Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Workshop „Data Protection by Design“ des Kompetenzverbunds Software Systems Engineering, Kiel, 14. November 2018

Vorgehensmodelle und Softwareunterstützung zur Umsetzung des Standard-Datenschutzmodells

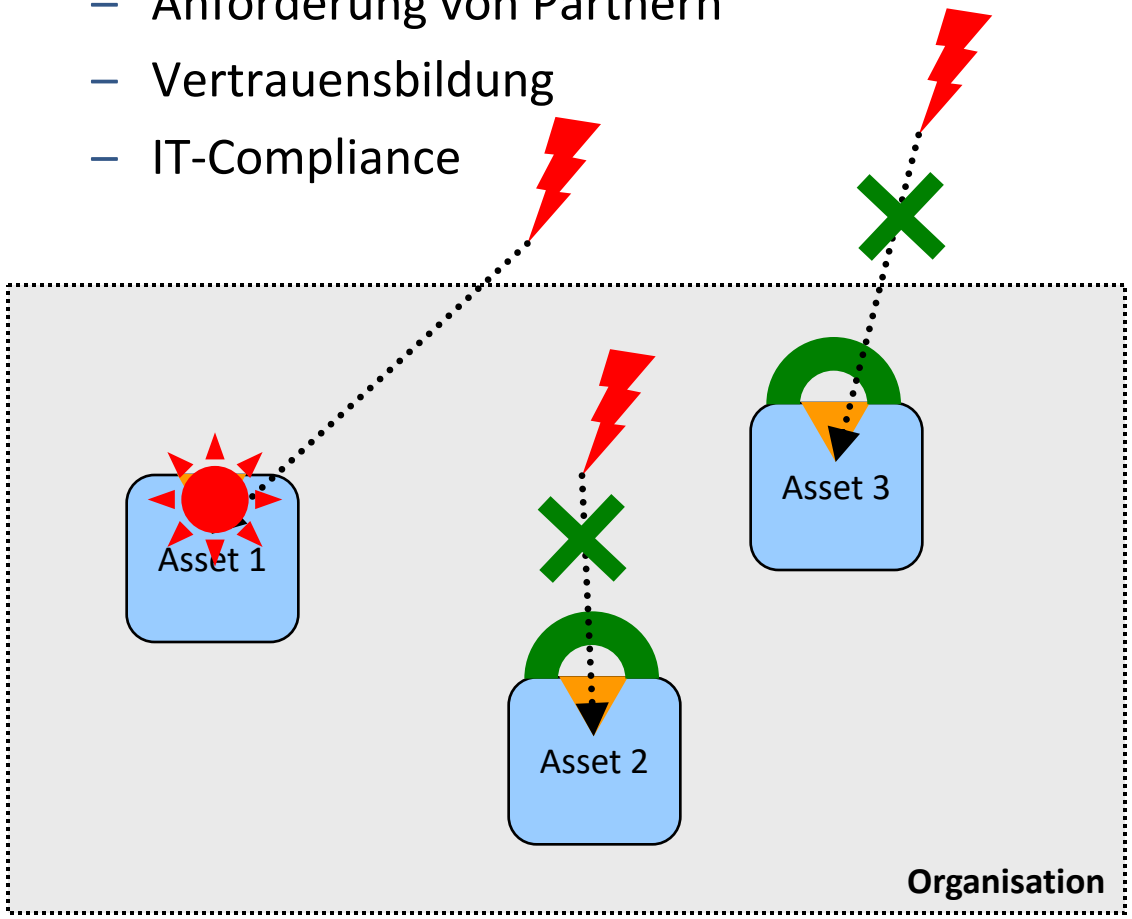
Hannes Federrath, Jan Osterkamp
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Vorgehensmodelle und Softwareunterstützung zur Umsetzung des Standard-Datenschutzmodells

- Sicherheitsmanagemement
  - Schutzziele und Vorgehensweise nach dem Standard 200-2 des Bundesamts für Sicherheit in der Informationstechnik
- Datenschutzmanagement
  - Gewährleistungsziele und Vorgehensweise nach dem Standard-Datenschutzmodell
- Gemeinsamkeiten und Unterschiede
  - Sicherheitsmanagement und Datenschutzmanagement im Vergleich
- Möglichkeiten einer Softwareunterstützung

Von der Bedrohung zum Sicherheitsvorfall

- Warum IT-Sicherheitsmanagement?
  - Schutz von Unternehmenswerten (Assets)
  - Anforderung von Partnern
  - Vertrauensbildung
  - IT-Compliance



Bedrohungen, z.B.
- Viren, Würmer
- DoS
- Hacking
- Spionage
- Social Engineering

Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

Schutzziele
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

vgl. Nowey, 2011

Von der Bedrohung zum Sicherheitsvorfall

- Präventive Maßnahmen
  - Einsatz kryptographischer Verfahren
    - obligatorische Datenverschlüsselung
    - gegenseitige starke Authentifizierung
  - Perimeterschutz mit Firewalls
  - Aufteilung Test- und Produktivumgebung
- Detektive Maßnahmen
  - Einsatz von Intrusion Detektion Systemen
  - Malware-Schutz
- Reaktive Maßnahmen
  - Systemtrennung
  - Fail-Safe-Prozeduren
  - Protokollierung

Bedrohungen, z.B.
- Viren, Würmer
- DoS
- Hacking
- Spionage
- Social Engineering

Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

Schutzziele
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

Abgrenzung von IT-Sicherheit und Datenschutz

- IT-Sicherheit = Schutz der Daten
  - IT-Sicherheit versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

- Datenschutz = Schutz der Menschen
  - Mit dem Begriff Datenschutz wird das Recht des Einzelnen auf informationelle Selbstbestimmung umschrieben. »Das Grundrecht gewährleistet [...] die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.« (BVerfG) Eine Organisation hat technisch-organisatorische Maßnahmen zu treffen, um dieses Recht zu gewährleisten.

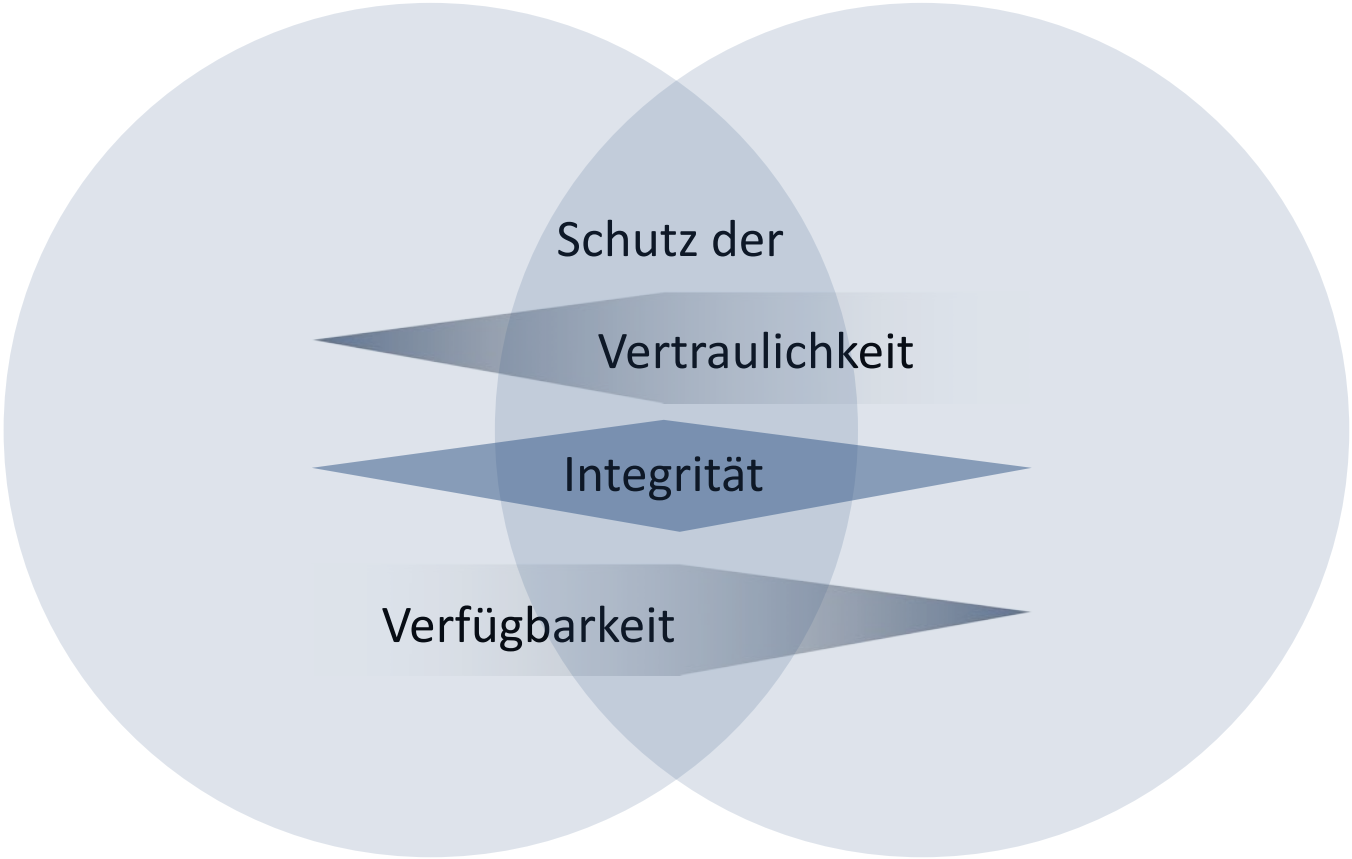
Verknüpfung von Sicherheit und Datenschutz

IT-Sicherheit

Schutz der Daten

Datenschutz

Schutz der Menschen



Schutzziele

Voydock, Kent, 1983

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

Vertraulichkeit	unbefugter Informationsgewinn
Integrität	unbefugte Modifikation
Verfügbarkeit	unbefugte Beeinträchtigung der Funktionalität

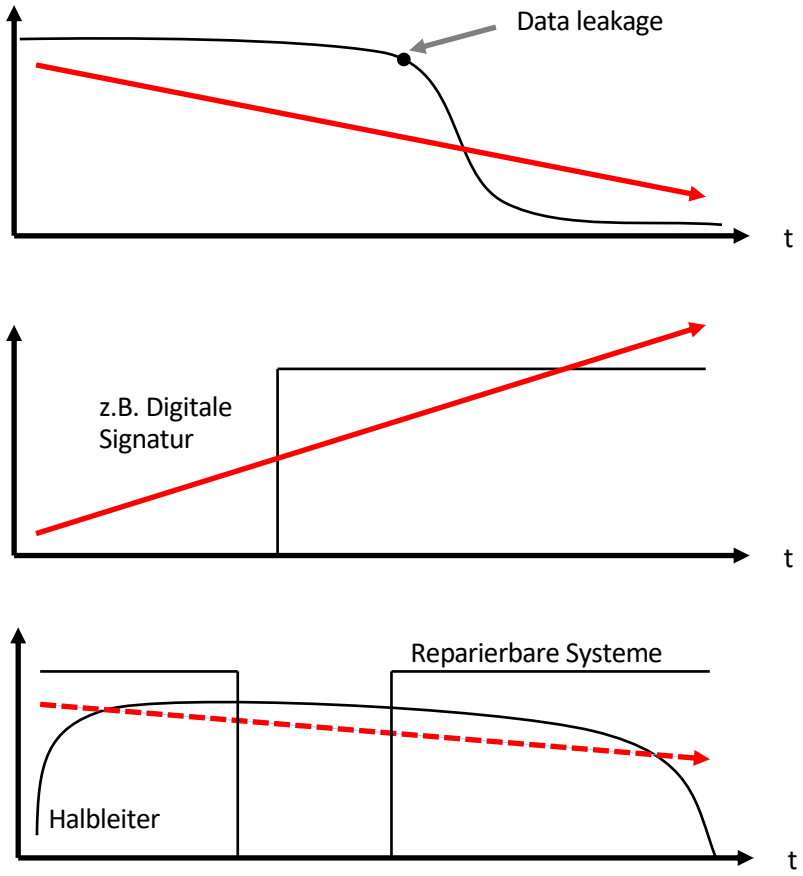
Beobachtungen zum Monotonieverhalten

- Das Monotonieverhalten von Schutzzielen gibt Hinweise auf die Prioritäten bei der Umsetzung von Schutzzielen und das praktisch erreichbare Schutzniveau.

Vertraulichkeit

Integrität

Verfügbarkeit

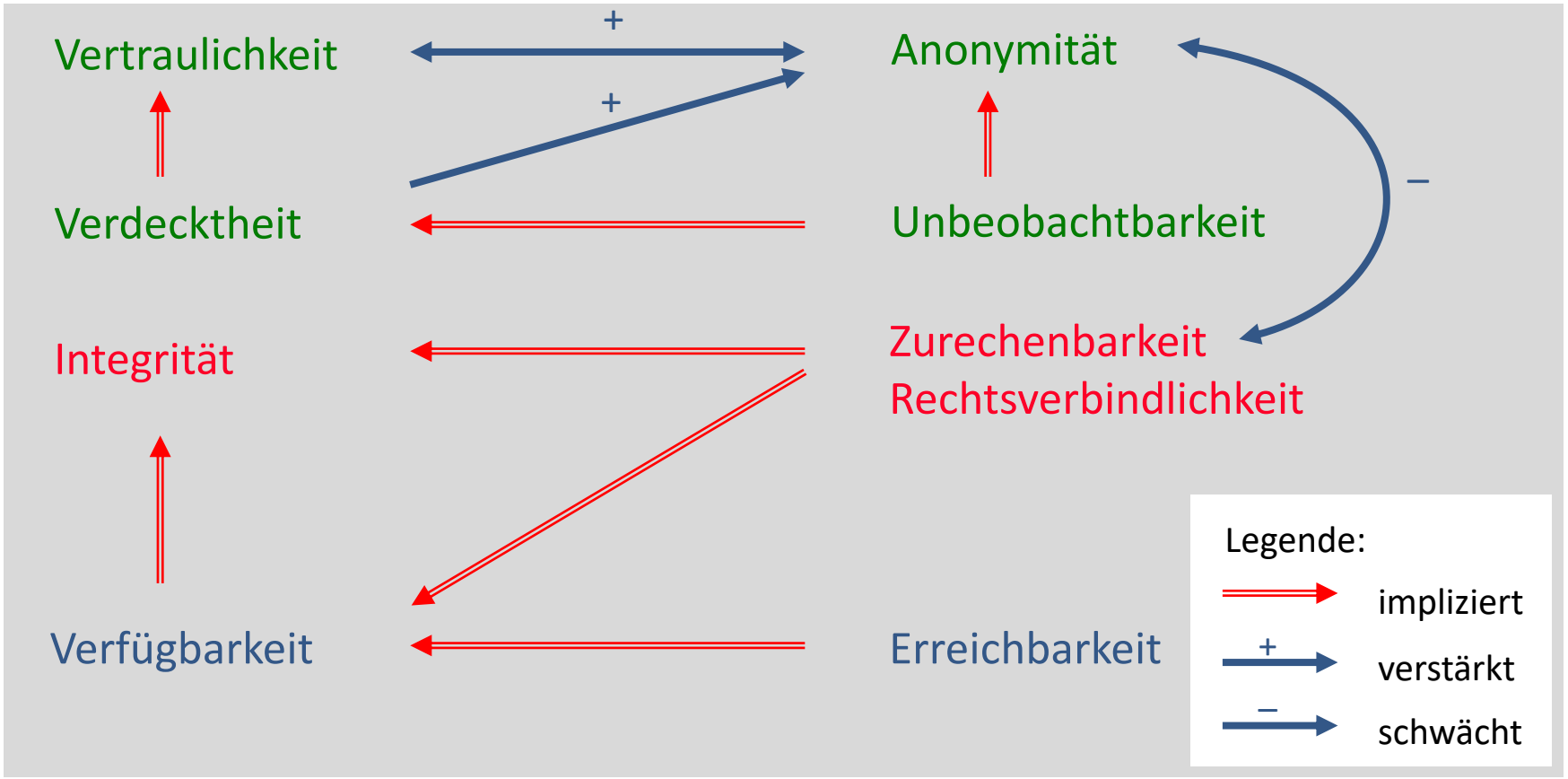


Schutzziele und Verfahren

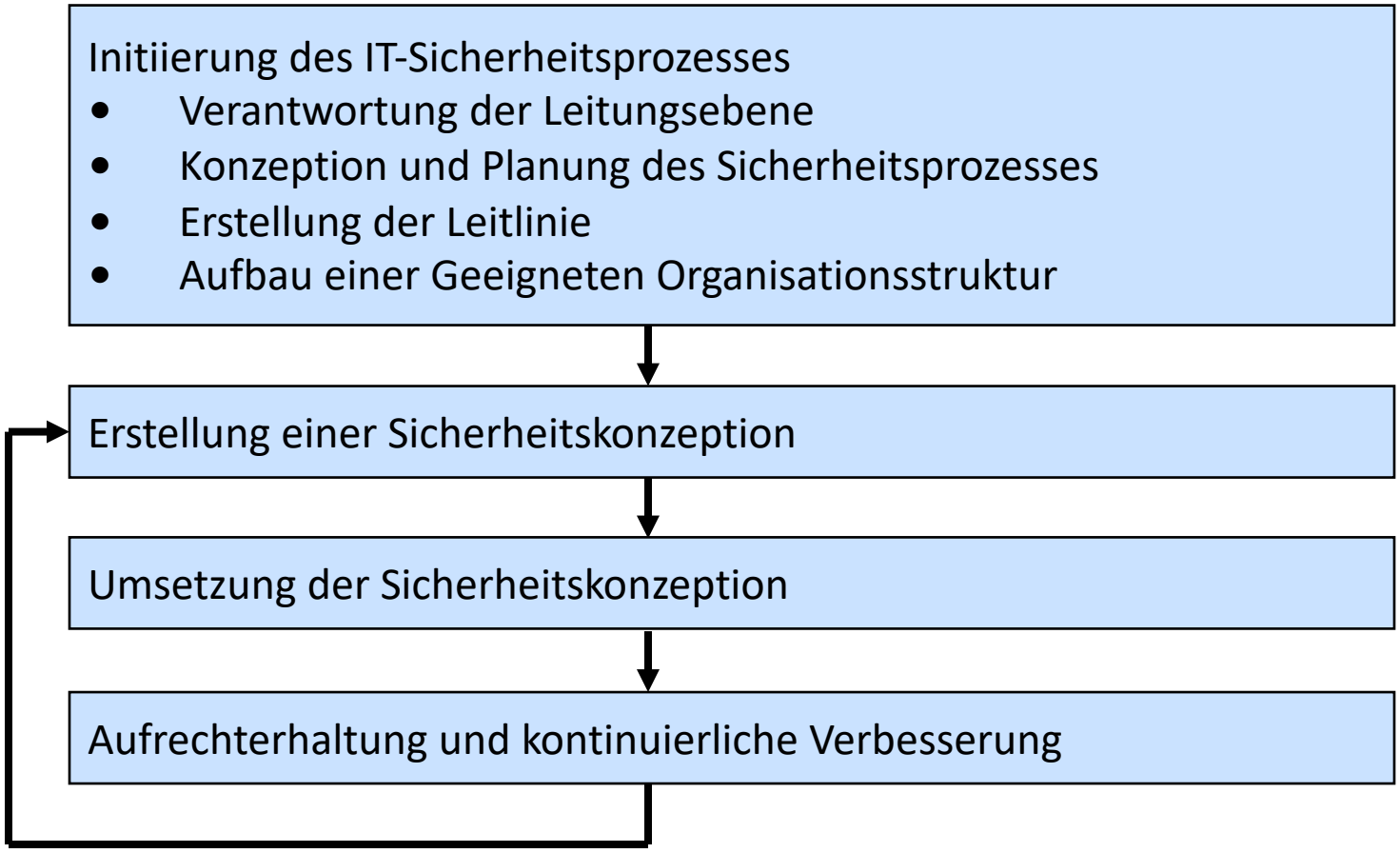
Kommunikationsgegenstand Was?, Worüber? Inhaltsdaten	Kommunikationsumstände Wann?, Wo?, Wer? Verkehrsdaten
Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Verschlüsselung Steganographie	Web-Anonymisierer, Remailer, anonyme Zahlungssysteme
Integrität	Zurechenbarkeit Rechtsverbindlichkeit
Message Authentication Codes Challenge-Response-Authentikation	Digitale Signaturen
Verfügbarkeit	Erreichbarkeit
Redundanz, Diversität	

Wechselwirkungen

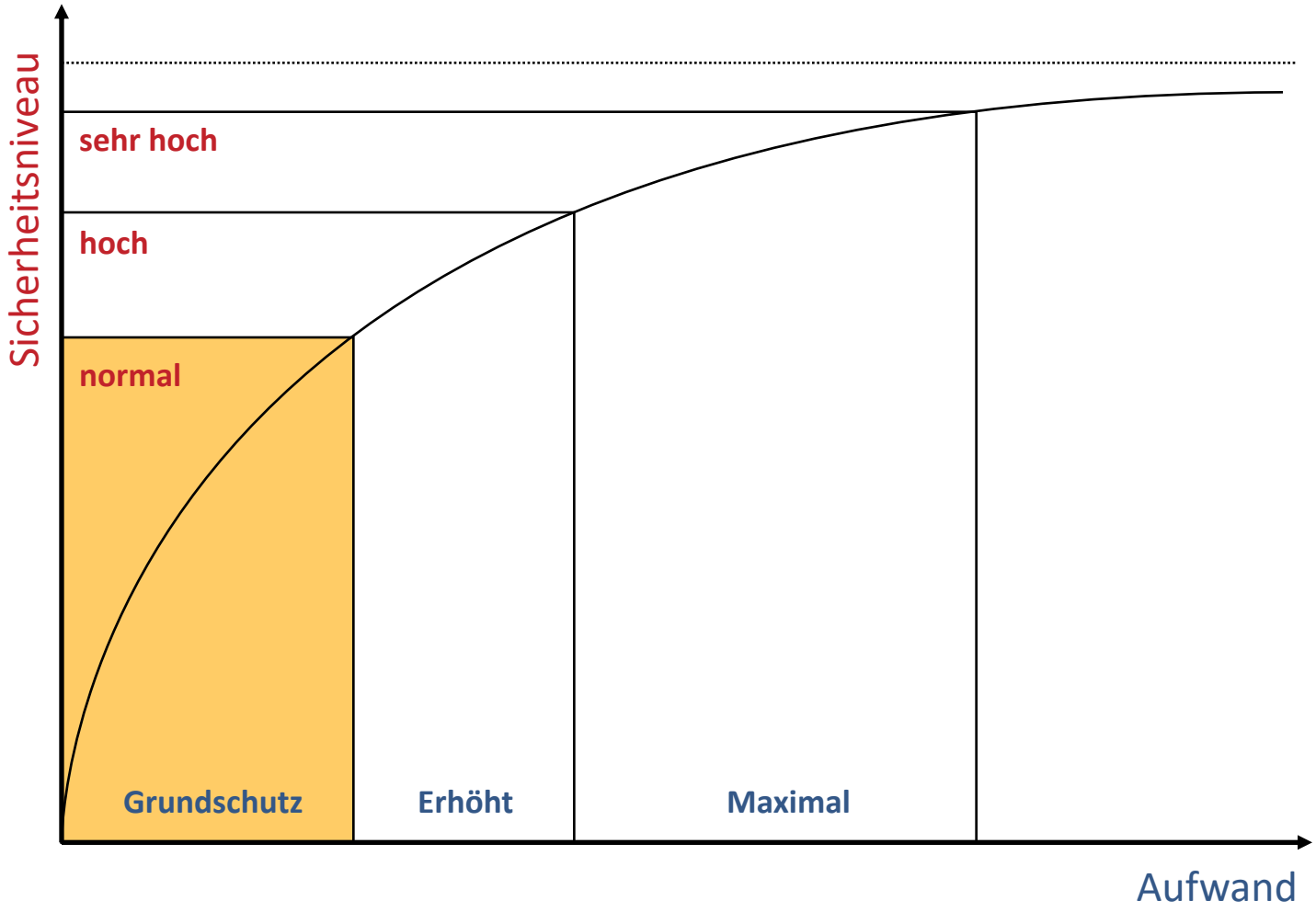
vgl. A. Pfitzmann, G. Wolf, 2000



IT-Sicherheitsprozess in der Standard-Absicherung nach BSI 200-2, S. 26

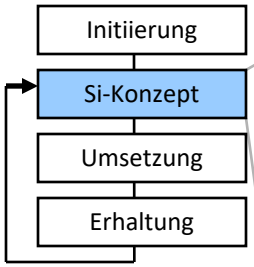


Aufwand-Nutzen-Relation nach BSI-Grundschutz



Erstellung einer IT-Sicherheitskonzeption

nach BSI 200-2



Strukturanalyse (Erfassung der Prozesse und Anwendungen)

Schutzbedarfsfeststellung

Modellierung (Auswahl der Sicherheitsanforderungen, Bausteine)

IT-Grundschutz-Check (Teil 1 Soll-Ist-Vergleich)

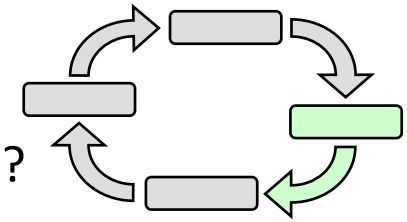
Risikoanalyse

- bei erhöhtem Schutzbedarf
- bei nicht hinreichenden Bausteinen
- bei besonderen Einsatzszenarien

Konsolidierung und IT-Grundschutz-Check (Teil 2 Soll-Ist-Vergleich)

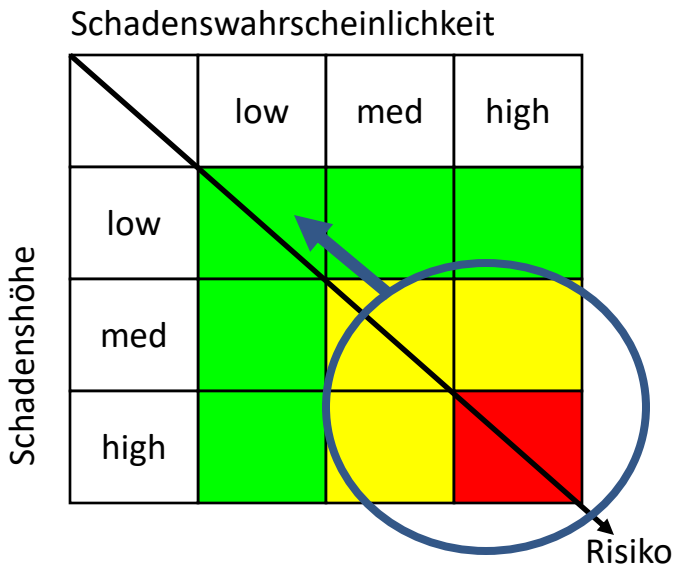
Bewertung von Risiken

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

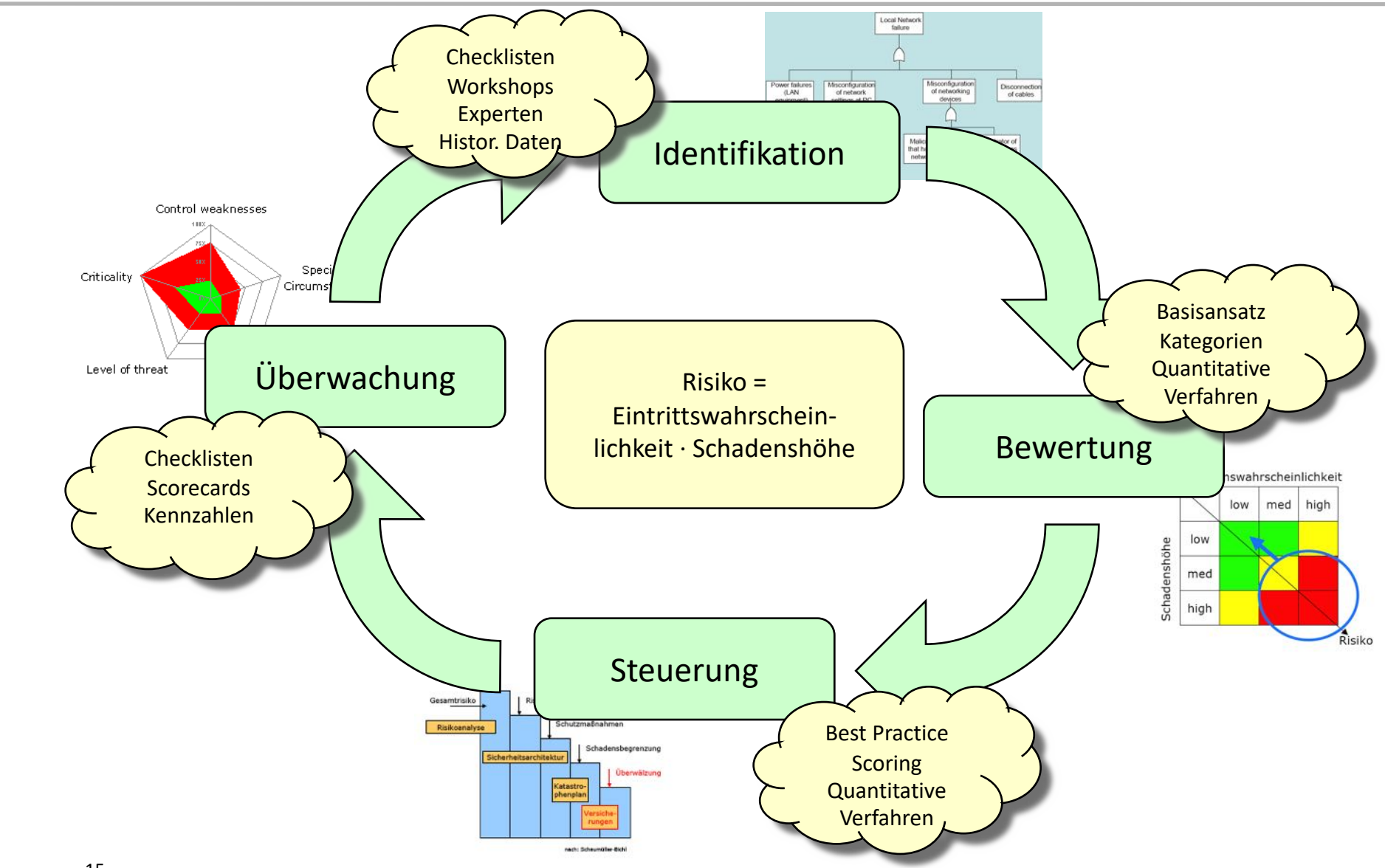


- Methoden & Werkzeuge
  - Qualitative Bewertung
  - Quantitative Bewertung
  - Spieltheorie
  - Maximalwirkungsanalyse

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



Risikomanagement Kreislauf



Vorgehensmodelle und Softwareunterstützung zur Umsetzung des Standard-Datenschutzmodells

- Sicherheitsmanagemement
  - Schutzziele und Vorgehensweise nach dem Standard 200-2 des Bundesamts für Sicherheit in der Informationstechnik
- Datenschutzmanagement
  - Gewährleistungsziele und Vorgehensweise nach dem Standard-Datenschutzmodell
- Gemeinsamkeiten und Unterschiede
  - Sicherheitsmanagement und Datenschutzmanagement im Vergleich
- Möglichkeiten einer Softwareunterstützung

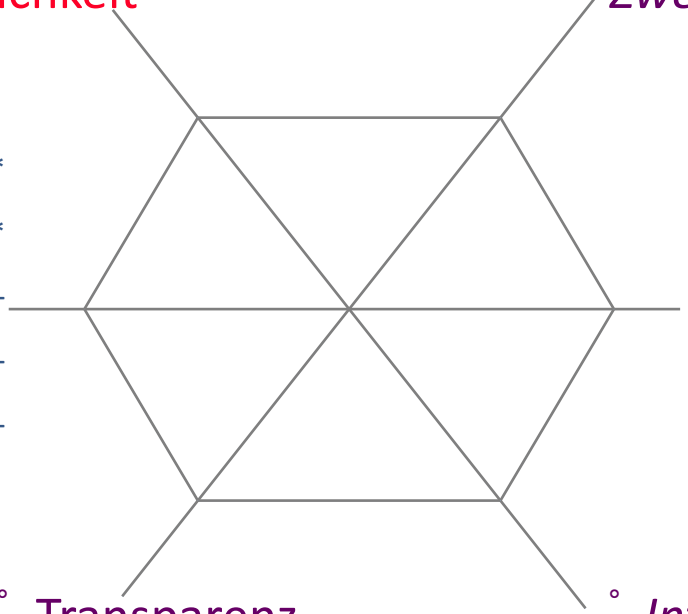
Standard-Datenschutzmodell

- Methode zur
  - Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele
  - Überprüfung der Übereinstimmung der gesetzlichen Anforderungen im Umgang mit personenbezogenen Daten und der entsprechenden Umsetzung dieser Vorgaben

- Von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder empfohlen
  - Ca. 50 Seiten Umfang
  - https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html

Gewährleistungsziele

in Anlehnung an Bock und Rost, 2011



*Integrität (Unversehrtheit)**
Zurechenbarkeit+
Rechtsverbindlichkeit+

°Nichtverkettbarkeit
(Zweckbindung, Zwecktrennung)

*Verfügbarkeit**
Findbarkeit*
Erreichbarkeit+
Ermittelbarkeit+
Verbindlichkeit+

**Vertraulichkeit*
*Verdecktheit
+Anonymität
+Unbeobachtbarkeit

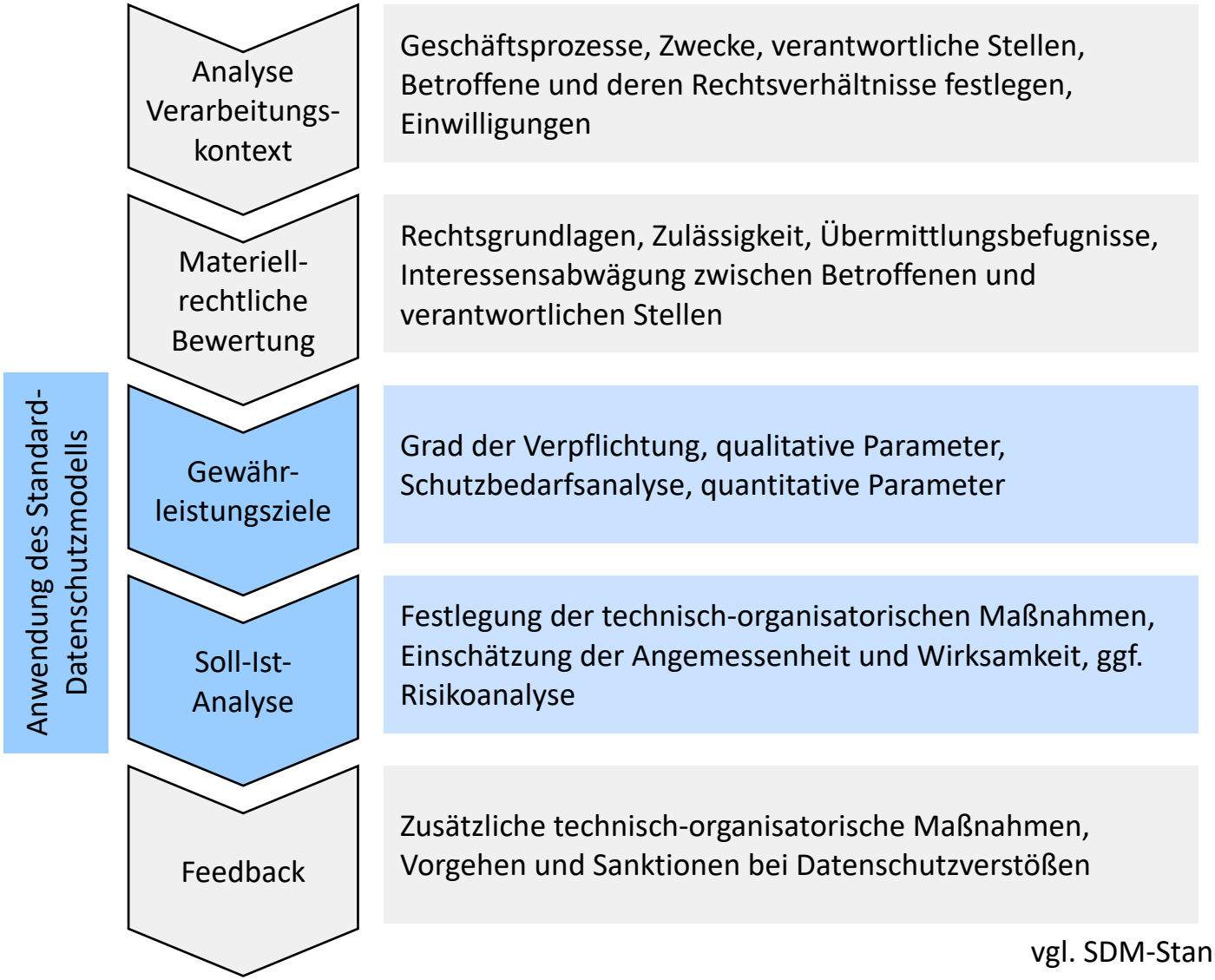
°Transparenz

°*Intervenierbarkeit (Eingreifbarkeit)*
+Kontingenz
+Abstreitbarkeit

kursiv = *elementare Schutzziele*
normal = abgeleitete Schutzziele
* = Schutz der Inhaltsdaten
+ = Schutz der Verkehrsdaten
° = spezifische Datenschutz-Schutzziele

x ——— y
Dualität

Standard-Datenschutzmodell



vgl. SDM-Standard 1.0, 2016

Vorgehensmodelle und Softwareunterstützung zur Umsetzung des Standard-Datenschutzmodells

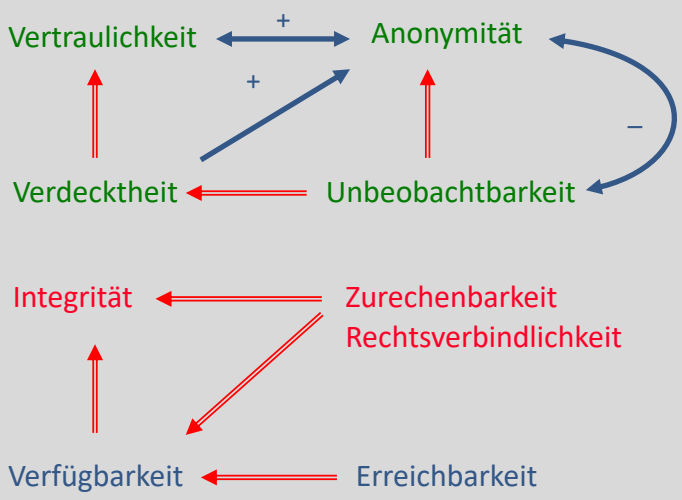
- Sicherheitsmanagemement
  - Schutzziele und Vorgehensweise nach dem Standard 200-2 des Bundesamts für Sicherheit in der Informationstechnik
- Datenschutzmanagement
  - Gewährleistungsziele und Vorgehensweise nach dem Standard-Datenschutzmodell
- Gemeinsamkeiten und Unterschiede
  - Sicherheitsmanagement und Datenschutzmanagement im Vergleich
- Möglichkeiten einer Softwareunterstützung

Verknüpfung von Sicherheit und Datenschutz

IT-Sicherheit

Schutz der Daten

Schutzziele der mehrseitigen Sicherheit



Datenschutz

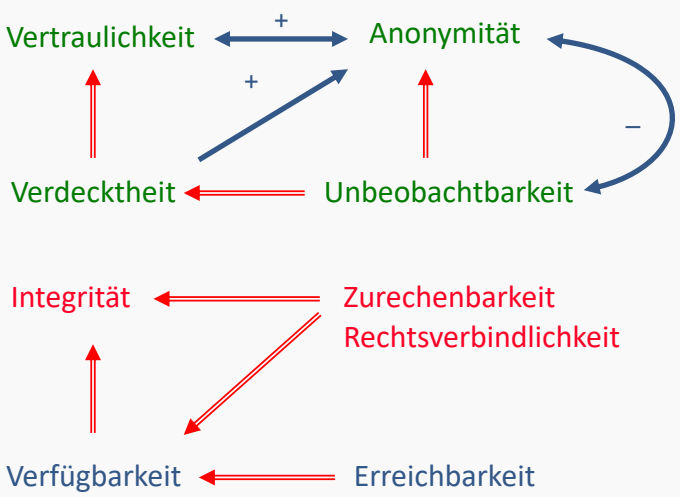
Schutz der Menschen

Gewährleistungsziele im Datenschutz

Schutzziele und Gewährleistungsziele im Vergleich

- entnommen aus den Schutzzielen der mehrseitigen Sicherheit: (2000)
  - Vertraulichkeit, Verdecktheit, Anonymität, Unbeobachtbarkeit, Integrität, Zurechenbarkeit, Rechtsverbindlichkeit, Verfügbarkeit, Erreichbarkeit

Schutzziele der mehrseitigen Sicherheit



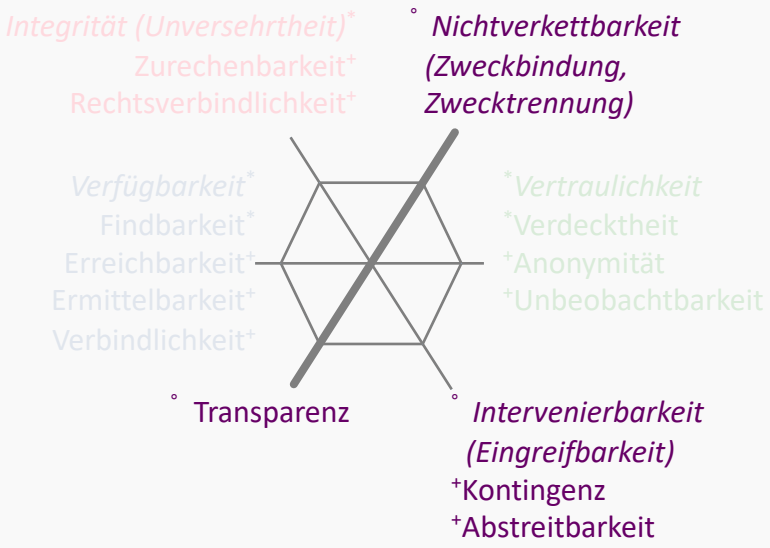
Gewährleistungsziele im Datenschutz

Schutzziele und Gewährleistungsziele im Vergleich

- hinzugekommen als (neue) Gewährleistungsziele: (2011)
  - Intervenierbarkeit/Abstreitbarkeit als Gegenteil zu Zurechenbarkeit/…
  - Nichtverkettbarkeit und Transparenz als Gegensatzpaare
- Idee: Erzeugen einer Dualität innerhalb der Gewährleistungsziele

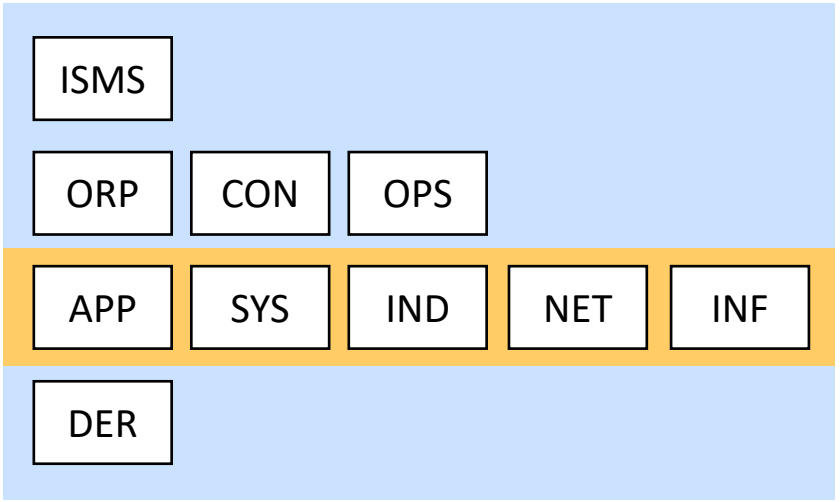
Schutzziele der mehrseitigen Sicherheit

Gewährleistungsziele im Datenschutz



Bausteine des IT-Grundschutz-Kompendiums des BSI

- Prozessorientierte Bausteine
  - ISMS (Sicherheitsmanagement)
  - ORP (Organisation und Personal)
  - CON (Konzeption und Vorgehensweise)
  - OPS (Betrieb)
  - DER (Detektion und Reaktion)
- Systemorientierte Bausteine
  - APP (Anwendungen)
  - SYS (IT-Systeme)
  - IND (Industrielle IT)
  - NET (Netze und Kommunikation)
  - INF (Infrastruktur)



Stand der öffentlich zugänglichen Bausteinbeschreibungen

- IT-Grundschutz-Kompendium des BSI
  - 39 Prozessorientierte Bausteine
  - 49 Systemorientierte Bausteine

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/bausteine_node.html

- Standard-Datenschutzmodell
  - Baustein 11 "Aufbewahrung"
  - Baustein 41 "Planung und Spezifikation"
  - Baustein 42 "Dokumentation"
  - Baustein 43 "Protokollierung"
  - Baustein 50 "Trennung"
  - Baustein 60 "Löschen und Vernichten"
  - Baustein 80 "Datenschutzmanagement"

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

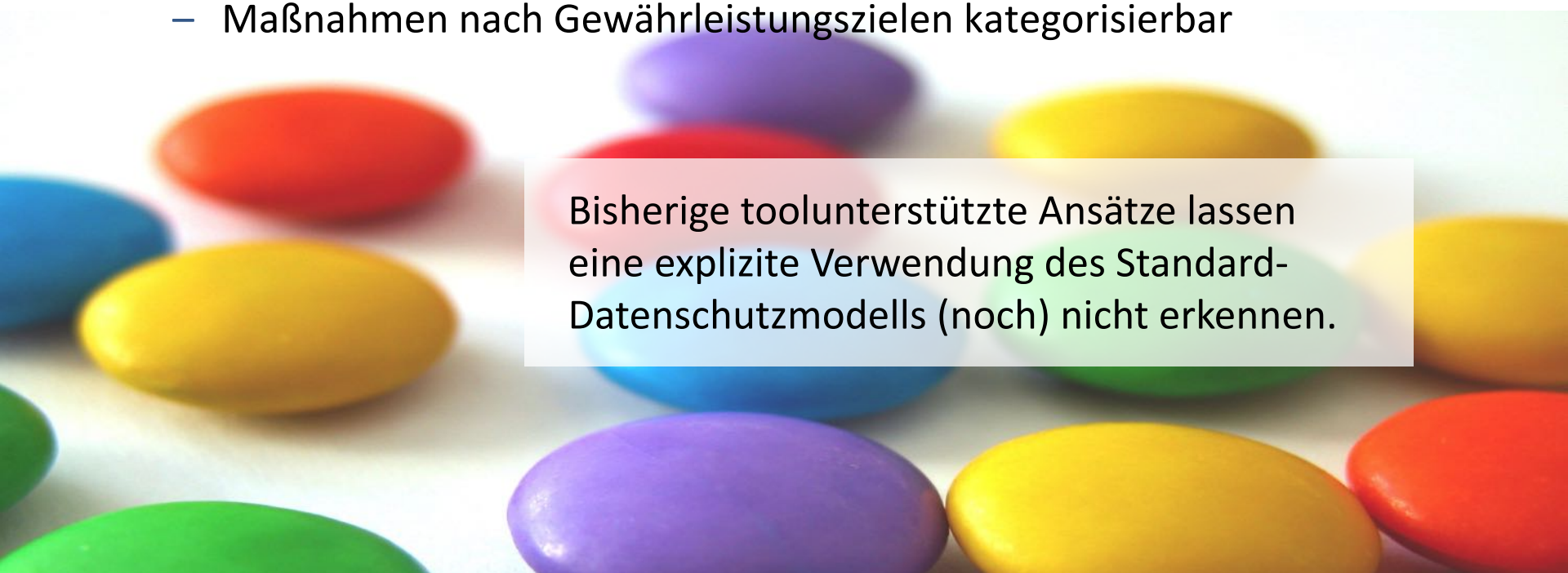
Vorgehensmodelle und Softwareunterstützung zur Umsetzung des Standard-Datenschutzmodells

- Sicherheitsmanagemement
  - Schutzziele und Vorgehensweise nach dem Standard 200-2 des Bundesamts für Sicherheit in der Informationstechnik
- Datenschutzmanagement
  - Gewährleistungsziele und Vorgehensweise nach dem Standard-Datenschutzmodell
- Gemeinsamkeiten und Unterschiede
  - Sicherheitsmanagement und Datenschutzmanagement im Vergleich
- Möglichkeiten einer Softwareunterstützung

Jan Osterkamp

Anforderungen an eine Softwarelösung aus dem SDM

- Verfahrensorientiert
  - Daten, Prozesse und Systeme als Komponenten
  - PDCA-Zyklus fördernd
- Priorisierung von Gewährleistungszielen
  - auf Verfahrensebene
  - teils auch für einzelne Teilverfahren
  - Maßnahmen nach Gewährleistungszielen kategorisierbar



Bisherige toolunterstützte Ansätze lassen eine explizite Verwendung des Standard-Datenschutzmodells (noch) nicht erkennen.

Anforderungen an eine Softwarelösung aus dem SDM

- Schaffung von Verständnis
  - Juristen, Techniker und Datenschützer zusammenbringen
  - Diskussionen ermöglichen
- Austausch unter Datenschützern
  - Maßnahmen erweitern, verfeinern und diskutieren
  - Plattform für Feedback bieten oder komfortabel kanalisieren

Bisherige toolunterstützte Ansätze lassen eine explizite Verwendung des Standard-Datenschutzmodells (noch) nicht erkennen.

SDM in existierenden Softwarelösungen

Bisherige toolunterstützte Ansätze lassen eine explizite Verwendung des Standard-Datenschutzmodells (noch) nicht erkennen.

- verinice. Datenschutzmodul (https://verinice.com/datenschutz/)
  - Übersicht über Verarbeitungstätigkeiten
  - »Integration von EU-DSGVO« auf der Roadmap
- HiScout Datenschutz (https://www.hiscout.com/module/hiscout-datenschutz)
  - Verarbeitungstätigkeitsverzeichnis
  - Speichern von bestimmten Datenschutz-Konzepten

SDM in existierenden Softwarelösungen

Bisherige toolunterstützte Ansätze lassen eine explizite Verwendung des Standard-Datenschutzmodells (noch) nicht erkennen.

- Intervalid (https://intervalid.com)
  - Verzeichnis von Verarbeitungen
  - Erfassung von Maßnahmen und deren Fortschritt
  - Zuordnung von Maßnahmen zu Verarbeitungen

- Das Datenschutz Tool (https://datenschutz-tool.de)
  - Verzeichnis von Verarbeitungen
  - Analyse nach den sechs Gewährleistungszielen
  - Übersicht über Verarbeitungen mit Prüffragen

Das SDM-Tool Protectheus

PROTECTHEUS

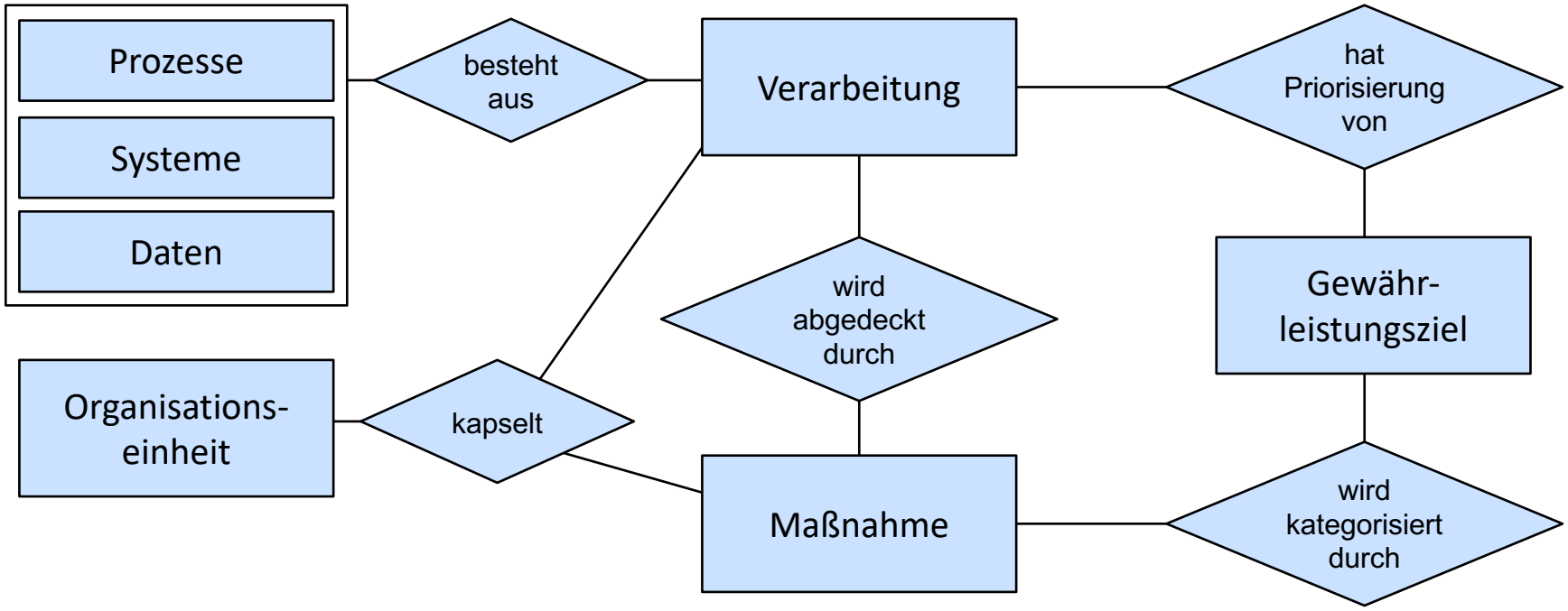
Zielsetzung: Unterstützung der SDM-Vorgehensweise, des gemeinsamen organisationsinternen und -übergreifenden Datenschutzmanagements

- Diskussionsmöglichkeit direkt am Verfahren
- Austausch über Maßnahmen intern und extern
- Priorisierung von Gewährleistungszielen für jedes (Teil-)Verfahren
- Maßnahmen nach Gewährleistungszielen

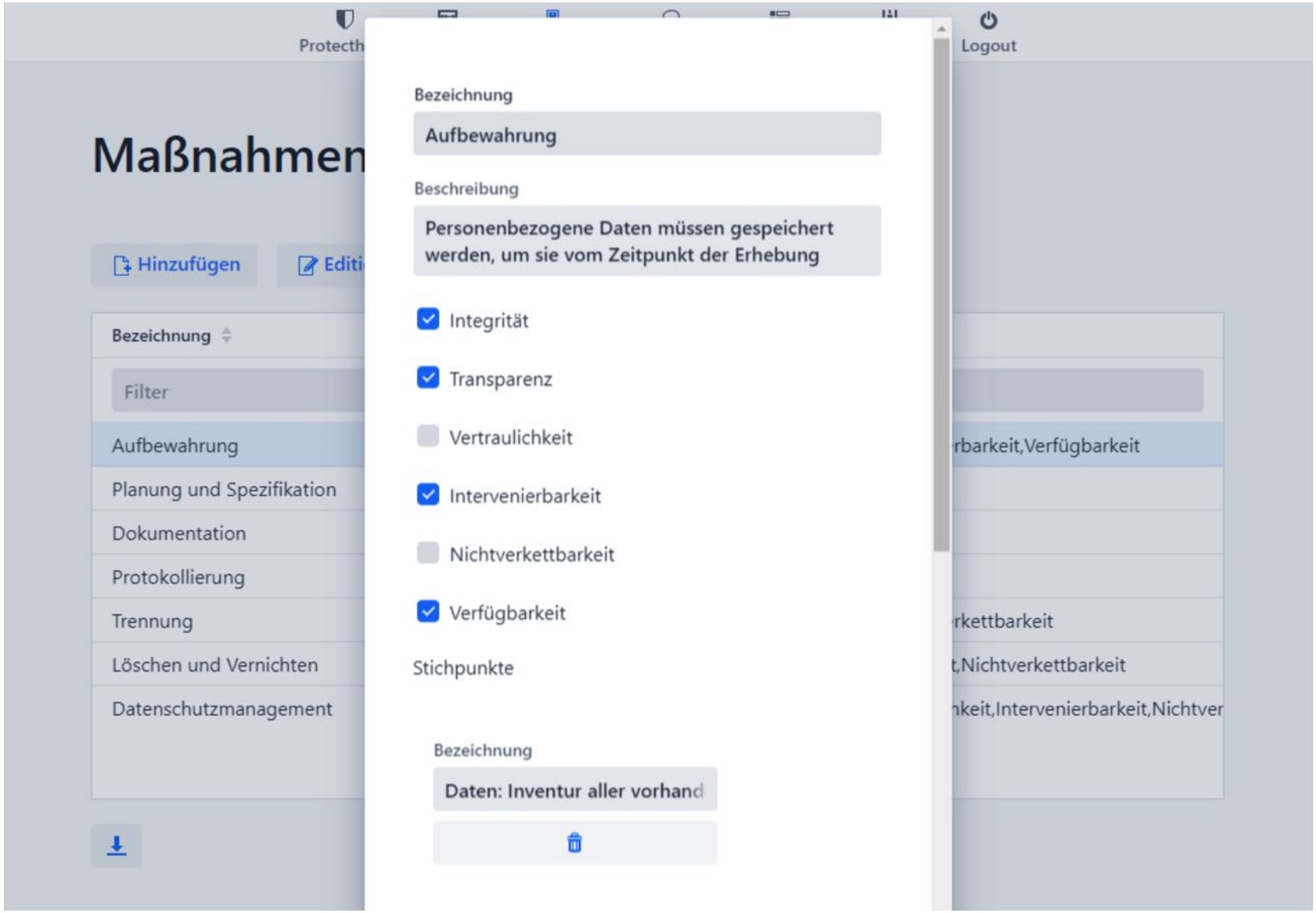
Das SDM-Tool Protectheus

PROTECTHEUS

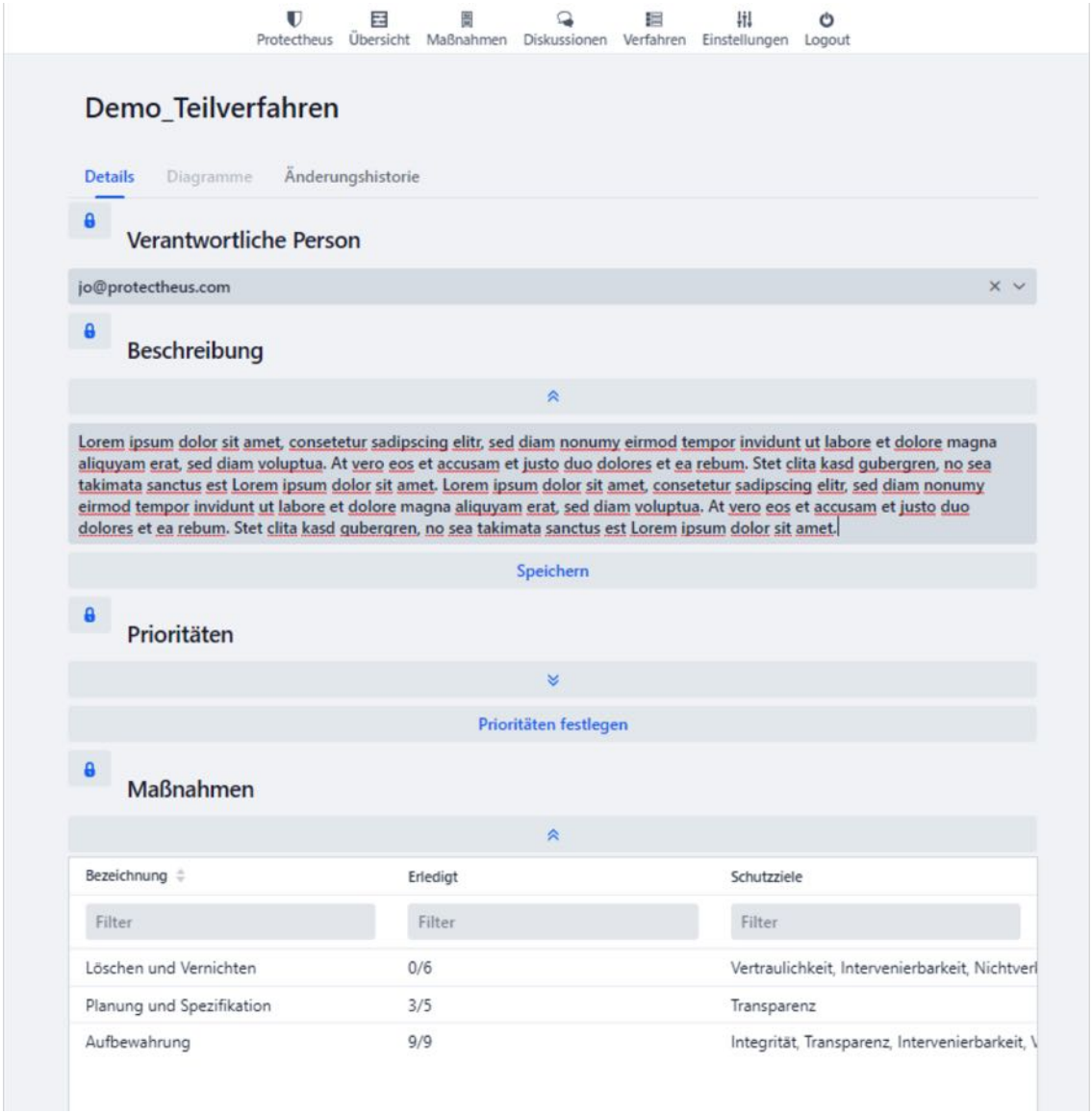
- Diskussionsmöglichkeit direkt am Verfahren
- Austausch über Maßnahmen intern und extern
- Priorisierung von Gewährleistungszielen für jedes (Teil-)Verfahren
- Maßnahmen nach Gewährleistungszielen



Das SDM-Tool Protectheus

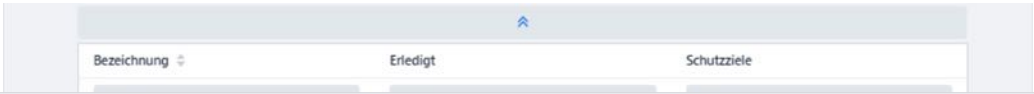


Das SDM-Tool Protectheus



Das SDM-Tool Protectheus

PROTECTHEUS



Maßnahmen

Bezeichnung	Erledigt	Schutzziele
Filter	Filter	Filter
Löschen und Vernichten	0/6	Vertraulichkeit, Intervenierbarkeit, Nichtverl
Planung und Spezifikation	3/5	Transparenz
Aufbewahrung	9/9	Integrität, Transparenz, Intervenierbarkeit, V

- [ ] Planung der Erstellung der Dokumentation der Prozessabläufe
- [x] Planung der Spezifikation der Fachapplikation
- [x] Planung der Erstellung eines Lasten- und Pflichtenhefts
- [x] Planung der Spezifikation der Schnittstellen
- [ ] Erstellung eines Planes zur Gestaltung der Planungsphase

Maßnahmen editieren

Offene Punkte

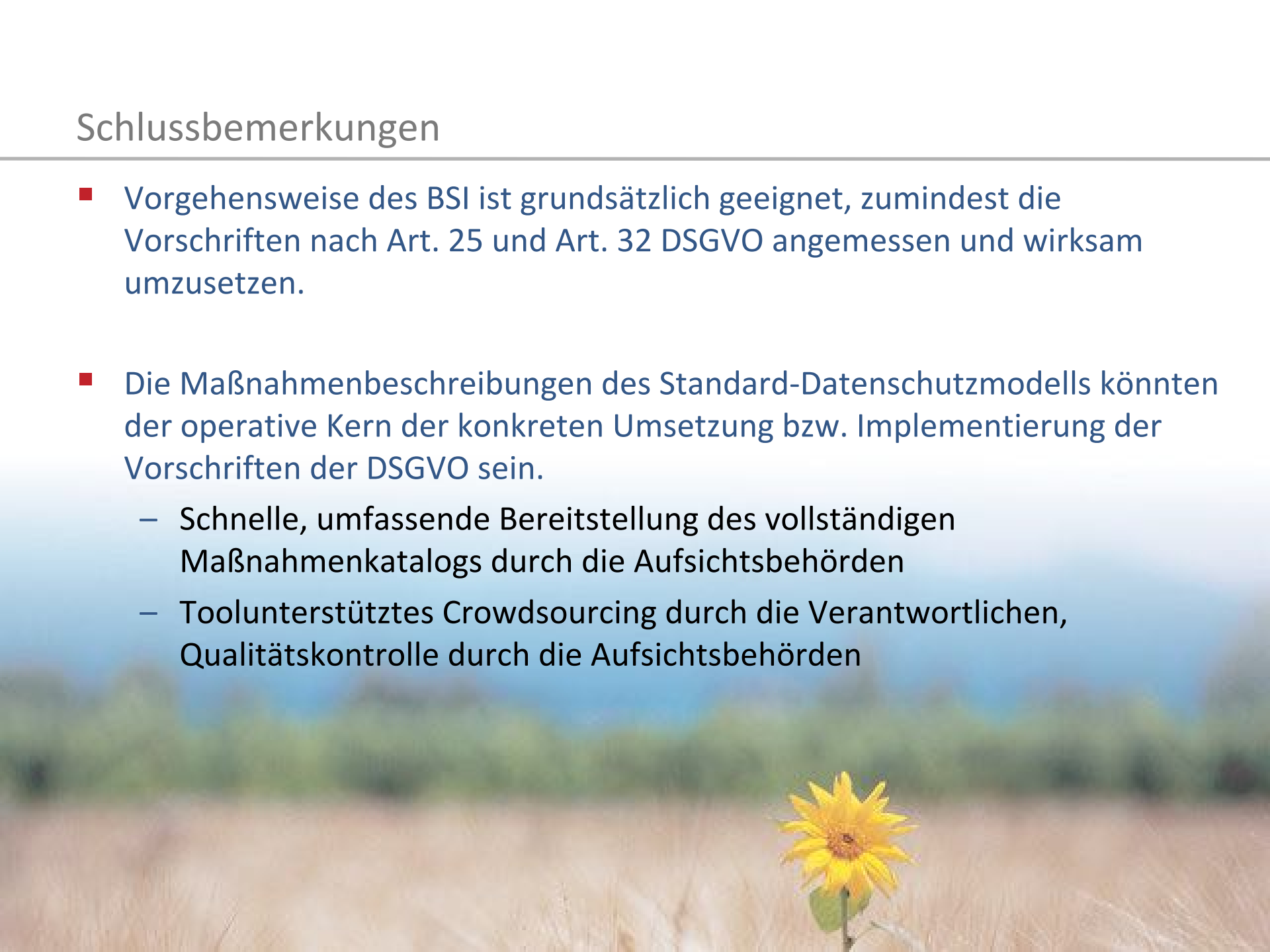
PROTECTHEUS

- Diskussionsplattform für Maßnahmen
  - Diskussionspunkte in Form von schließbaren »Issues«
  - Bewertung von Maßnahmen durch andere Nutzer
- Klarere Teilung zwischen Daten, Prozessen und Systemen
- Timer und Benachrichtigungen für Fristen
- Visualisierungen

Schlussbemerkungen

- Vorgehensweise des BSI ist grundsätzlich geeignet, zumindest die Vorschriften nach Art. 25 und Art. 32 DSGVO angemessen und wirksam umzusetzen.

- Die Maßnahmenbeschreibungen des Standard-Datenschutzmodells könnten der operative Kern der konkreten Umsetzung bzw. Implementierung der Vorschriften der DSGVO sein.
  - Schnelle, umfassende Bereitstellung des vollständigen Maßnahmenkatalogs durch die Aufsichtsbehörden
  - Toolunterstütztes Crowdsourcing durch die Verantwortlichen, Qualitätskontrolle durch die Aufsichtsbehörden



inf.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DEPARTMENT OF INFORMATICS
SECURITY AND PRIVACY

HOME COURSES THESES RESEARCH PEOPLE SERVICE

UHH → MIN-Fakultät → Fachbereich Informatik → Einrichtungen → Arbeitsbereiche → Security and Privacy → **Home**

WORKING GROUP ON «SECURITY AND PRIVACY»

Security and Privacy

Information systems become more and more important in critical infrastructures, while the Internet has evolved to a critical infrastructure itself. The secure operation of these infrastructures is vital and their failure can have severe impacts up to the loss of human lives.
Security refers to the fact that protection goals are achieved in the presence of malicious attacks and system failures. Typical security goals can be confidentiality, integrity, accountability, and availability. Security and privacy in information systems addresses both technical and organizational aspects, such as building and establishing security concepts and security infrastructures as well as risk analysis and risk management.
Privacy can be a conflicting goal to security, but they can also benefit from each other. Hence, it is necessary to balance both when developing secure information systems.

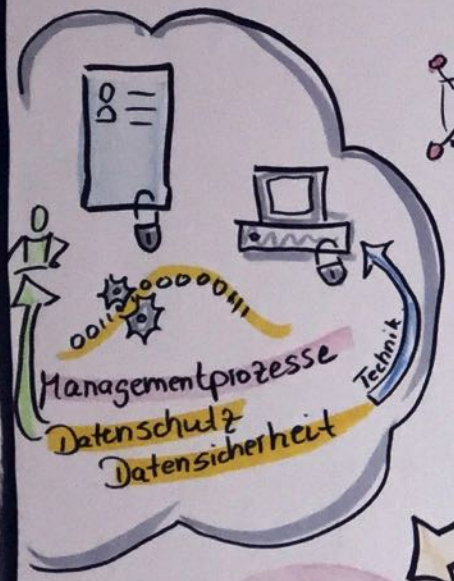
Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

Telefon +49 40 42883 2358

federrath@informatik.uni-hamburg.de

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

Vorgehensmodelle und Softwareunterstützung zur Umsetzung des Standard-Datenschutzmodells



Gewährleistungsziele

7 Bausteine

Bausteine in verschiedenen Kategorien

Strukturierte Vorgehensweise

Risikobetrachtung

Softwarelösung SDM

Dokumentation

Datenschützer

"Verbesserung"

Zusammenarbeit

Qualitätskontrolle