WS 2020/2021

Betriebssysteme und Sicherheit

Einführung in Datenschutz und Datensicherheit

3. Informationssicherheitsmanagement

Folien von: Elke Franz
Elke.Franz@tu-dresden.de

Professur Datenschutz und Datensicherheit

3 IT-Sicherheitsmanagement – Grundsätzliches

Relevanz von Datensicherheit

- Wirtschaftliche Aspekte
  - Kosten und Folgekosten durch Ausfall
  - Wettbewerbsvorteil
- Rechtliche Aspekte
  - Haftungsfragen

Vielfältige Bedrohungen

- Unbeabsichtige Fehler und Ereignisse
  - Ausfälle, Fehlverhalten
  - Fahrlässigkeit
- Beabsichtigte Angriffe
  - Vorsätzliche Handlungen

Notwendigkeit eines (IT-)Sicherheitsmanagements

- Unternehmen/Organisationen: Gesamtheit aller Handlungen zur Erreichung von IT-Sicherheit (Sicherung der Funktion und Eigenschaften eines IT-Systems trotz unerwünschter Ereignisse)
- Ziel: Beschränkung der Restrisiken auf ein tragbares Maß

Sicherheit um jeden Preis?

Sicherheit

- verursacht Kosten
- reduziert eventuell die Systemleistung
- kann Unbequemlichkeiten zur Folge haben

  … nicht nur Einfluss auf Effizienz, sondern auch auf Akzeptanz der Schutzmechanismen durch die Nutzer

Grundsatz:

Was ist **nötig** und **nicht** was ist **möglich**!

→ Prinzip der Angemessenheit

ausgewogenes Verhältnis zwischen Sicherheitsanforderungen und Aufwand für Realisierung der Maßnahmen, Reduzierung der Risiken

Erreichbare Sicherheit

- Keine 100%ige Sicherheit möglich
  - Kein Schutz gegen alle möglichen Bedrohungen
  - Schutzmaßnahmen selbst können keine absolute Sicherheit bieten

- Erreichtes Sicherheitsniveau ist nicht dauerhaft
  - Ausgewählte Schutzmaßnahmen „statisch“
  - Bisher nicht bekannte Sicherheitslücken bzw. Schwachstellen; neue Angriffsmöglichkeiten

Security is a process, not a product.

(Bruce Schneier, 2000)

https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

3 IT-Sicherheitsmanagement – Grundsätzliches

- Erreichtes Sicherheitsniveau bezieht sich auf genau abgegrenztes Szenario
  - Grundlage für Auswahl der Maßnahmen: gegenwärtige Strukturen (Systeme, Netz, Geschäftsprozesse) und Annahmen über Einsatzumgebung
  - Selbst geringe Änderungen an Geschäftsprozessen, Infrastruktur etc. können sich auf die Sicherheit auswirken
  - Änderung externer Rahmenbedingungen wie vertragliche oder gesetzliche Vorgaben

- Sicherheit funktioniert nur in einem sensibilisierten Umfeld
  - Problembewusstsein und Problemwissen („Awareness")

➢ **Sicherheit ist kein erreichbarer Zustand, sondern ein Prozess.**

Problembewusstsein und Problemwissen („Awareness“)

- Sensibilisierung
  - sowohl auf Leitungsebene als auch bei Mitarbeitern erforderlich
- Schulung
  - Vermittlung des notwendigen Sicherheitswissens – jeder Mitarbeiter muss die für seinen Arbeitsplatz wichtigen Sicherheitsziele und Sicherheitsmaßnahmen kennen
- Training
  - Verankerung der sicherheitskritischen Tätigkeiten, so dass sie im Bedarfsfall routiniert und fehlerfrei ausgeführt werden können
- Awareness-Plan und Nachweise

Sicherheitsmanagement: Allgemeine Anforderungen

- Klare Verantwortlichkeiten und genaue Abgrenzung zu anderen Aufgaben
- Schaffung eines einheitlichen Begriffsverständnisses zwischen allen Beteiligten
- Verständliche Dokumentation
- Regelmäßige Überprüfung von Vorgaben und ihrer Einhaltung
- Nutzung erprobter (ggf. standardisierter) Vorgehensmodelle z.B.: ISO 27002, IT-Grundschutz (BSI)

Überblick über ISO/IEC 2700x

- Adressiert Management von Informationssicherheit

- Beispiele
  - ISO 27000: Überblick über Managementsysteme zur Informationssicherheit (ISMS) und über die weiteren Standards der 2700x-Reihe, Terminologie
  - ISO 27001: Zertifizierungsanforderungen an ein ISMS
  - ISO 27002: Leitfaden zum Informationssicherheitsmanagement (vorher: ISO 17799)
  - ISO 27003: Implementierungsrichtlinien für ein ISMS
  - ISO 27004: Kennzahlensysteme für ein ISMS
  - ISO 27005: Rahmenempfehlungen zum Risikomanagement

ISO/IEC 27002

- „Code of practice for information security controls“
  Leitfaden zum Informationssicherheitsmanagement
  Veröffentlichung: Oktober 2005, aktuell: 27002:2013

- Ziel
  - Darstellung der erforderlichen Schritte, um ein funktionierendes Sicherheitsmanagement aufzubauen und in der Organisation zu verankern
  - Richtlinien und allgemeine Prinzipien für das Initiieren, Umsetzen, Aufrechterhalten und Verbessern des Informationssicherheitsmanagements

3 IT-Sicherheitsmanagement – Standards

- Empfehlungen sind in erster Linie für die Management-Ebene gedacht und enthalten daher *kaum konkrete technische Hinweise*
- erforderliche Sicherheitsmaßnahmen werden nur kurz beschrieben
- Zielgruppe: Unternehmen und Organisationen aller Branchen
- Umsetzung der Sicherheitsempfehlungen der ISO 27002 ist eine von vielen Möglichkeiten, die Anforderungen des ISO-Standards 27001 („Information security management systems - Requirements“ – Anforderungen an ISMS) zu erfüllen (Zertifizierung erfolgt nach ISE/IEC 27001)
- Struktur: 14 Überwachungsbereiche, 35 Hauptkategorien, 114 Sicherheitsmaßnahmen

ISO 27002 – Inhalt

1. Security Policy
2. Organization of Information Security
3. Human Resources Security
4. Asset Management
5. Access Control
6. Cryptography
7. Physical and Environmental Security
8. Operations Security
9. Communications Security
10. Information Systems Acquisition, Development, Maintenance
11. Supplier Relationships
12. Information Security Incident Management
13. Information Security Aspects of Business Continuity
14. Compliance

BSI-Standards

- 200-1 Managementsysteme für Informationssicherheit (ISMS)
  Allgemeine Anforderungen an ein ISMS, kompatibel mit ISO/IEC 27001, Begriffe entsprechend ISO/IEC 27000

- 200-2 IT-Grundschutz-Methodik
  Anleitung zum Aufbau und Betrieb eines ISMS in der Praxis;
  unterschiedliche Vorgehensweisen: Basis-Absicherung, Kern-Absicherung und Standard-Absicherung;
  konkrete Umsetzungshinweise: IT-Grundschutz-Kompendium (prozess- und systemorientierte Bausteine)

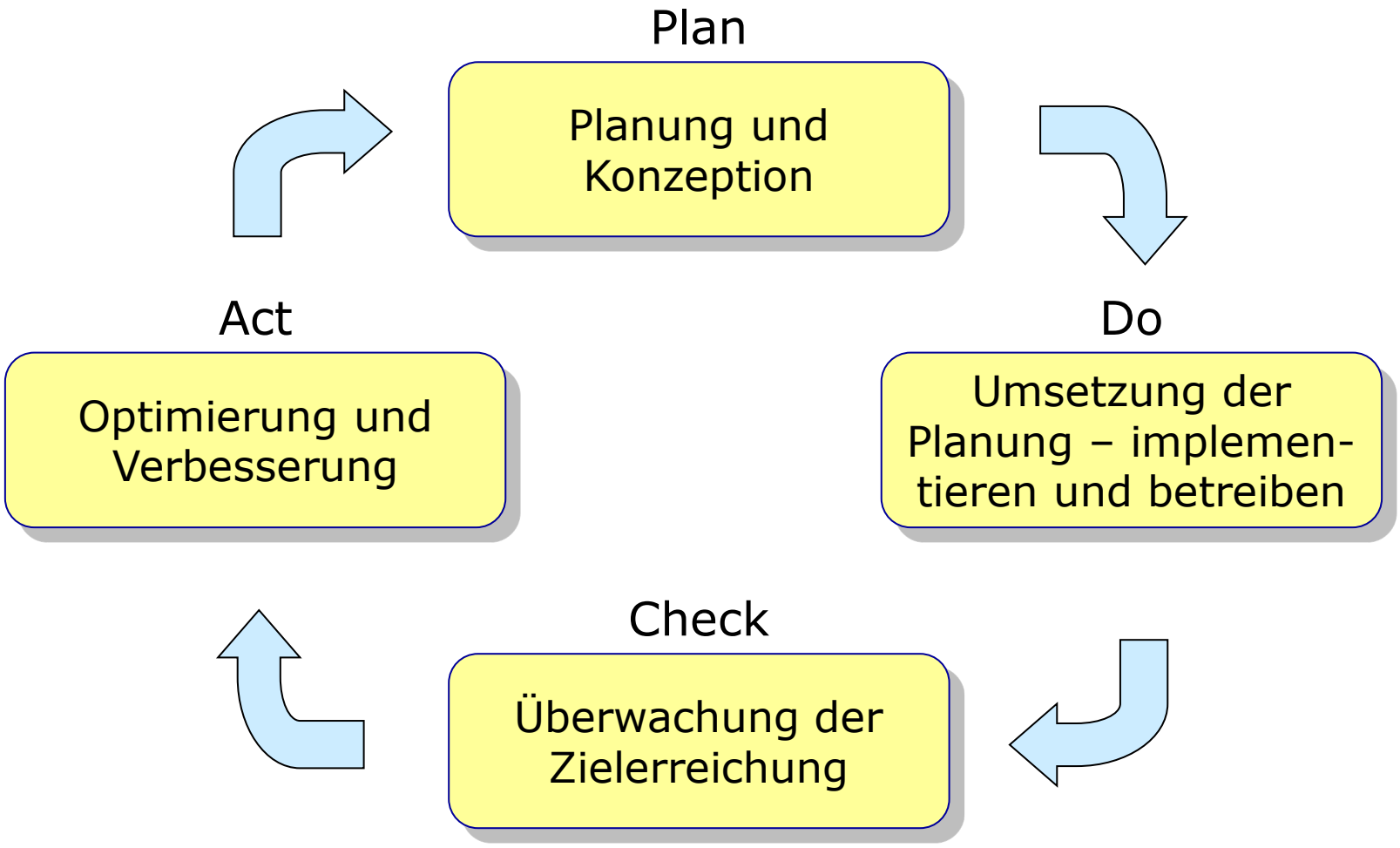
- 200-3 Risikoanalyse auf der Basis von IT-Grundschutz
  Vereinfachte Analyse von Risiken auf Basis des IT-Grundschutzes

- 200-4 Notfallmanagement

Informationssicherheits-Management-System (ISMS)

- Teil des Managementsystems, das sich mit Informationssicherheit befasst
- Ziel: Aufbau und kontinuierliche Umsetzung von Informationssicherheit
- Komponenten des ISMS
  - Management-Prinzipien
  - Ressourcen
  - Mitarbeiter
  - Sicherheitsprozess
    - Sicherheitsleitlinie (Sicherheitspolitik)
    - Sicherheitskonzept
    - Sicherheitsorganisation
- Kontinuierlicher Prozess → Lebenszyklus (PDCA-Modell)

PDCA-Zyklus


Plan
Planung und Konzeption
Do
Umsetzung der Planung – implementieren und betreiben
Check
Überwachung der Zielerreichung
Act
Optimierung und Verbesserung

ISMS: Komponenten

- Management-Prinzipien
  - Aufgaben und Pflichten des Managements
  - Kommunikation und Wissen
  - Erfolgskontrolle
  - Kontinuierliche Verbesserung des Sicherheitsprozesses

- Ressourcen
  - Finanzielle, personelle und zeitliche Ressourcen

- Mitarbeiter
  - Einbinden aller Mitarbeiter
  - Awareness

ISMS: Sicherheitsprozess

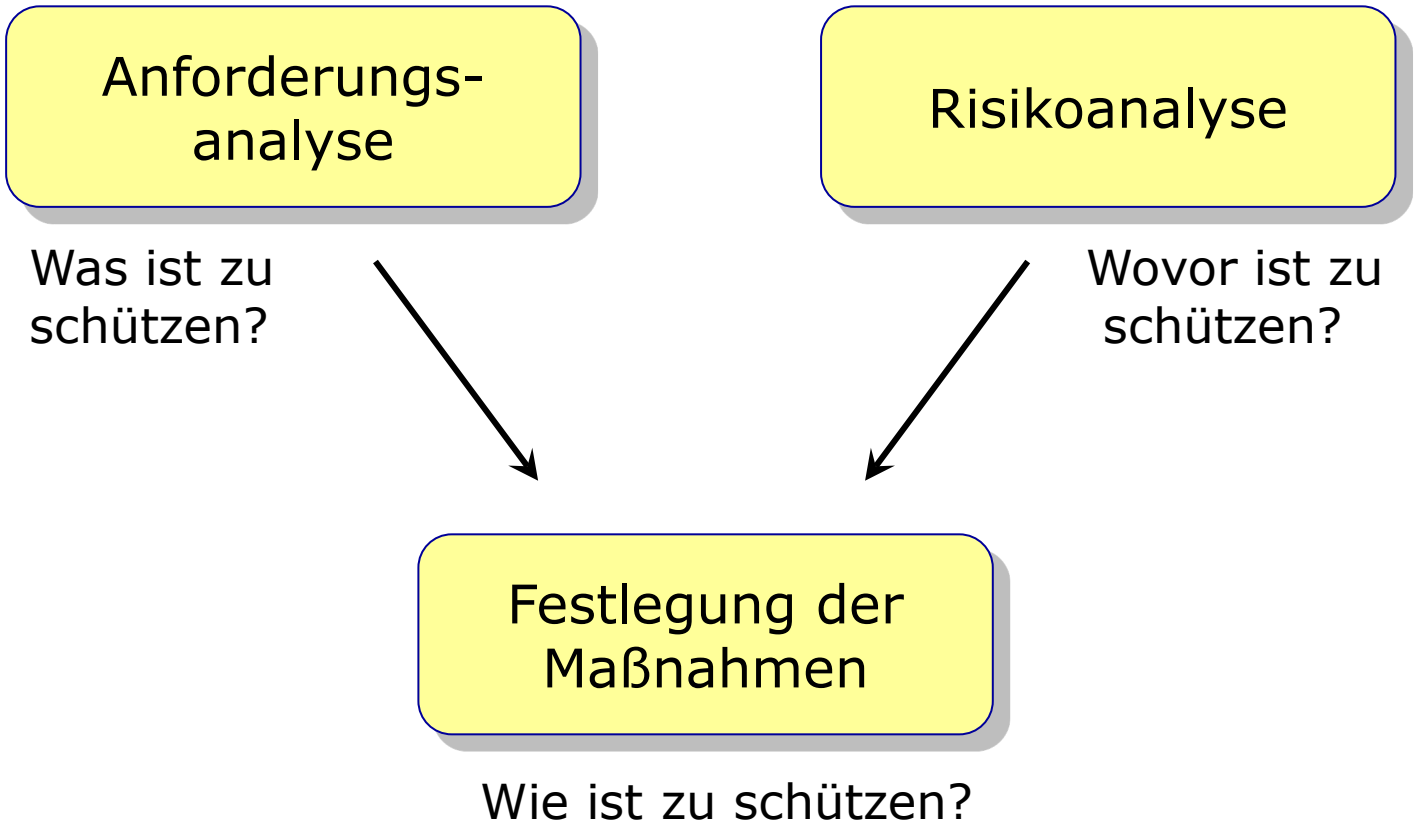
- Planung des Sicherheitsprozesses
  - Ermittlung der Rahmenbedingungen, Formulierung der allgemeinen Sicherheitsziele
  - Erstellung einer IT-Sicherheitspolitik
- Aufbau einer Sicherheitsorganisation
  - Gesamtverantwortung: Leitungsebene; mindestens ein Verantwortlicher (Informationssicherheitsbeauftragter)
  - Verantwortlichkeit jedes Mitarbeiters
- Umsetzung der Sicherheitsziele: IT-Sicherheitskonzept
  - Erstellung eines IT-Sicherheitskonzepts:
    Analyse der Sicherheit, Auswahl und Begründung von Maßnahmen
- Aufrechterhaltung der Sicherheit und Verbesserung
  - Regelmäßige Überprüfungen (interne Audits zur Umsetzung der Sicherheitsmaßnahmen; Überprüfung der Rahmenbedingungen; Awareness-Maßnahmen)
  - Nutzung der Ergebnisse für Optimierung und Verbesserung

IT-Sicherheitspolitik (IT-Sicherheitsleitlinie)

- Grundsatz-Erklärung der Unternehmensleitung zur IT-Sicherheit
- Ableitung allgemeiner Sicherheitsziele aus grundsätzlichen Zielen der Institution und allgemeinen Rahmenbedingungen

- Inhalt
  - Charakterisierung des Unternehmens
  - Geltungsbereich der Sicherheitspolitik
  - Bedeutung der Sicherheit
  - Gefährdungslage
  - Weitere Vorgaben
  - Organisationsbeschluss und Verpflichtungserklärung

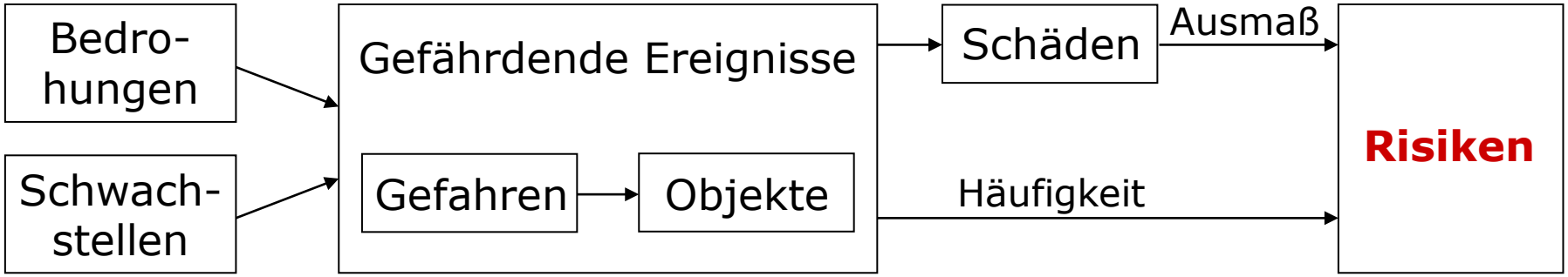
IT-Sicherheitskonzept



Anforderungsanalyse

- „Bestandsaufnahme“: Objekte, die für den festgelegten Geltungsbereich relevant sind
  - IT-Anwendungen und Geschäftsprozesse
  - IT-Systeme, Netze, Kommunikationsverbindungen
  - Infrastruktur
  - Daten
- Schutzbedarfsfeststellung
  - Betrachtung von Schäden für die Anwendungen und Daten bei Beeinträchtigung von Vertraulichkeit, Integrität und Verfügbarkeit
  - Wichtung der Schutzziele (z.B. „normal“, „hoch“, „sehr hoch“)
- Gesetze, Verträge und unternehmensinterne Regelungen

Risikoanalyse: Risikobildungsmodell



- Risiko: nach Häufigkeit (Eintrittserwartung) und Auswirkung (Schadensmaß) bewertete Gefährdung eines Systems
- Betrachtet wird immer die negative, unerwünschte und ungeplante Abweichung von Systemzielen und deren Folgen

Risikoanalyse

- Risiko-Identifikation
  - Ermittlung von Bedrohungen und Schwachstellen, die zu Gefährdungen führen können
- Risiko-Einschätzung
  - Einschätzung der Eintrittswahrscheinlichkeiten und der möglichen Schäden
- Risiko-Bewertung
  - Grundlage zur Auswahl der Maßnahmen

- Analysemethoden
  - Bottom-up (Ursache → Schadensereignis, z.B. Failure Mode and Effects Analyses, FMTA) vs. Top-Down (Schadensereignis → Ursachen, z.B. Fault Tree Analysis, FTA)
  - Quantitativ vs. qualitativ

- Quantifizierung von Risiko nach der Berechnungsformel

$$R = p_{st} \cdot S_H$$

[VDE 3100 Teil 2]

R – Risiko

p_{st} – Bewertung der Wahrscheinlichkeit für das Auftreten einer Störung

S_H – Bewertung der Schadenshöhe für den Fall der eingetretenen Störung

Probleme:

- Grundlage: Statistiken, Erfahrungen; Randbedingungen der Statistiken?
- Ermitteln der Wahrscheinlichkeiten schwierig (z.B. Motivation von Angreifern, Sekundärschäden, …)
- Ungenauigkeiten werden durch die Multiplikation verschärft

- Einführung von Klassen zur qualitativen Risikobewertung

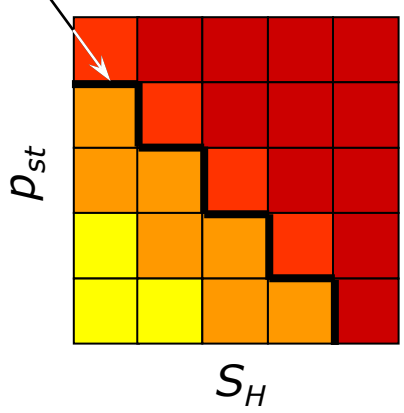
Klassen für p_{st} und S_H (Beispiel; max. 5 Klassen)

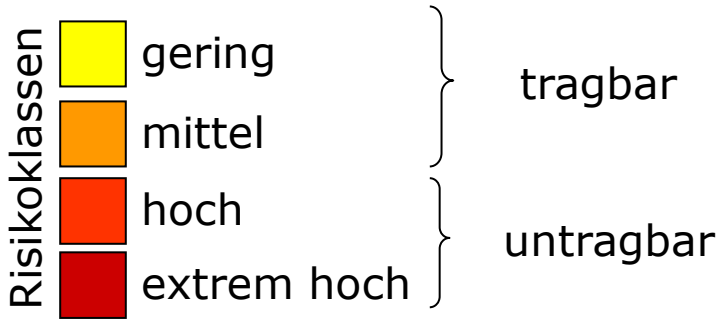
Definition der Klassen notwendig!

p_{st}	S_H
Sehr gering	Unbedeutend
Gering	Gering
Mittel	Mittel
Hoch	Groß
Sehr hoch	Katastrophal

Akzeptanzlinie (durch Unternehmens-leitung festgelegt)

Risikomatrix (Beispiel)





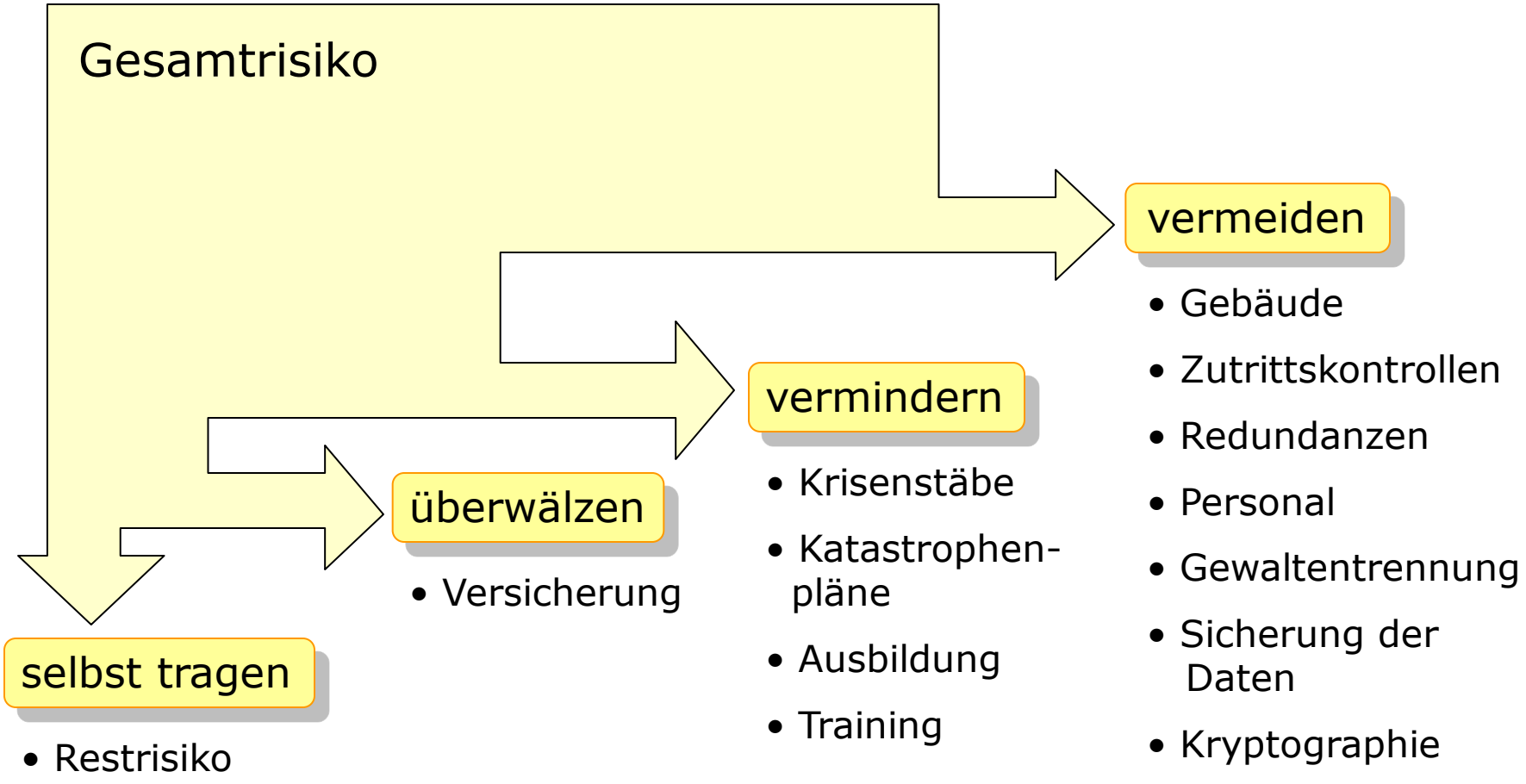
Festlegung der Maßnahmen

- Risiken auf ein akzeptables Maß reduzieren
- Anforderungen aus einzuhaltenden Gesetzen und Verträgen sowie interne Regeln des Unternehmens erfüllen

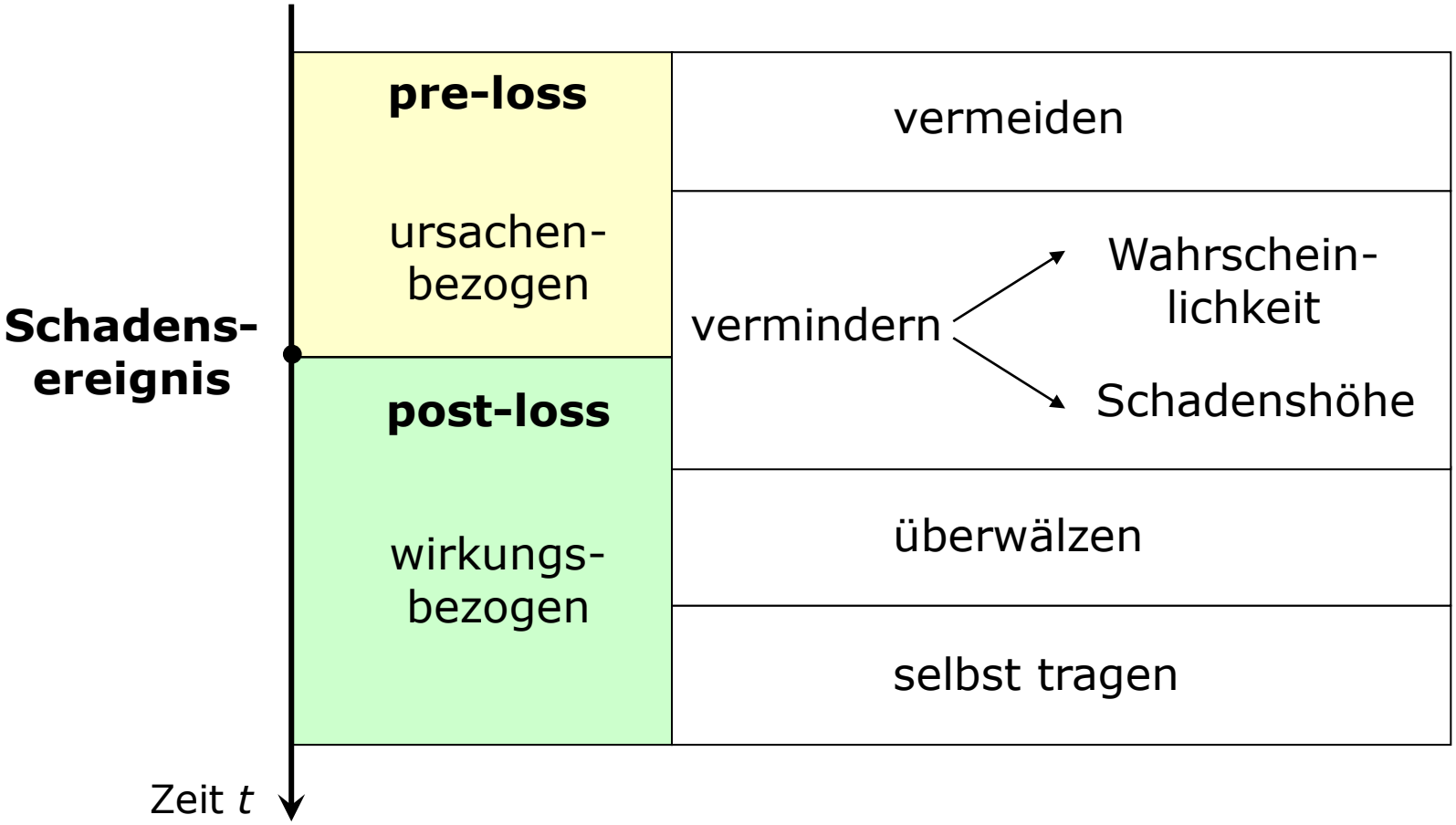
- Aufgaben
  - Auswahl von Maßnahmen
  - Validierung der Maßnahmen
  - Analyse des Restrisikos

- Auswahl von Maßnahmen
  - Hinweise und Beispiele in Standards/Normen
  - gesetzliche, vertragliche oder unternehmensinterne Vorgaben
  - Fachliteratur, Beratung

Maßnahmenklassifikation: Zielrichtung



Maßnahmenklassifikation: Zeitpunkt der Wirkung



Maßnahmenklassifikation: Objektklassen (Beispiele)

- Infrastrukturelle Maßnahmen
  - Gebäudesicherung bzgl. Elementarschäden und Naturkatastrophen
  - Zutrittskontrolle
  - redundante Stromversorgung, …
- Organisatorische Maßnahmen
  - Festlegung von Rollen und Verantwortlichkeiten
  - Definition von Zugriffsberechtigungen
  - Konzepte für Datensicherung, …
- Personelle Maßnahmen
  - Maßnahmen bei Einstellung und Ausscheiden
  - Arbeitsumgebung
  - Awarenessmaßnahmen, …
- Technische Maßnahmen
  - Authentikation, Verschlüsselung
  - Schlüsselmanagement
  - Datensicherung, …

- Validierung der Maßnahmen
  - **Eignung** (Maßnahme muss sich gegen die betrachtete Bedrohung richten bzw. den erwarteten Schaden mindern)
  - **Wirksamkeit** (Maßnahme muss ausreichend stark sein)
  - **Zusammenwirken** (geplante Maßnahme darf nicht genutzt werden können, um andere Sicherheitsmaßnahmen zu unterlaufen)
  - **Praktikabilität** (leicht verständlich, einfach anwendbar, wenig fehleranfällig)
  - **Akzeptanz** (für alle Benutzer ohne Beeinträchtigung anwendbar)
  - **Wirtschaftlichkeit** und Angemessenheit

- Analyse des Restrisikos
  - Gegen welche Bedrohungen wird in welchem Maß Schutz erreicht
  - kein untragbar hohes Risiko mehr nach diesem Schritt

Ergebnis: IT-Sicherheitskonzept

- Vorspann mit Zusammenfassung für das Management, Glossar
- Gegenstand des Sicherheitskonzepts (Geltungsbereich)
- Anforderungsanalyse
- Risikoanalyse: Beschreibung des Ist-Zustandes
- Festlegung der Maßnahmen mit Begründung der Auswahl
- Beschreibung des Restrisikos

Lebenszyklus des IT-Sicherheitskonzepts

- Plan:
  - IT-Sicherheitskonzept
- Do:
  - Realisierungsplan für das Konzept
  - Umsetzung der Maßnahmen
  - Sensibilisierung und Schulung
- Check:
  - Detektion von Sicherheitsvorfällen
  - Überprüfung der Einhaltung der Maßnahmen
  - Berichte
- Act:
  - Beseitigung von Fehlern
  - Verbesserungen, Anpassungen an geänderte Bedingungen