Städtisches Klinikum Dresden

Krankenhausspezifische Gefährdungen

Auswahl eines Gefährdungskatalogs

Städtisches Klinikum Dresden

Im Kern geht es „nur“ um

Informations-Risikomanagement

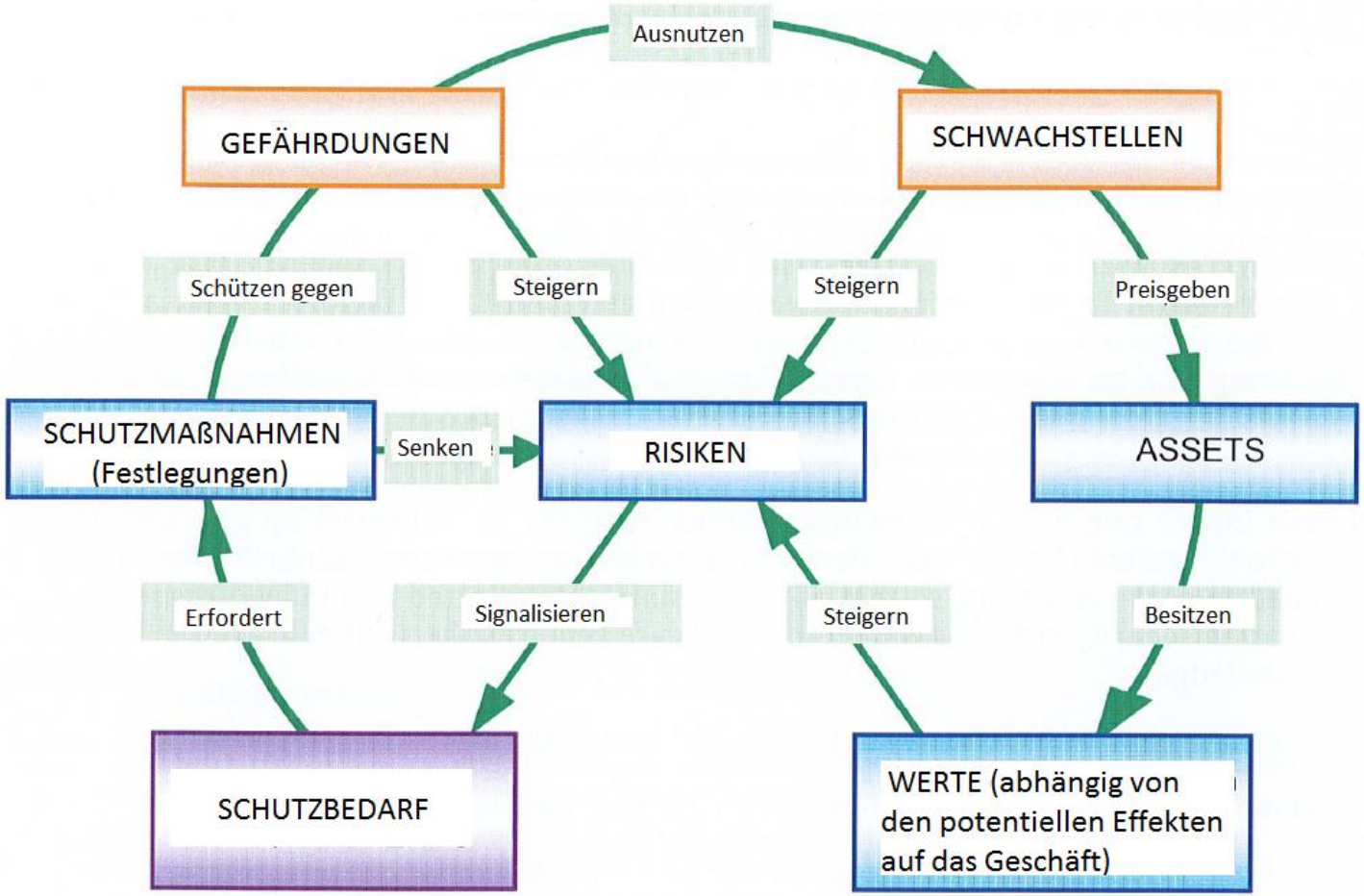

Figure B.3 — Relationship between risks and risk sources in a simplified risk model

Bekannte Gefährdungskataloge

Städtisches Klinikum Dresden

IT-Grundschutz-Kompendium 1. Edition 2018

- Nachfolger des IT-Grundschutzkatalogs
- Listet 47 elementare Gefährdungen (G0) auf
- Identisch mit BSI-Standard 200-3

ISO-Norm 27005:2011 (Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement)

- Anhang C listet 43 Beispiele typischer Bedrohungen sowie Motive für Gruppen menschlicher Angreifer
- Bedrohungen werden klassifiziert in A - absichtlich, V - versehentlich, U – Umgebungseinflüsse

ISO-Norm 27799:2016 (Medizinische Informatik - Informationsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002)

- Anhang A listet 25 Beispiele für Bedrohungen für die Sicherheit von Patienteninformationen
- zu jedem Beispiel gibt es eine kurze Erläuterung und einen Hinweis auf die Ursachen (unterlassene Maßnahmen)

Bekannte Gefährdungskataloge

Frage:

Unterscheiden sich die Kataloge?

→ Excel-Tabelle

Zu treffende Entscheidung:

Welcher Katalog soll verwendet werden?

Empfehlung:

Da es keine gravierenden Unterschiede gibt, kann man mit keinem Gefährdungskatalog viel falsch machen.

Die größte Risikoabdeckung erreicht man mit einer Kombination der Kataloge