STEFAN SCHREINER 2023

DATENSCHUTZ & DATENSICHERHEIT

Das ungleiche Geschwisterpaar im Informationssicherheitsmanagement

ISMS KOMPAKT

IT SICHERHEITSMANAGEMENT

Datensicherheit ist wichtig, weil

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

Bedrohungen

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

DARUM BRAUCHT ES EIN (IT-) SICHERHEITSMANAGEMENT

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
- Benötigt Ressourcen und schränkt die Systemleistung ein
- Kann negativen Einfluss, umständliche Bedienung, zur Folge haben
  (Damit ist nicht nur der Einfluss auf die Effizienz der Maßnahmen gemeint, sondern vor allem die abnehmende Akzeptanz der Schutzmechanismen durch den Benutzer!)

Grundsatz:

Was ist nötig und nicht was ist möglich!

* **Prinzip der Angemessenheit**

Ausgewogenes Verhältnis zwischen Sicherheitsanforderungen und Aufwand für die Realisierung der Maßnahmen zur Reduzierung der Risiken.

SICHERHEIT UND PARETO

Erreichbare Sicherheit

- Mehr als 100% Sicherheit ist nicht möglich.
  Einen umfassenden Schutz gegen alle möglichen Bedrohungen gibt es nicht - man bezeichnet das ein Defizitrisiko. Die ersten 80 Prozent zu erreichen verursachen in etwa den selben Aufwand wie die letzten 20 Prozent. Schutzmaß-nahmen können keine absolute Sicherheit bieten.

Erreichtes/ aktuelles Sicherheitsniveau ist nicht dauerhaft

- Schutzmaßnahmen sind statisch
- Bisher nicht bekannte Sicherheitslücken bzw. Schwachstellen bieten neue Angriffsmöglichkeiten

SECURITY IS A PROCESS, NOT A PRODUCT.

(BRUCE SCHNEIER, 2000)

SICHERHEIT GRUNDSÄTZE

- Erreichtes Sicherheitsniveau bezieht sich immer nur auf ein abgegrenztes Szenario
  - Grundlage für Auswahl der Maßnahmen sind,
    - Gegenwärtige Strukturen (Systeme, Netze, Geschäftsprozesse)
    - Annahmen über Einsatzumgebung
  - Selbst geringe Änderungen an Geschäftsprozessen, Infrastruktur etc. wirken sich auf die Sicherheit aus.
  - Änderungen externer Rahmenbedingungen, wie vertragliche oder gesetzliche Vorgaben, sind begrenzende Muss Kriterien.
- Sicherheit funktioniert nur in einem sensibilisierten Umfeld
  - Problembewusstsein und Problemwissen (aka „Awareness“) muss laufend gefordert werden.

SICHERHEIT IST KEIN ERREICHBARER ZUSTAND, SONDERN EIN DAUERHAFTER PROZESS!

AWARENESS

Problembewusstsein & Problemwissen

- **Sensibilisierung**

  Auf allen Ebenen des Unternehmens und der Organisation erforderlich.

- **Schulung**

  Vermittlung des notwendigen Sicherheitswissens - alle Mitarbeiter müssen die für Ihren Arbeitsplatz wichtigen und vereinbarten Sicherheitsziele und Sicherheitsmaßnahmen kennen.

- **Training**

  Verankerung der sicherheitskritischen Tätigkeiten, so dass diese im Bedarfsfall routiniert und fehlerfrei ausgeführt werden können.

- **Awareness-Plan und Nachweis**

  Strukturierte Handlungsanleitung und Nachweis über Erfüllung von Vorgaben und Richtlinien.

ALLGEMEINE ANFORDERUNGEN

Sicherheitsmanagement

- Klare Verantwortlichkeiten und genaue Abgrenzung zu anderen Aufgaben
  - Transparenz des Tätigkeitfelds
  - Kollisionsvermeidung im Vorfeld von Rollenkonflikten
- Schaffung eines einheitlichen Begriffsverständnisses zwischen allen Beteiligten
- Verständliche Dokumentation
- Regelmäßige Überprüfung von Vorgaben und ihrer Einhaltung
- Nutzung erprobter (ggf. standardisierter) Vorgehensmodelle (ISO 27000 Reihe, IT Grundschutz, NIST etc.)

ISO/IEC 2700X REIHE

- Adressiert Management von Informationssicherheit
- Auswahl:
  - 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 (vormals ISO 17799)
  - ISO 27003: Implementierungsrichtlinien für ein ISMS
  - ISO 27004: Kennzahlen für ein ISMS
  - ISO 27005: Rahmenempfehlungen zum Risikomanagement
  - ISO 27018: Leitfaden zum Schutz personenbezogener Daten (PII) in der Auftragsdatenverarbeitung (vgl.: Cloud Dienst)

ISO/IEC 27002

Im speziellen

- „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.

ISO/IEC 27002

Fortsetzung

- Empfehlung sind in erster Linie für die Management-Ebene gedacht und enthalten daher kaum konkrete technische Hinweise.
- Erforderliche Sicherheitsmaßnahmen werden nur kurz beschrieben.
- Zielgruppe sind Unternehmen und Organisationen aller Branchen.
- Umsetzung der Sicherheitsempfehlungen der ISO 27002 ist eine von vielen Möglichkeiten, die Anforderungen des ISO (defacto) Standards 27001 (vgl.: Information security management systems - requirements) zu erfüllen. Eine Zertifizierung erfolgt nach ISO/IEC 27001.
- Dokumentstruktur/ Gliederung, 14 Überwachungsbereiche, 35 Hauptkategorien und 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 System Acquisition, Development, Maintenance
11. Supplier Relationships
12. Information Security Incident Management
13. Information Security Aspects of Business Continuity
14. Compliance

IT GRUNDSCHUTZ

BSI Standard, Österreich in Anlehnung dazu

- 200-1 Management für Informationssysteme (ISMS)
  Allgemeine Anforderungen an ein ISMS, kompatibel mit ISO/IEC 27001, Begriffsdefinitionen entsprechend ISO/IEC 27000
- 200-2 IT-Grundschutz-Methodik
  Anleitung zum Aufbau und Betrieb eines ISMS in der Praxis. Mögliche Vorgehensweisen sind, Basis-Absicherung, Kern-Absicherung und Standard-Absicherung. Es gibt konkrete Umsetzungshinweise im IT Grundschutz Kompendium. Die Bausteine sind prozess- und systemorientiert.
- 200-3 Risikoanalyse auf der Basis von IT Grundschutz
  Vereinfachte Analyse von Risiken auf Basis des IT Grundschutzes.
- 200-4 Notfallmanagement
  Vorgehensmodell beim Risikoeintritt

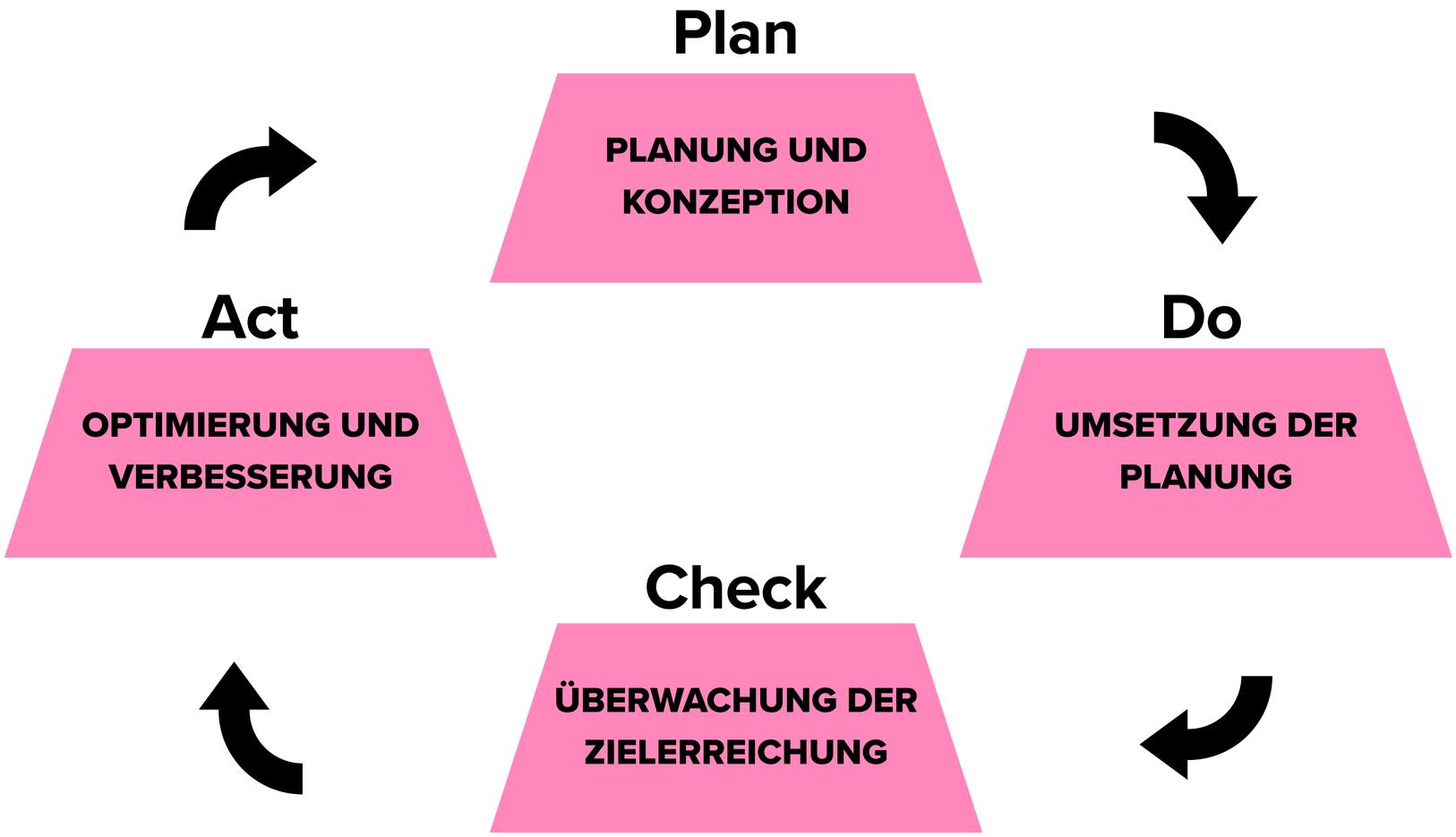
ISMS

Informations Sicherheit Management System

- Teil des Managementsystems, das sich mit Informationssicherheit befasst.
- Ziel ist der Aufbau und die kontinuierliche Umsetzung von Informationssicherheit.
- Komponenten des ISMS sind,
  - Management Prinzipien
  - Ressourcen
  - Mitarbeiter
  - Sicherheitsprozesse
    - Sicherheitsleitlinie (vgl. Sicherheitspolitik)
    - Sicherheitskonzept
    - Sicherheitsorganisation
- Kontinuierlicher Prozess bildet sich im Lebenszyklus (vgl.: PDCA Zyklus/ Demming Rad)

DEMMING RAD

PDCA Zyklus



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 (vgl.: Informationssicherheitsbeauftragter)
  - Regelung Verantwortlichkeit jedes Mitarbeiters (vgl.: Betriebsvereinbarung, Dienstanweisung etc.)
- Umsetzung der Sicherheitsziele in Form des IT Sicherheitskonzepts
  - 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. Ebenso Überprüfung der Rahmenbedingungen und Awareness Maßnahmen auf Gültigkeit und Wirksamkeit.)
  - Nutzung der Ergebnisse für Optimierung und Verbesserung

ISMS

IT Sicherheitspolitik (vgl.: IT Sicherheitsleitlinie)

- Grundsatzerklärung 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
  - Weiter Vorgaben
  - Organisationsbeschluss und Verpflichtungserklärung

ISMS

IT Sicherheitskonzept

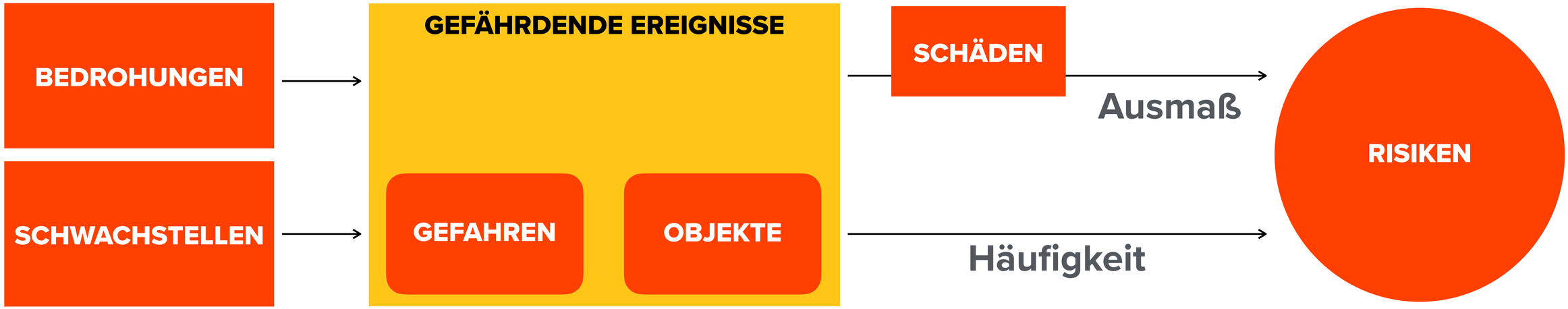
ISMS

Anforderungsanalyse

- Bestandsaufnahme: Objekte, die für den festgelegten Geltungsbereich relevant sind
  - IT Anwendungen und Geschäftsprozesse
  - IT Systeme, Netze, Kommunikationsverbindungen
  - Infrastruktur
  - Daten
- Schutzbedarf Feststellung
  - Betrachtung von Schäden für die Anwendung und Daten bei Beeinträchtigung von Vertraulichkeit, Integrität und Verfügbarkeit
  - Gewichtung der Schutzziele (vgl.: normal, hoch, sehr hoch)
- Gesetze, Verträge, Richtlinien und interne Regelungen und Vereinbarungen

ISMS

Risikomodell



- Risiko: nach Häufigkeit (Eintrittswahrscheinlichkeit) und Auswirkung (Schadensausmaß) bewertete Gefährdung eines Systems.
- Betrachtet wird immer die negative, unerwünschte und ungeplante Abweichung von System- und Unternehmenszielen und deren Folgen.

ISMS

Risikoanalyse

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

Analysemethoden

- Bottom-Up: Von der Ursache auf das Schadensereignis schliessen. (Vgl.: Failure Mode and Effects Analysis, FMTA)
- Top-Down: Vom Schadensereignis auf die Ursache schliessen. (Vgl.: Fault Tree Analysis, FTA)
- Qualitativ und qualitative Methoden.

ISMS

Quantifizierung von Risiken

$R = p_{st} * S_H$

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 (vgl.: Motiv der Angreifer, Sekundärschäden uvm.)
- Ungenauigkeit wird durch Multiplikation verstärkt.

ISMS

Klassifizierung zur qualitativen Risikobewertung

Klassen für p_{st} und S_H

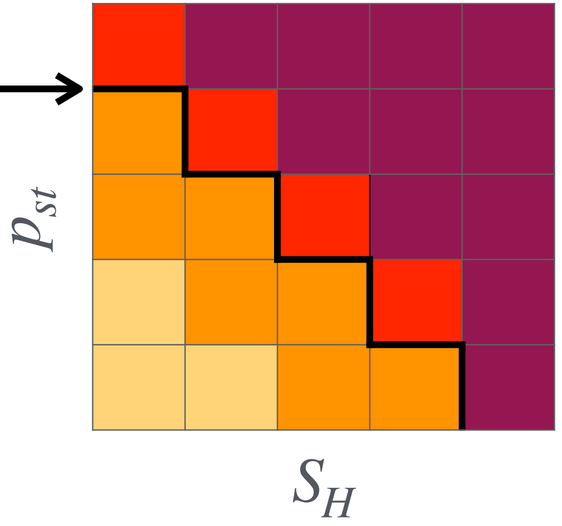
(Hier mit fünf Klassen)

Definition der Klassen notwendig und im Verhältnis zur wirtschaftlichen Fähigkeit betrachten.

Akzeptanzlinie (Durch Unternehmensleitung festgelegt)

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

Risikomatrix



Risikoklassen

- gering
- mittel

tragbar

- hoch
- extrem hoch

untragbar

ISMS

Festlegung der Maßnahmen

- Risiken auf ein akzeptables Maß reduzieren.
- Anforderungen aus einzuhaltenden Gesetzen und Verträgen sowie interne Richtlinien des Unternehmens erfüllen.
- Aufgaben
  - Auswahl von Maßnahmen
  - Validieren der Maßnahmen
  - Analyse des Restrisikos
- Auswahl der Maßnahmen
  - Hinweise und Beispiele in Standards, Normen und Handbüchern
  - Gesetzliche, vertragliche und unternehmensinterne Vorgaben
  - Fachliteratur und externe Unterstützung (vgl.: Beratung)

ISMS

Maßnahmenklassifikation: Zielrichtung

VERMEIDEN

- Gebäude
- Zutrittskontrolle
- Redundanzen
- Personal
- Gewaltentrennung
- Sicherung der Daten
- Kryptographie

VERMINDERN

- Krisenstab
- Katastrophen-plan
- Ausbildung
- Training

ÜBERWÄLZEN

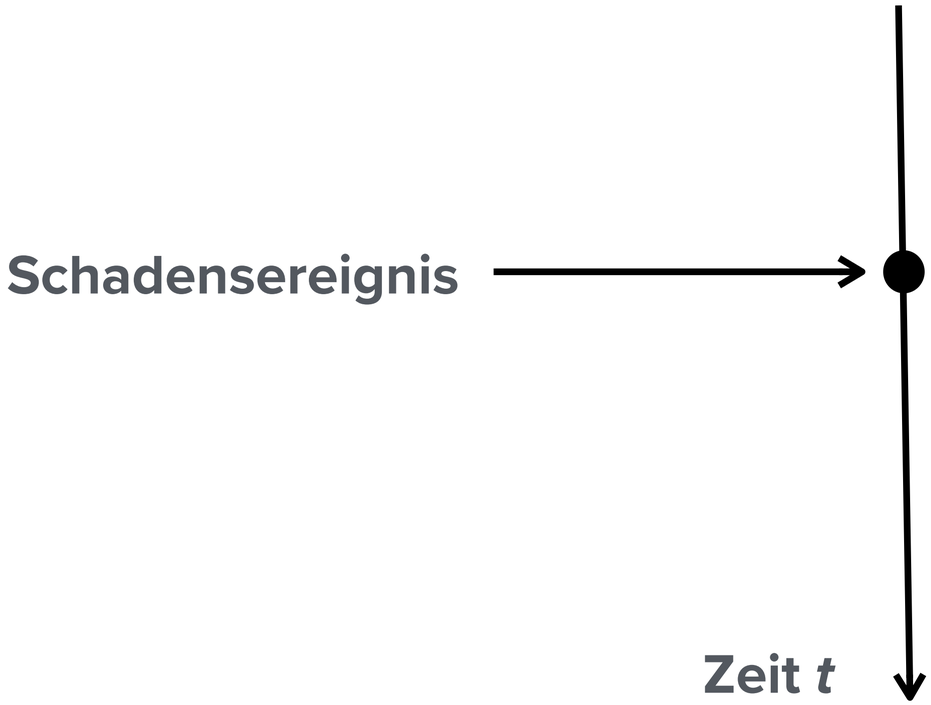
- Versicherung

SELBER TRAGEN

- Restrisiko

ISMS

Maßnahmenklassifikation zum Zeitpunkt der Wirkung



pre-loss ursachenbezogen	vermeiden	
	vermindern	Wahrscheinlichkeit
		Schadenshöhe
post-lost wirkungsbezogen	überwälzen	
	selbst tragen	

ISMS

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
  - Authentifikation, Verschlüsselung
  - Schlüsselmanagement
  - Datensicherung ...

ISMS

Validieren 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 und wenig fehleranfällig.
- **Akzeptanz**
  Für alle Benutzer ohne Beeinträchtigung anwendbar.
- **Wirtschaftlichkeit und Angemessenheit**

Analyse des Restrisikos

- **Gegen welche Bedrohungen wird in welchem Ausmaß Schutz erreicht?**
- **Kein untragbares Risiko nach diesem Schritt mehr vorhanden.**

ISMS

Ergebnis ist ein IT Sicherheitskonzept

- Vorspann mit Zusammenfassung für das Management und ein Glossar
- Gegenstand des Sicherheitskonzepts und sein Geltungsbereich
- Anforderungsanalyse
- Risikoanalyse (vgl.: Beschreibung Ist Zustand)
- Festlegung der Maßnahmen mit Begründung der Auswahl
- Beschreibung des Restrisikos

ISMS

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
  - Beseitigen von Fehlern
  - Verbesserung und Anpassung an geänderte Bedingungen