



IT-Sicherheit und Datenschutzmanagement

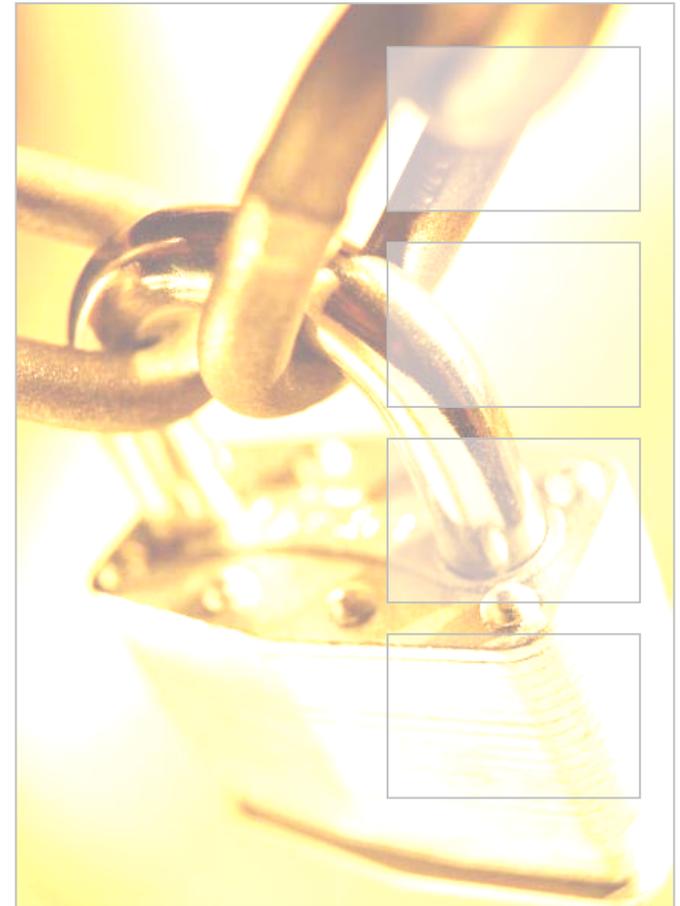
Gemeinsamkeiten und Unterschiede

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg

<http://www-sec.uni-regensburg.de/>

Gliederung des Vortrags

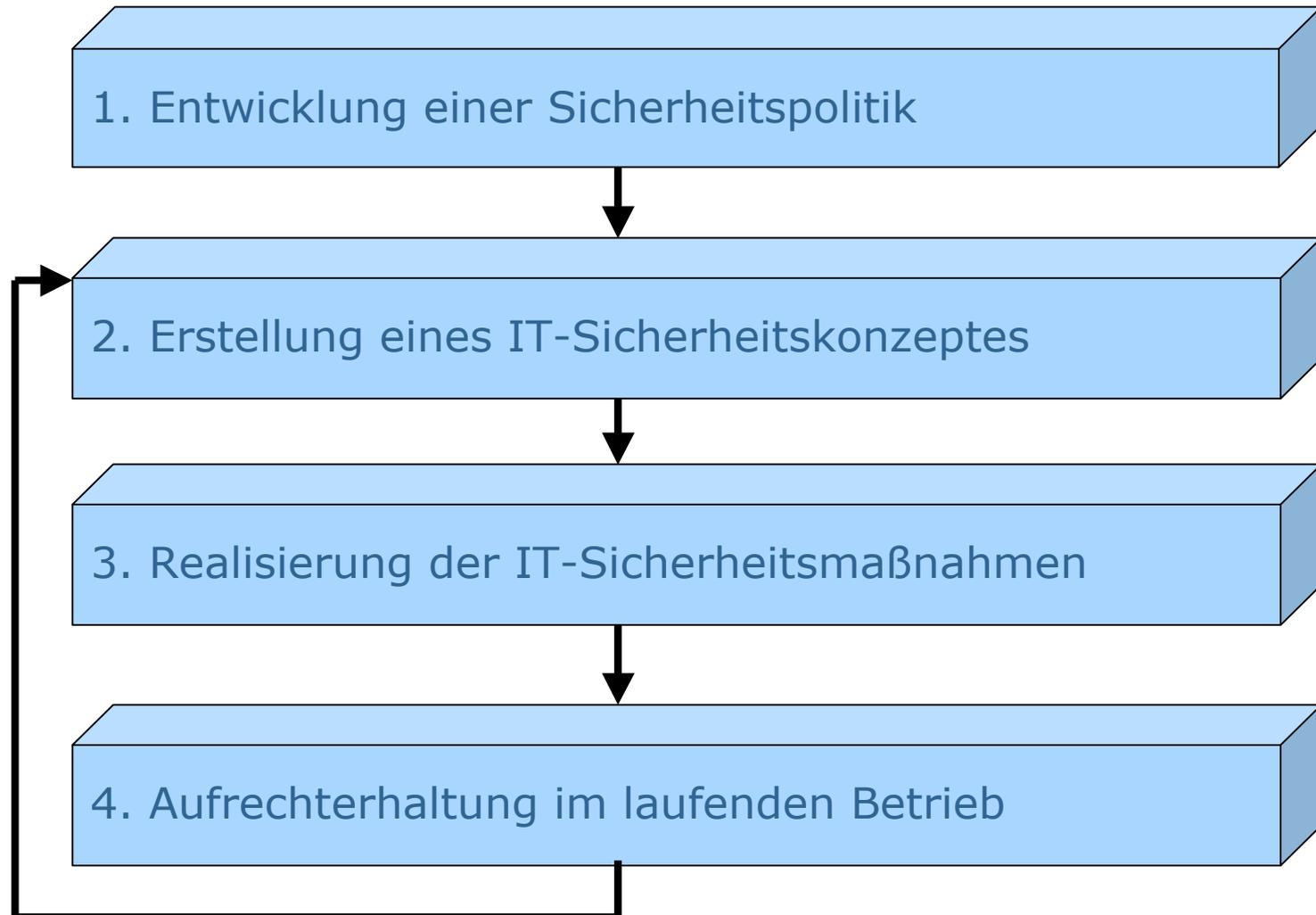
- Einführung: Begriffe
- Vorgehensmodell IT-Sicherheit
- Risikomanagementkreislauf
- Verknüpfung zu Datenschutz?
- Grundlagen des Datenschutzes
- Einbettung in den Risikomanagementkreislauf
- Schlussbemerkungen



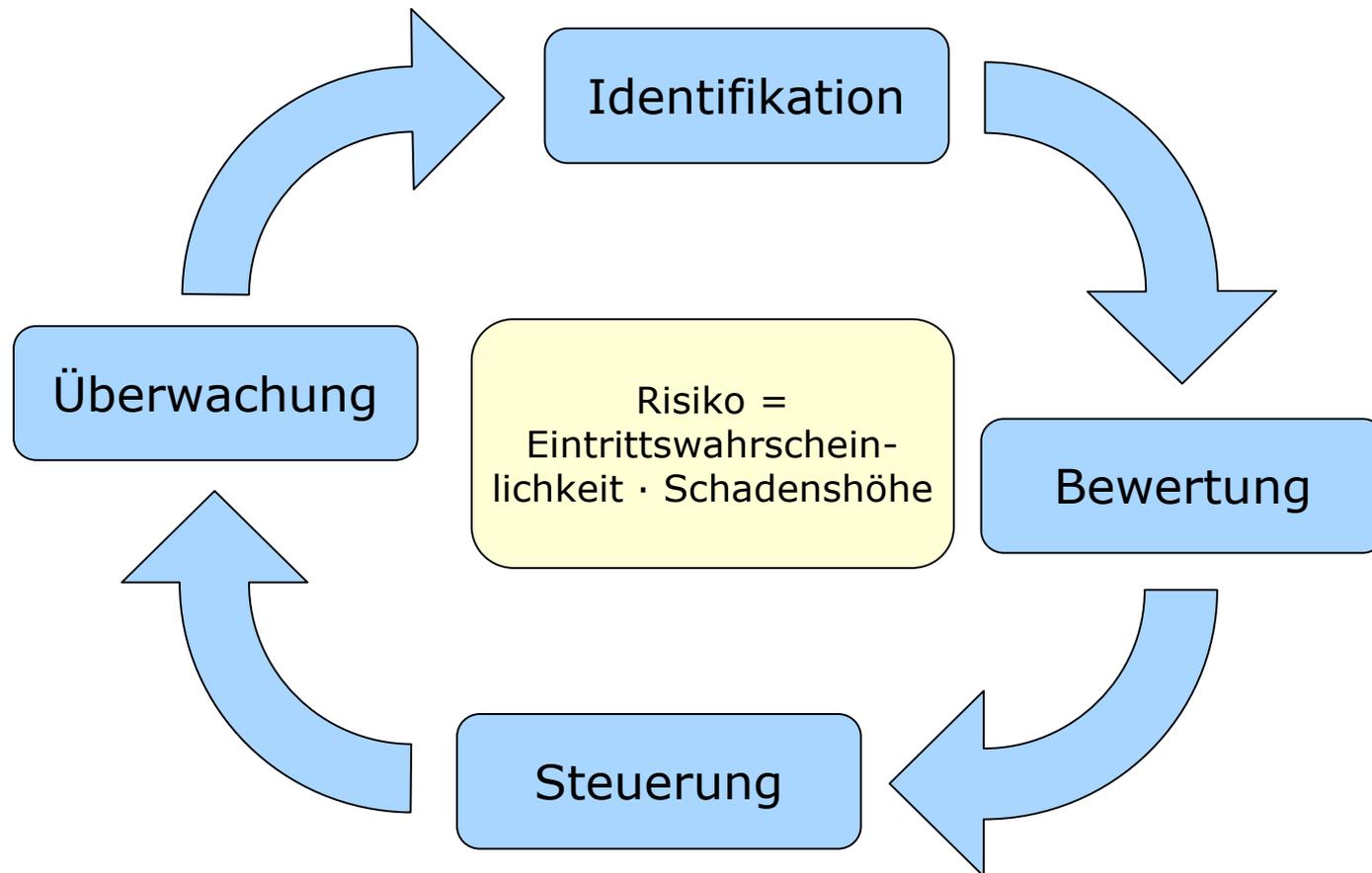
Begriffe

- IT-Sicherheitsmanagement
 - IT-Sicherheitsmanagement 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
 - 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.

Sicherheitsmanagement-Vorgehensmodell

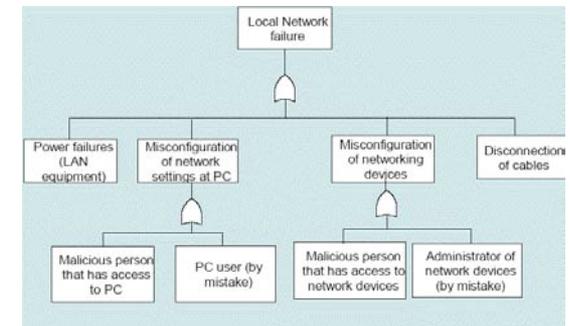
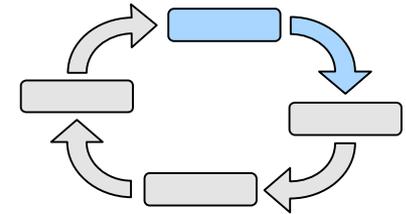


Risikomanagement Kreislauf



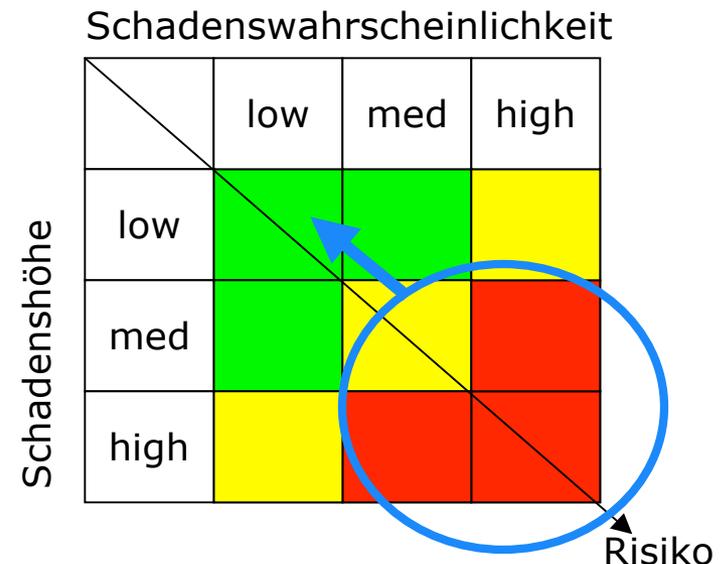
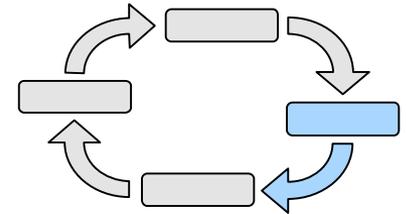
Identifikation von Bedrohungen

- Frage
 - »Welche Bedrohungen sind für das jeweilige Schutzobjekt relevant? «
- Methoden & Werkzeuge
 - OCTAVE-Methodik, CORAS-Framework
 - Checklisten
 - Workshops
 - Fehlerbäume, Attack-Trees
 - Szenarioanalysen
- Herausforderungen
 - Vollständige Erfassung aller Bedrohungen



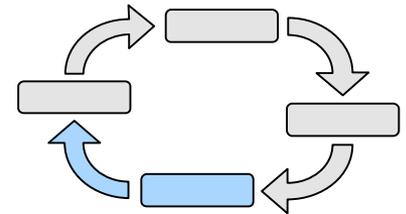
Bewertung von Risiken

- 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

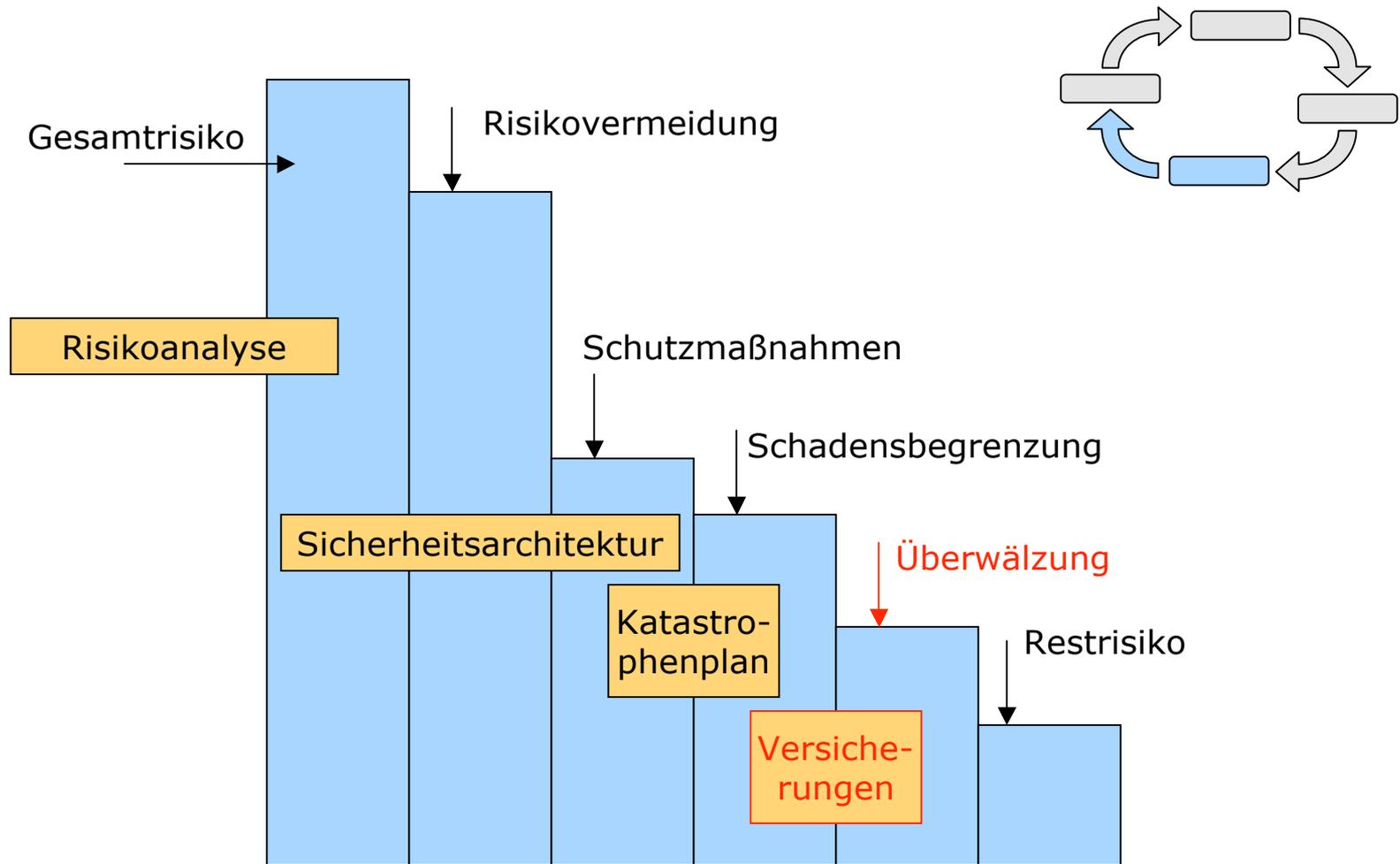


Steuerung der Risiken

- Frage
 - »Welche Risiken sollen wie behandelt werden?«
- Methoden
 - Best Practice Ansätze / Grundschatz
 - Hilfsmittel aus der Investitionsrechnung und Entscheidungstheorie, z.B. NPV, IRR, AHP
- Herausforderungen
 - Qualität der Entscheidung hängt von zu Grunde liegenden Daten ab (baut auf dem Bewertungsschritt auf)



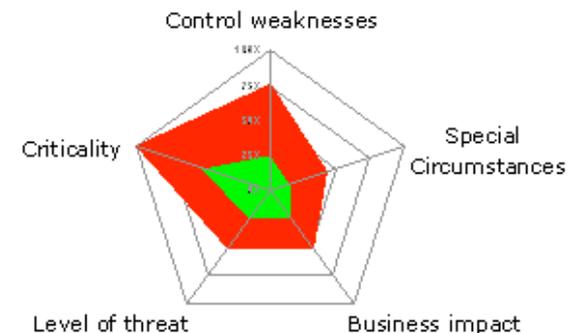
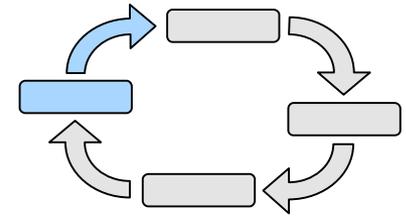
Risiko-Management für IT-Systeme



nach: Schaumüller-Bichl

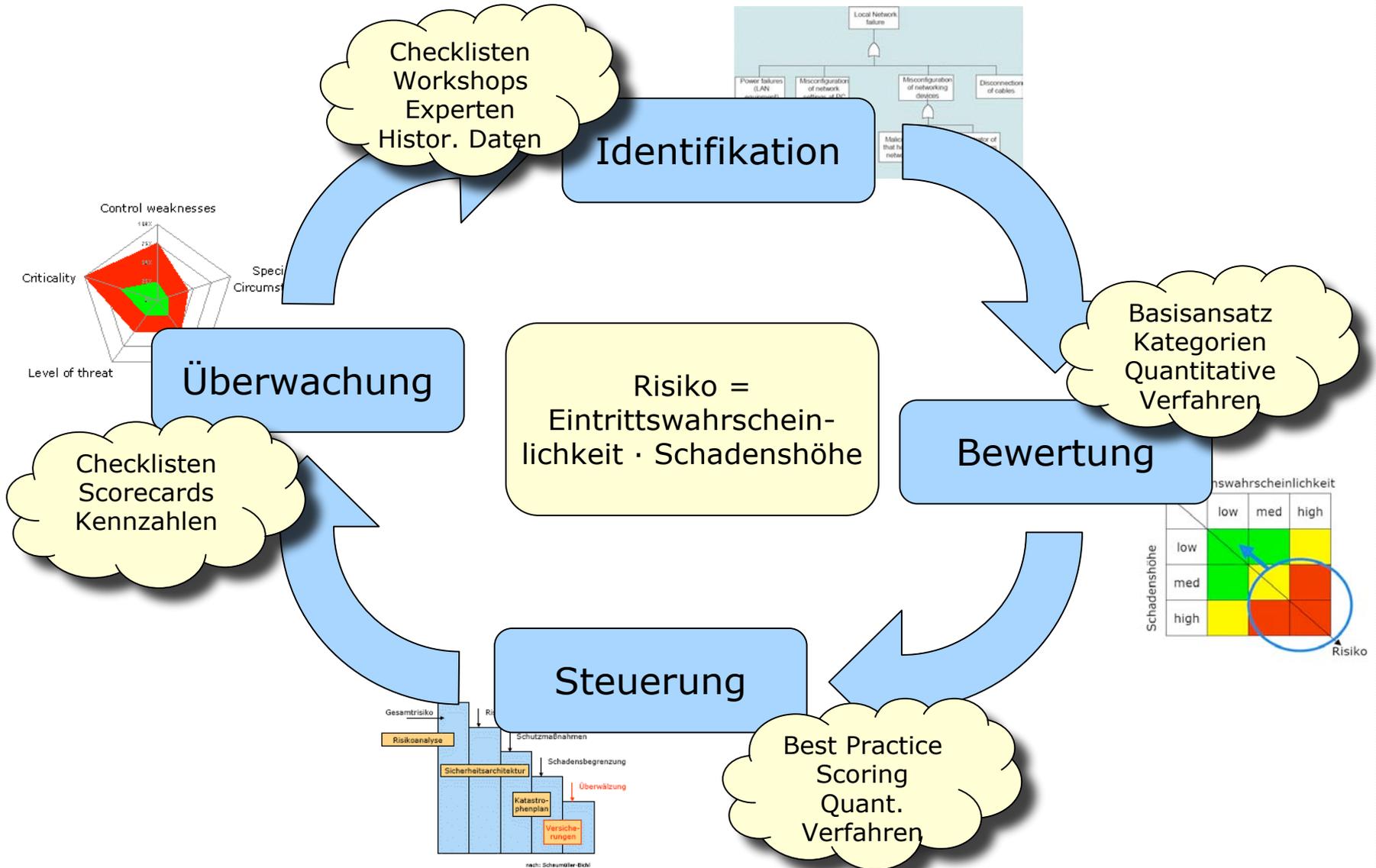
Überwachung der Risiken und Maßnahmen

- Frage
 - »Waren die Maßnahmen effektiv und effizient? Wie sicher ist die Organisation?«
- Methoden
 - Kennzahlen Systeme (z.B. TÜV Secure IT)
 - Security Scorecard oder Integration in Balanced Scorecard
- Herausforderungen
 - Die „richtigen“ Kennzahlen verwenden
 - Kennzahlen „richtig“ ermitteln/messen
 - Kennzahlen aktuell halten

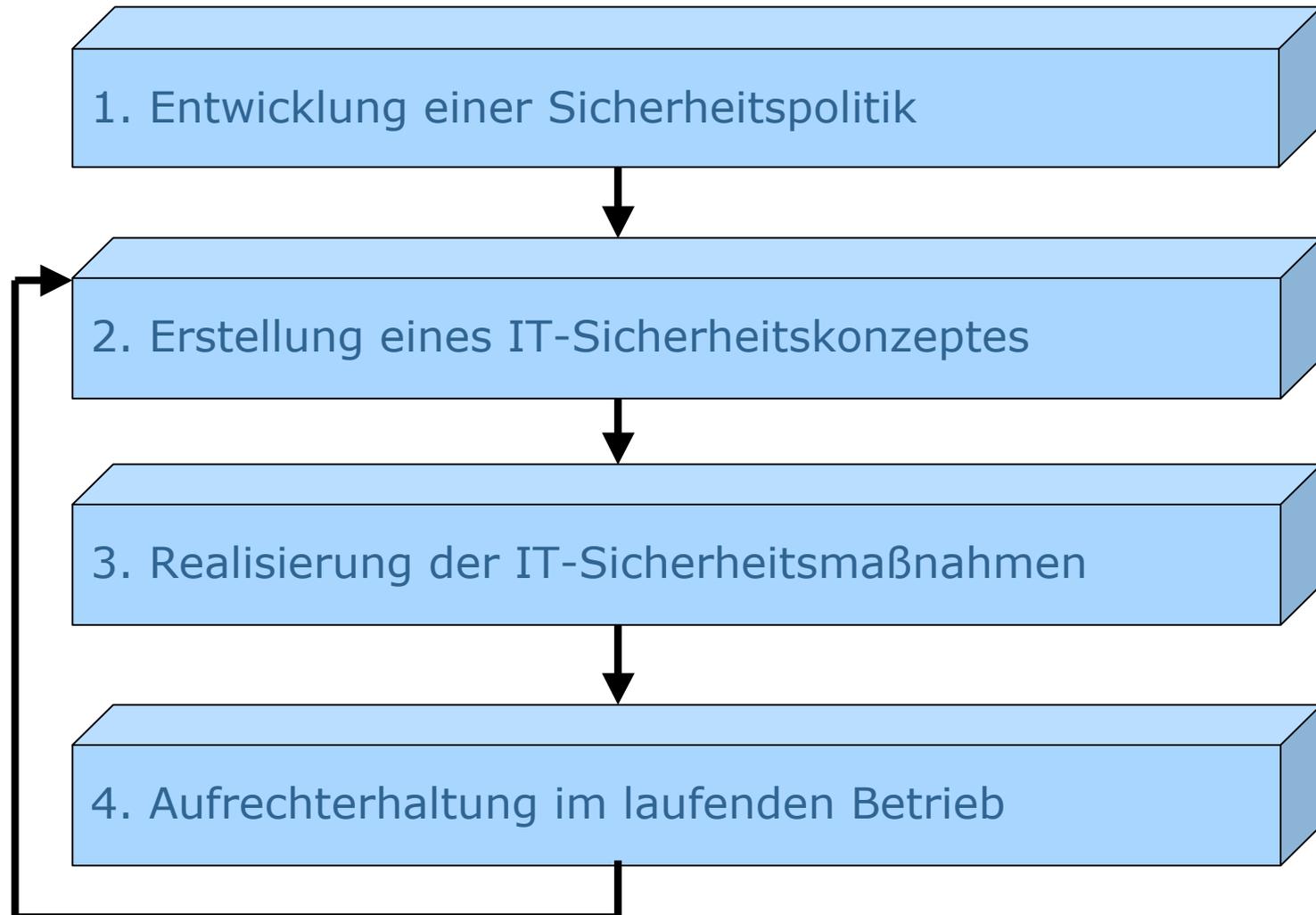


nach: Loomans, 2002

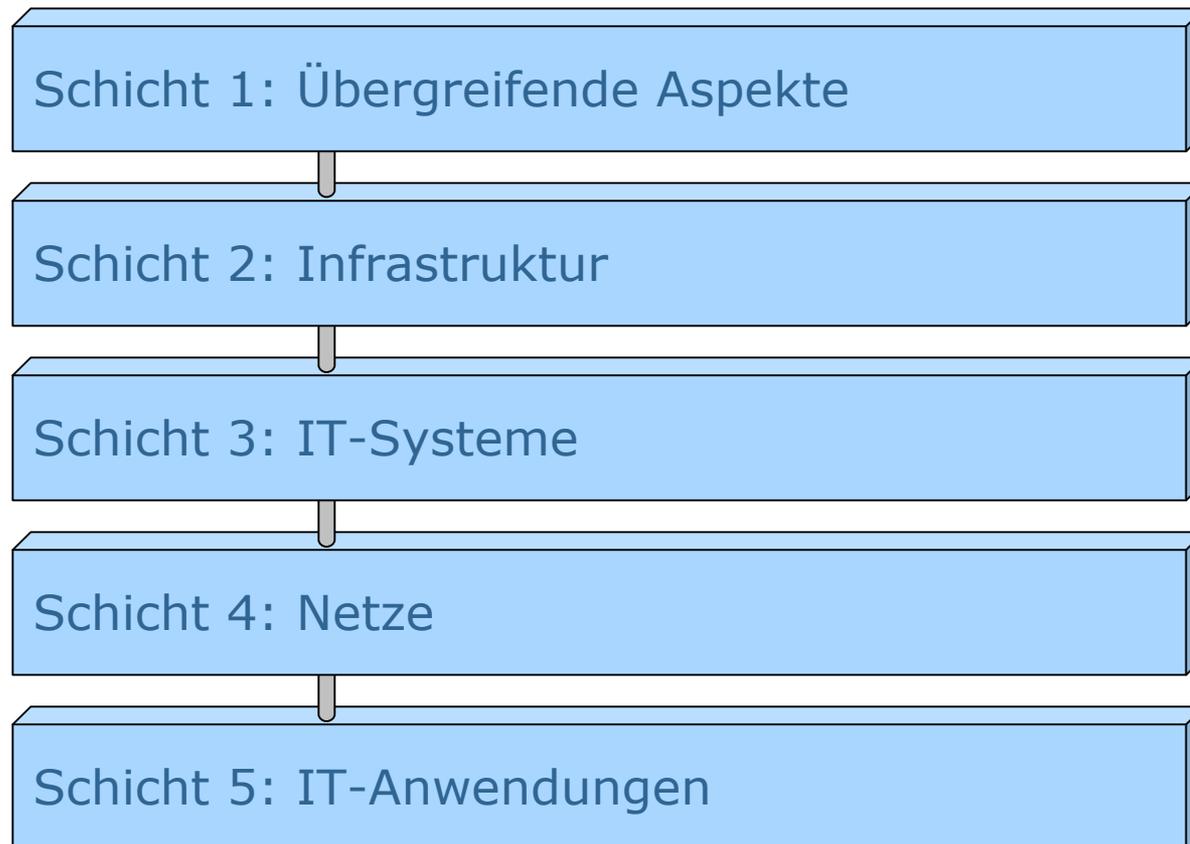
Risikomanagement Kreislauf



Sicherheitsmanagement-Vorgehensmodell

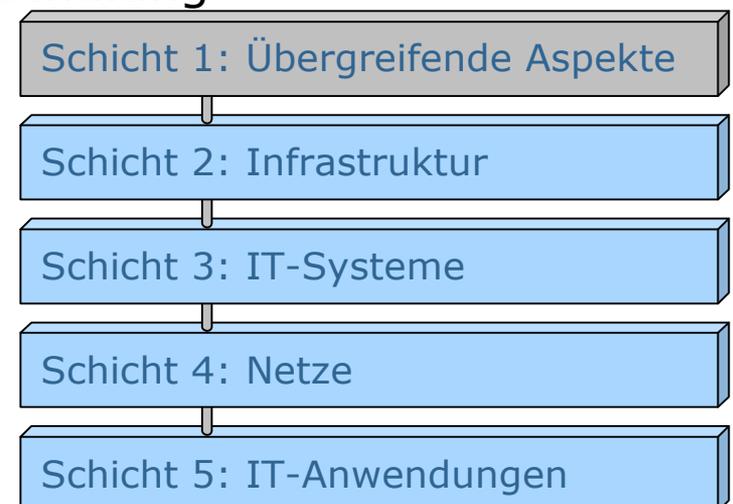


Schichtenmodell nach IT-Grundschutz



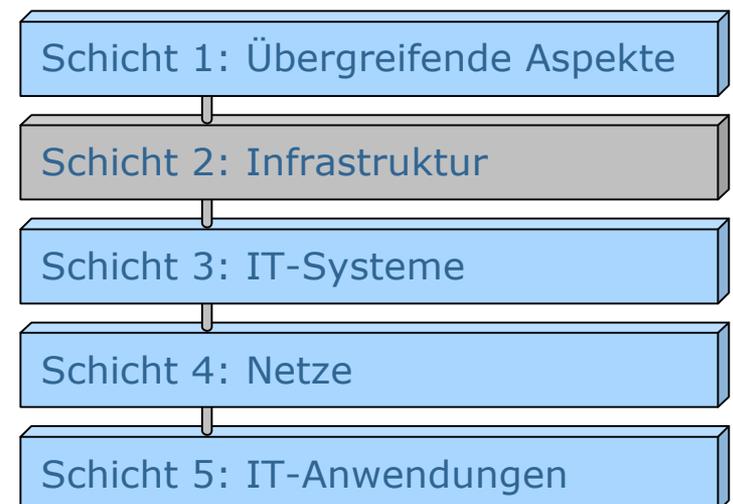
Bausteinkataloge

- Übergreifende Aspekte
 - IT-Sicherheitsmanagement
 - Organisation
 - Personal
 - **Datenschutz**
 - Kryptokonzept
 - Behandlung von Sicherheitsvorfällen
 - Outsourcing
 - IT-Sicherheitssensibilisierung und -schulung
 - ...



Bausteinkataloge

- Infrastruktur
 - Gebäude
 - Verkabelung
 - Büroraum
 - Serverraum
 - Datenträgerarchiv
 - Raum für technische Infrastruktur
 - ...



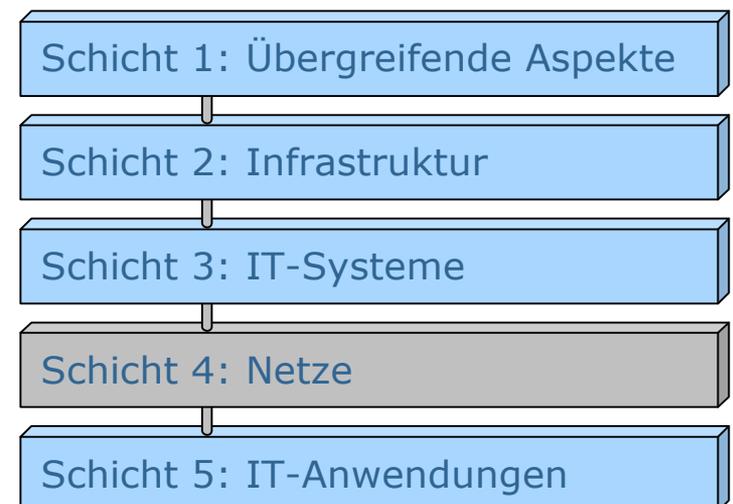
Bausteinkataloge

- IT-Systeme
 - Bausteingruppe Server
 - Bausteingruppe Client
 - Bausteingruppe Netzwerkkomponenten
 - Bausteingruppe Telekommunikationssysteme



Bausteinkataloge

- Netze
 - Heterogene Netze
 - Netz- und Systemmanagement
 - Modem
 - Remote-Access
 - LAN-Anbindung eines IT-Systems über ISDN
 - WLAN
 - VoIP
 - ...

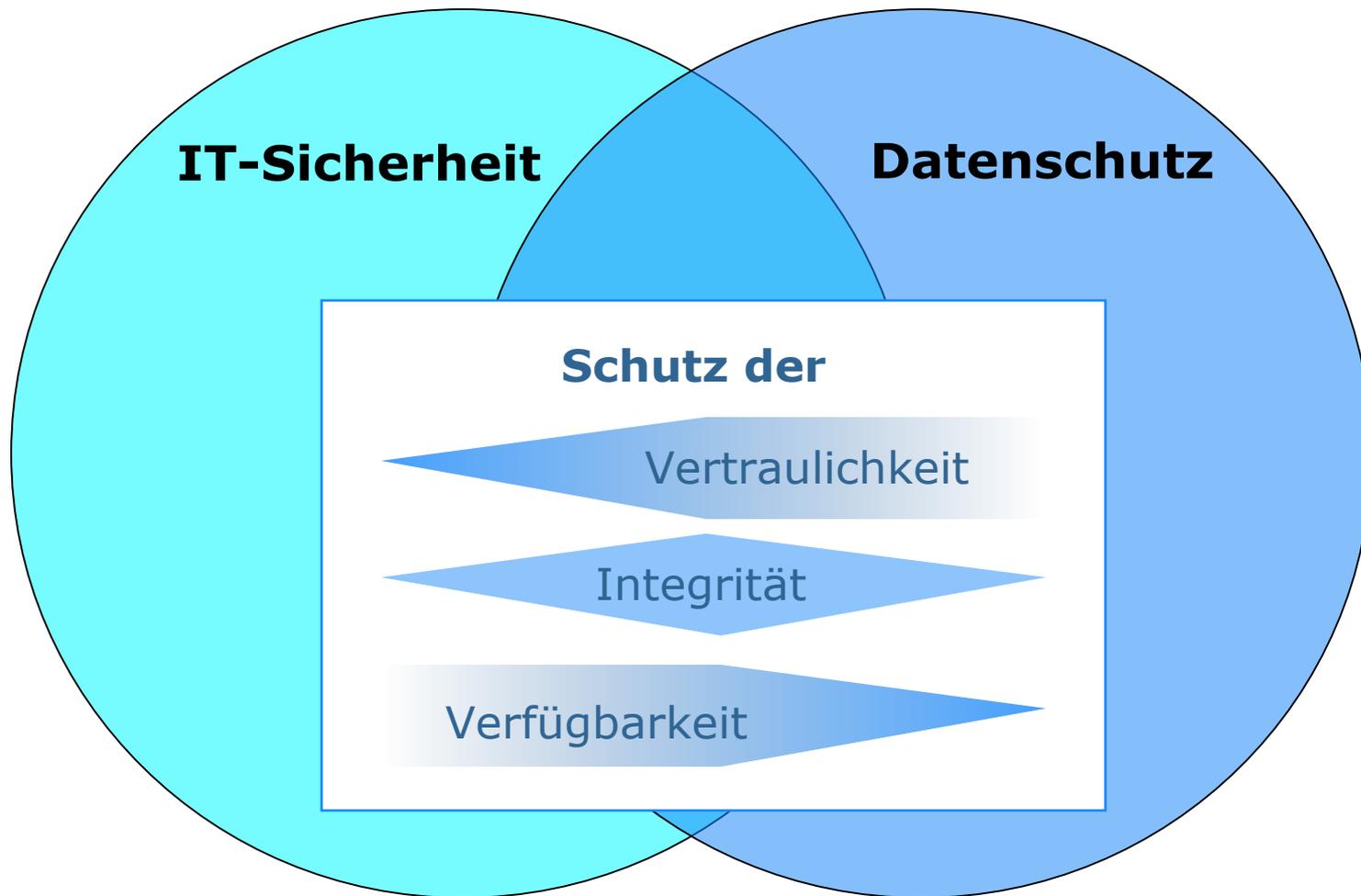


Bausteinkataloge

- IT-Anwendungen
 - Peer-to-Peer-Dienste
 - Datenträgeraustausch
 - E-Mail
 - Webserver
 - Faxserver
 - Datenbanken
 - Telearbeit
 - Novell eDirectory
 - SAP System



Verknüpfung von Sicherheit und Datenschutz



Was ist zu schützen?

Kommunikationsgegenstand WAS?

Vertraulichkeit
Verdecktheit

Inhalte

Kommunikationsumstände WANN?, WO?, WER?

Anonymität
Unbeobachtbarkeit

Sender

Ort

Empfänger

Integrität

Inhalte

Zurechenbarkeit
Rechtsverbindlichkeit

Absender

Bezahlung

Empfänger

Verfügbarkeit

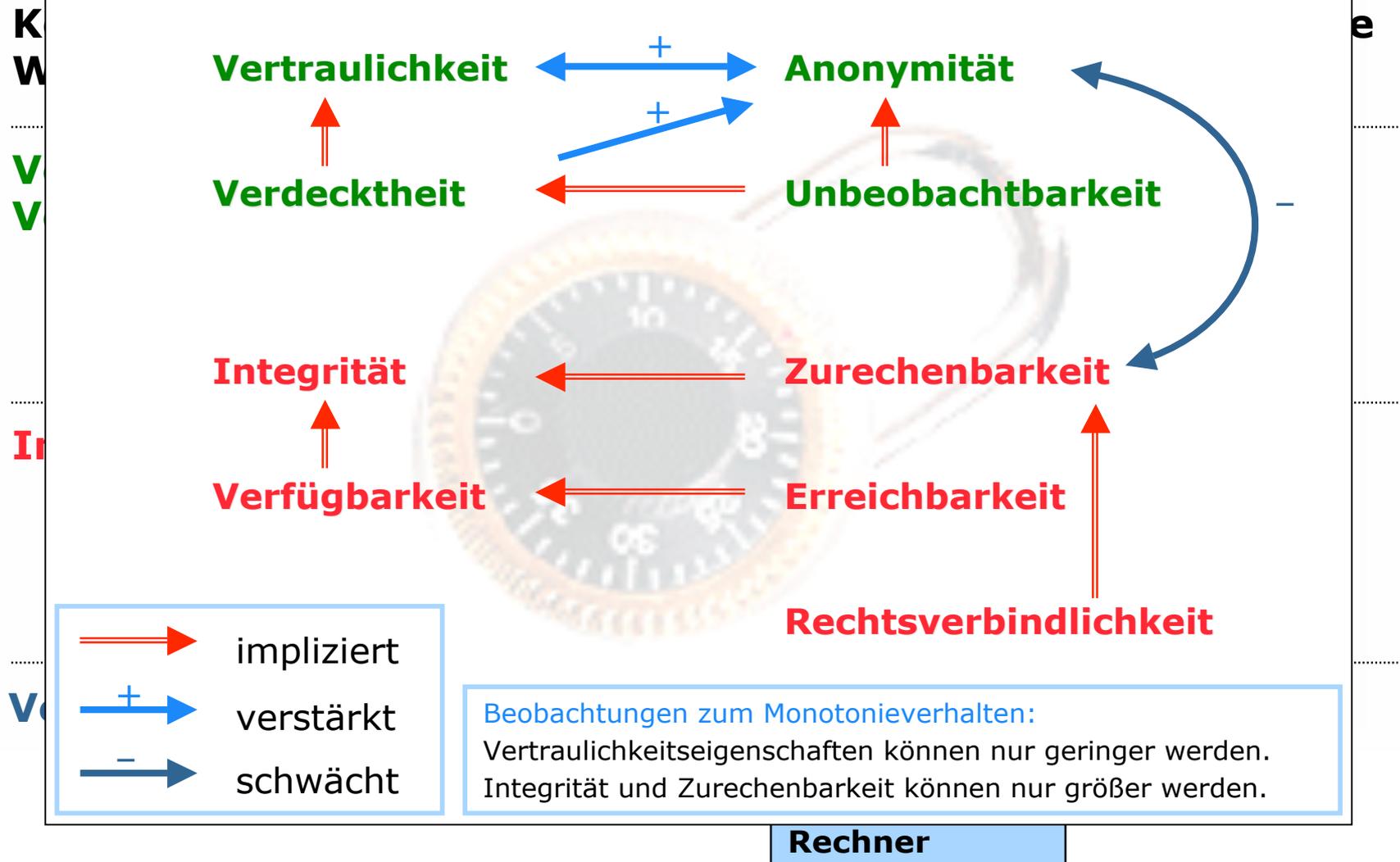
Inhalte

Erreichbarkeit

Nutzer

Rechner

Was ist zu schützen?



Datenschutz

**Kommunikationsgegenstand
WAS?**

**Vertraulichkeit
Verdecktheit**

Inhalte

**Kommunikationsumstände
WANN?, WO?, WER?**

**Anonymität
Unbeobachtbarkeit**

Sender

Ort

Empfänger

Integrität

Inhalte

**Zurechenbarkeit
Rechtsverbindlichkeit**

Absender

Bezahlung

Schutz personenbezogener Daten:
Inhaltsdaten, Verkehrsdaten
Interessensdaten

Personenbezogene Daten in Netzen

- Bestandsdaten
 - Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses mit dem Kunden anfallen, z.B. Name, Adresse, Login-Kennung des Benutzers, Angaben über Bankverbindung
- Verkehrsdaten
 - Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden

Personenbezogene Daten – Warum Datenschutz?

Name, Vorname

Geburtsdatum

Telefonnummer

Wohnort

Religionszugehörigkeit

Steuernummer

Krankenversicherungs-Nr.

Autokennzeichen

Kreditkarten-Nr.

**Grundbuch- und
Katasterbezeichnung**

Kontonummer

Email-Adresse

«Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person

(Betroffener).»

Def. gemäß § 3 Abs. 1 BDSG

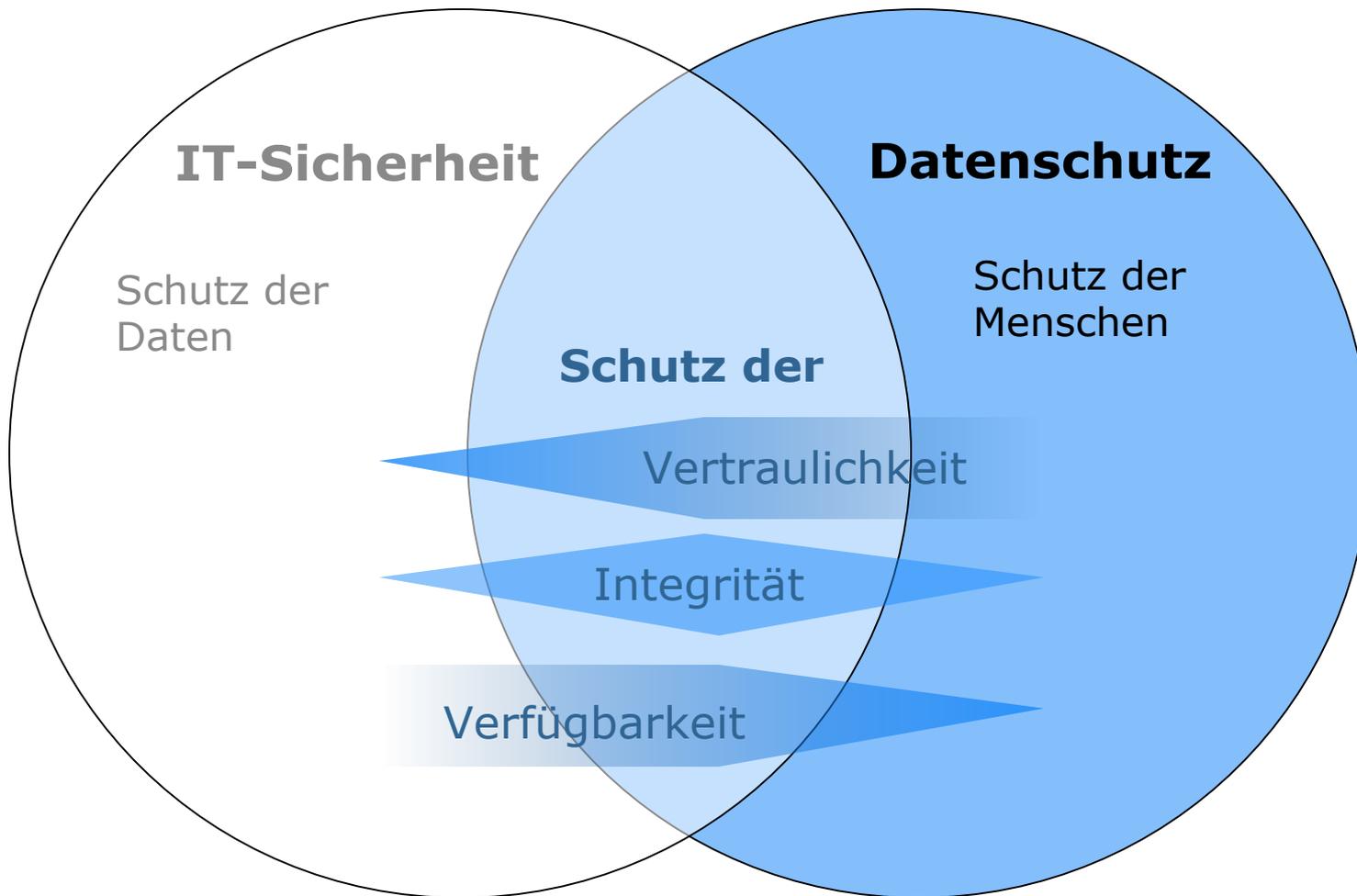
Recht auf informationelle Selbstbestimmung

»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. ...

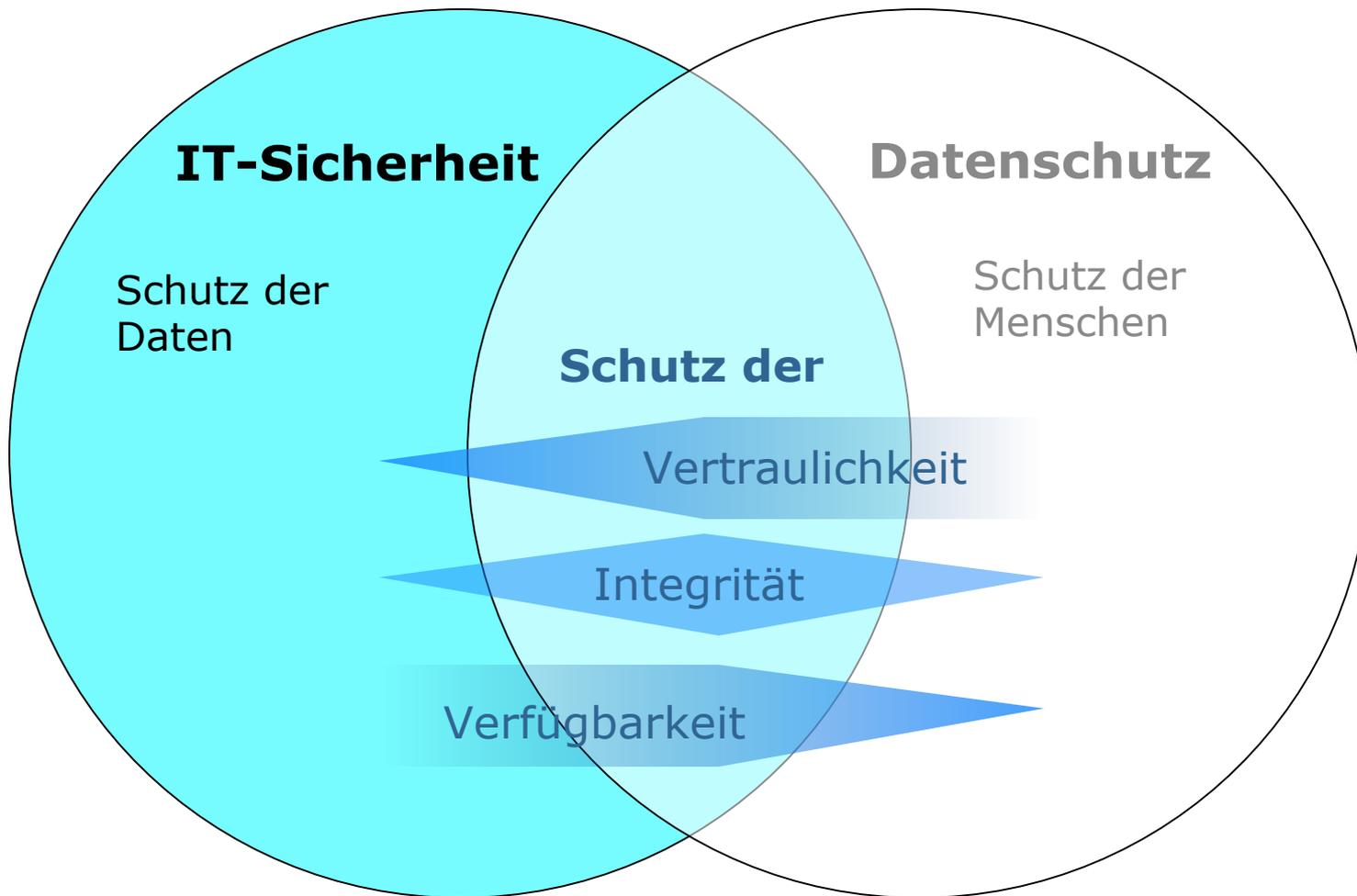
Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus 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

Verknüpfung von Sicherheit und Datenschutz

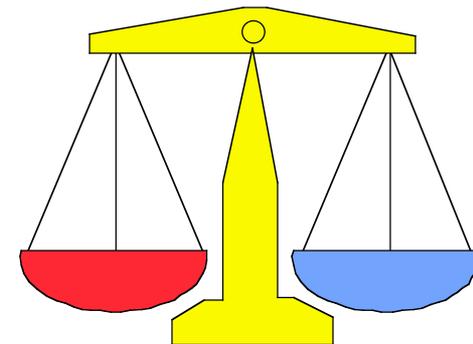


Verknüpfung von Sicherheit und Datenschutz



Geltungsbereiche von Datenschutzgesetzen

- **Datenschutz**
 - = Schutz der Menschen
 - ≠ (Schutz der Daten = Datensicherheit)
- **Datenschutz**
 - **allgemeine Regeln**
 - Bundesdatenschutzgesetz (BDSG)
 - Landesdatenschutzgesetze
 - EG-Datenschutzrichtlinie(n)
 - **bereichsspezifische Regeln**
 - Gesundheit/Soziales
 - Polizei/Verfassungsschutz
 - **Telekommunikation**
- **Grundsatz**
 - Bereichsspezifische Regeln gehen den allgemeinen vor!



«Drei Schichten» des Datenschutzrechts in Netzen

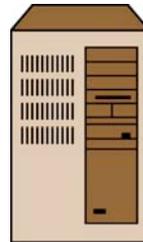
Ebene der
Anwendung/Inhalte



z.B. Kundendaten nach
Warenbestellung
im virtuellen Kaufhaus

BDSG, LDSG

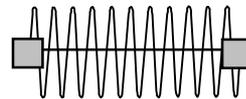
Ebene der Dienste
«Internet»



z.B. **Clickstream** nach
Zugriff auf den
Web-Server

TMG

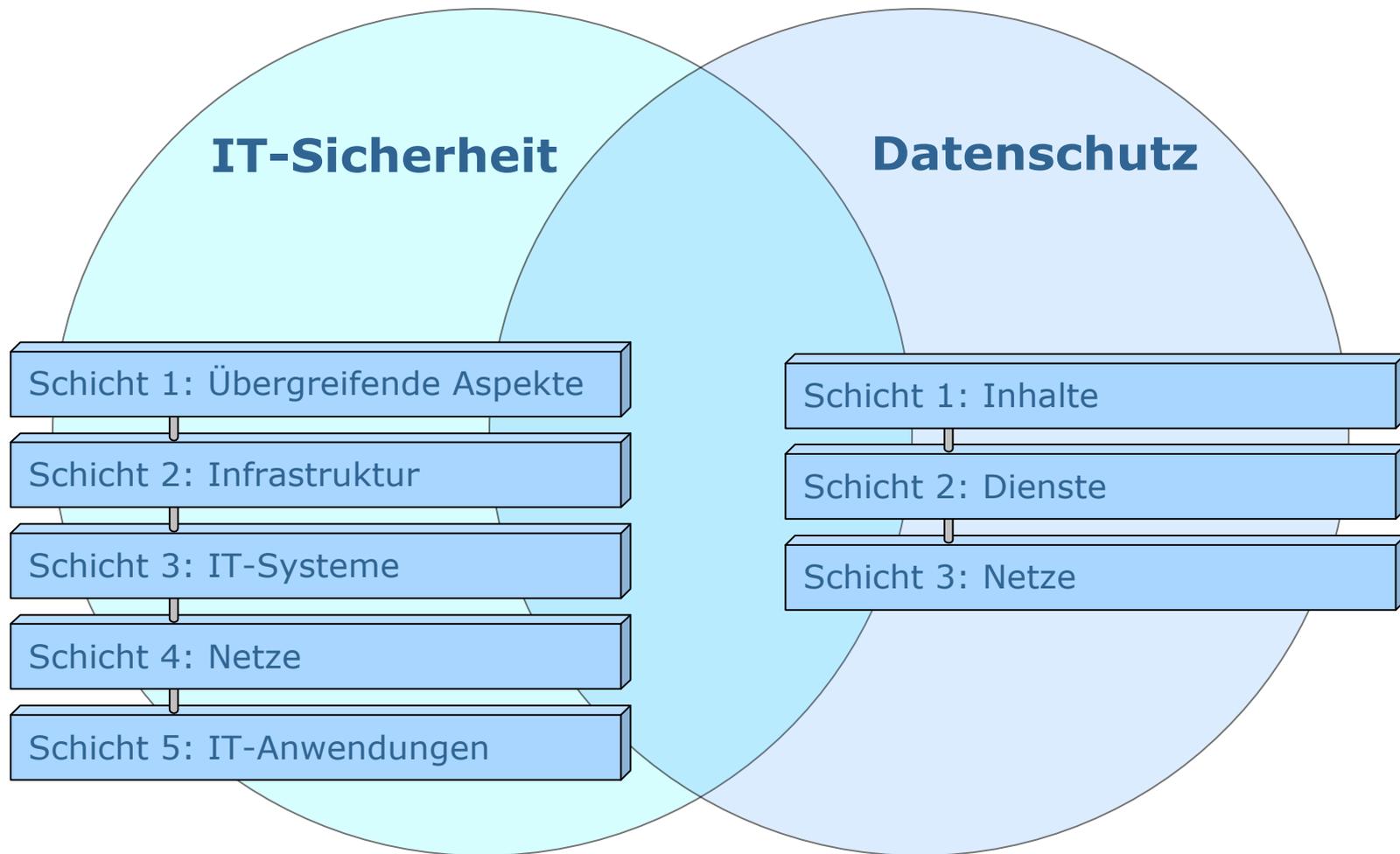
Ebene der Netze
«Telekommunikation»



z.B. **ISDN-Verkehr** über
die Leitungen der Telekom
zwischen dem Nutzer und
dem Access-Provider

TKG

Verknüpfung von Sicherheit und Datenschutz



Datenschutz in der Telekommunikation

Überblick zu den wichtigsten bereichsspezifischen Regelungen (1/4)

- Art. 10 Grundgesetz
 - «(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.»
 - «(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt. »

Datenschutz in der Telekommunikation

Überblick zu den wichtigsten bereichsspezifischen Regelungen (2/4)

- Telekommunikationsgesetz (TKG)
 - Rahmenbedingungen für chancengleichen und funktionierenden TK-Markt (seit 1996 liberalisiert)
 - Grundversorgung zu erschwinglichen Preisen
 - Fernmeldegeheimnis (§§ 88 – 90)
 - regelt Umfang der Erhebung, Verarbeitung und Nutzung personenbezogener Daten bei TK-Dienstleistungen (§§ 91 – 107)
 - Kundenschutz (§§ 44 – 47)

Datenschutz in der Telekommunikation

Überblick zu den wichtigsten bereichsspezifischen Regelungen (3/4)

- EG-Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG)
 - Datenschutz bei öffentlich zugänglichen TK-Diensten
 - regelt Netzsicherheit, Vertraulichkeit der Kommunikation, Datenverarbeitung für Entgeltabrechnung, Rufnummernanzeige, Anrufweilerschaltung, Gestaltung von Teilnehmerverzeichnissen
 - Regelungen zur Verarbeitung von Standortdaten in Mobilfunknetzen
 - Schutz vor unerwünschten E-Mails (Spam)
 - nur teilweise in nationales Recht umgesetzt

Datenschutz in der Telekommunikation

Überblick zu den wichtigsten bereichsspezifischen Regelungen (4/4)

- Telemediengesetz (TMG)
 - Zulassungs- und Anmeldefreiheit von Telemediendiensten
 - Informationspflichten und Anbieterkennzeichnung
 - Verantwortlichkeit für Inhalte
 - Regeln zum Datenschutz
 - Unterstützung anonymer und pseudonymer Kommunikation
 - Bußgeldvorschriften
- Telekommunikations-Überwachungsverordnung (TKÜV)
 - regelt die technischen und organisatorischen Vorgaben für die Umsetzung von Überwachungsmaßnahmen staatlicher Stellen (z.B. Abhören und Aufzeichnen von Inhalten, Erfassung der näheren Umstände der Kommunikation)

Grundsätze des Datenschutzes und Rechte der Betroffenen

- Grundsätze des Datenschutzes
 - Verbot mit Erlaubnisvorbehalt
 - Einwilligung des Betroffenen
 - Grundsatz der Zweckbindung
 - Grundsatz der Verhältnismäßigkeit

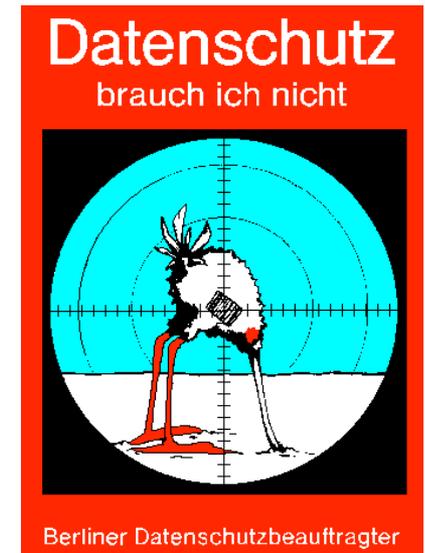
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist zulässig, soweit diese durch ein Gesetz oder eine andere Rechtsvorschrift erlaubt ist oder der Betroffene eingewilligt hat.

- Rechte der Betroffenen
 - Recht auf Auskunft
 - Recht auf Berichtigung, Sperrung oder Löschung
 - Widerspruchsrecht des Betroffenen gegen die Datenverarbeitung
 - Recht auf Anrufung des BfD und anderer Kontrollinstitutionen
 - Recht auf Schadenersatz

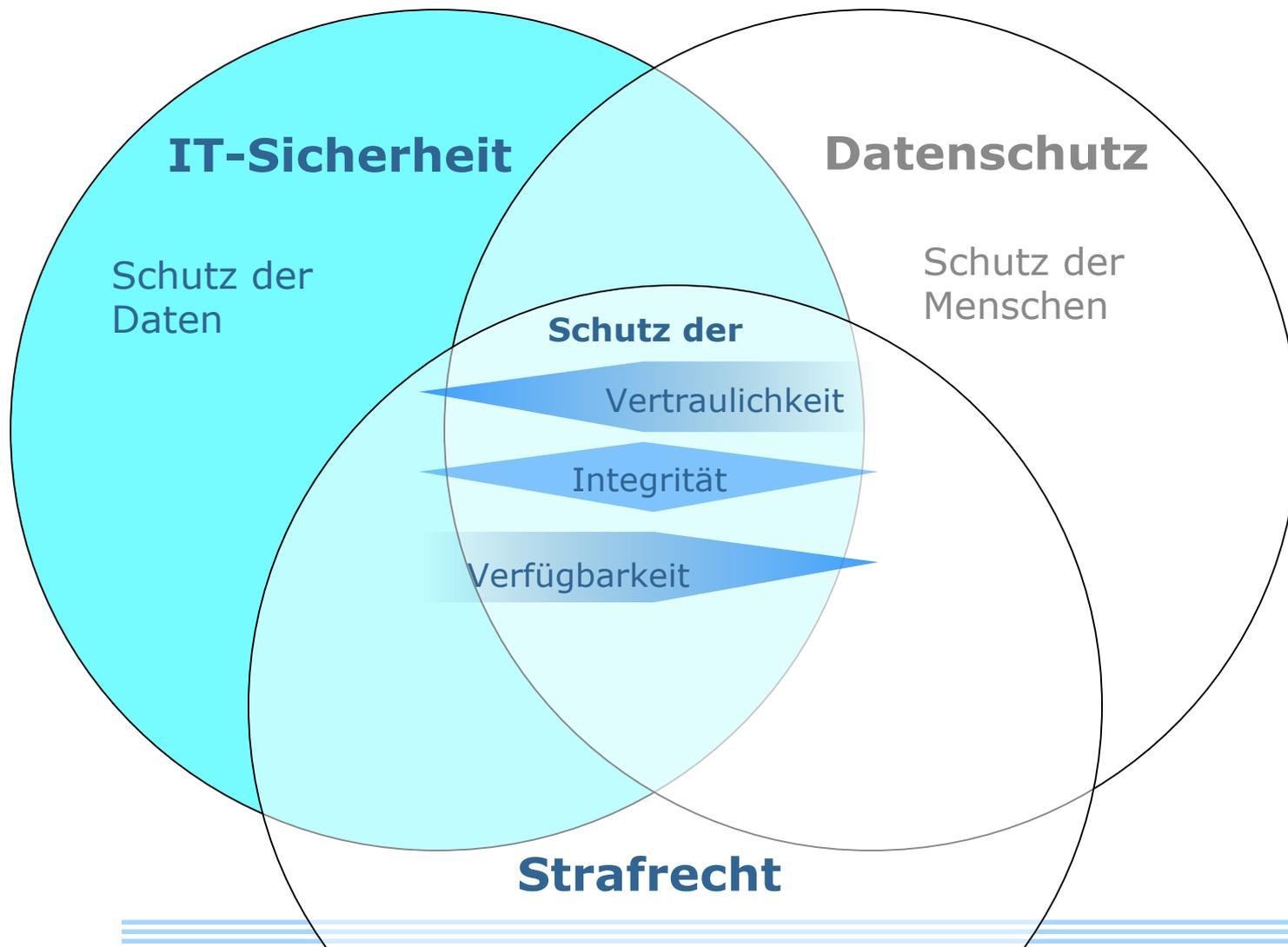


www.datenschutz.de

Virtuelles Datenschutzbüro

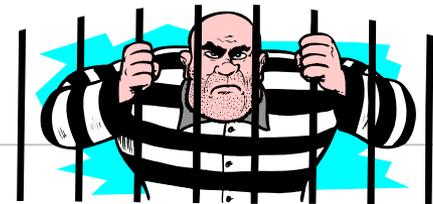


Verknüpfung von Sicherheit, Datenschutz und Strafrecht

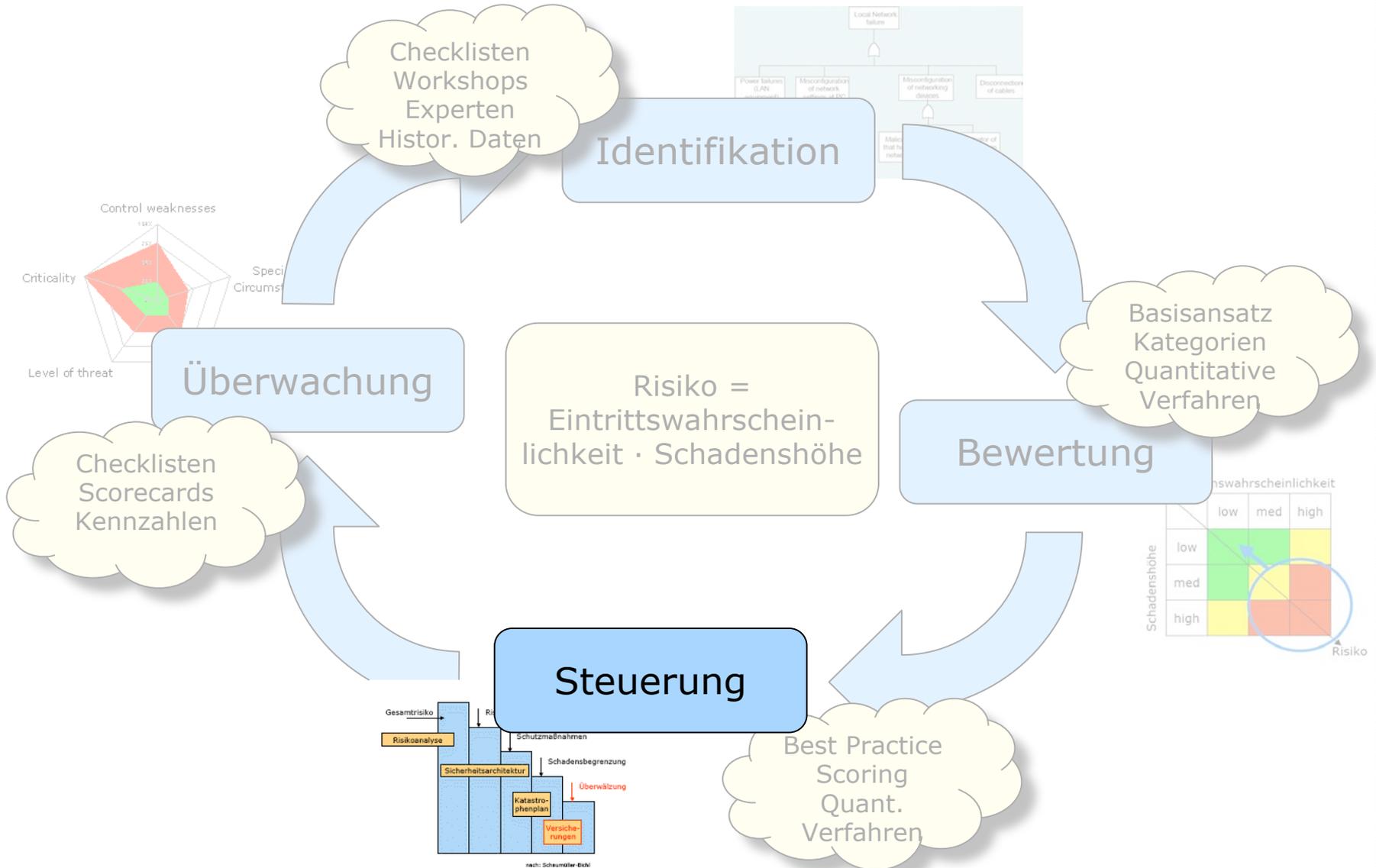


IT-Sicherheit aus strafrechtlicher Sicht

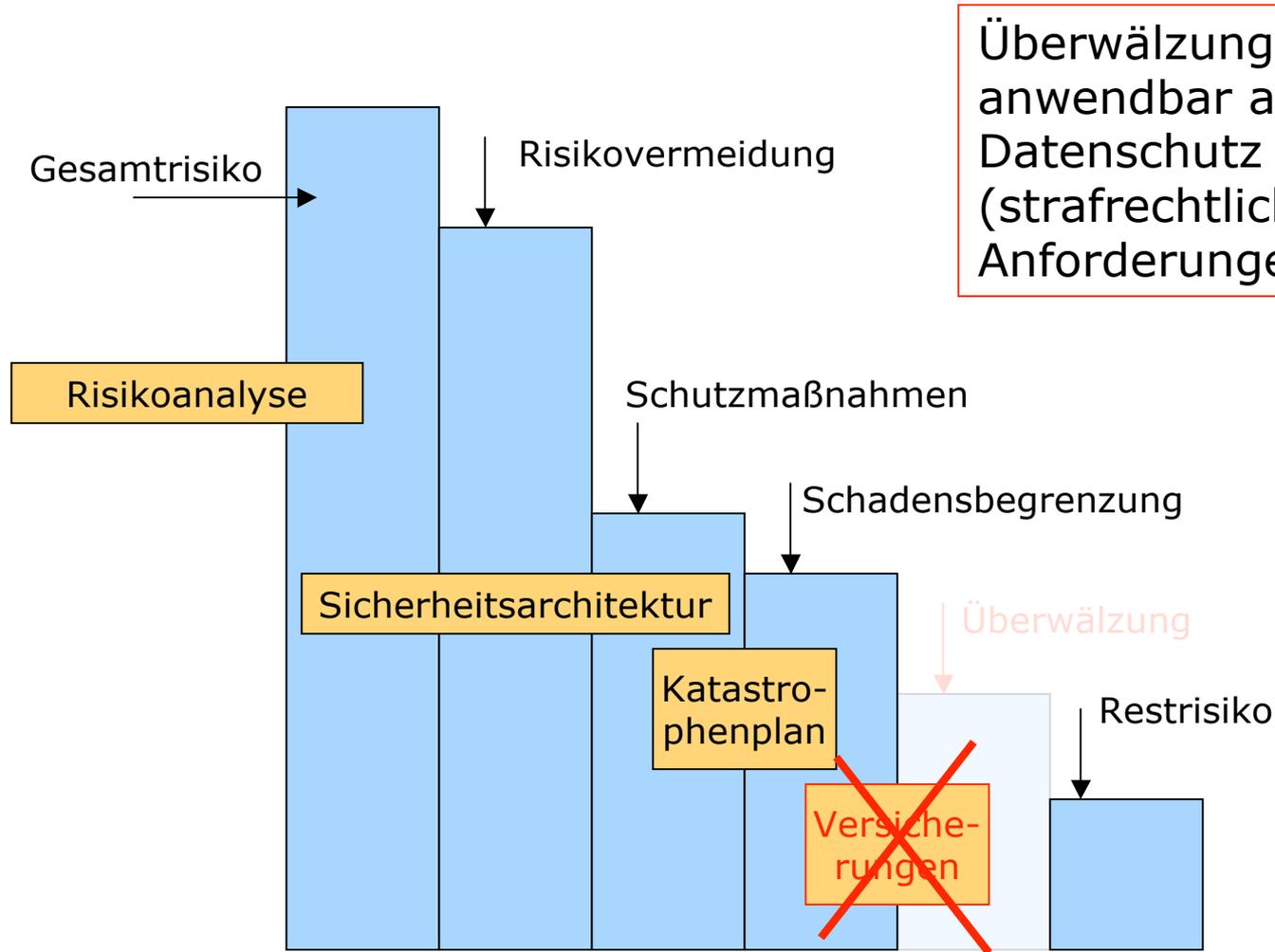
- Vertraulichkeit
 - § 202a StGB Ausspähen von Daten
 - § 203 StGB Verletzung von Privatgeheimnissen
 - Integrität
 - § 263a StGB Computerbetrug
 - § 265a StGB Erschleichen von Leistungen
 - § 268 StGB Fälschung technischer Aufzeichnungen
 - § 269 StGB Fälschung beweiserheblicher Daten
 - § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung
 - § 303a StGB Datenveränderung
 - Verfügbarkeit
 - § 303b StGB Computersabotage
-
- Strafandrohung
 - zwischen 2 und 5 Jahren Freiheitsstrafe oder Geldstrafe
 - Beschlagnahme von Beweismitteln
 - § 94 Strafprozessordnung StPO
 - Datenträger oder ganze Computersysteme



Risikomanagement Kreislauf



Risiko-Management für IT-Systeme

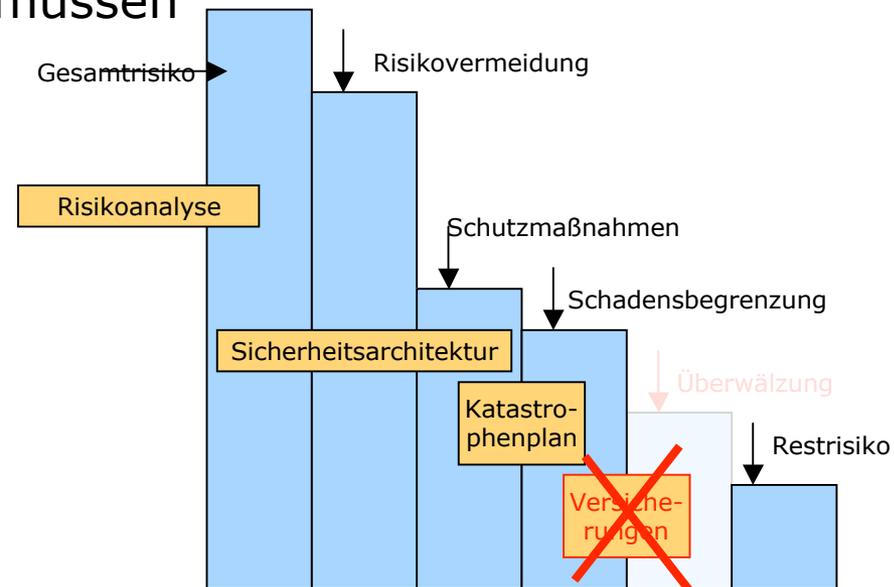
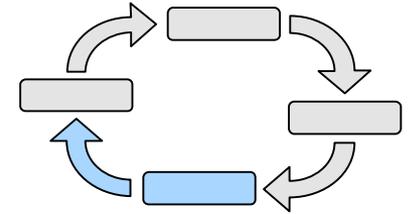


Überwälzung **nicht**
anwendbar auf
Datenschutz (und
(strafrechtliche
Anforderungen))

nach: Schaumüller-Bichl

Risiko-Management im Datenschutz

- IT-Sicherheit:
 - Risiko = Wahrscheinlichkeit · Schadenshöhe
 - Schäden sind systematisch tolerierbar
- Datenschutz:
 - Alles-Oder-Nichts-Ansatz
 - Rechtliche Vorgaben müssen umgesetzt werden



nach: Schaumüller-Bichl

Zivilrechtliche Aspekte

SOX, Basel 2, KontraG

IT-Sicherheit

Schutz der Daten

Datenschutz

Schutz der Menschen

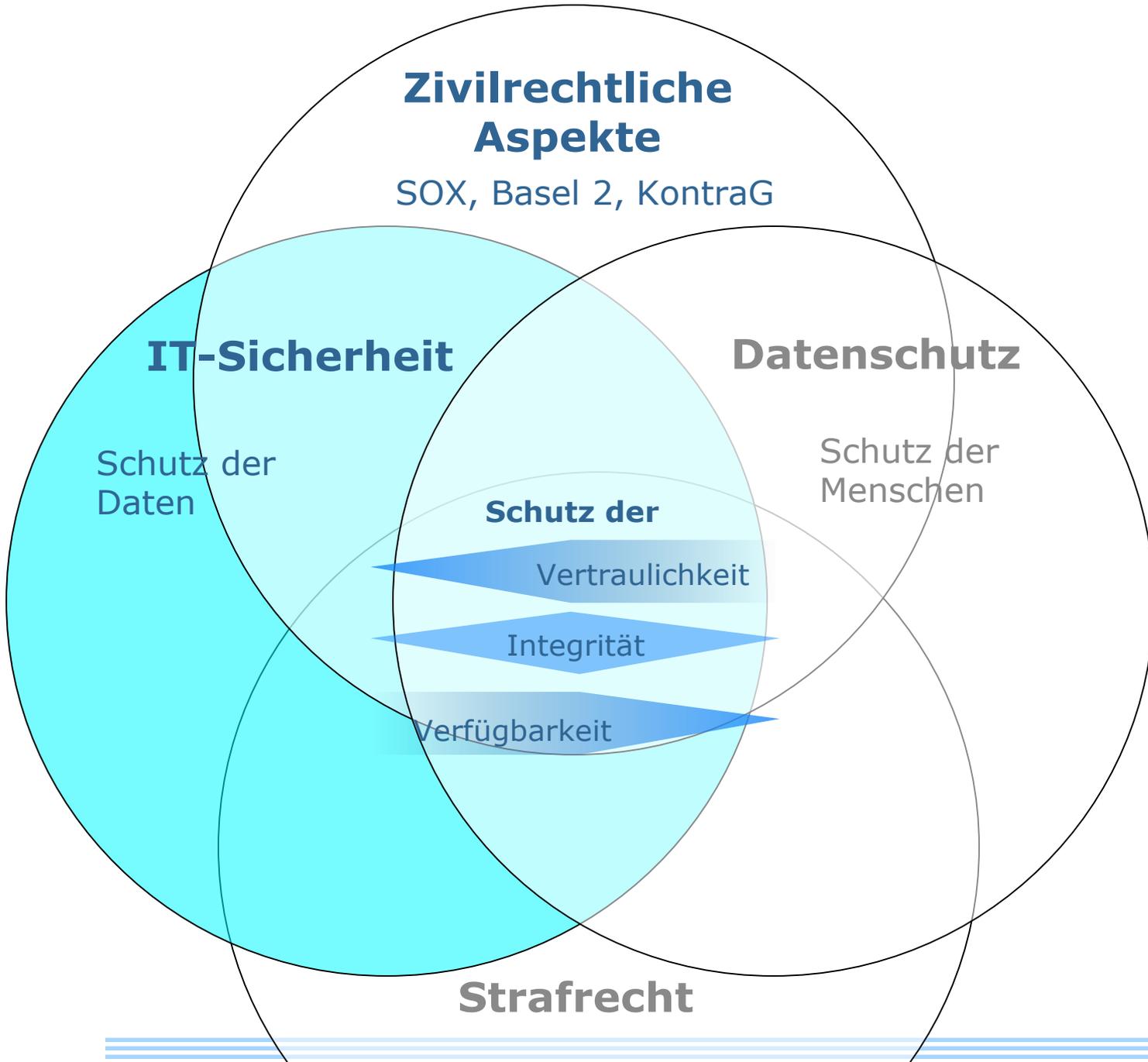
Schutz der

Vertraulichkeit

Integrität

Verfügbarkeit

Strafrecht



Goldene Regeln zur Umsetzung von Datenschutz

- Aus Sicht der IT-Sicherheit:
 - Informieren (Transparenz)
 - Auskunftsverfahren etablieren
 - Einwilligung, wo nötig
 - Weniger (speichern) ist mehr (Datenschutz)
 - Regelmäßige Sensibilisierung (wie Umwelt- und Arbeitsschutz)
 - Sanktionen bei Verstößen klarmachen
 - Aber: Kontrollieren und beraten, nicht gleich bestrafen!
- Immer fragen: Was ist die Grundlage der Erhebung/Verarbeitung/Speicherung?
 - Einwilligung?
 - Gesetzliche Vorgabe?
 - Aufrechterhaltung des laufenden Betriebs? (IT-Sicherheit)

Zusammenfassung

IT-Sicherheit

- kaum gesetzliche Vorgaben
- etablierte Standards (best practices), konkrete Vorgehensmodelle enthalten auch Datenschutz
- meist freiwillig umgesetzt
- Im Mittelpunkt stehen die Interessen des Betreibers und deren Nutzer.

Datenschutz

- höhere Regelungsdichte
- wenig konkrete Vorgaben (technisch organisatorische Maßnahmen nach BDSG § 9)
- gesetzlicher »Zwang«
- Im Mittelpunkt stehen die Interessen des Betroffenen.

IT-Sicherheit und Datenschutz

- Beides ist notwendig
- Ähnliche Mechanismen und Vorgehensweise
- Prävention ist besser als Reaktion
- IT-Sicherheit ohne Datenschutz geht nicht

Zusammenfassung

IT-Sicherheit

- kaum gesetzliche Vorgaben
- etablierte Standards (best practices), konkrete Vorgehensmodelle enthalten auch Datenschutz
- meist freiwillig umgesetzt
- Im Mittelpunkt stehen die Interessen des Betreibers und deren Nutzer.

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

IT-Sicherheit und Datenschutz

- Beides ist notwendig
- Ähnliche Mechanismen und Vorgehensweise
- Prävention ist besser als Reaktion
- IT-Sicherheit ohne Datenschutz geht nicht

Zusammenfassung

IT-Sicherheit

- kaum gesetzliche Vorgaben
- etablierte Standards (best practices), konkrete Vorgehensmodelle enthalten auch Datenschutz
- meist freiwillig umgesetzt
- Im Mittelpunkt stehen die Interessen des Betreibers und deren Nutzer.

Anlage zu § 9 Abs. 1 BDSG

1. Zutrittskontrolle (räumlicher Zutritt, Gebäude)
2. Zugangskontrolle (Benutzung, Passwort)
3. Zugriffskontrolle (Berechtigung, Administratoren)
4. Weitergabekontrolle (Transport, Netze)
5. Eingabekontrolle (Nutzer-Protokoll)
6. Auftragskontrolle (Outsourcing, Wartung)
7. Verfügbarkeitskontrolle (Zerstörung)
8. Trennungsgebot (Zwecktrennung)

IT-Sicherheit und Datenschutz

- Beides ist notwendig
- Ähnliche Mechanismen und Vorgehensweise
- Prävention ist besser als Reaktion
- IT-Sicherheit ohne Datenschutz geht nicht

Zusammenfassung

IT-Sicherheit

- kaum gesetzliche Vorgaben

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg
D-93040 Regensburg

E-Mail: hannes.federrath@wiwi.uni-regensburg.de
WWW: <http://www-sec.uni-regensburg.de>

Phone +49-941-943-2870
Telefax +49-941-943-2888

Datenschutz

- höhere Regelungsdichte
wenig konkrete Vorgaben
(technisch organisatorische
Maßnahmen nach BDSG § 9)
gesetzlicher »Zwang«

Im Mittelpunkt stehen die
Interessen des Betroffenen.

IT-Sicherheit und Datenschutz

- Beides ist notwendig
- Ähnliche Mechanismen und Vorgehensweisen
- Prävention ist besser als Reaktion
- IT-Sicherheit ohne Datenschutz geht nicht

