AWK GROUP

Consulting
Engineering
Project Management

Sicherer Erfolg dank ISDS-Konzept:
Erfahrung, Erkenntnisse und Umsetzungsempfehlungen für kantonale Polizeiorganisationen

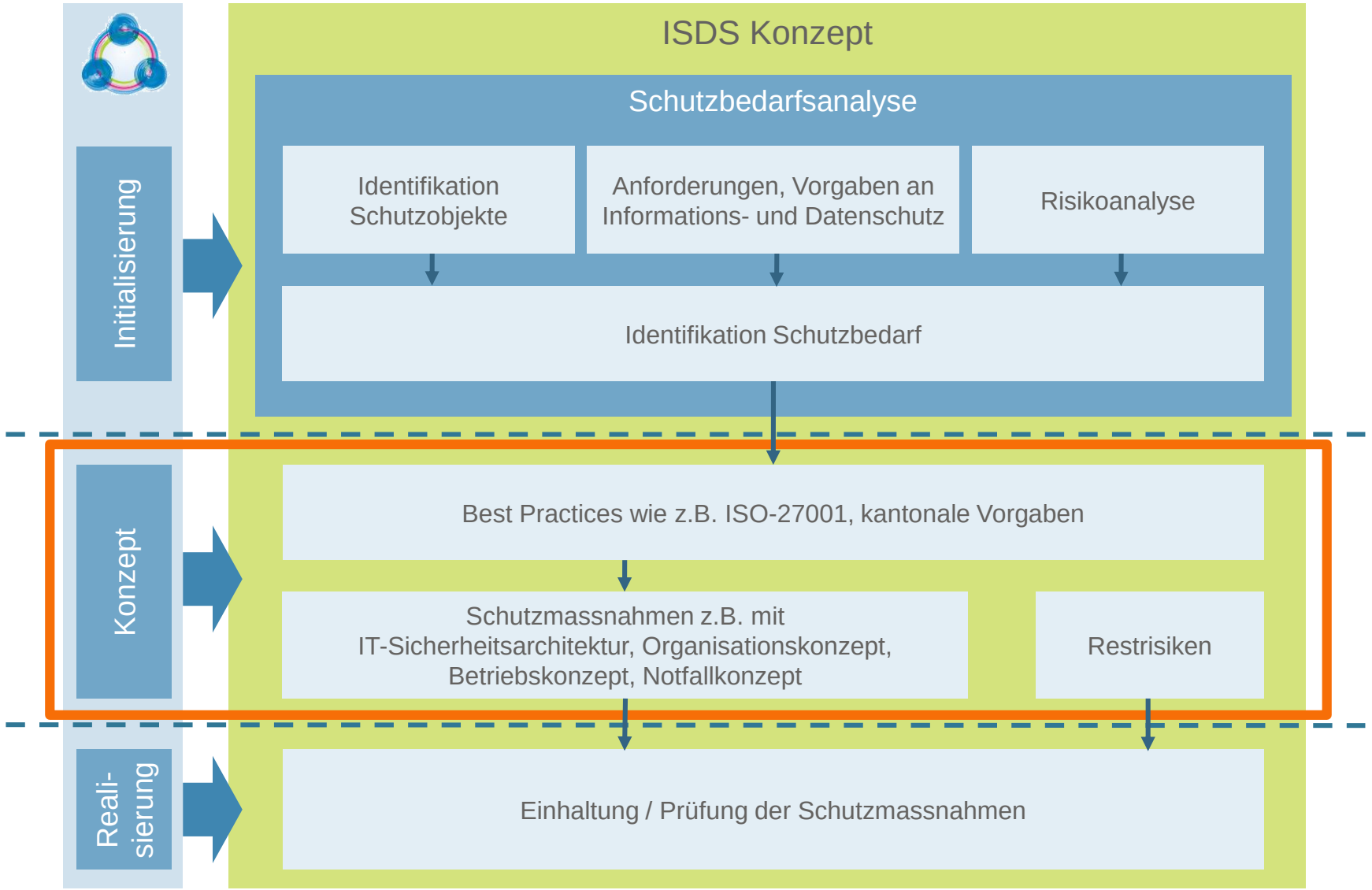
SPIK 2018, 22. März 2018

Marcel Schönbächler, Senior Consultant

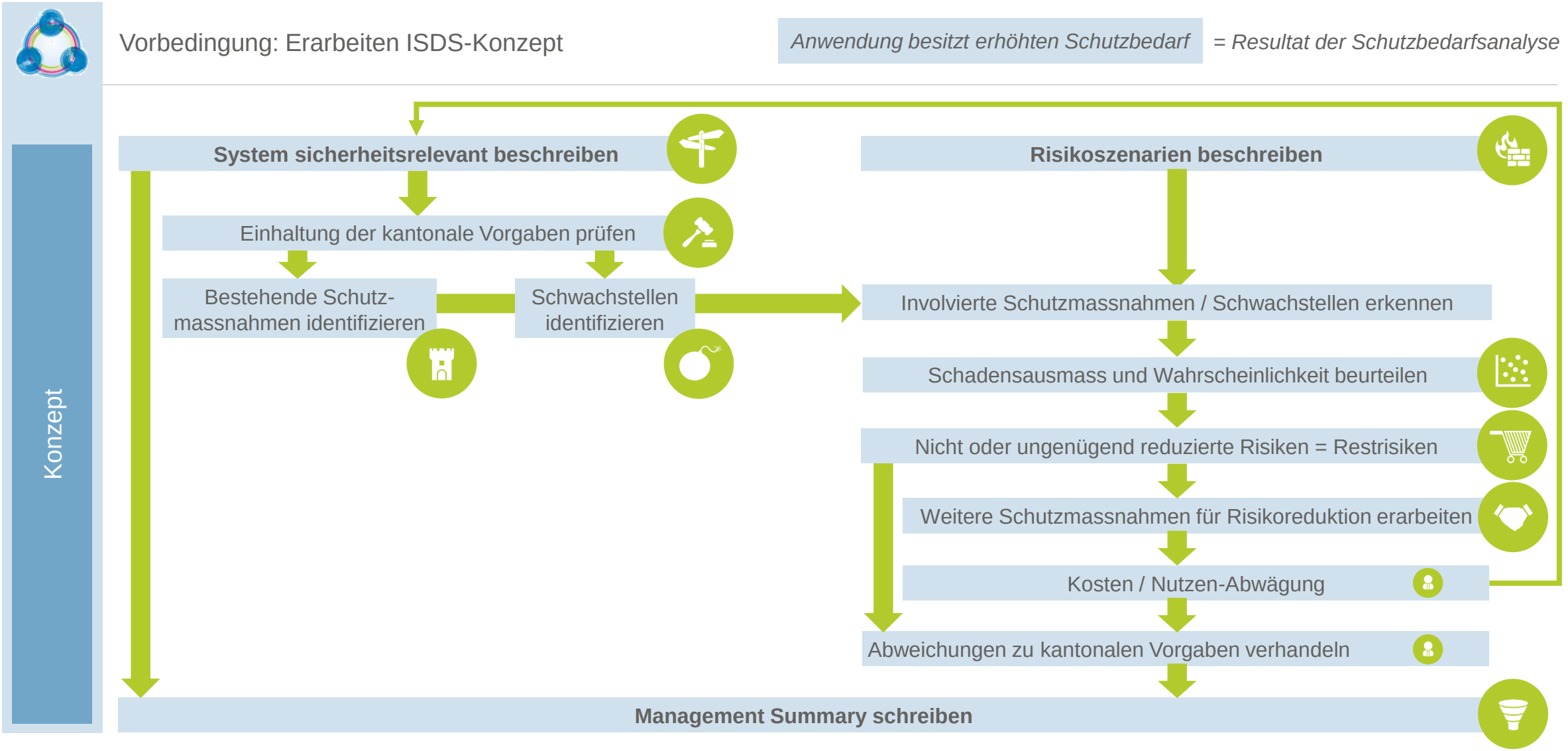
Themen

- Die Erstellung eines polizeilichen ISDS-Konzeptes praxisnah erläutern.
- Der nur indirekte bestehende Zusammenhang zwischen kantonalen Vorgaben und Risiko aufzeigen.
- Das systematische Ableiten von Risiken auf Basis von Risikoszenarien anhand von Beispielen erklären.

Erarbeitung / Überprüfung / Ergänzung ISDS Konzepte



Von der Sicherheitsbeurteilung zum ISDS-Konzept

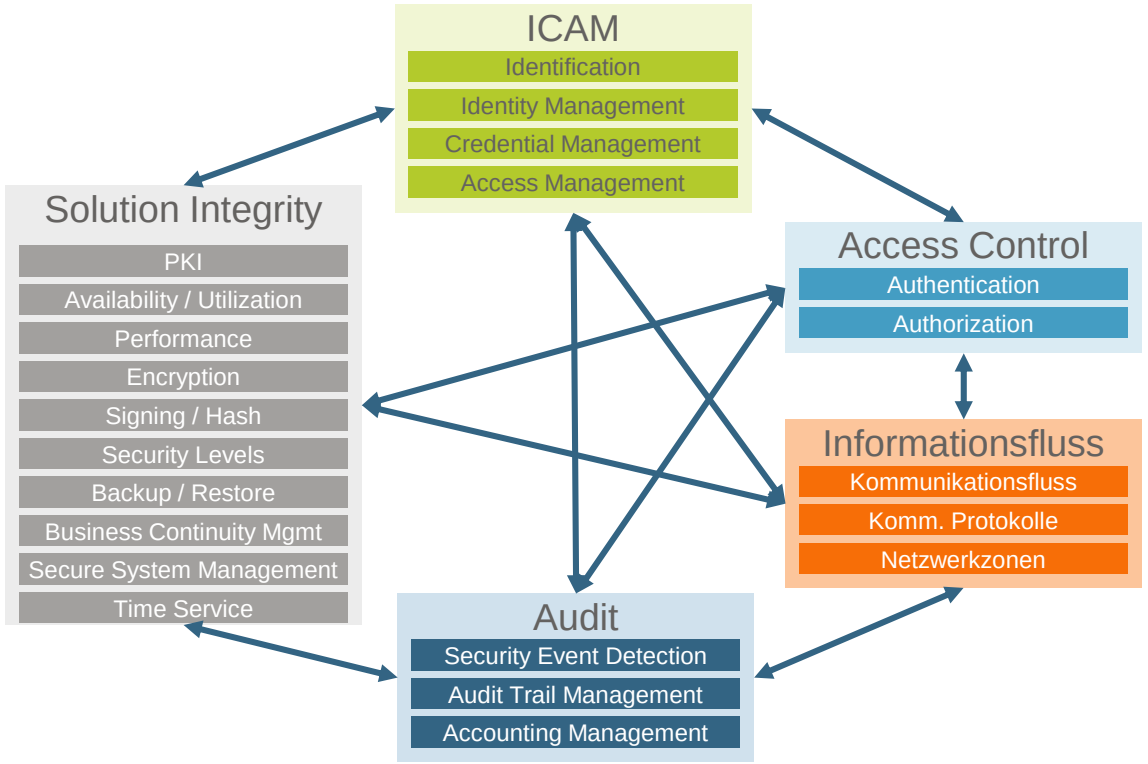


System sicherheitsrelevant beschreiben

Vorgehen

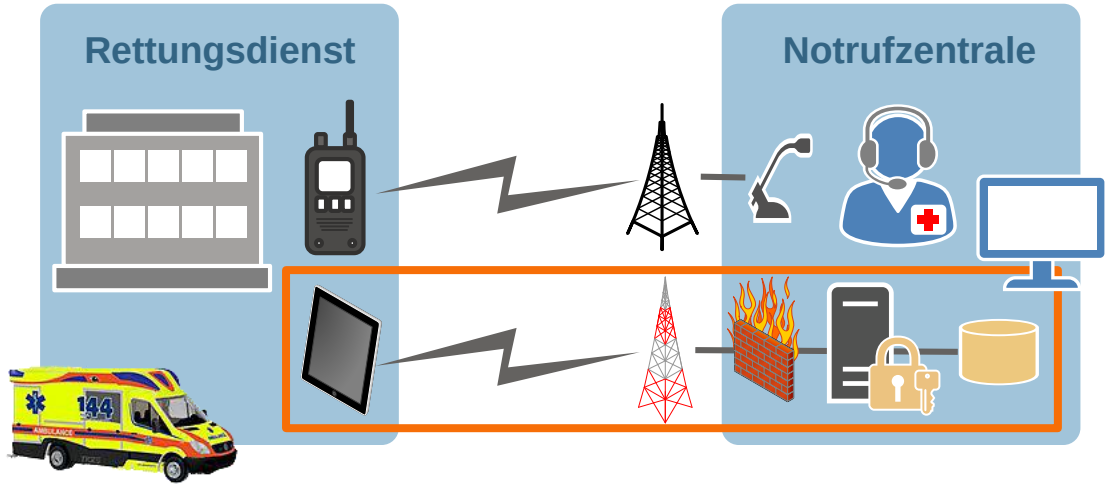
- Systemgrenzen bestimmen (In-Scope / Out-of-Scope)
- Einzelne relevante Interessensdimensionen beschreiben

Interessensdimensionen



Praxisbeispiel: "mobile unpersönliche Geräte (iPad) in Einsatzfahrzeugen"

- Resultat der Schutzbedarfsanalyse
  ➔ besonders schützenswerte Daten
- Begründung:
  - Patientendaten
  - Aktuelle Einsatzorte
- Systemgrenzen:



Einhaltung der kantonalen Vorgaben prüfen

Vorgehen

1. Relevante Vorgaben identifizieren

- Welche relevanten Weisungen gibt es?

2. Einhaltung dieser Vorgaben prüfen

- Sind die Compliance-Anforderungen eingehalten?

3. Klären, ob dadurch Schwachstellen bestehen

Praxisbeispiel

1. Relevante Vorgaben

- 1019-Übergeordnete Sicherheitsbestimmungen
- 1124-Weisung Sicherheit Smartphones

2. Einhaltung dieser Vorgaben

- Verwendung *unpersönliche Benutzerkonten*, weil iPad dem Fahrzeug und nicht einem Rettungsteam zugewiesen ist.

3. Schwachstellen?

- Keine weitere Schwachstelle, weil im Einsatzleitsystem die Dienstpläne historisiert sind. Die Nachvollziehbarkeit ist gegeben.

Bestehende Schutzmassnahmen und Schwachstellen identifizieren

Vorgehen

Schwachstellen identifizieren

- Über welche bestehenden Schwachstellen könnten Verfügbarkeit, Vertraulichkeit, Integrität oder Nachvollziehbarkeit gefährdet sein?

Bestehende Schutzmassnahmen identifizieren

- Welche Massnahmen wurden speziell getroffen und bereits umgesetzt, um das System sicherer zu machen?
- Zum Beispiel
  - IT-Sicherheitsarchitektur
  - Organisationskonzept
  - Betriebskonzept
  - Notfallkonzept

Praxisbeispiel

Schwachstelle

- Patientendaten sind auf dem mobilen iPad sichtbar.

Schutzmassnahmen

- IT-Sicherheitsarchitektur:
  - Es befinden sich nur Daten des aktuellen Einsatzes auf dem iPad.
- Betriebskonzept:
  - Das iPad kann vom IT-Helpdesk aus der Ferne gelöscht werden.

Risikoszenarien beschreiben

Vorgehen

Mögliche Risikoszenarien beschreiben

- Schadensablauf anhand von generischen Beispielen
- Zentrale Frage: Welche Risikoursachen bestehen?
- Die Risikoszenarien sind den vier "Säulen" der Informatiksicherheit zu zuweisen:
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität
  - Nachvollziehbarkeit von Informationen und Daten
- Welche Schwachstellen und Schutzmassnahmen sind involviert?

Praxisbeispiel

Risikoszenario für "Vertraulichkeit"

- "Zugang zu Patientendaten aufgrund eines Verlustes eines iPads während eines Einsatzes"
- Involvierte Schwachstellen
  - Patientendaten sind auf dem iPad sichtbar.
- Involvierte Schutzmassnahmen
  - Es befinden sich nur Daten des aktuellen Einsatzes auf dem iPad.
  - Das iPad kann vom IT-Helpdesk aus der Ferne gelöscht werden.

Schadensausmass und Wahrscheinlichkeit der Risikoszenarien beurteilen

Vorgehen

Eintretenswahrscheinlichkeit des Risikoszenarios

- Wie wahrscheinlich ist es, dass das Risikoszenario eintritt?

Schadensausmass beim Eintreten dieses Risikoszenarios

- Was ist das erwartete Schadensausmass?

Risikohöhe ableiten

- Die Risikomatrix ist in der Regel von der Organisation vorgegeben.

Praxisbeispiel

- "Zugang zu Patientendaten aufgrund eines Verlustes eines iPads während eines Einsatzes"

Eintretenswahrscheinlichkeit

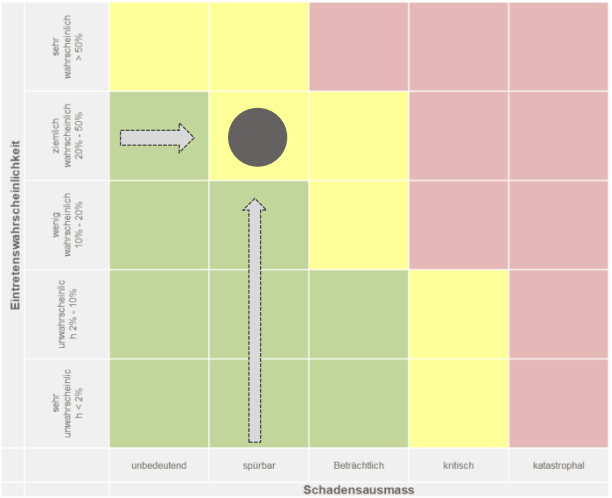
- Ziemlich wahrscheinlich

Schadensausmass

- spürbar

= Risiko

- Mittleres Risiko

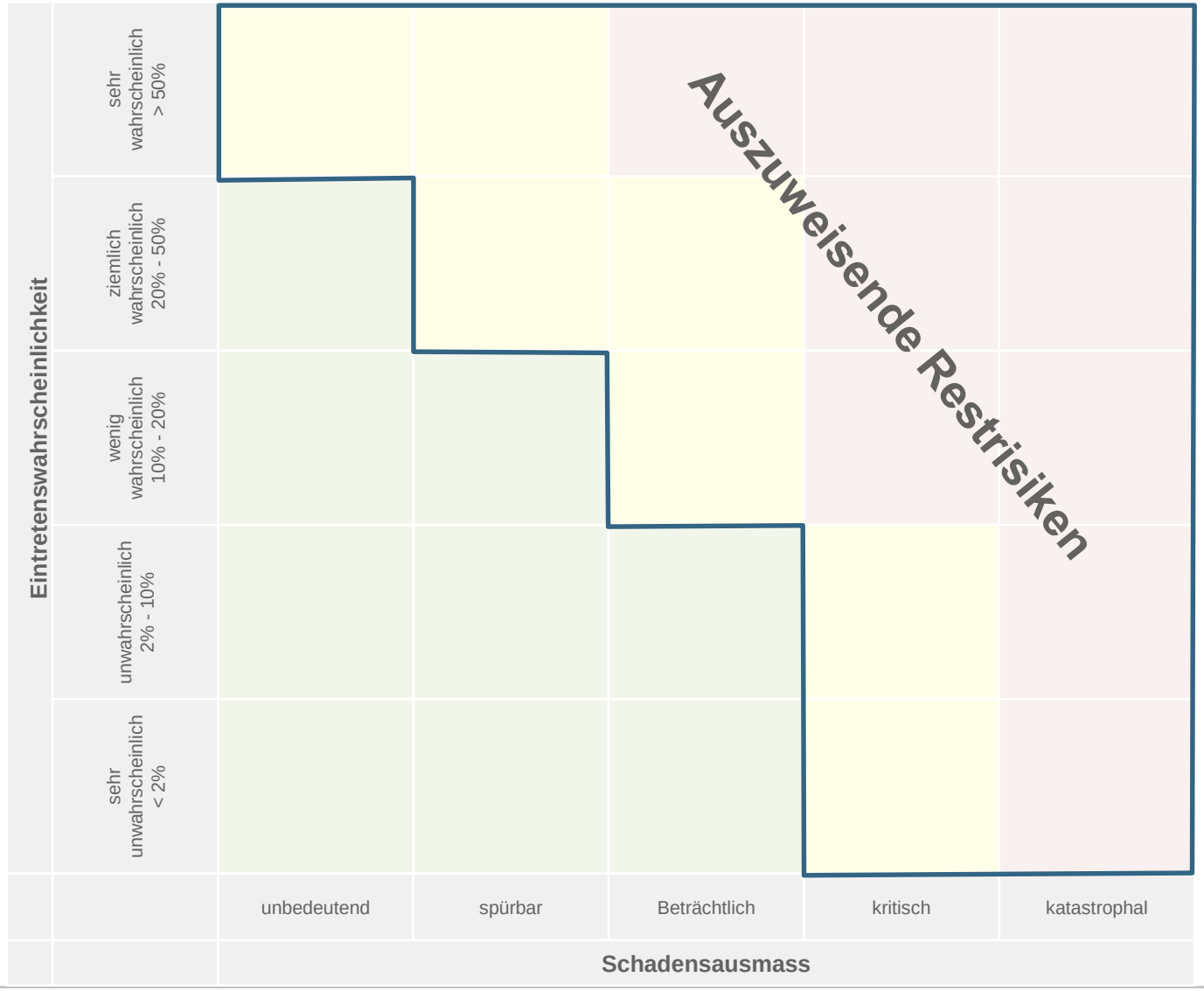


Restrisiken erkennen

Die Restrisiken können aus der Risikomatrix abgeleitet werden.

- Geringe Risiken (grün)
- Mittlere Risiken (gelb)
- Hohe Risiken (rot)

- Als Restrisiken sind die mittleren und hohen Risiken auszuweisen.



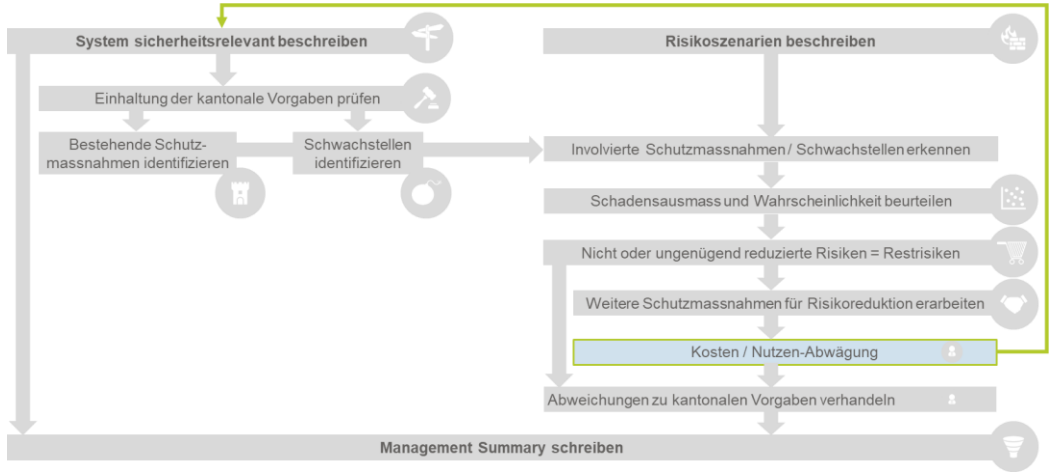
Weitere Massnahmen für Risikoreduktion erarbeiten

Regelmässige Absprachen mit Datenherr:

- Zentrale Frage: Welche Restrisiken ist der Datenherr bereit zu tragen?

Bei Bedarf sind weitere Schutzmassnahmen dem Projekt vorzuschlagen, welche die Restrisiken weiter reduzieren zu können.

Bei "Genehmigung" einer Schutzmassnahme nach Kosten/Nutzenabwägung:
Iteration über Systembeschreibung notwendig



Fiktives Praxisbeispiel

- Auf iPad sind alle Patientendaten aller aktuellen vergangenen Einsätze enthalten. Das iPad ist nicht geschützt.

Mögliche Schutzmassnahmen:

Massnahme	Kosten	W'keit	Schaden
PIN anfordern	o	↓	
Fingerprint hinterlegen	+	↓	
Sperrzeit: 5 Minuten	+	↓	
Nur aktueller Einsatz auf iPad	++		↓

↗ ↓ *Mittlerer Einfluss*
↑ ↓ *Hoher Einfluss*

Management Summary schreiben

Zweck eines ISDS-Konzepts:

- Der Risikoträger wird vollständig, in einer ihm verständlichen Form, über alle Risiken informiert
- Die Erfüllung der Vorgaben ist eindeutig deklariert.
- Der Erfüllungsgrad der Informationssicherheits-Anforderungen ist eindeutig ersichtlich.

- **Im Management Summary muss festgehalten werden, welche Restrisiken die Risikoträger (Datenherr / Geschäftsprozessverantwortlicher) übernehmen müssen.**

Nutzen eines ISDS-Konzepts:

- **Es werden nur Massnahmen umgesetzt, welche Mehrwert bringen und mit dem Management abgestimmt sind.**
- **Gewissheit, dass Restrisiken auch vom Management getragen werden.**

Take-Aways

- Mit einem systematischen Vorgehen und regelmässigen Absprachen mit dem Datenherr können ISDS-Konzepte effizient und schlank erstellt werden.
- Iterationen bei der Erarbeitung sind wichtig für Verbesserungen!
- In Projekten ermöglicht eine frühzeitige Erarbeitung der Schutzmassnahmen einen "Security by Design"-Ansatz und verhindert, dass viele Risiken mit unbequemen und wenig kontrollierbaren organisatorischen Weisungen reduziert werden müssen.

Fragen

AWK GROUP

Peter Hunziker
Dipl. El.-Ing. HTL, EMBA
Bereichsleiter

+41 58 411 96 23
peter.hunziker@awk.ch

AWK GROUP

Marcel Schönbächler
Dipl. Inform.
Senior Consultant

+41 58 411 96 84
marcel.schoenbaechler@awk.ch