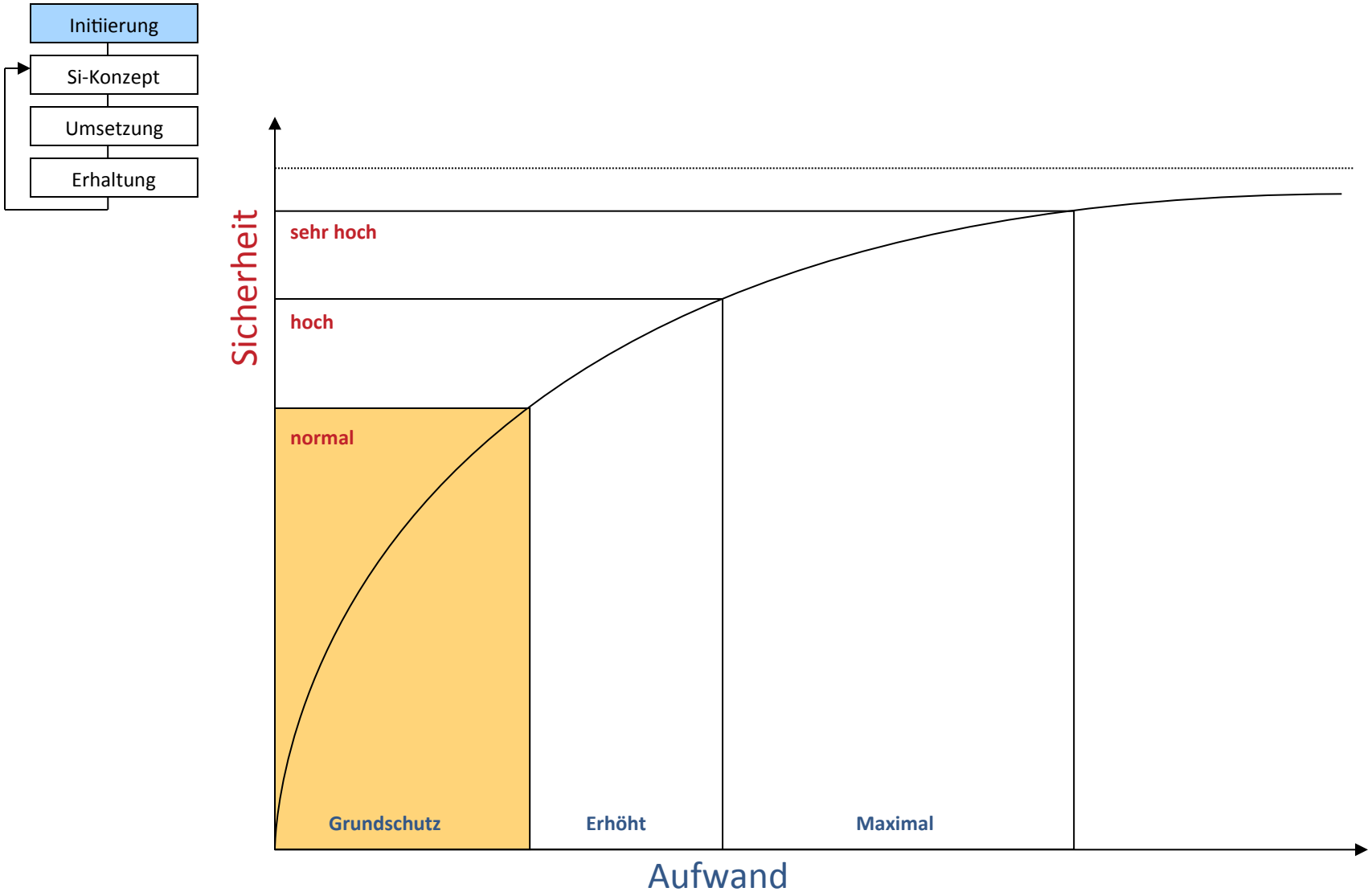


Der IT-Sicherheitsprozess nach BSI-Standard 100-2

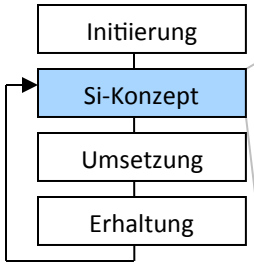


vgl. BSI-Standard 100-2

Aufwand-Nutzen-Relation nach BSI-Standard 100-2



Erstellung eines IT-Sicherheitskonzepts



IT-Strukturanalyse
- Erfassung der IT und der IT-Anwendungen
- Gruppenbildung

Schutzbedarfsfeststellung

IT-Grundschutzanalyse
- Modellierung nach IT-Grundschutz
- Basis-Sicherheitscheck mit Soll-Ist-Vergleich

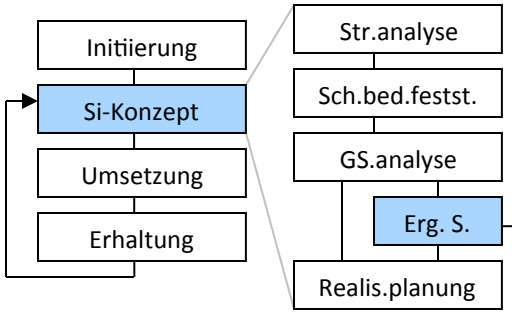
Ergänzende Sicherheitsanalyse
- bei hohem Schutzbedarf
- bei zusätzlichem Analysebedarf

Konsolidierung der Maßnahmen

Realisierung der Maßnahmen («Planung der …»)

vgl. BSI-Standard 100-2

Ergänzende Sicherheitsanalyse …

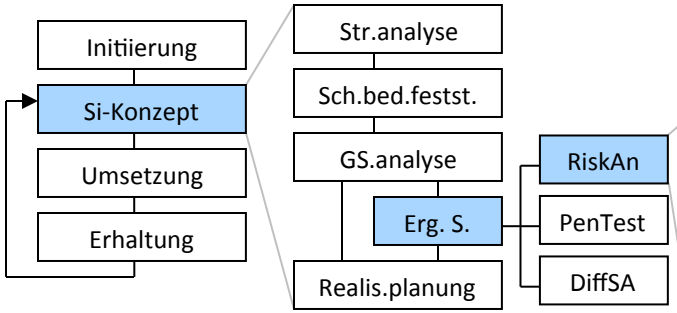


… notwendig für Systeme mit hohem bzw. sehr hohem Schutzbedarfsniveau

Drei mögliche Methoden:

- Risikoanalyse
- oder
- Penetrationstest
- oder
- Differenz-Sicherheitsanalyse

Risikoanalyse auf der Basis von IT-Grundschutz (BSI 100-3)



Vorgehen:

- Relevante Bedrohungen erkennen
- Eintrittswahrscheinlichkeit und Schutzbedarf ermitteln
- Geeignete Sicherheitsmaßnahmen auswählen, um die Eintrittswahrscheinlichkeit zu senken bzw. die Schadenshöhe zu reduzieren

Gefährdungsübersicht
- Tabellarische Zuordnung von Schutzobjekten und Gefährdungen

↓

Zusätzliche Gefährdungen
- Gefährdungen die nicht im Grundschutz-Katalog enthalten sind

↓

Gefährdungsbewertung
- Ausreichender Schutz durch Standard-Maßnahmen?

↓

Behandlung von Risiken
- Risiko-Vermeidung, Risiko-Reduktion durch zusätzliche Maßnahmen, Risiko-Transfer, Risiko-Akzeptanz

↓

Konsolidierung der Maßnahmen

vgl. BSI-Standard 100-3

Privacy by Design

Stand der Technik

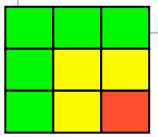
Kosten

Art, Umfang, Umstände, Zwecke

Privacy by Default

- Beschränkung auf Verarbeitungszweck
- Beschränkung des Umfangs
- Beschränkung auf Speicherfristen
- Beschränkung der Zugänglichkeit

Risiko-management



Technisch-organisatorische Maßnahmen

Datenschutz-grundsätze

Transparenz

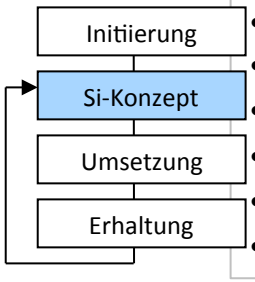
Daten-sparsamkeit

Zweckbindung

Datensicherheit

- Pseudonymisierung
- Verschlüsselung
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit
- Wiederherstellbarkeit
- Notfallmanagement
- Überprüfbarkeit
- Bewertung
- Evaluierung

Bereitschaft zur datenschutzfreundlichen Gestaltung und gute Dokumentation



Betroffenen-rechte

- Transparenz
- Benachrichtigung
- Auskunft
- Berichtigung
- Löschung
- Widerspruchsrecht
- Recht auf Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

Return on Security Investment (ROSI)

- Frage
  - Waren die Maßnahmen effektiv und effizient? Wie sicher ist die Organisation?

- ROSI
  - basiert auf dem ALE-Konzept (Annual Loss Expenditure) aus den 70er Jahren
  - soll Analogie zum klassischen Return on Investment herstellen
  - verschiedene Darstellungsformen und Weiterentwicklungen

ROSI – Return on Security Investment – «Ersparnis» durch Abwenden der wahrscheinlichen Schäden abzügl. der Kosten der Sicherheitsmaßnahmen

Privacy by Design

Stand der Technik

Kosten

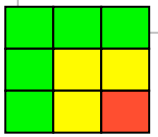
ROSI

Art, Umfang, Umstände, Zwecke

Privacy by Default

- Beschränkung auf Verarbeitungszweck
- Beschränkung des Umfangs
- Beschränkung auf Speicherfristen
- Beschränkung der Zugänglichkeit

Risiko-management



Technisch-organisatorische Maßnahmen

Datenschutz-grundsätze

Betroffenen-rechte

- Transparenz
- Benachrichtigung
- Auskunft
- Berichtigung
- Löschung
- Widerspruchsrecht
- Recht auf Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

Transparenz

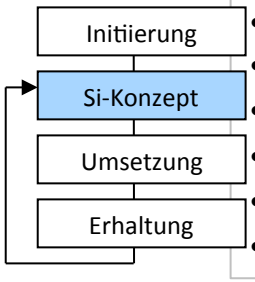
Daten-sparsamkeit

Zweckbindung

Datensicherheit

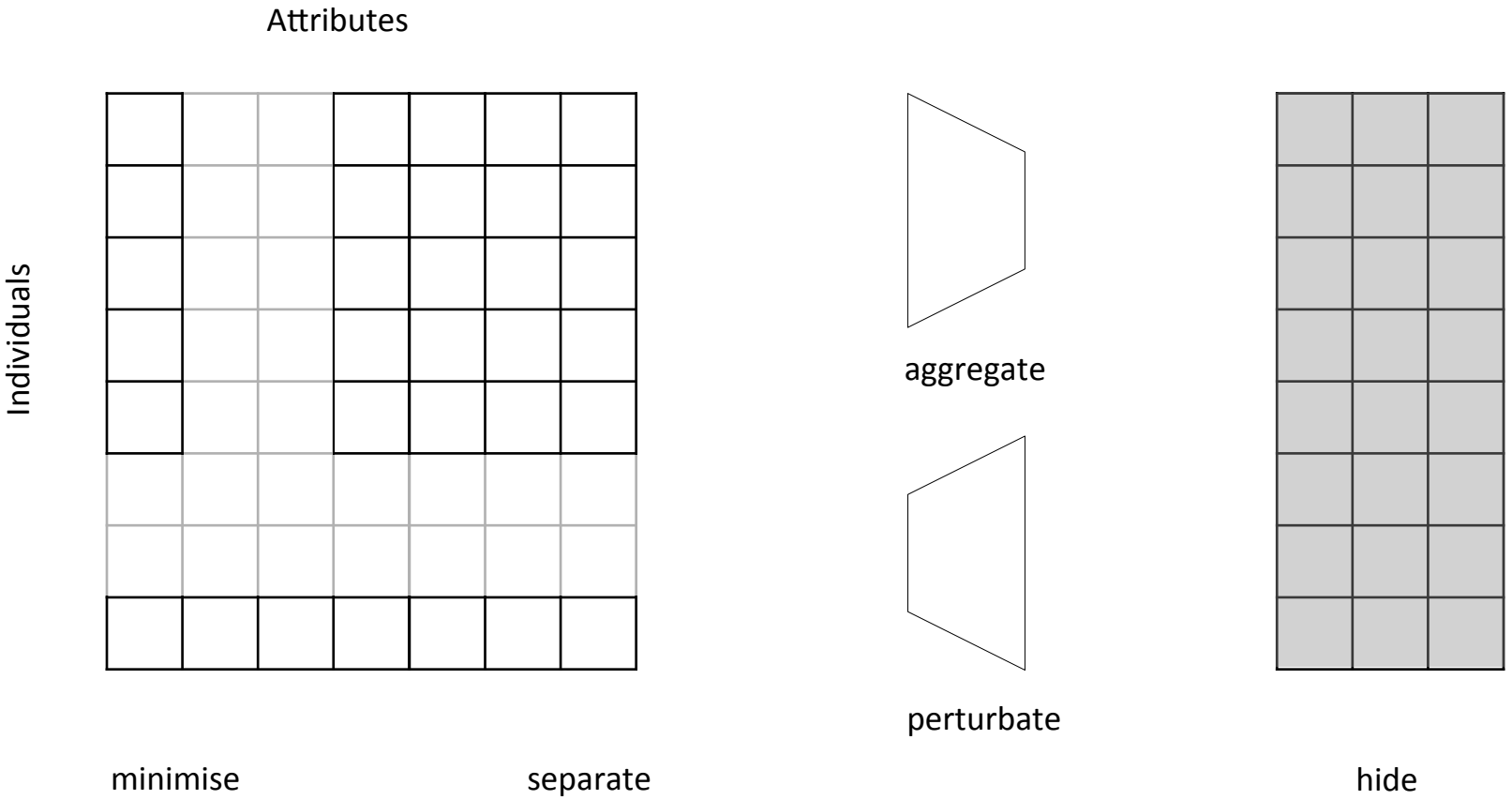
- Pseudonymisierung
- Verschlüsselung
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit
- Wiederherstellbarkeit
- Notfallmanagement
- Überprüfbarkeit
- Bewertung
- Evaluierung

Bereitschaft zur datenschutzfreundlichen Gestaltung und gute Dokumentation



Privacy design strategies

in Anlehnung an Hoepmann, 2013



Privacy design strategies

in Anlehnung an Hoepmann, 2013

- Technisch
  - Minimise: Nur notwendige Daten speichern und verarbeiten
  - Separate: Daten verteilt verarbeiten und speichern
  - Aggregate: Daten auf das notwendige Maß zusammenfassen
  - Perturbate: Daten durch zufällige Störungen ungenau machen
  - Hide: Daten nicht in offener Form speichern

- Organisatorisch
  - Enforce: Durchsetzung einer Datenschutz-Policy (access control)
  - Inform: Betroffene über Datenverwendung informieren (P3P)
  - Control: Eingriffsmöglichkeit der Betroffenen (informed consent)
  - Demonstrate: Überprüfbarkeit (privacy management, logging)

Anwendungsfall x Schlüsselbeziehung

	Konzelation (Verschlüsselung)	Authentikation
symmetrische	*One-time-pad, DES, Triple-DES, AES, IDEA, A5/1 (GSM), A5/2 (GSM) …* GnuPG/PGP, WPA2, IPSec, SSL/TLS	*Symmetrische Authentikationscodes, CCM, A3 (GSM), …* SecurID, WPA2, IPSec, SSL/TLS
asymmetrische	*RSA, ElGamal, McEliece, …* GnuPG/PGP, HBCI, SSL/TLS	*RSA, ElGamal, DSA, GMR, …* GnuPG/PGP, HBCI, SSL/TLS

Algorithmus

Anwendung

Welche Schlüssellängen und Kryptoalgorithmen sind sicher?

Jährlicher Algorithmenkatalog nach § 17 (1) SigG des Bundesamts für die Sicherheit in der Informationstechnik (BSI)

Tabelle 3: Geeignete Schlüssellängen für DSA

Parameter \ Zeitraum	bis Ende **2015**	bis Ende **2021**
p	2048	2048
q	224	256

Tabelle 8: Nicht mehr geeignete RSA-Schlüssellängen

Modullänge n	geeignet bis
768	Ende 2000
1024	Ende März 2008*
1280	Ende 2008
1536	Ende 2009
1728	Ende 2010

* Januar – März 2008: Übergangsfrist

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung

(Übersicht über geeignete Algorithmen)

Vom 15. 12. 2014

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständige Behörde gemäß § 3 Signaturgesetz (SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091), veröffentlicht gemäß Anlage 1 Abschnitt 1 Nr. 2 Signaturverordnung (SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542), im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt.

Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001

Vorbemerkung: Wie in den Vorjahren werden im Folgenden geeignete Algorithmen und Schlüssellängen für den Zeitraum der kommenden sieben Jahre anstatt des in der SigV vorgesehenen Mindestzeitraums von sechs Jahren aufgeführt. Das heißt konkret, dass geeignete Algorithmen und Schlüssellängen bis Ende 2021 statt bis Ende 2020 aufgeführt sind. Im Allgemeinen sind solche längerfristigen Prognosen schwer möglich. Die vorliegende Übersicht über geeignete Algorithmen unterscheidet sich von der zuletzt veröffentlichten Übersicht vom 20. Februar 2014 (BAnz AT 20.02.2013 B4) im Wesentlichen in folgenden Punkten:

1. Die Eignung von Nyberg-Rueppel-Signaturen wird nicht über das Jahr 2020 hinaus verlängert. Dies hat keine Sicherheitsgründe, sondern dient der Vereinfachung der Pflege des Algorithmenkatalogs. Nachdem die Streichung von Nyberg-Rueppel-Signaturen in den letzten beiden Versionen der vorliegenden Bekanntmachung angekündigt und in den entsprechenden Expertenanhörungen diskutiert wurde, sind bei den zuständigen Stellen im Bundesamt für Sicherheit in der Informationstechnik und in der Bundesnetzagentur keine Einsprüche gegen die Streichung dieses Verfahrens eingegangen. Es wird daher davon ausgegangen, dass es keine praktische Verwendung findet im Bereich der qualifizierten elektronischen Signatur.

2. Wie bereits im vorigen Algorithmenkatalog angekündigt wurde, wird die Eignung von Zufallsgeneratoren, die entsprechend der Funktionalitätsklassen nach [31] zertifiziert wurden, von wenigen Ausnahmefällen abgesehen nicht über das Jahr 2020 hinaus verlängert.

https://www.bsi.bund.de/Algorithmenkatalog

Privacy by Design

Stand der Technik

Kosten

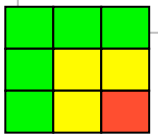
ROSI

Art, Umfang, Umstände, Zwecke

Privacy by Default

- Beschränkung auf Verarbeitungszweck
- Beschränkung des Umfangs
- Beschränkung auf Speicherfristen
- Beschränkung der Zugänglichkeit

Risiko-management



Technisch-organisatorische Maßnahmen

Datenschutz-grundsätze

Betroffenen-rechte

- Transparenz
- Benachrichtigung
- Auskunft
- Berichtigung
- Löschung
- Widerspruchsrecht
- Recht auf Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

Transparenz

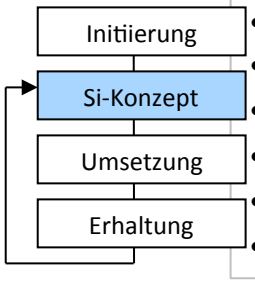
Daten-sparsamkeit

Zweckbindung

Datensicherheit

- Pseudonymisierung
- Verschlüsselung
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit
- Wiederherstellbarkeit
- Notfallmanagement
- Überprüfbarkeit
- Bewertung
- Evaluierung

Bereitschaft zur datenschutzfreundlichen Gestaltung und gute Dokumentation



Bereitschaft

Aus einer Folie von 2004…

Stand der Sicherheitstechnik

Schutzziel	Technik	Stand der Technik	Nutzbarkeit
Vertraulichkeit	Verschlüsselung	sehr gut	gut
Verdecktheit	Steganographie	mittel	schlecht
Anonymität Unbeobachtbarkeit	Remailer, Proxies, Mixe	mittel	mittel
Zurechenbarkeit Rechtsverbindlichkeit	Digitale Signatur	schlecht	schlecht

https://www2.informatik.uni-hamburg.de/svs/publ.php?search=2004-03-12IT-Speicher

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

https://svs.informatik.uni-hamburg.de

Folien unter:
http://tinyurl.com/pbd17fed