Technische Universität Berlin

Block IV - IT Sicherheit

E-Health Grundlagen | Prof. Zarnekow | Block IV

MiG Management im Gesundheitswesen

IKM

Technische Universität Berlin

Gliederung

1. Grundlagen der IT-Sicherheit
2. IT-Sicherheitsmanagement
3. IT-Sicherheitsmaßnahmen

MiG Management im Gesundheitswesen

IKM

Begriffe und Grundkonzepte der IT-Sicherheit - Definitionen

Sicherheit

- „Sicherheit ist das Vorhandensein von Integrität, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit in einem geplanten Ausmaß.“
  (Heinrich, 2002, S. 278)

Informationssicherheit

- „Informationssicherheit ist der Schutz von Informationen vor einer Vielzahl von Bedrohungen. Sie dient der Aufrechterhaltung des Geschäftsbetriebes. Des Weiteren soll sie Geschäftsrisiken minimieren und die Rendite und die Geschäftschancen maximieren.“
  (Schlegel, 2010, Steuerung der IT im Klinikmanagement, S. 163)

Datensicherheit

- Zustand, in dem Daten sowohl inhaltlich und formal unverändert bleiben als auch geschützt vor unberechtigtem Zugriff sind.

Begriffe und Grundkonzepte der IT-Sicherheit - Vertraulichkeit

Vertraulichkeit (confidentiality) ist gegeben, wenn sicher gestellt werden kann, dass Informationen nicht durch unauthorisierte Personen, Instanzen oder Prozesse eingesehen werden können:

- Datenvertraulichkeit (Schutz persönlicher und geschäftskritischer Daten)
- Teilnehmer-Anonymität bei bestimmten Geschäftstransaktionen
- Anonymität der Nutz- und Vermittlungsdaten (Schutz vor Verkehrsanalyse)

Beispiele für Verlust der Vertraulichkeit:

- Abhören von Datenpaketen in einem Netzwerk durch Unbefugte
- Unsicheren Aufbewahrung von unverschlüsselte Backup-Medien
- Penetration und Diebstahl vertraulicher Daten aufgrund von Sicherheitslücken in einem IT-System

Begriffe und Grundkonzepte der IT-Sicherheit - Integrität

Integrität (integrity) bezieht sich auf Integrität von Daten und Systemen:

- Datenintegrität ist die Sicherstellung, dass Daten nicht in einer unauthorisierten Art und Weise verändert oder zerstört wurden.
- Systemintegrität ist die Sicherstellung, dass ein System unbeeinträchtigt mit der gewünschten Performance zur Verfügung steht und nicht durch unauthorisierten Zugang manipuliert wurde.

Beispiele für Verlust der Integrität:

a) Unzulässige Änderung der Daten durch Befugte
    - Unbeabsichtigt durch Bedienungsfehler
    - Missbräuchliche Änderung

b) Unzulässige Änderung durch andere Ursachen
    - Fehlfunktion der IT-Systeme
    - Störungen bei der Datenübertragung
    - Manipulation durch Unbefugte

Begriffe und Grundkonzepte der IT-Sicherheit - Verfügbarkeit

Verfügbarkeit (availability) ist gewährleistet, wenn die Funktionalität von Software und Hardware nicht beeinträchtigt ist:

- Funktionales Versagen (z.B. Hard - und Softwarefehler)
- Betriebskontinuität (z.B. Katastrophen, technisches Versagen, Sabotage)

Beispiele für Verlust der Verfügbarkeit:

1. Daten sind für Nutzer nicht mehr vorhanden:
    - Absichtliches Löschen der Daten durch Befugte (missbräuchliche Vorenthaltung)
    - Unabsichtliches Löschen der Daten durch Befugte
    - Technische Defekte
    - Manipulation durch Unbefugte
2. Daten sind vorhanden, aber nicht in akzeptabler Zeit verfügbar, bspw. aufgrund nicht ausreichender Verfügbarkeit des IT-Systems

Zeitpunkt der Erkennung eines Verlusts

Verlust der Verfügbarkeit			
Verlust der Integrität			
Verlust der Vertraulichkeit			
frühzeitig	bald	spät	Evtl. gar nicht

Begriffe und Grundkonzepte der IT-Sicherheit - Verbindlichkeit

Verbindlichkeit (accountability, non-repudiation) bezieht sich auf die Sicherstellung, dass die Aktionen einer Instanz (Benutzer, Prozesse, Systeme, Informationen, etc.) ausschließlich dieser Instanz zugeordnet werden können und dass die Kommunikations-beziehung bzw. der Informationsaustausch nicht geleugnet werden kann.

- Nachweisbarkeit der Urheberschaft (Ausstellerauthentizität)
- Nachweisbarkeit von Kommunikationsvorgängen (Beweissicherung, Protokollierung)
- Rechtssicherheit der Kommunikation
- Zertifizierung

Begriffe und Grundkonzepte der IT-Sicherheit - Authentizität

Authentizität (authenticity) befasst sich mit der Sicherstellung der Identität eines Subjektes.

Ein Subjekt kann in diesem Zusammenhang ein Benutzer, ein Prozess, ein System oder eine Information sein.

Authentizität ist die Voraussetzung für Verbindlichkeit.

Begriffe und Grundkonzepte der IT-Sicherheit - Betriebssicherheit

Betriebssicherheit (reliability) ist gegeben, wenn konsistente und gewünschte Funktion und Verhalten der Daten und Systeme sicher gestellt werden kann.

Betriebssicherheit ist die Voraussetzung für Integrität und Verbindlichkeit.

Datensicherheit und Datenschutz

Datensicherheit in einem Unternehmen bedeutet, dass für jedes betrachtete Informations- und Datenobjekt die Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit und Verhinderung von Missbrauch in der gewünschten Zusammenstellung und Abstufung erreicht und aufrechterhalten wird.

Unter **Datenschutz** versteht man den Schutz von personenbezogenen Daten als Teil der Privatsphäre, die sie in entsprechenden Datenschutzgesetzen (z.B. BDSG) gefordert wird.

Anforderungen des BGSG:

- Datensparsamkeit und Datenvermeidung
- Zweckbindung von Daten: Erhobene Daten dürfen nur für den beabsichtigten Zweck verwendet werden. Diese sind entweder
  - gesetzlich definiert
  - oder ihnen muss durch die betroffene Person zugestimmt werden.

Quelle: Kersten & Klett, *Der IT Security* Manager, 2015

Beispielhafte Ziele der Informationssicherheit in einem Krankenhaus

Informationssicherheit dient dem Unternehmen und darf nicht pauschal als Hindernis gesehen werden

- Unternehmenswichtige IT-Systeme sind hoch verfügbar
- Alle Systeme werden vor einem Zugriff durch Unbefugte geschützt
- Anforderungen an die ärztliche Schweigepflicht werden eingehalten
- Kosten für die Geschäftsprozesse werden optimiert
- Schadensfälle durch nicht gesicherte IT-Systeme werden unterbunden

Gliederung

2. IT-Sicherheitsmanagement

Wichtige Aspekte des Sicherheitsmanagements in der Praxis

Die **Aufgaben des Management-Prozesses** sind:

- ein akzeptables Sicherheitsniveau zu konzipieren und erstmalig zu erreichen,
- dieses solange aufrechtzuerhalten, wie die Anforderungen gleich bleiben,
- bei Änderungen der Anforderungen die Sicherheit entsprechend anzupassen,
- sie insgesamt weiterzuentwickeln bzw. zu verbessern (Verbreitung der Sicherheit, Anpassung des Sicherheitsniveaus, Awareness)

Verantwortlichkeiten werden vom Management festgelegt, durch

- klare Aufgabenbeschreibungen
- Festlegung der Schnittstellen zu anderen Verantwortlichkeiten
- Planung der erforderlichen Aktivitäten und dafür notwendige Ressourcen

Umfang

Das Sicherheitsmanagement muss Vorgaben für die Sicherheit entwickeln UND deren Einhaltung bzw. Beachtung durch interne Audits, Inspektionen, Tests etc. überwachen.

Wichtige Aspekte des Sicherheitsmanagements in der Praxis

Vorgehensmodelle

ISO 27000/27001

- Prinzipien: kontinuierliche Verbesserung (PDCA-Modell), Änderungsmanagement, Lenkung/Steuerung der Dokumentation
- Hohe Ähnlichkeit zu anderen Managementkonzepten

BSI IT-Grundschutz

- Vom BSI* entwickelte Katalogmaßnahmen für den normalen Schutzbedarf
- Bei höherem Schutzbedarf ist eine ergänzende Analyse und ggf. stärkere Maßnahmen nötig

In der Praxis findet man zwei unterschiedliche **Mentalitäten**:

– Prozess- und Managementorientiert → ISO 27000
– Maßnahmenorientiert → BSI IT-Grundschutz

*Bundesamt für Informationssicherheit

Wichtige Aspekte des Sicherheitsmanagements in der Praxis

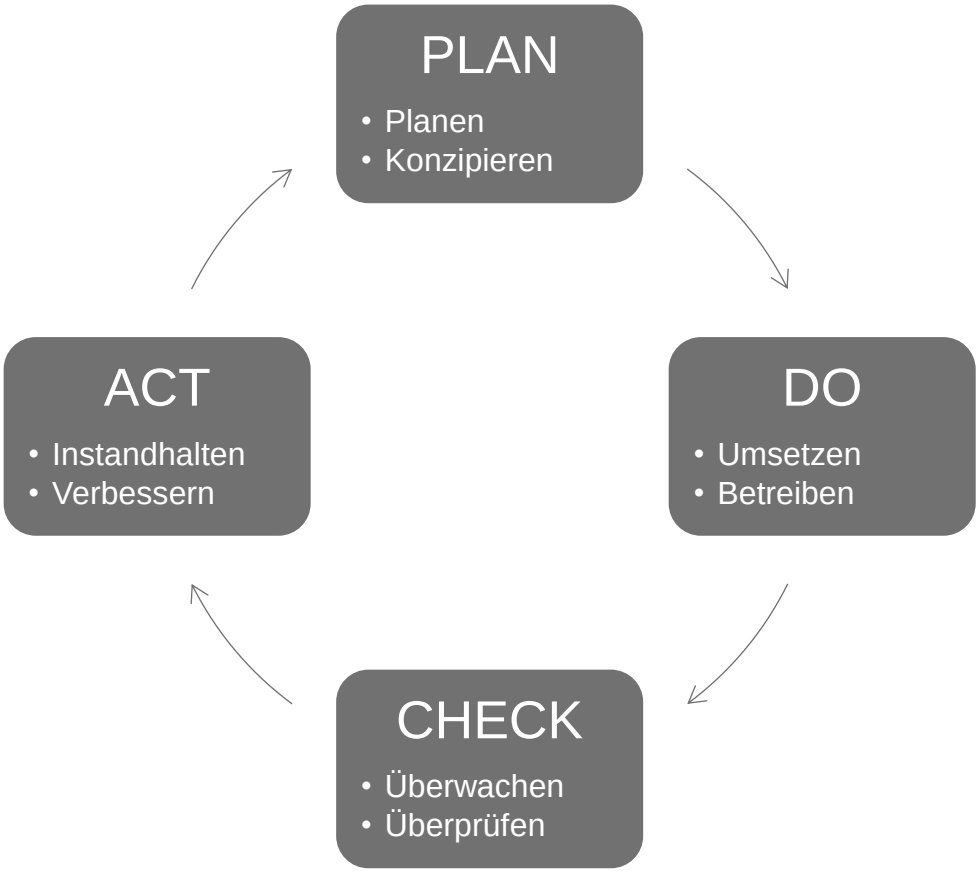
Betrachtungsebene

- Sicherheit der Informationsverarbeitung zur Unterstützung der Geschäftstätigkeit
- Betrachtungsgegenstand des Sicherheitsmanagements (primäre Geschäftsprozesse, digitale Informationen oder analoge, Sourcing/Cloud, Management-Prozesse)

Ganzheitliches Vorgehen bedeutet folgende Trends zur *selektiven* Sicherheit zu **vermeiden**:

- Insellösungen, d.h. separate Absicherung von miteinander agierenden IT-Infrastrukturen
- Thematische Isolierung, d.h. Fragen der rechtlichen, organisatorischen und personellen Sicherheit, der Infrastruktursicherheit, der Sicherheit der IT-Systeme und Netze werden oft isoliert betrachtet und in separaten „Konzepten“ behandelt
- Ausschließliche Konzentration auf die IT-*Technik*, obwohl die Informations*verarbeitung* auch ohne IT und ggf. auch außerhalb der eigenen IT stattfindet.

Kontinuierlicher Verbesserungsprozess



Kontinuierlicher Verbesserungsprozess

Mit dem PDCA-Modell:

- Plant und konzipiert man die Erreichung von Ziele (*plan*)
- Realisiert man die Planung und Konzeption (*do*)
- Überprüft man, ob die Konzepte sich in der Praxis bewähren bzw. wo es Probleme gibt (*check*)
- Leitet man aus den gewonnenen Erkenntnissen und neuen zwischenzeitlich gestellten Anforderungen notwendige Veränderungen ab (*act*)

Für die **Leitungsebene** einer Organisation besteht *plan* darin, eine Zielvorgabe für die Sicherheit zu geben; dies muss schriftlich geschehen, und zwar mit der sogenannten *Sicherheitslinie*.

Auf der Ebene des **Sicherheitsmanagements** wird mit der Zielvorgabe der Sicherheitslinie als Input die gewünschte Sicherheit konzipiert (*plan*).

Kontinuierlicher Verbesserungsprozess

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Plan		
Plan1	eigene Sensibilisierung (wenn nötig)	
Plan2	Informationen beschaffen, ggf. eigene Schulung	
Plan3	Sicherheitsleitlinie und sonstige Vorgaben der Leitungsebene identifizieren	die geänderte Sicherheitsleitlinie und sonstige Vorgaben der Leitungsebene identifizieren
Plan4	Sicherheitskonzept und Begleitdokumente erstellen (lassen)	Sicherheitskonzept und Begleitdokumente ggf. anpassen und überarbeiten (lassen)
Plan5	Abstimmung und Genehmigung des Sicherheitskonzeptes und der Begleitdokumente	Abstimmung und Genehmigung der Änderungen bzw. Neuerungen
Do		
Do1	Sicherheitskonzept (resp. Änderungen) durch zuständige Fachabteilungen umsetzen lassen	
Do2	Umsetzung überwachen	
Do3	Maßnahmen aus den Bereichen Sensibilisierung, Schulung, Training umsetzen	
Do4	Sicherheitskonzept in Kraft setzen	
Do5	Sicherheitsvorfälle managen	
Check		
Check1	Praxis der Sicherheit überprüfen	
Check2	Sicherheitsvorfälle auswerten	
Check3	sonstige Erkenntnisse einbringen	
Act		
Act1	Material analysieren, Verbesserungspotenzial feststellen	
Act2	Berichte an die Leitung	

Kontinuierlicher Verbesserungsprozess

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Plan		
Plan1	eigene Sensibilisierung (wenn nötig)	
Plan2	Informationen beschaffen, ggf. eigene Schulung	
Plan3	Sicherheitsleitlinie und sonstige Vorgaben der Leitungsebene identifizieren	die geänderte Sicherheitsleitlinie und sonstige Vorgaben der Leitungsebene identifizieren
Plan4	Sicherheitskonzept und Begleitdokumente erstellen (lassen)	Sicherheitskonzept und Begleitdokumente ggf. anpassen und überarbeiten (lassen)
Plan5	Abstimmung und Genehmigung des Sicherheitskonzeptes und der Begleitdokumente	Abstimmung und Genehmigung der Änderungen bzw. Neuerungen

Kontinuierlicher Verbesserungsprozess

Phase	Erst-Aktivitäten	Folge-Aktivitäten
Do		
Do1	Sicherheitskonzept (resp. Änderungen) durch zuständige Fachabteilungen umsetzen lassen	
Do2	Umsetzung überwachen	
Do3	Maßnahmen aus den Bereichen Sensibilisierung, Schulung, Training umsetzen	
Do4	Sicherheitskonzept in Kraft setzen	
Do5	Sicherheitsvorfälle managen	
Check		
Check1	Praxis der Sicherheit überprüfen	
Check2	Sicherheitsvorfälle auswerten	
Check3	sonstige Erkenntnisse einbringen	
Act		
Act1	Material analysieren, Verbesserungspotenzial feststellen	
Act2	Berichte an die Leitung	

Sicherheitspolitik

Beinhaltet **Grundsatzentscheidungen** basierend auf der Unternehmenspolitik

Legt die **Rahmenbedingungen** für die Gewährleistung der **Informationssicherheit** und der damit verbundenen Informationsverarbeitungsprozesse fest

- Was erreicht werden soll und warum

Stellt eine Menge von **Regeln** dar, die festlegen

- Gegen welche Bedrohungen das System geschützt werden soll
- Wie das Systemmodell aussieht (Subjekte, Objekte, Aktionen, Umfeld)
- Welche Grundsätze und Regeln die Sicherheit betreffend in diesem Modell gelten
- Welche Schutzwürdigkeit die Modellelemente besitzen
- Welches Restrisiko der Systemeigner akzeptieren kann

Definiert **organisatorische_Elemente**

- Wer die Erreichung der Ziele vertreten soll

Quelle: Brenner

Sicherheitsanalyse nach IT-Grundschutz

Schutzbedarf: Ausgangspunkt des IT-Grundschutzes

Schutzbedarf	Schadensauswirkung
normal	Geringfügig/tolerabel
hoch	Beträchtlich
sehr hoch	Existenziell bedrohlich

Der Schutzbedarf bei dem *gleichen* Objekt kann je nach Sicherheitsziel (**Grundwert**) unterschiedlich sein.

Nach der Grundschutzmethode ordnet man zunächst den Anwendungen (über die IT abgewickelte Geschäftsprozesse) nach subjektiver Einschätzung einen Schutzbedarf zu. Danach gilt das **Vererbungsprinzip**:

- IT-Systeme, die für die Anwendungen benötigt werden, erben deren Schutzbedarf
- Räume, in denen diese IT-Systeme aufgestellt werden, erben den Schutzbedarf der IT-Systeme

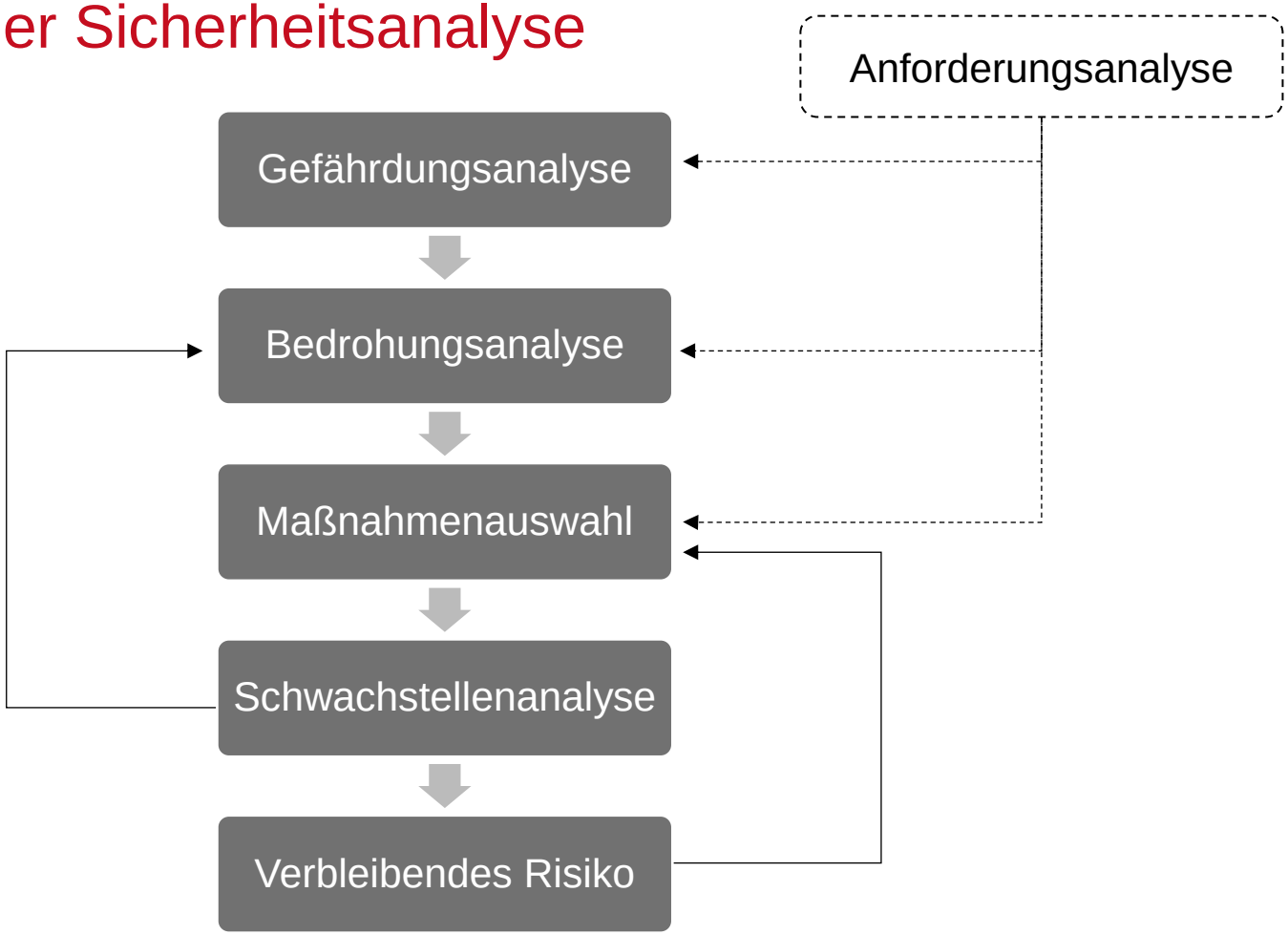
Sicherheitsanalyse nach IT-Grundschutz

Maximumsprinzip: Wenn mehrere Anwendungen auf dem gleichen IT-System laufen, bestimmt der höchst vorkommende Schutzbedarf den Schutzbedarf des IT-Systems.

Wenn der resultierende Schutzbedarf mehrerer Anwendungen auf einem IT-System höher ist als der sich aus dem Maximumsprinzip ergebende, liegt ein **Kumulationseffekt** vor. (Bsp: viele Anwendungen mit hohen Schutzbedarf auf einem IT-System führt dazu, dass das System einen sehr hohen Schutzbedarf hat)

Umgekehrt kann sich ein **Verteilungseffekt** ergeben, wenn ein *geringerer* Schutzbedarf angesetzt wird als laut Vererbungsprinzip .

Prozess der Sicherheitsanalyse



IT-Risiko-Management - Definitionen, Grundlagen

Risiko ist ein unsicheres Ereignis mit negativen Auswirkungen

Grundgleichung:

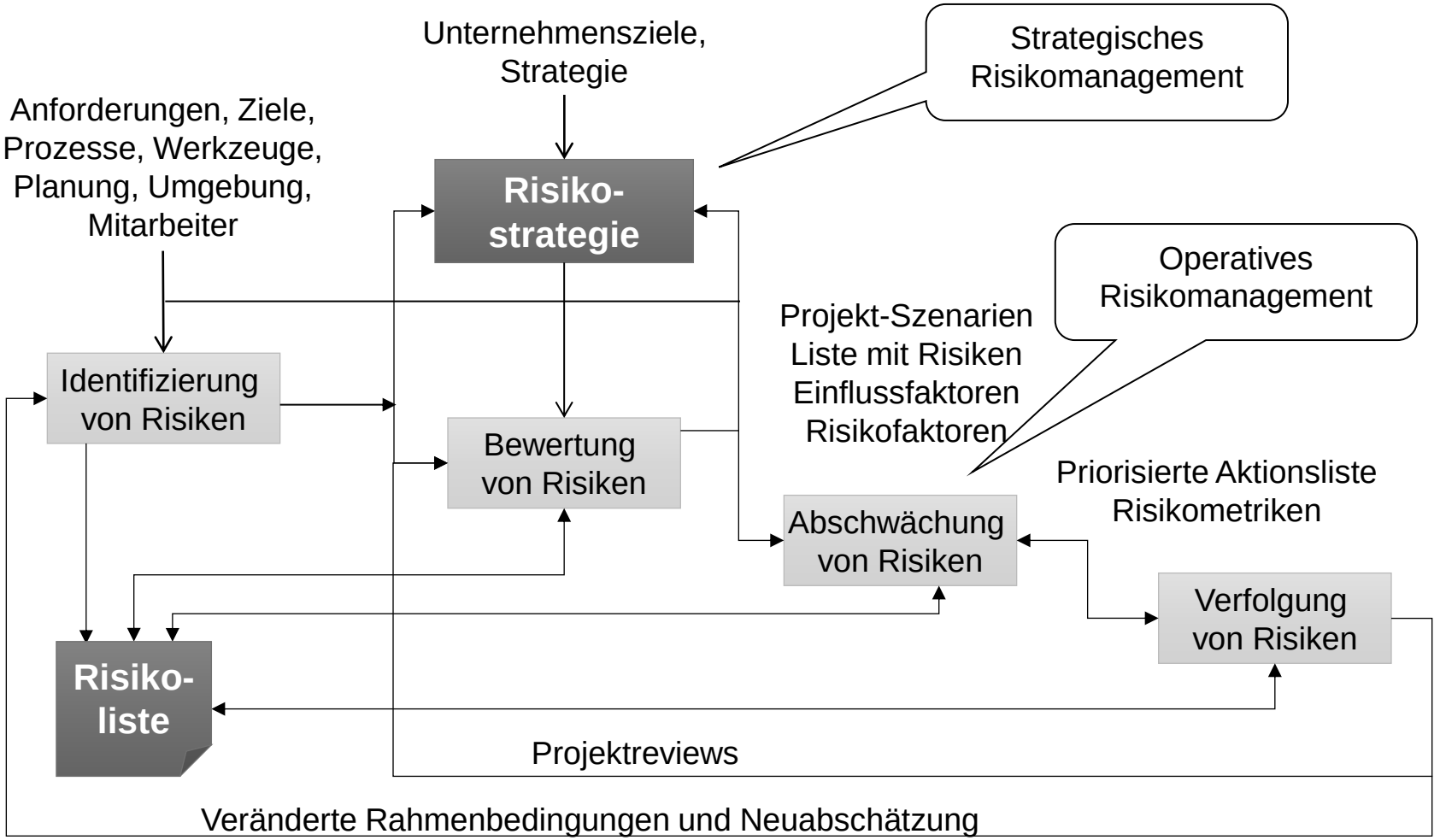
Risiko = Eintrittswahrscheinlichkeit x Auswirkungen

Ziele des Risikomanagements:

- Identifizieren potenzieller Probleme
- Planen von Maßnahmen zur Behandlung dieser Risiken
- Maßnahmenumsetzung durch den gesamten Lebenszyklus des Projekts oder Produkts, damit die Risiken nicht zum Problem werden und damit die Projektziele gefährden.

Quelle: Ebert 2006: Risikomanagement kompakt

IT-Risiko-Management - Prozess des Risikomanagements



Quelle: Ebert 2006: Risikomanagement kompakt

IT-Risiko-Management - Arten von Risiken

Operative Risiken

- Tägliche Unsicherheiten innerhalb des Projekts, die kurzfristig beherrscht werden müssen, um das Projekt erfolgreich abzuschließen
- Haben einen Einfluss auf Zeitrahmen, Kosten, Inhalte, Qualität oder Funktionalität

Technische Risiken	z.B. Einsatz neuer Technologien, die noch nicht beherrscht werden; Lieferanten liefern zu spät oder in unzureichender Qualität
Implementierungsrisiken	z.B. gewählte Architektur und Design erweisen sich im Projekt als unzureichend, um alle Anforderungen zu erfüllen; Anforderungen ändern sich ständig; die Qualität der Lösung ist zu schlecht
Wirtschaftliche Risiken	z.B. Budgetengpässe oder -überschreitungen; geplante Ressourcen stehen nicht zur Verfügung
Industrielle Risiken	z.B. Lieferanten sind nicht mehr lieferfähig oder ändern die Preise unerwartet; Kunden wollen unerwartet andere Standards und Funktionen
Geschäftsrisiken	z.B. Kunden entscheiden sich gegen das Produkt; Wettbewerber treten unerwartet mit einem anderen, besseren Produkt auf; Kritisches Know-how wandert unerwartet ab

Strategische Risiken

- Langfristige Einwirkungen auf das Unternehmen, die heute behoben werden müssen, um nicht zu einer unternehmensweiten Gefahr zu werden

Quelle: Ebert 2006: Risikomanagement kompakt

IT-Risiko-Management - Bewertung von Risiken

Eintrittswahrscheinlichkeit:

Stufe	Wert	→	Kriterien
5	Fast sicher	→	alles deutet darauf hin, dass dies zum Problem wird
4	Häufig	→	große Wahrscheinlichkeit, dass dies zum Problem wird
3	Gelegentlich	→	gleichverteilte Chance, dass dies eintritt
2	Selten	→	manchmal wird dies zum Problem
1	Fast unmöglich	→	sehr unwahrscheinlich, dass dies jemals eintritt

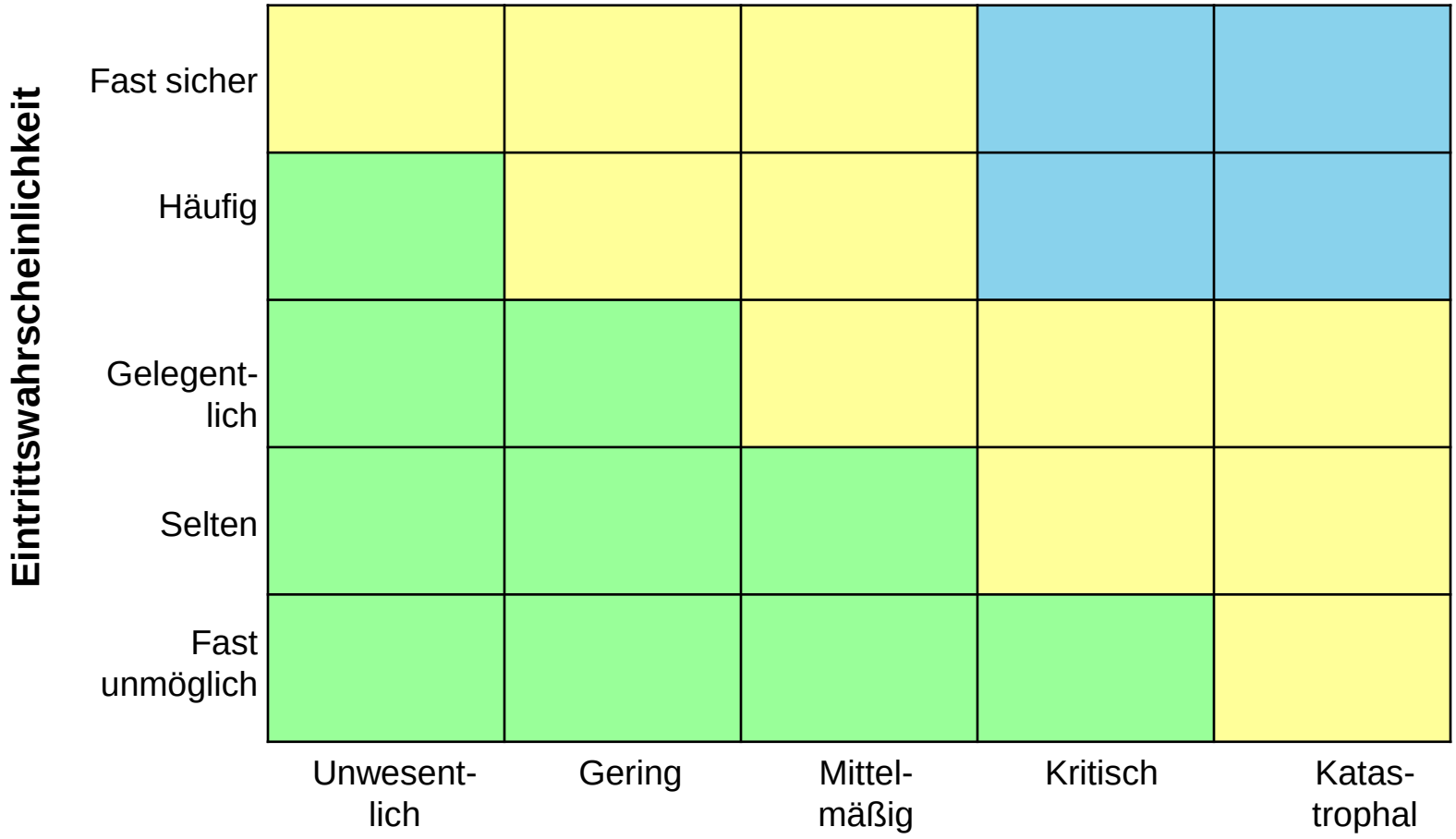
Auswirkung:

Stufe	Wert	Technische Kriterien	Kostenkriterien *	Zeitrahmen-Kriterien
5	Katastrophal	keine Kontrolle möglich	> 50 M€	Abbruch
4	Kritisch	gravierende Mängel, Schäden	10-50 M€	Einfluss auf Folgeprojekt
3	Mittelmäßig	beträchtliche Abweichungen	1-10M€	Beträchtlich; Umplanung
2	Gering	Performanzeinflüsse	0,1-1 M€	> 1 Monat Verzögerung
1	Unwesentlich	unbedeutend	unbedeutend	unbedeutend

* Unternehmensspezifisch angepasst

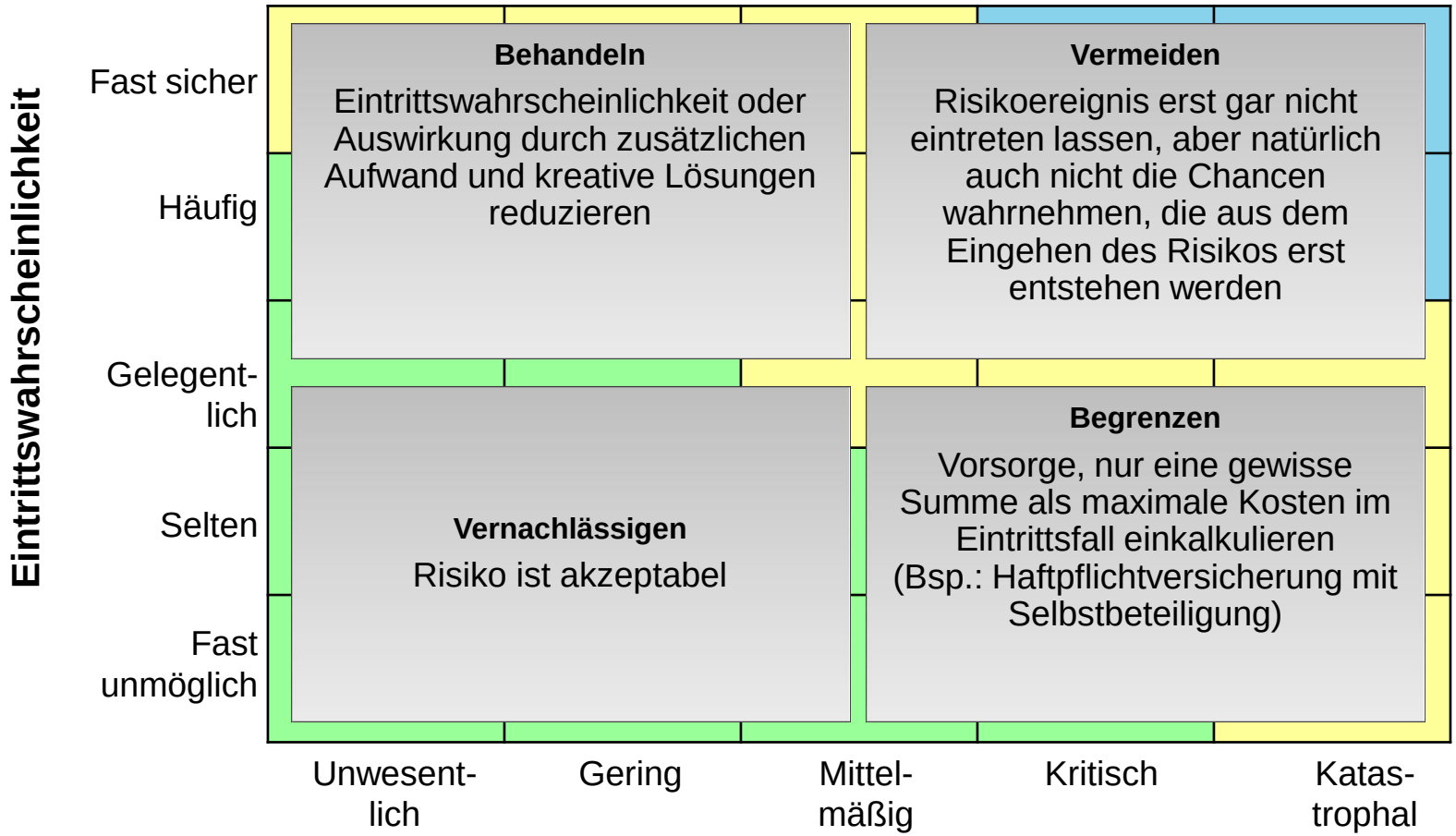
Quelle: Ebert 2006: Risikomanagement kompakt

IT-Risiko-Management - Klassifizierung von Risiken



Quelle: Ebert 2006: Risikomanagement kompakt

IT-Risiko-Management - Maßnahmen zur Abschwächung von Risiken



Quelle: Ebert 2006: Risikomanagement kompakt

IT-Risiko-Management - Beispiel: Template zur Risikoverfolgung

Als das Risiko identifiziert wurde

Nach der Abschwächung

Nach der neusten Analyse

Projekt	**Network-Loader 2005 v3**				Startdatum	01. Jan 04		**Risiko = Wahrscheinlichkeit x Auswirkung**					
Projektmanager	Paula Paul				Übergabe	31. Jul 04							
Datum	01. Mrz 04				Phase	Design							

					Ursprüngl.			mit Abschwächung			Heute							
Identifikationsnummer	Rang (Priorität)	Beschreibung	Verantwortlich	Identifikationsdatum	Wahrscheinlichkeit	Auswirkung	Risiko	Wahrscheinlichkeit	Auswirkung	Risiko	Wahrscheinlichkeit	Auswirkung	Risiko	Status	Einfluss – Kosten	Einfluss – Termin	Aktionen	Triggerpunkt	Kommentare
1	1	IP-Stack Nicht verfügbar	Müller	01. Feb 04	3	4	12	1	4	4	1	4	4	Behandelt		3 Mon	Ersatz-anbieter identifiziert	01. Apr 04	
2																			
3																			

- identifiziert
- Offen
- Obsolet
- Behandelt
- Eingetreten

Eintritts-Wahrscheinlichkeit
Nur wenige Stufen werden unterschieden

Auswirkung auf Kosten, Planung, Funktionalität, Qualität. Nur wenige Stufen werden unterschieden

Quelle: Ebert (2006)

Sicherheitsleitlinie

Notwendige Inhalte:

- Festlegung der Verantwortlichkeiten
- Bekenntnis des Managements zur Informationssicherheit
- Stellenwert der Informationsverarbeitung
- Definition der Sicherheitsziele
- Festlegung des Geltungsbereichs
- Definition des Informationssicherheitsmanagements
- Erläuterung der geltenden Prinzipien und Standards
- Hinweis auf mitgeltende und weiterführende Unterlagen

Bereiche der IT-Sicherheit:

- Physikalische Sicherheit (z.B. Redundanzen)
- Logische Sicherheit (z.B. Verschlüsselung, Datensicherung)
- Administrative Sicherheit (z.B. Berechtigungskonzept)
- Organisatorische Sicherheit (z.B. Aufklärung der Anwender)

Quelle: H. Schlegel, *Steuerung der IT im Klinikmanagement*, 2010

Inhalte der Sicherheitsleitlinie

1. Unternehmen
2. Anwendungsbereich

3a. Vorgaben

3b. Gefährdungslage

3c. Ziele

4. Bedeutung der Sicherheit
5. Grundsätzliche Regelungen
6. Erklärungen

Quelle: Kersten & Klett, *Der IT Security* Manager, 2015

Beispielhafte Sicherheitsleitlinien im Krankenhaus

- Physikalische Sicherheit
  - Redundante Server
  - Redundante Rechenzentren (Ausweichrechenzentrum)
  - Redundante Stromversorgung
  - Redundante Netzwerkanbindungen für unternehmenskritische Anwendungen
  - Zutrittssicherung zu Rechenzentren und Netzwerk-Verteilerräumen
  - Klimatisierung der Technikräume
  - Schutz der Technikräume vor Naturkatastrophen
- Logische Sicherheit
  - Verschlüsselung von mobilen Datenträgern (Festplatten von Laptops,
  - USB-Festplatten, USB-Speichersticks, Memory-Cards, CDs, DVDs),
  - wenn dort sensitive Daten (z.B. Patientendaten) gespeichert sind
  - Verschlüsselung von WAN-Verbindungen zu entfernten Unternehmensteilen
  - Verschlüsselung von Telemedizin-Verbindungen
  - Verschlüsselung von Fernwartungsverbindungen
  - Verschlüsselung von Kommunikationsdaten von bzw. zu Einweiserportalen
  - Verschlüsselung von Wireless-LAN-Verbindungen
  - Verschlüsselung von Videokonferenzen nach Extern (z.B. Second Opinion)
  - Verschlüsselung von sensiblen Voll'-Telefongesprächen

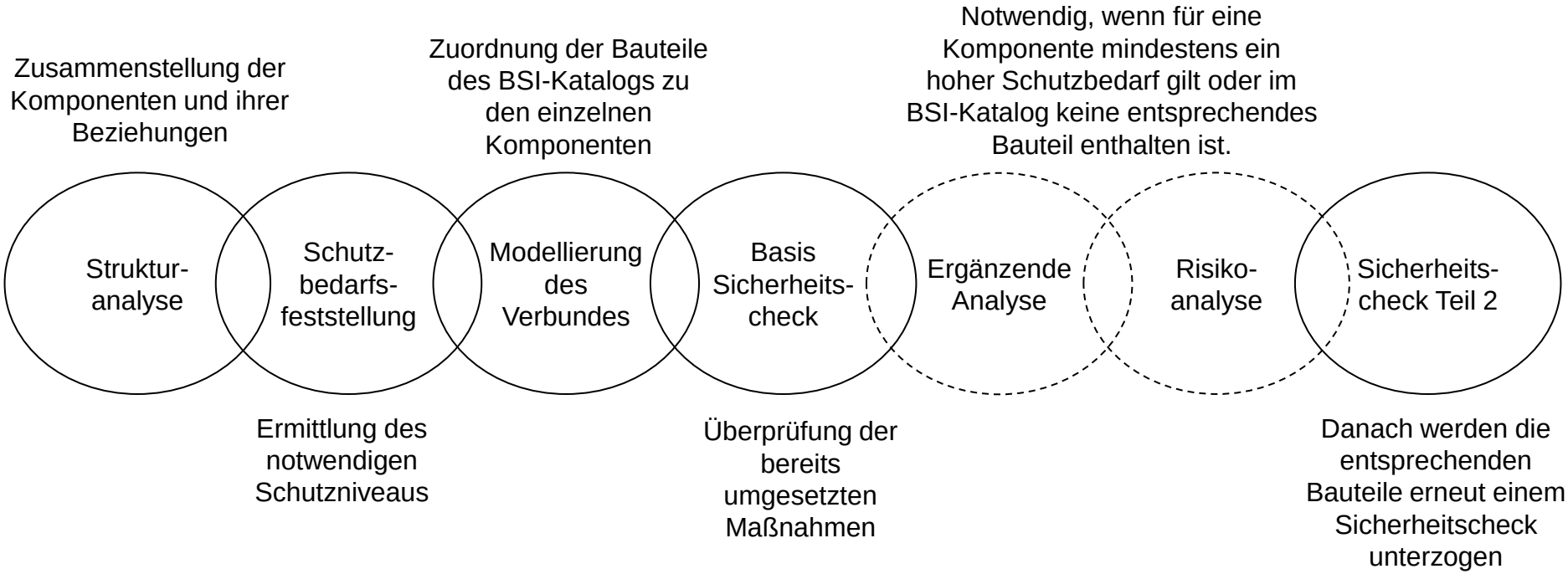
Beispielhafte Sicherheitsleitlinien im Krankenhaus

- Der wichtigste Bestandteil der **administrativen Sicherheit** ist das Berechtigungskonzept. Es legt fest, welcher Nutzer auf welche Datenbestände mit welchen Rechten zugreifen kann.

- Zur **organisatorischen Sicherheit** gehört die Erstellung einer Sicherheitsleitlinie für das Unternehmen, die von der Geschäftsleitung eingeführt und überwacht wird. Dazu müssen zunächst die wesentlichen Prozesse des Krankenhauses definiert werden. Anschließend werden die Auswirkungen für den Fall bewertet werden, dass die Prozesse nicht funktionieren sollten.

- Die **Notfallvorsorge** umfasst Maßnahmen, die auf die Wiederherstellung der Regel-Betriebsfähigkeit nach dem Ausfall eines IT-Systems zielen oder diesen im Vorfeld verhindern sollen. So werden für denkbare Störfälle im IT-Bereich vorher Handlungsanweisungen festgelegt und technische Lösungen wie eine redundante Stromversorgung installiert. Schon bei Eintritt einer Störung, die sich zu einem Notfall entwickeln könnte, sind die erforderlichen Maßnahmen zu ergreifen, die genau dies verhindern.

Sicherheitskonzept nach IT-Grundschutz



Quelle: H. Schlegel, *Steuerung der IT im Klinikmanagement*, 2010

Gliederung

3. Sicherheitsmaßnahmen

Klassen von Sicherheitsmaßnahmen

- **Vertragliche Regelungen** können in
  - Arbeitsverträgen,
  - Verpflichtungserklärungen,
  - Outsourcing-Verträgen
  - oder in Verträgen mit Kunden und Lieferanten enthalten sein.

- **Organisatorischen Regelungen**
  - die Festlegung von Rollen und Verantwortlichkeiten
  - Verhaltensregeln
  - Arbeitsanweisungen und Verfahrensbeschreibungen
  - Besucherregelungen
  - Regeln betreffend die private Nutzung von IT-Systemen des Unternehmens oder die Verwendung privater Geräte für dienstliche Zwecke
  - Verbot der Nutzung privater Software im Unternehmen
  - Passwortregeln

Klassen von Sicherheitsmaßnahmen

- **Personelle Maßnahmen**
  - Anforderungen an die Ausbildung, Projekt- und Berufserfahrung
  - Sensibilisierung, Schulung und Training des Personals

- **Infrastruktur-Maßnahmen** schützen die Sicherheitszonen durch
  - Überwachungseinrichtungen wie Zutrittskontrollen, alarmgesicherte Türen und Fenster
  - Geschützte Verlegung von Versorgungsleitungen und Datenkabeln
  - Maßnahmen gegen Elementarereignisse (z.B. Brandschutz)
  - Akustische und elektromagnetische Abschirmung

- **Technische Maßnahmen**
  - Zugriffskontrolle in einem Betriebssystem
  - Verschlüsselung von E-Mails
  - Sichere Schlüsselspeicherung in einer Krypobox
  - Kameraüberwachung von Sicherheitszonen
  - Abschirmung eines Rechners im Sinner von Abstrahlschutz

Infrastruktur-Maßnahmen

Zugangskontrolle

- physischer Zugang nur für berechtigte Personen (z.B. durch Schlüssel, Magnetkarte, biometrische Merkmale)

Feuer- & Wasserschutz

Allgemeine Katastrophenplanung

Ausweichlösungen

Redundante Datenhaltung

geografische Verteilung des Systems

Evakuierungspläne

Unterbrechungsfreie Stromversorgung

Überspannungsschutz

Technische Maßnahmen

Zugriffskontrolle

- Passwort, Schutzklassen, Zuständigkeiten
- Digitale Zertifikate

Verschlüsselung (Kryptographie) und digitale Signaturen

- Symmetrische Private-Key-Verfahren (z.B. DES)
- Asymmetrische Public-Key-Verfahren (z.B. RSA)

Systematische Durchführung von Datensicherungen

- Backup

Integritätssicherung (z.B. durch Checksummen)

Verkehrserzeugung (Fülldaten zur Verhinderung von Verkehrsflussanalysen)

Fire Walls und Routingkontrolle

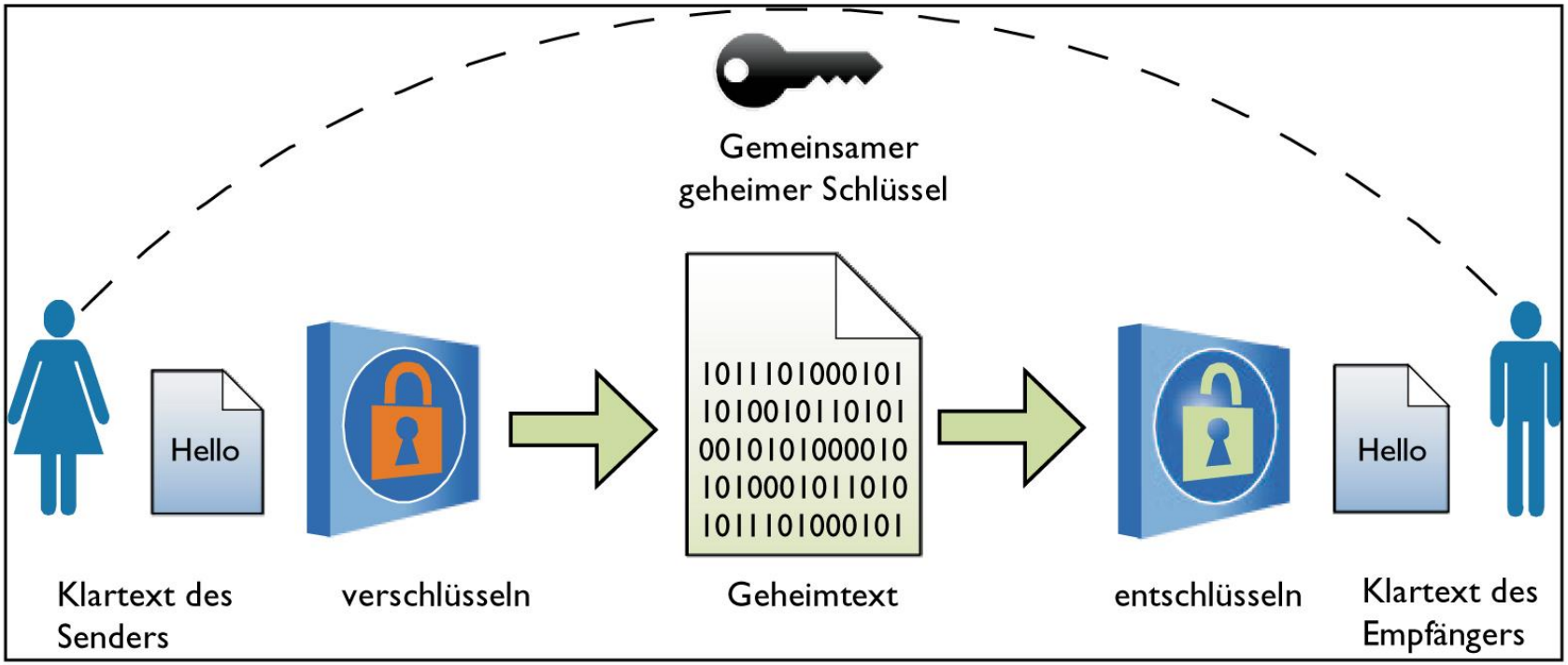
- Intrusion Detection Systems (Analyse des Datenverkehrs)

Notarisierung (Dienste im Rahmen eines Trust Center)

Virenschutzprogramme

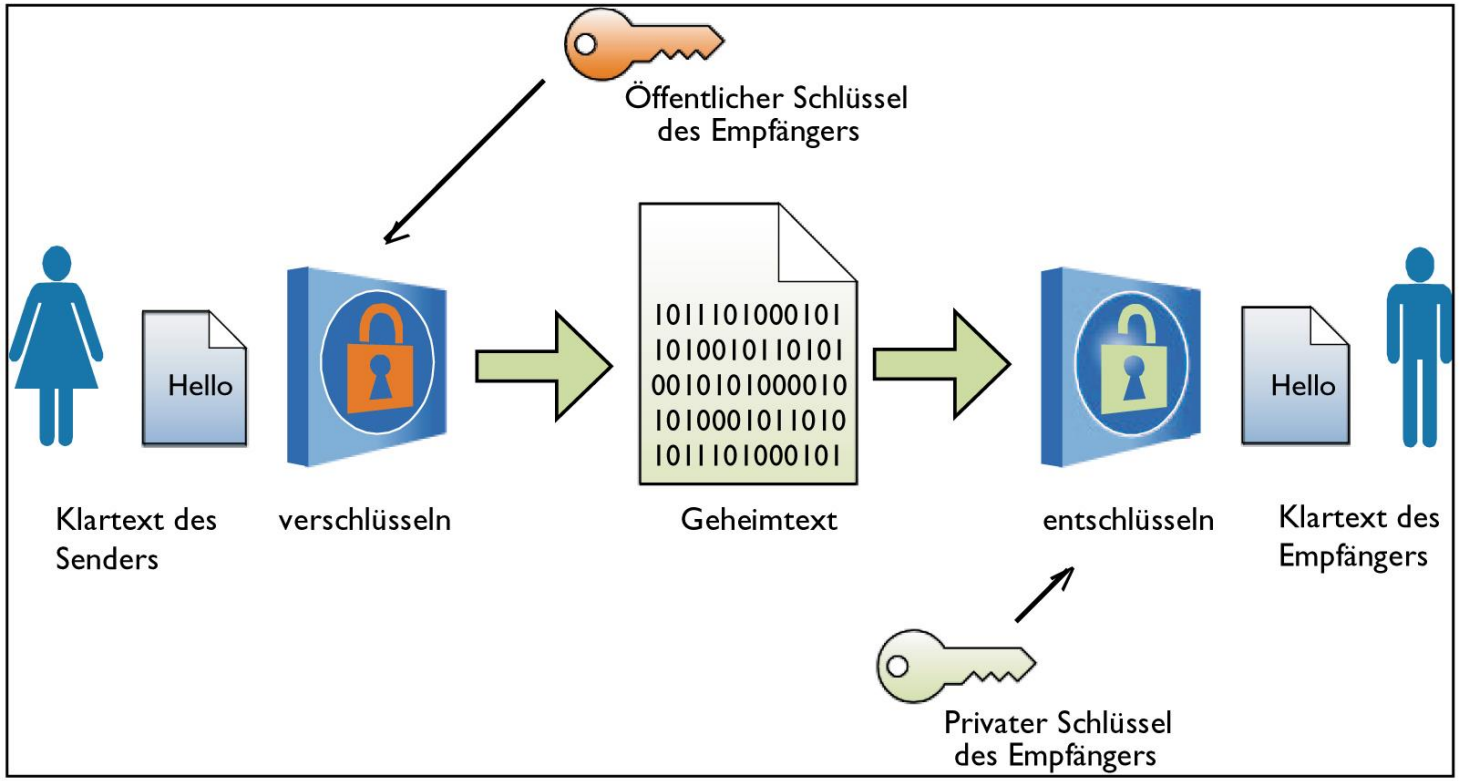
Ausgewählte Aspekte des Sicherheitsmanagements

Symmetrische Private-Key-Verfahren



Ausgewählte Aspekte des Sicherheitsmanagements

Asymmetrische Private-Key-Verfahren



Hybrid-Verfahren

1. Verwendung der asymmetrischen Schlüsselpaare, um die Schlüssel für das symmetrische Verfahren sicher zu übertragen
2. Symmetrische Verschlüsselung der Daten

- Kombiniert die hohe Geschwindigkeit symmetrischer Verfahren mit der einfachen Schlüsselverteilung asymmetrischer Verfahren

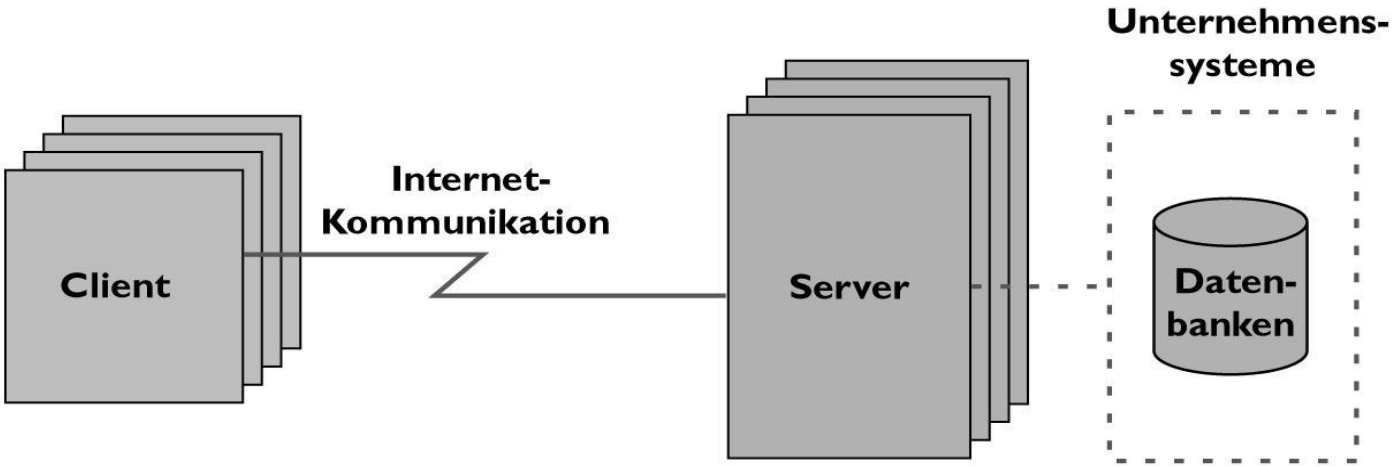
- **Man-in-the-Middle-Angriff**: ein Angreifer schaltet sich unbemerkt zwischen die beiden Kommunikationspartner, wobei er vortäuscht der jeweilige Gegenüber zu sein.
  Lösung: elektronische Zertifikate, um sich gegenseitig zu authentifizieren.

- Das **SSL-Protokoll** nutzt das Hybrid-Verfahren in Verbindung mit Zertifikaten und ist ein sicheres Protokoll für Internet-Anwendungen.

- **PGP** (Pretty Good Privacy) ist ein asymmetrisches Kryptographieverfahren.

Technische Universität Berlin

Sicherheit im Internet



- Computerviren
- Abgehörte Leitungen
- Verlust einer Maschine

- Abhören
- Sniffing
- Abänderung von Nachrichten
- Diebstahl und Betrug

- Hacking
- Computerviren
- Diebstahl und Betrug
- Abhören von Leitungen
- Vandalismus
- DoS-Angriffe

- Diebstahl von Daten
- Kopieren von Daten
- Änderung von Daten

MiG Management im Gesundheitswesen

IKM