TeleTrusT "IT-Sicherheitsrechtstag 2023"

Berlin, 28.09.2023

Modell für ein allgemeines IT-Sicherheitsrecht - Aufräumen im Legacy-System der Regulierung

Nils Brinker, Digital Society Institute, ESMT Berlin

Was haben wir vor?

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

1. Einführung/ Vorstellung des Projekts ITSR.sys
2. Erläuterung generelle Forschungsfrage
3. Einführung in das Modell
    1. Klassifikation von System
    2. Schutzgutangemessene Risikoanalyse
    3. Stand der Technik

Zusammenfassung der Projektergebnisse der Projekt ITSR.sys

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

ITSR·sys

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Förderkennzeichen: **16KIS1225K**

DSI DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

KIT Karlsruher Institut für Technologie

Verbundprojekt ITSR.sys – Systematisierung des IT-Sicherheitsrecht

Projektpartner:

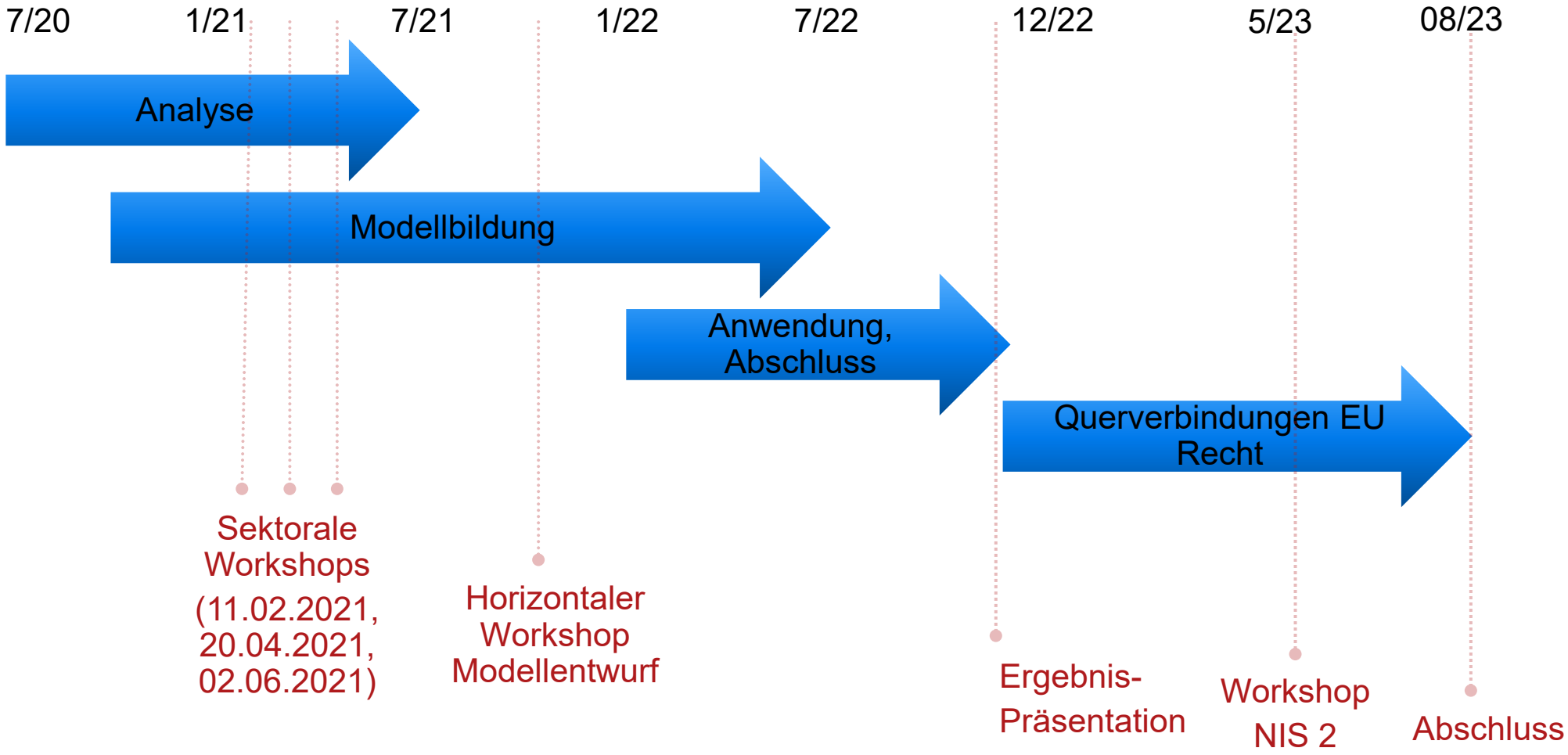
Digital Society Institute der ESMT Berlin

Karlsruher Institute für Technologie (KIT) (bis 31.12.2022)

Projektlaufzeit:

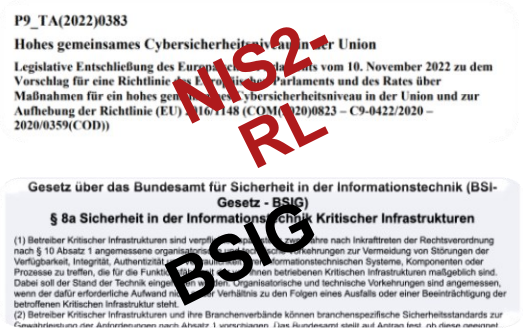
- 1. Juli 2020 bis 31. Juli 2023

Projektverlauf



Forschungsfrage

IT-Sicherheitsrecht Status Quo



Querschnittliches IT-Sicherheitsrecht

Sektorales IT-Sicherheitsrecht

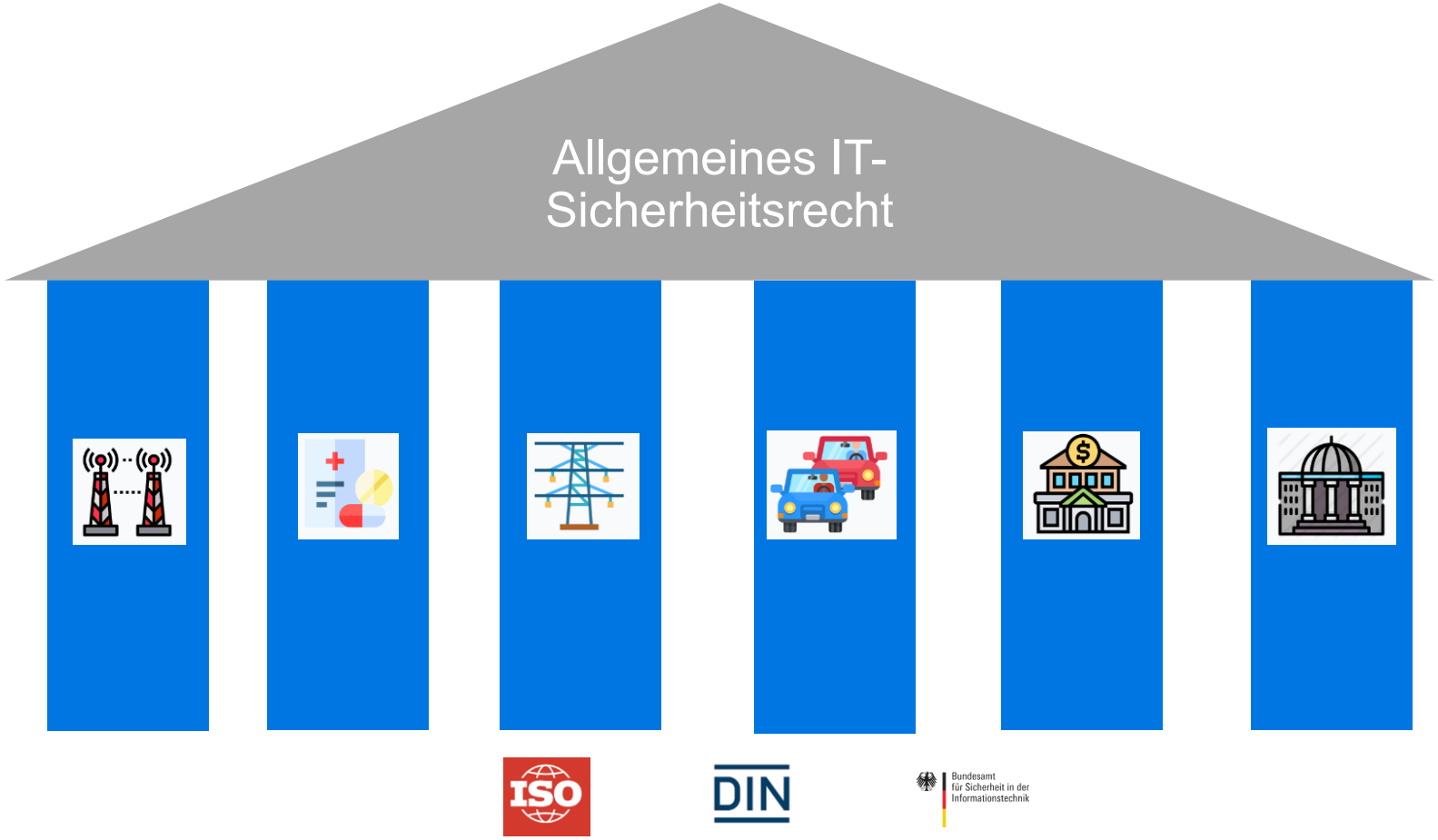
ISO

DIN

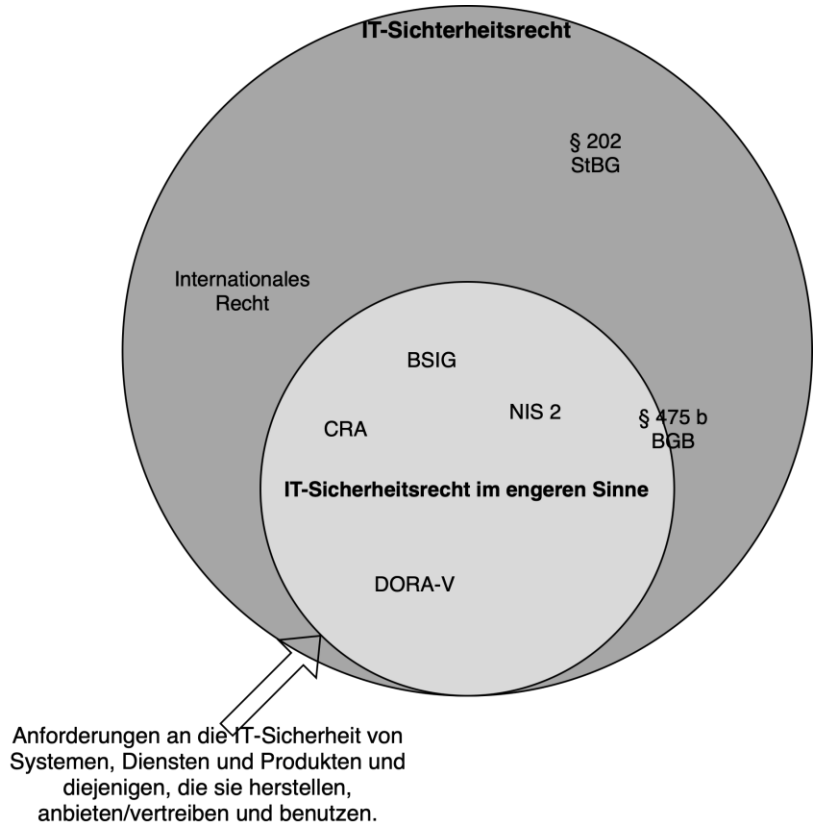
Bundesamt für Sicherheit in der Informationstechnik

Technische Normen

Zielbild


Allgemeines IT-Sicherheitsrecht
ISO
DIN
Bundesamt für Sicherheit in der Informationstechnik

Scope


IT-Sichterheitsrecht
§ 202
StBG
Internationales
Recht
BSIG
NIS 2
CRA
§ 475 b
BGB
IT-Sicherheitsrecht im engeren Sinne
DORA-V
Anforderungen an die IT-Sicherheit von
Systemen, Diensten und Produkten und
diejenigen, die sie herstellen,
anbieten/vertreiben und benutzen.

Wesentliche Forschungsfragen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Klassifikation von Systemen

Einheitliche Klassifizierung informationstechnischer Systeme als Grundlage für IT-Sicherheitsregulierung

Schutzgutangemessene Risikobewertung

Methode zur Betrachtung der Risiken durch Sicherheitsverletzungen informationstechnischer Systeme, die datensicherheitsrechtlich und IT-sicherheitsrechtlich gleichermaßen tauglich ist

Einbeziehung des Standes der Technik

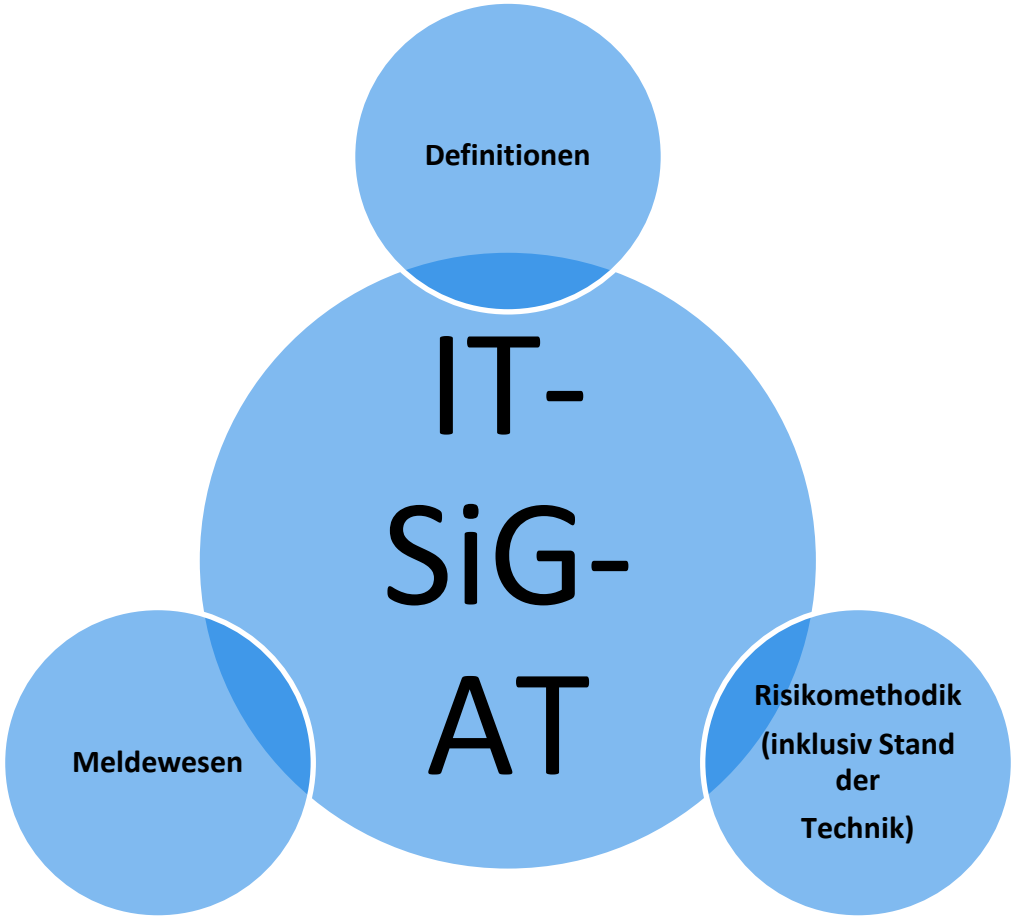
Systematisierung der Ansätze und Methoden mit dem Ziel der Entwicklung einer Metamethode zur Feststellung des „Standes der Technik“

Übergreifende Modellbildung

Modell eines „Allgemeinen IT-Sicherheitsrechts“

Modellübersicht

- **Definitionen: § 2**
- **Risikomethodik: §§ 4-12**
- **Meldewesen: § 16**



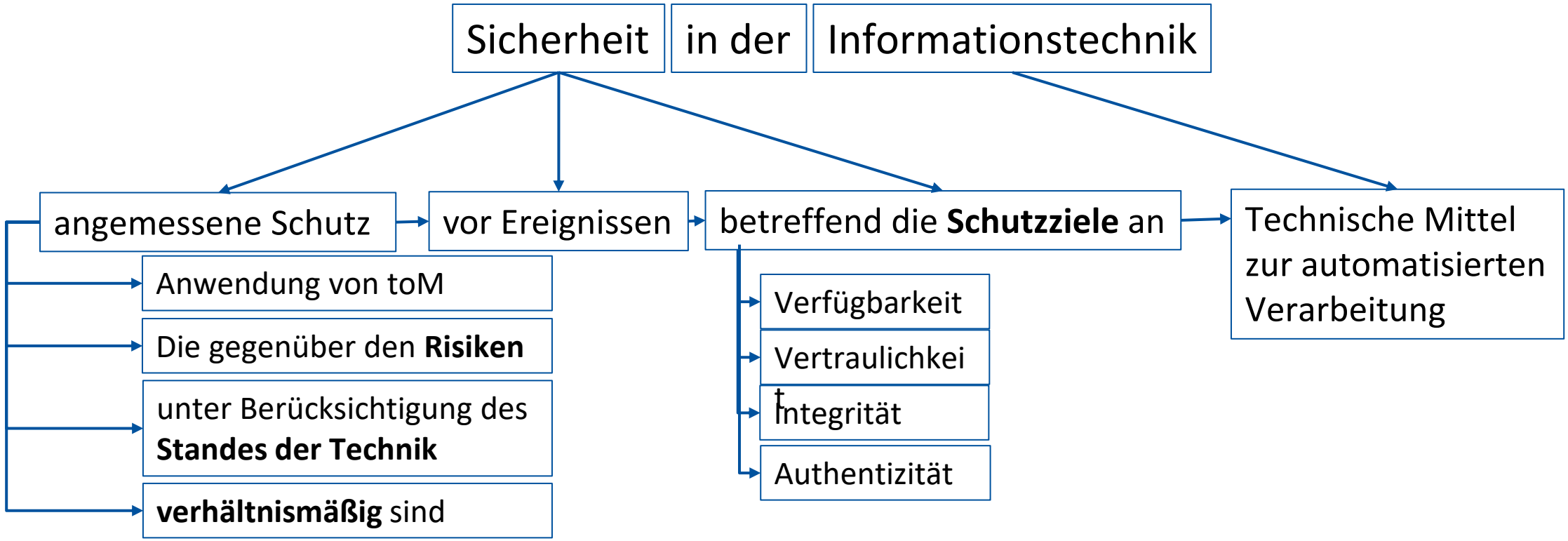
Modellübersicht

- Der Ergebnistext ist verfügbar unter:
  - bit.ly/itsrsys

Weitere wesentliche Erkenntnisse wurden in folgenden Fachbeiträgen veröffentlicht:

- *Werner/Brinker/Raabe*, Grundlagen für ein gesetzliches IT-Sicherheitsrisikomanagement, in Computer und Recht 12/2022, S. 817-824.
- *Sterz/Werner/Raabe*, Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen – Teil 1, in Recht der Datenverarbeitung 6/2022, S. 291-299.

Regelungszweck eines IT-SiG-AT



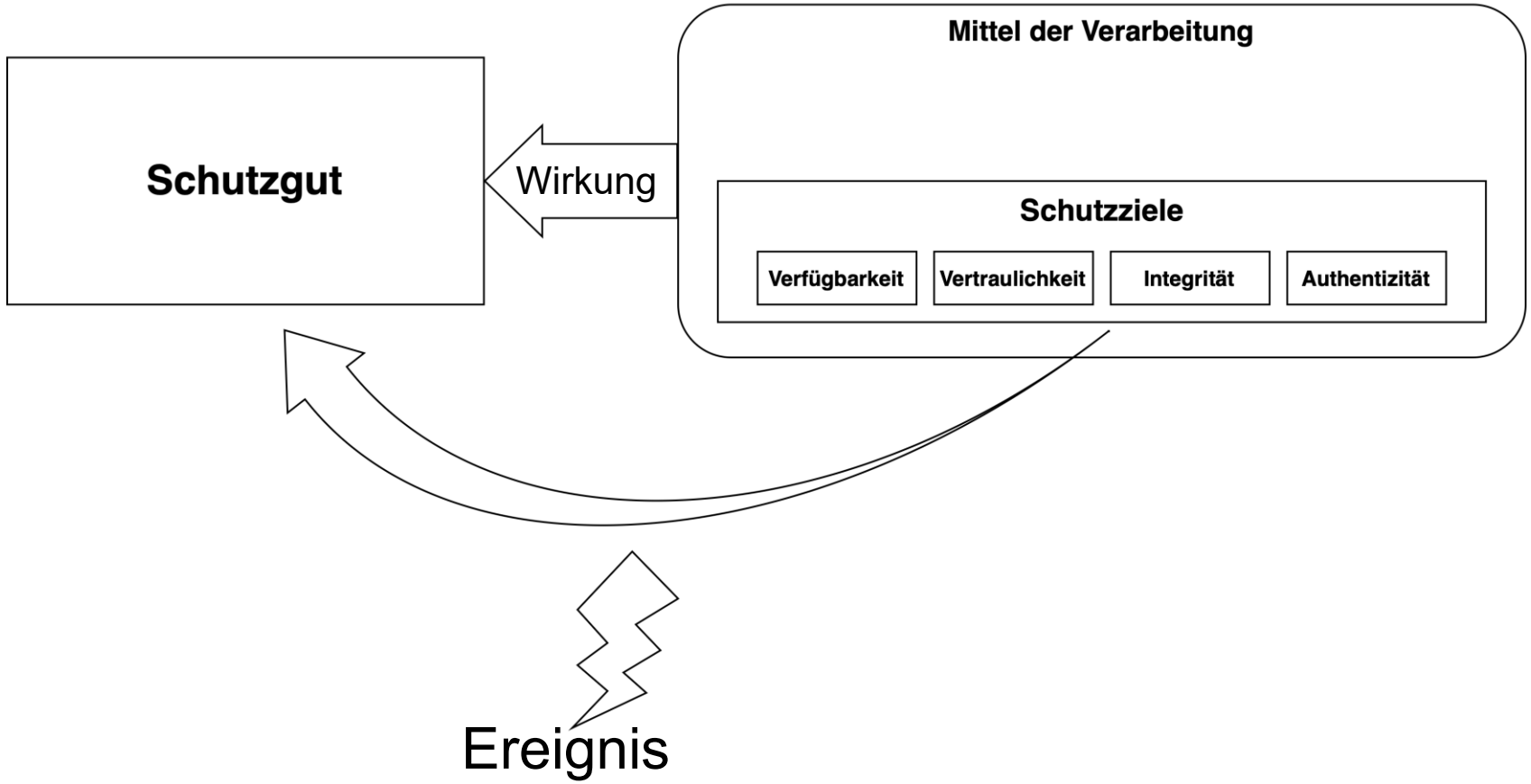
Mit dem Ziel der Sicherung von **Schutzgütern**

Regelungszweck eines IT-SiG-AT

- **Vergleich Definition in Art. 5 Nr. 2 NIS 2**

2. „Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können;

Exkurs: Schutzziele und Schutzgüter



Klassifikation von Systemen

Themenblock 1: Klassifikation von Systemen

Fragestellungen

1. Welche Referenz in die technische Beschreibung eines Systems wird gewählt?
2. Wie wird diese fachspezifisch begründet?
3. Wie wird eine anwendungsbezogene Klassifikation von der auf universelle technische Systeme und querschnittliche digitale Dienste bezogenen Klassifikation unterschieden?

GG, NIS2-RL, CRA, CSA, DSGVO, BSIG, BDSG, TMG, TKG, eIDAS-VO, MDStV, EnWG, MsbG, SGB V, KHG, MedProdVO, KWG, PSD II, ZAG, OZG, ..

Rekonstruktion der Begrifflichkeiten

1. Ausgehend vom „Informations-technischen System“
2. Anwendungs-spezifische Profilierung
3. Bildung von Klassen

1. „Informationstechnik“ die technischen Mittel zur automatisierten Verarbeitung von Daten in Form von

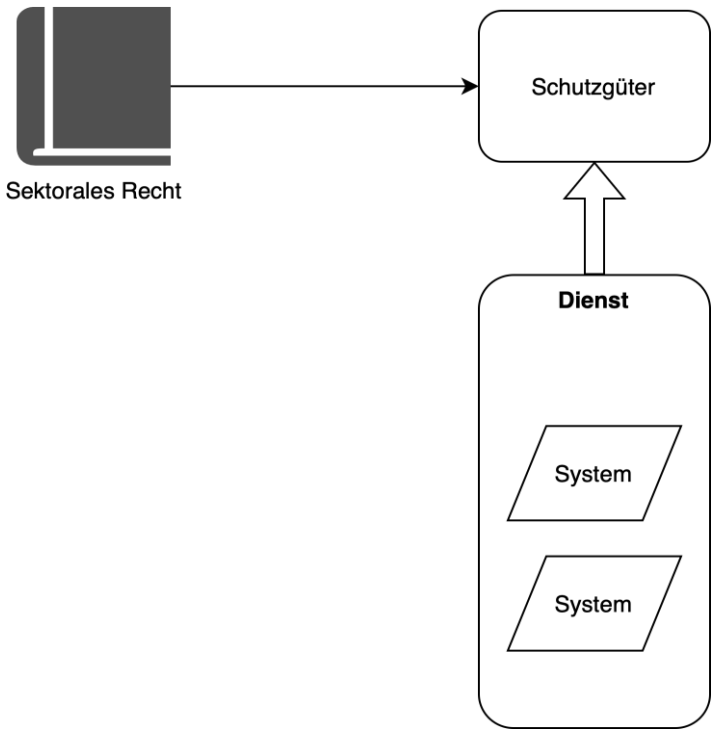
a) Komponenten als abgrenzbare Teilfunktionen eines Systems;

b) Systemen als abgrenzbare und zusammengehörige Einheiten von Funktionen;

c) Diensten als das zweckspezifische Leistungsangebot von Systemen;

- Systeme als die Mittel
- Schutzgüter werden durch Dienst beeinflusst. Systeme als „Werkzeuge“ zunächst neutral
- Dienstparadigma notwendig um Schutzgutrelevante Systeme als Mittel Abgrenzen zu können

Verhältnis der System- und Dienstbegriffe zueinander und Wirkungskette auf die Schutzgüter



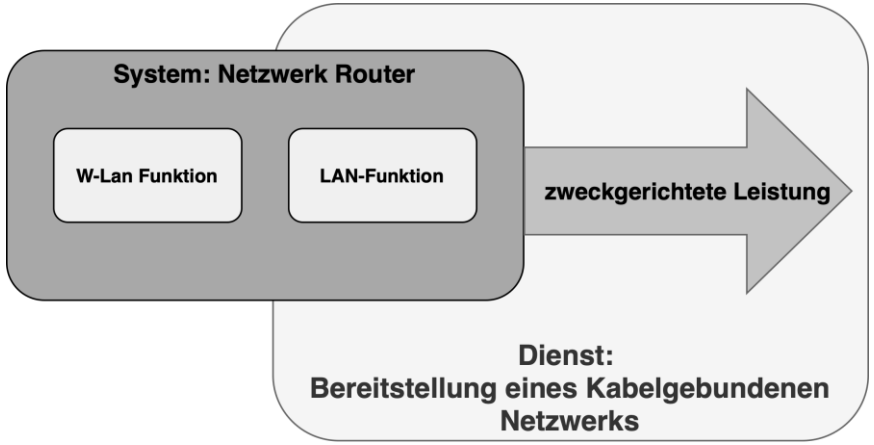
Beispiel für ein	
Schutzgut	Versorgungssicherheit der Bevölkerung
Dienst	Technischer Betrieb eines Kraftwerk; Ausgabe der Systemzeit
System	Betriebstechnik eines Kraftwerks, Rechner
Funktion	Signalübertragung, Berechnungen etc.
Zweck	Energieversorgung, Zeiterfassung

- Zur Bestimmung der eingesetzten Systeme zur Realisierung eines Dienstes sind funktionale Aspekte geeignet
- Da Ziel des Risikomanagements jedoch die konkrete Umsetzung von Maßnahmen sind, spielen zur Bestimmung der Systemgrenzen für einen Betreiber auf Kontrollaspekte eine Rolle

Funktionale Dimension der Systemgrenzen

- Es geht darum, sämtliche Funktionen, die ein Einfluss auf einen Dienst haben können zu identifizieren.
- Hierzu gehören die Funktionen, die zur Umsetzung des Zwecks des Dienstes notwendig sind, bzw. aktiv genutzt werden.
- Jedoch können auch Funktionen die aufgrund ***domänenspezifischer Konvention oder Eigenschaften ausreichend Sachnähe*** aufweisen einen sicherheitskritischen Einfluss auf einen Dienst haben.

Beispiele für „domänenspezifischer Konventionen oder Eigenschaften“	
Hardware	Körperliche Grenzen
Software	Funktionale Bündelung in Software Bibliotheken
Netzwerke	Agenten innerhalb eines internen Netzwerkes



Kontroll- und Verfügungsdimension

Kontrolle als Verfügungsgewalt und ausreichende Information über die konkrete Ausgestaltung eines Systems

Verfügungsgewalt

Notwendig, um im Rahmen der Risikobehandlung konkrete Maßnahmen umsetzen zu können.

In Gestalt von:

- tatsächliche physische oder nichtphysische (etwa im Fall von Fernwartung) Verfügungsgewalt
- vertragliche Verfügungsgewallt (etwa in Form von Weisungsbefugnis)

ausreichende Informationen

Notwendig um Risikobeurteilung vornehmen zu können.

In Gestalt von:

- Tatsächlichen Informationen
- ggf. geeignete Zertifizierungen

Schutzgutangemessene Risikobewertung

Initiale Fragestellung Schutzgutangemessene Risikobewertung

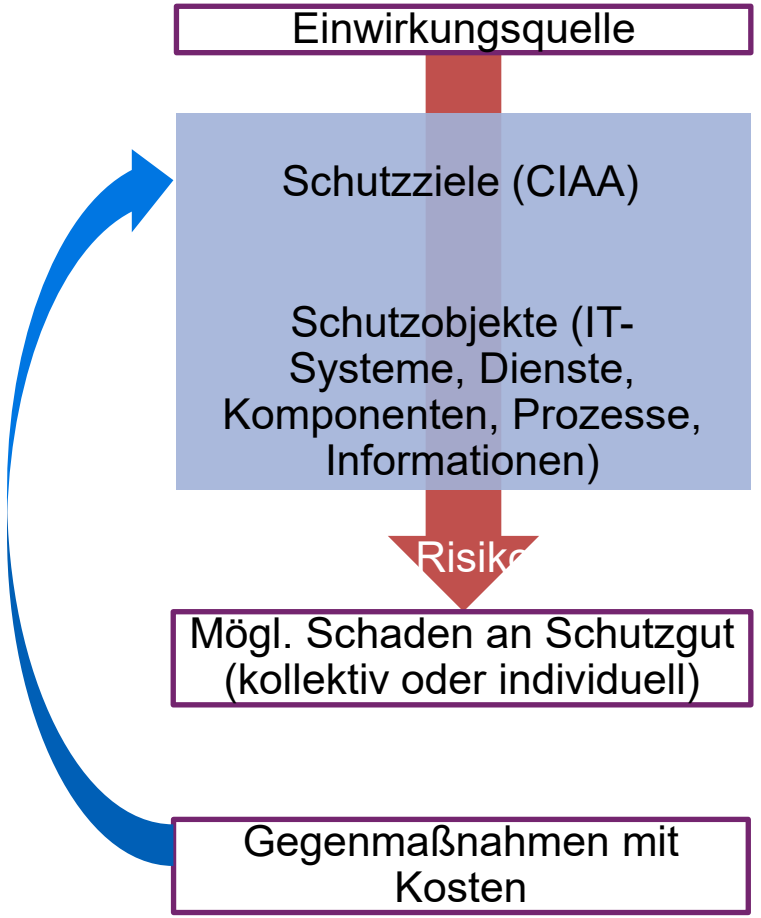
Fragestellungen

1. Erforderliche Schutzziele und Schutzobjekte, um die (durch IT wirkenden) Risiken für die jeweiligen verfassungs-rechtlichen Schutzgüter präzise zu erfassen

2. (Methodische) Anforderungen an den Risikobegriff mit Blick auf die Erfordernisse des Rechts

3. Ist der Verweis auf die Methodik des „Risikomanagements“ nach der ISO 2700X-Familie (so etwa im Energierecht) sachgerecht?

4. **Wie muss eine „prinzipienbasierte Risikomethodik“ aussehen, die praxisgerecht gestaltet und gleichzeitig rechtlich tragfähig ist?**



Gesetzliches Risikomanagement

- Das Modell umfasst eine rechtlich ausformulierte Methodik zum Risikomanagement. Die wesentlichen Schritte sind an privaten etablierten Standards wie dem ISO 27005 orientiert.

- **§ 4 Kontexterstellung**
- **§ 5 Risikoidentifikation**
- **§ 6 Risikoanalyse**
- **§ 7 Risikobewertung**
- **§ 8 Risikobehandlung**

Schutzgutangemessene Risikobewertung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

§ 4 Kontexterstellung

(1) Die Betreiber haben mit **vernünftigem** Aufwand alle extern und intern veranlassten Risiken zu identifizieren.

(2) Die Identifikation bezieht sich dabei insbesondere auf

- Risikoquellen jeder Art und jeden Ursprungs einschließlich Drittdiensten,
- mögliche künftige und vergangene Ereignisse, mit informationstechnischen Auswirkungen, die von diesen Risikoquellen ausgehen können,
- Schwachstellen technischer, organisatorischer oder menschlicher Art, vorhandene Maßnahmen

und

- mögliche kausale Schadfolgen an den relevanten Schutzgütern.

(3) Dies schließt die Nutzung von Warn- und Informationsdiensten nach § 10 sowie die aktive und regelmäßige Durchführung von Testverfahren zur Aufdeckung von Schwachstellen mit ein.

§ 5 Risikoidentifikation

(1) Die Risiken sind jeweils in ihrer Höhe zu bemessen. Zur Bemessung der Ereigniswahrscheinlichkeit und der möglichen Schadfolgen kann eine empirisch fundierte quantitative, eine subjektiv schätzende qualitative oder eine kombinierende semi-quantitative Bewertung der Ereigniswahrscheinlichkeit und der möglichen Schadfolgen gewählt werden.

(2) Die Berechnung der Wahrscheinlichkeit von Ereignissen soll auf Basis empirischer Daten vorgenommen werden, sofern diese Daten bereits erhoben sind oder mit vernünftigem Aufwand erhoben werden können. Andernfalls sind fundierte Schätzungen vorzunehmen.

(3) Schließlich sind das Gewicht der informationstechnischen Auswirkungen der Ereignisse sowie die daraus resultierende- Höhe der Schadfolgen für Schutzgüter zu analysieren.

(4) Handelt es sich bei der identifizierten Risikoquelle um eine natürliche Person, sind insbesondere auch deren Motivation, Fähigkeiten, und Ressourcen abzuschätzen.

(5) Soweit Risiken nicht identifiziert oder vollständig analysiert werden können (Ungewissheit), aber für kritisch betroffene Schutzgüter vermutet werden, ist dies als Ausgangspunkt für Maßnahmen nach § 10 zu dokumentieren.

Schutzgutangemessene Risikobewertung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

§ 6 Risikoanalyse

(1) Die Risiken sind jeweils in ihrer Höhe zu bemessen. Zur Bemessung der Ereigniswahrscheinlichkeit und der möglichen Schadfolgen kann eine empirisch fundierte quantitative, eine subjektiv schätzende qualitative oder eine kombinierende semi-quantitative Bewertung der Ereigniswahrscheinlichkeit und der möglichen Schadfolgen gewählt werden.

(2) Die Berechnung der Wahrscheinlichkeit von Ereignissen soll auf Basis empirischer Daten vorgenommen werden, sofern diese Daten bereits erhoben sind oder mit vernünftigem Aufwand erhoben werden können. Andernfalls sind fundierte Schätzungen vorzunehmen.

(3) Schließlich sind das Gewicht der informationstechnischen Auswirkungen der Ereignisse sowie die daraus resultierende- Höhe der Schadfolgen für Schutzgüter zu analysieren.

(4) Handelt es sich bei der identifizierten Risikoquelle um eine natürliche Person, sind insbesondere auch deren Motivation, Fähigkeiten, und Ressourcen abzuschätzen.

(5) Soweit Risiken nicht identifiziert oder vollständig analysiert werden können (Ungewissheit), aber für kritisch betroffene Schutzgüter vermutet werden, ist dies als Ausgangspunkt für Maßnahmen nach § 10 zu dokumentieren.

§ 7 Risikobewertung

(1) Im Rahmen der Risikobewertung sind die jeweils identifizierten und bemessenen Risiken für die Schutzgüter mit dem Aufwand für mögliche Maßnahmen ins Verhältnis zu setzen.

(2) Bei der Maßnahmenwahl ist der Stand der Technik zu berücksichtigen. Der Stand der Technik ist mit Blick auf die Risiken objektiv zu bestimmen. Vorhandene Veröffentlichungen oder Feststellungen zuständiger Behörden können als Stand der Technik angenommen werden, wenn die Anwendbarkeit für die analysierten Risiken gewährleistet ist.

(3) Die Maßnahmen sind dabei mit Blick auf ihre risikoreduzierende Wirkung, insbesondere auf die Wahrscheinlichkeit des Auftretens einer informationstechnischen Auswirkung zu untersuchen. Anschließend ist zu untersuchen, ob das Risiko sich hierdurch soweit reduzieren lässt, dass ein angemessener Schutz erreicht wird. Ist dies nicht der Fall, sind weitere oder wirksamere Maßnahmen zu betrachten.

(4) Das Erfordernis an Maßnahmen kann im Einzelfall über den Stand der Technik hinausgehen oder innerhalb der Grenzen des Abs. 2 Satz 1 hinter diesem zurückbleiben. Letzteres ist in der Dokumentation gemäß § 11 besonders zu begründen.

Schutzgutangemessene Risikobewertung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

§ 8 Risikobehandlung

(1) Die Maßnahmen sind unverzüglich umzusetzen. Nach Vornahme aller Maßnahmen sind diese auf ihre beabsichtigte Gesamtwirksamkeit hin zu überprüfen.

(2) Ist durch die Maßnahmen kein angemessener Schutz im Sinne des § 7 Abs. 3 erreichbar, ist der Einsatz der Informationstechnik in seiner konkreten Gestalt unzulässig.

§ 9 Iteration

Der Risikomanagementprozess ist turnusmäßig zu wiederholen. Der Turnus bestimmt sich insoweit nach der Bedeutung der gefährdeten Schutzgüter. Ungeachtet dessen ist der Risikomanagementprozess bei wesentlichen Veränderungen der sicherheitskritischen Sach- oder Informationslage (z.B. in der Informationstechnik) unverzüglich zu wiederholen.

Stand der Technik

Initiale Fragestellung Stand der Technik

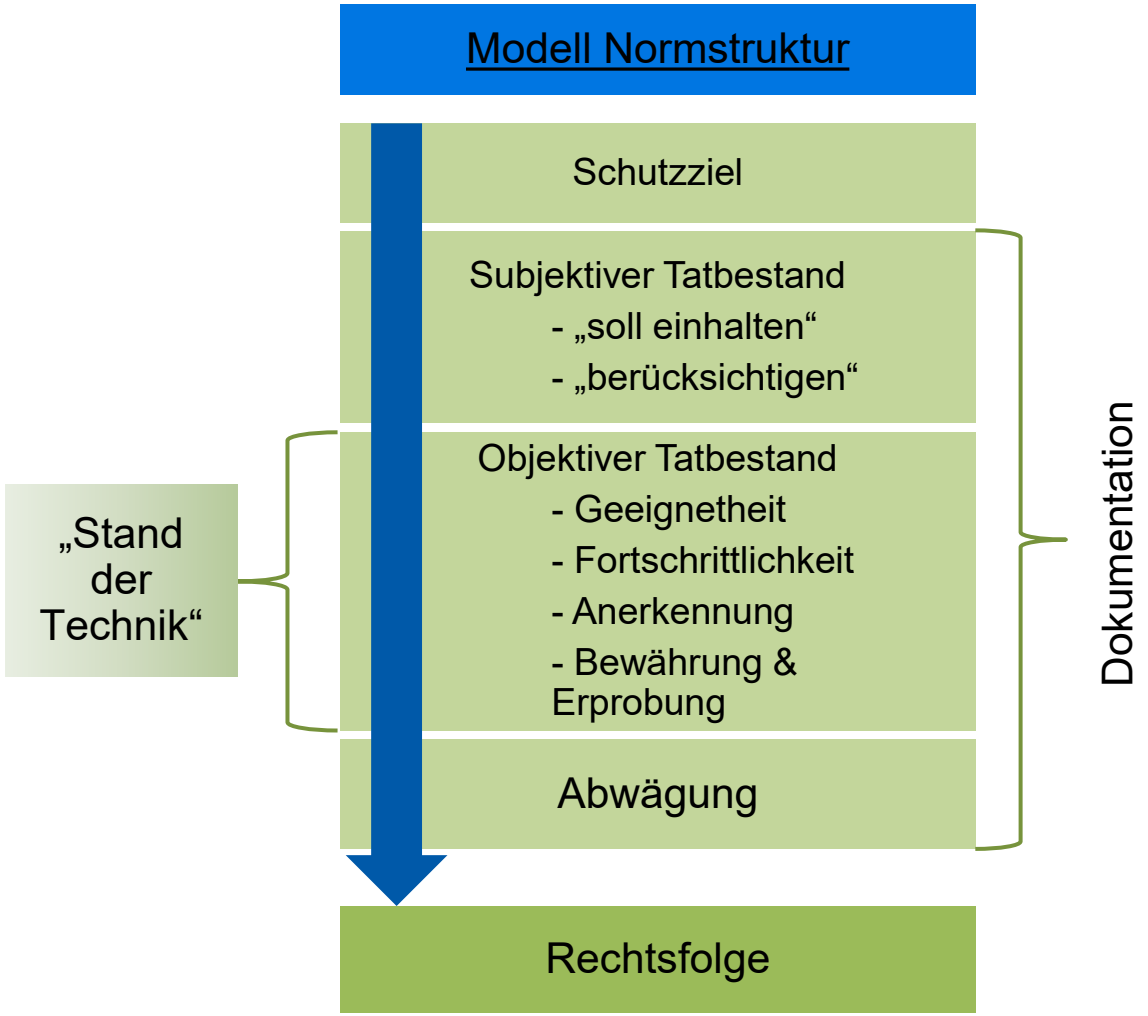
Initiale Fragestellungen

1. Wie sich die subjektiven Tatbestands-merkmale zu definieren und wie lässt sich ihre Einhaltung dokumentieren?

2. Wie wird „Stand der Technik“ in anderen Regelungsmaterien verstanden?

3. Wie wird „Stand der Technik“ europarechtlich verstanden?

4. **Wie lässt sich eine Metamethode zur Ermittlung des objektiven Merkmals „Stand der Technik“ unabhängig von jew. Schutzziel und Rechtsfolge beschreiben?**



Stand der Technik

- **§ 2 Begriffsbestimmungen**

  8. „Stand der Technik“ jene technisch-organisatorischen Maßnahmen, welche die schutzgutabhängigen Schutzziele fördern, sowie fortgeschritten, allgemein anerkannt und praktisch erprobt sind;

- **§15 Konkretisierung des Stands der Technik**

  Die Anforderungen an die Einbeziehung des Stands der Technik können fachgesetzlich konkretisiert werden. Auch kann der Stand der Technik durch die Fachgesetze inhaltlich näher konturiert werden. Schließlich kann in Fachgesetzen statt des Standes der Technik auch auf die anerkannten Regeln der Technik oder den Stand der Wissenschaft und Technik verwiesen werden.

- **§ 7 Risikobewertung**

  (1) Im Rahmen der Risikobewertung sind die jeweils identifizierten und bemessenen Risiken für die Schutzgüter mit dem Aufwand für mögliche Maßnahmen ins Verhältnis zu setzen.

  (2) **Bei der Maßnahmenwahl ist der Stand der Technik zu berücksichtigen.** Der Stand der Technik ist mit Blick auf die Risiken objektiv zu bestimmen. Vorhandene Veröffentlichungen oder Feststellungen zuständiger Behörden können als Stand der Technik angenommen werden, wenn die Anwendbarkeit für die analysierten Risiken gewährleistet ist.

Stand der Technik

- Der Stand der Technik ist im Modell generell zwar zu berücksichtigen, jedoch nicht zwingend. Im Rahmen der Maßnahmenwahl wird er als ein Wertungskriterium herangezogen.

- Sektorspezifisches Recht sollte hier die Möglichkeit der Konkretisierung erhalten, um den sektorspezifischen Eigenheiten gerecht werden zu können.

sonstiges

Sonstige lessons learned

- Schwierigkeiten im Rahmen der Regulierung:
  - IT-Sicherheit kein 0 oder 1 Zustand
  - Regulierung ist kein „Management“

- “Bigger Picture“:
  - Beste Regulierung/ konstruktivste Pflichten bringen wenig, wenn niemand da ist, um sie umzusetzen

Vielen Dank! Fragen?