

IT-Sicherheit

- Sicherheit vernetzter Systeme -

Kapitel 2: Grundlagen



Kapitel 2: Inhalt

1. Überblick über die OSI-Sicherheitsarchitektur
2. ISO/OSI Referenzmodell
3. Grundlegende Begriffe und Vorgehensweisen
4. Relevante Standards
 - OSI Sicherheitsarchitektur
 - Sicherheitsdienste
 - Sicherheitsmechanismen
 - ISO/IEC 27000
5. Unterscheidung Security vs. Safety

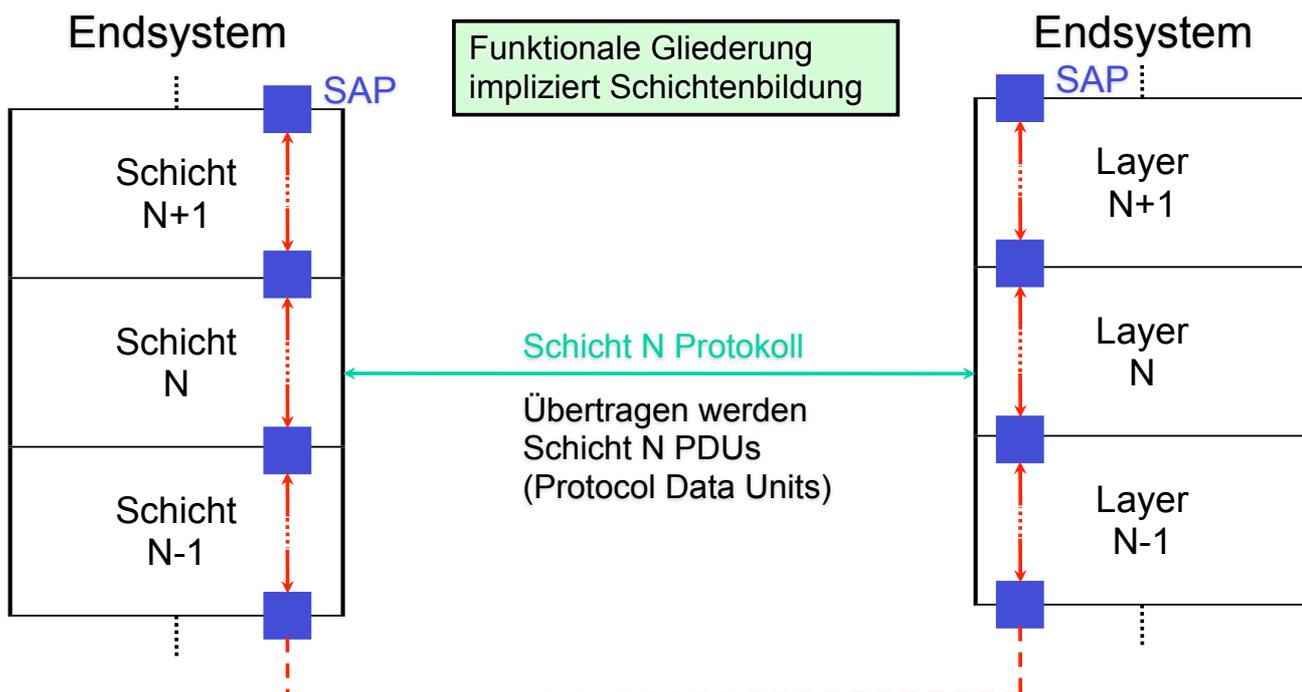


OSI Security Architecture: Überblick

- Standardisiert von der International Standardization Organization (ISO) 1988 und der International Telecommunication Union (ITU) 1991
- Dokumente:
 - ISO: ISO-7498-2; ISO-10181-1 bis -7 (Security Framework); ISO-11586-1 bis -6 (Upper Layer Security)
 - ITU: ITU-T X.800 – X.830
- Fokus liegt auf verteilten / vernetzten Systemen
- Beschreibung von Sicherheitsdiensten (Security Services), Sicherheitsmechanismen,.....
- Baut auf dem Open System Interconnection Reference Model (ISO/OSI-RM) auf



Prinzip des OSI-Referenzmodell



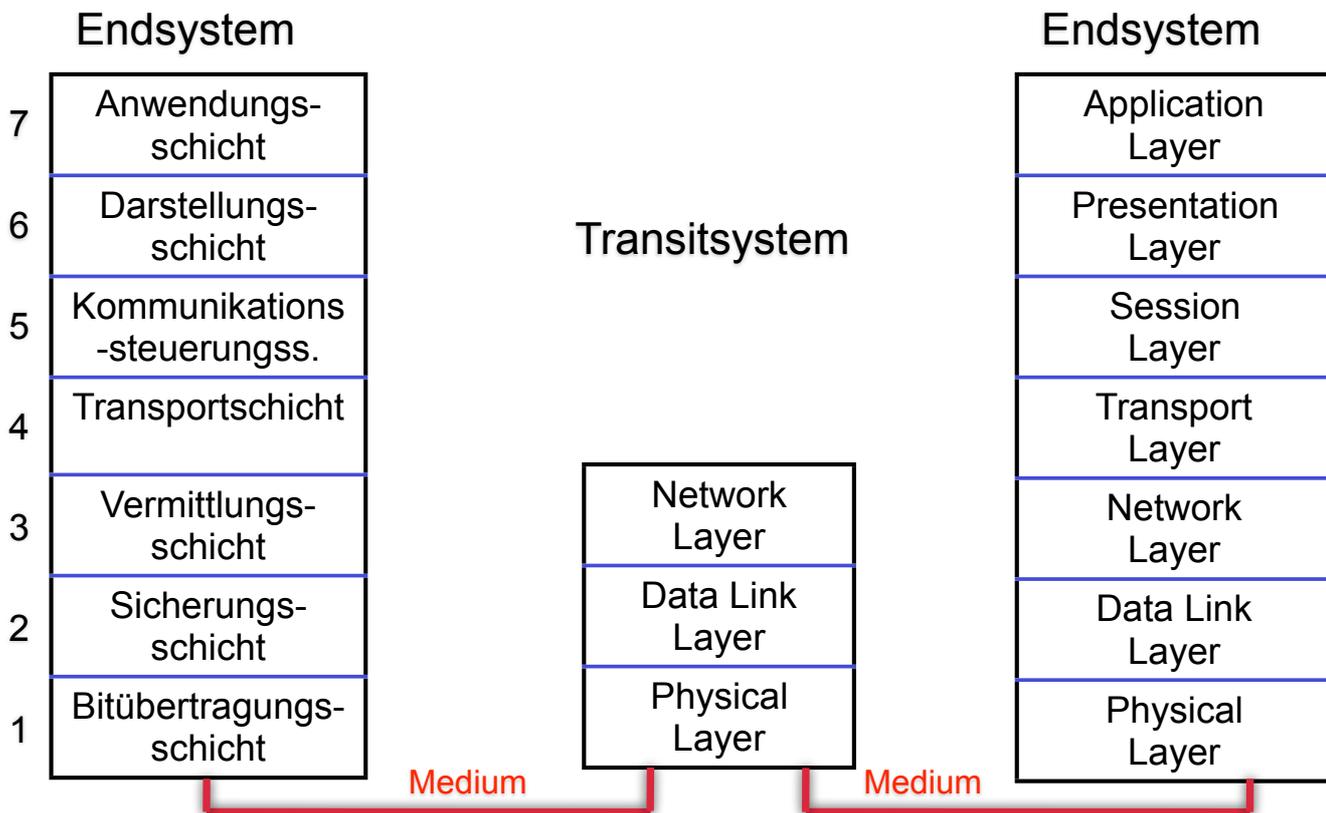
SAP = Service Access Point
(Dienstzugangsschnittstelle)

Logischer Datenfluss

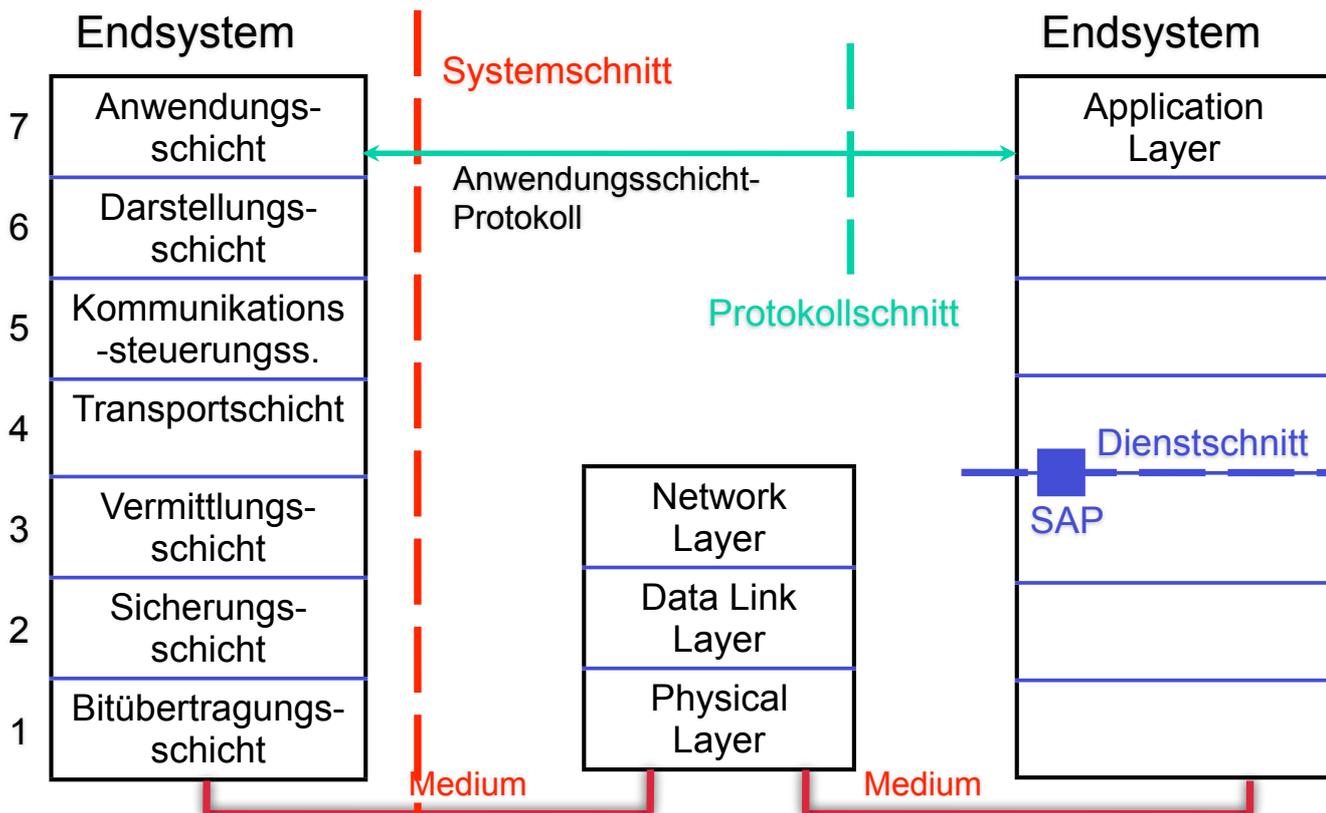
Physischer Datenfluss



OSI Referenzmodell: Schichten



OSI Referenzmodell: Schnittbildung



Kapitel 2: Inhalt

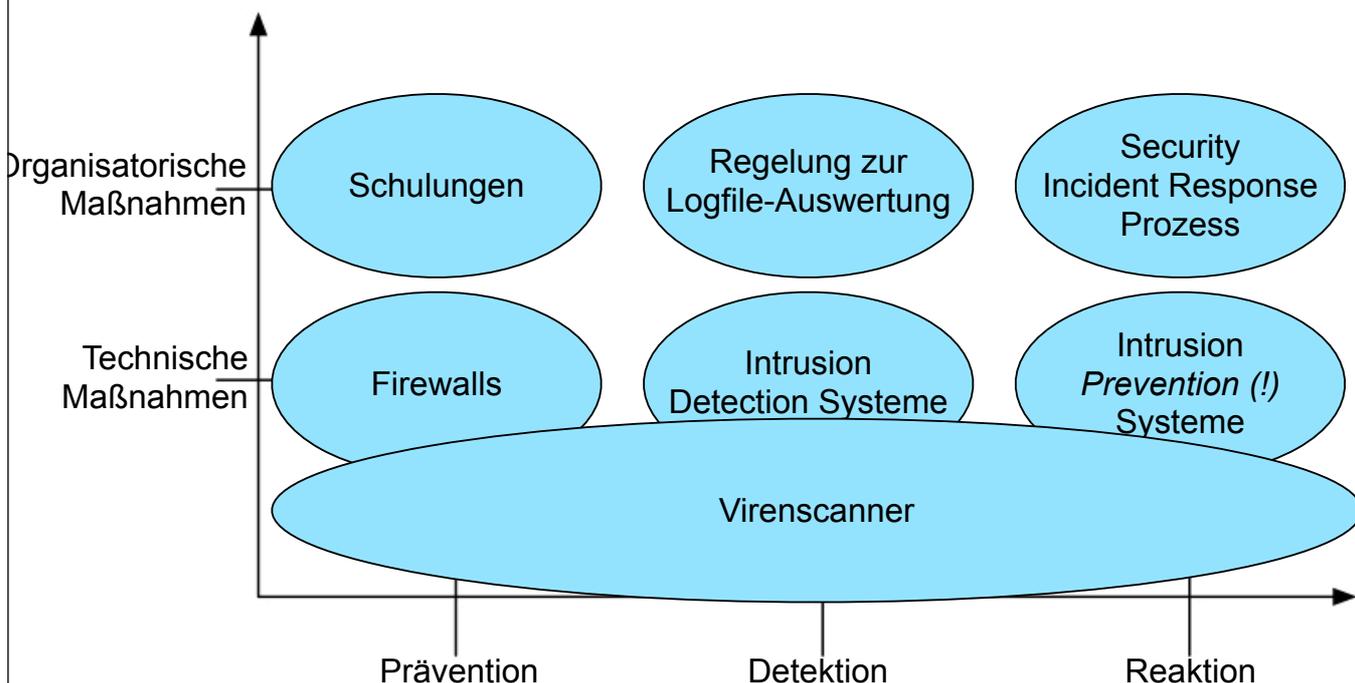
1. Überblick über die OSI-Sicherheitsarchitektur
2. ISO/OSI Referenzmodell

3. Grundlegende Begriffe und Vorgehensweisen

4. Relevante Standards
 - OSI Sicherheitsarchitektur
 - Sicherheitsdienste
 - Sicherheitsmechanismen
 - ISO/IEC 27000
5. Unterscheidung Security vs. Safety



Kategorisierung von Sicherheitsmaßnahmen



Risikogetriebenes Vorgehensmodell

■ Kernfragestellungen:

- Welche Sicherheitsmaßnahmen sollen wann und in welcher Reihenfolge ergriffen werden?
- Lohnen sich die damit verbundenen Kosten?

■ Voraussetzungen:

- Analyse des Schutzbedarfs
- Überlegungen zu möglichen Angriffen und deren Auswirkungen
- Evaluation in Frage kommender Lösungswege
- Quantitative (d.h. nicht nur qualitative) Bewertung von Lösungswegen



Ziele der Informationssicherheit

■ Hauptproblem:

Informationssicherheit (IS) kann nicht gemessen werden

- Es gibt keine Maßeinheit für IS
- Sicherheitskennzahlen (security metrics) sind bislang szenarienspezifisch und quantifizieren nur Teilaspekte

■ Lösungsansatz: Indirekte Definition von IS durch Teilziele

Vertraulichkeit	Confidentiality
Integrität	Integrity
Verfügbarkeit	Availability

Akronym **CIA** häufig in englischer IS-Literatur



1. Teilziel: Vertraulichkeit

■ Definition:

Vertraulichkeit (engl. confidentiality) ist gewährleistet, wenn geschützte Daten nur von Berechtigten abgerufen werden können.

■ In vernetzten Systemen zu betrachten bezüglich:

- Transport von Daten (über Rechnernetze)
- Speicherung von Daten (inkl. Backup)
- Verarbeitung von Daten

■ Typische Sicherheitsmaßnahme: Verschlüsselung

■ Teilziel gilt als verletzt, wenn geschützte Daten von unautorisierten Subjekten eingesehen werden können.



2. Teilziel: Integrität

■ Definition:

Integrität (engl. integrity) ist gewährleistet, wenn geschützte Daten nicht unautorisiert und unbemerkt modifiziert werden können.

■ Wiederum bei Transport, Speicherung und Verarbeitung sicherzustellen!

■ Typische Sicherheitsmaßnahme: Kryptographische Prüfsummen

■ Teilziel verletzt, wenn Daten von unautorisierten Subjekten unbemerkt verändert werden.



3. Teilziel: Verfügbarkeit

■ Definition:

Verfügbarkeit (engl. availability) ist gewährleistet, wenn autorisierte Subjekte störungsfrei ihre Berechtigungen wahrnehmen können.

- Bezieht sich nicht nur auf Daten, sondern z.B. auch auf Dienste und ganze IT-Infrastrukturen.
- Typische Sicherheitsmaßnahme: Redundanz, Overprovisioning
- Teilziel verletzt, wenn ein Angreifer die Dienst- und Datennutzung durch legitime Anwender einschränkt.

IS-Teilziele im Kontext des Angriffslebenszyklus

- Die Kombination aller in einem Szenario eingesetzten **präventiven** Maßnahmen dient der Erhaltung von *Vertraulichkeit, Integrität und Verfügbarkeit*.
- **Detektierende** Maßnahmen dienen dem Erkennen von Sicherheitsvorfällen, bei denen die präventiven Maßnahmen unzureichend waren.
- **Reaktive** Maßnahmen dienen der Wiederherstellung des Soll-Zustands nach dem Erkennen von Sicherheitsvorfällen.

Kapitel 2: Inhalt

1. Überblick über die OSI-Sicherheitsarchitektur
2. ISO/OSI Referenzmodell
3. Grundlegende Begriffe und Vorgehensweisen

4. Relevante Standards

- OSI Sicherheitsarchitektur
 - Sicherheitsdienste
 - Sicherheitsmechanismen
- ISO/IEC 27000

Fokussiert technische Maßnahmen

Fokussiert organisatorische Maßnahmen

5. Unterscheidung Security vs. Safety



OSI Security Architecture: Überblick

- Beschreibung von Sicherheitsdiensten (Security Services) und Sicherheitsmechanismen
- Beziehungen zwischen Services, Mechanismen und den Schichten des ISO/OSI-Referenzmodells
- Platzierung von Services und Mechanismen
- Hintergrundinformation:
 - Bedrohungen und Angriffe
 - Security Policy
 - Grundlegende Mechanismen
- Fokus der Sicherheitsarchitektur:
 - Sicherheitsbedürfnisse von verteilten / vernetzten Systemen
 - Betrachtet **keine** Host- oder Betriebssystem-Sicherheit



OSI Security Architecture: Dienste

■ Authentisierung (Authentication):

Jede Entität kann zweifelsfrei identifiziert werden

- ❑ Peer Entity Authentication:
Gegenseitige Authentisierung von zwei oder mehr Kommunikationspartnern
- ❑ Data Origin Authentication:
Identifikation des Senders bzw. des Autors einer Nachricht

■ Zugriffskontrolle (Access Control):

Schutz vor unberechtigter Nutzung von Ressourcen

■ Vertraulichkeit (Data confidentiality):

Schutz der Daten vor unberechtigter Offenlegung

- ❑ Connection confidentiality:
Alle Payload-Daten einer Verbindung
- ❑ Selective field confidentiality:
Bestimmte Felder der Payload-Daten
- ❑ Traffic flow confidentiality:
Schutz vor Verkehrsflussanalyse. (Wer kommuniziert mit wem in welchem Umfang und zu welcher Zeit?)



OSI Security Architecture: Dienste (Forts.)

■ Datenintegrität (Data integrity):

Erkennung von Modifikationen, Einfügungen, Löschungen, Umordnung, Duplikaten oder Wiedereinspielung von Daten

- ❑ Connection Integrity with/without Recovery
- ❑ Selective Field Connection Integrity

■ Verbindlichkeit (Non-repudiation):

Niemand kann das Senden oder Empfangen der Daten leugnen

- ❑ With proof of origin:
Sender kann das Senden nicht leugnen; Empfänger kann beweisen, welchen Ursprung die Daten haben.
- ❑ With proof of delivery:
Empfänger kann Empfang nicht leugnen; Sender kann die Auslieferung beweisen.



OSI SA: Mechanismen zur Umsetzung der Dienste

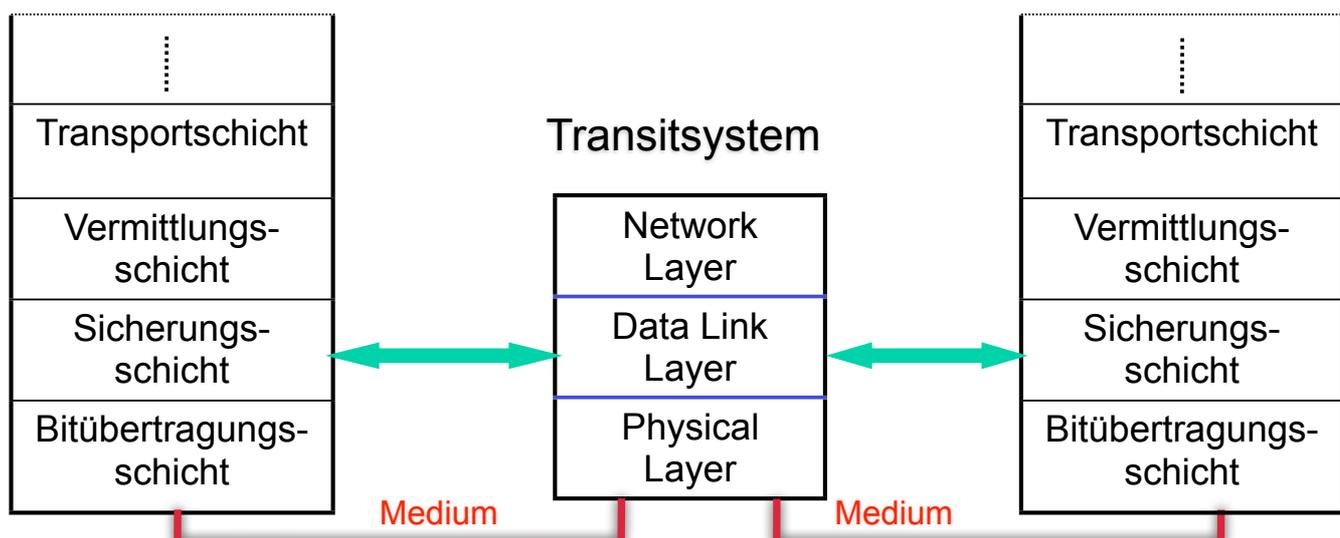
- Verschlüsselung (→ Vertraulichkeit)
 - symmetrisch
 - asymmetrisch
- Prüfsummenverfahren (→ Integrität)
- keine Mechanismen bzgl. Verfügbarkeit!

- Authentisierungsfunktionen (→ Authentizität)
- Elektronische Signaturen (→ Verbindlichkeit)
- Zugriffskontrolle (→ Autorisierung)
- Traffic Padding, Anonymisierung (→ keine Datenflussanalyse)
- Auditing und Logging (→ Revisionsfähigkeit)
- Beglaubigung von Daten (→ Notariatsfunktion)



Mechanismen auf unterschiedlichen Schichten

- Was soll gesichert werden?
- Wie weit reicht der Sicherheitsmechanismus?
Beispiel: Verschlüsselung auf Schicht 2 (Sicherungsschicht)
=> jedes Transitsystem muss entschlüsseln



Kapitel 2: Inhalt

1. Überblick über die OSI-Sicherheitsarchitektur
2. ISO/OSI Referenzmodell
3. Grundlegende Begriffe und Vorgehensweisen
4. **Relevante Standards**
 - OSI Sicherheitsarchitektur
 - Sicherheitsdienste
 - Sicherheitsmechanismen
 - ISO/IEC 27000
5. Unterscheidung Security vs. Safety



Motivation für ISO/IEC 27000

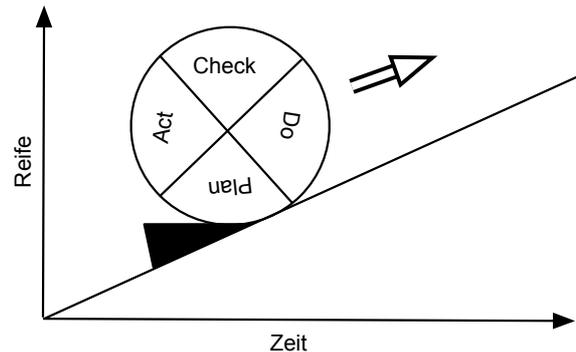
- Informationssicherheit Anfang der 1990er Jahre:
 - stark technikzentriert
 - Kosten-/Nutzenfrage kommt auf
 - Führungsebene wird stärker in IS-Fragestellungen eingebunden
- Wachsender Bedarf an Vorgaben und Leitfäden:
 - Kein „Übersehen“ wichtiger IS-Aspekte
 - Organisationsübergreifende Vergleichbarkeit
 - Nachweis von IS-Engagement gegenüber Kunden und Partnern
- Grundidee hinter ISO/IEC 27000:
Anwendung der Grundprinzipien des Qualitätsmanagements auf das Management der Informationssicherheit



Internationale Normenreihe ISO/IEC 27000

- ISO/IEC 27000 wird mehr als zwei Dutzend einzelner Standards umfassen
 - Mehr als die Hälfte davon ist noch in Arbeit und nicht veröffentlicht

- Norm ISO/IEC 27001 legt Mindestanforderungen an sog. Information Security Management Systems (ISMS) fest
 - Zertifizierungen möglich für:
 - Organisationen (seit 2005)
 - Personen (seit 2010)
 - Kernideen:
 - Kontinuierliche Verbesserung durch Anwendung des Deming-Zyklus
 - Risikogetriebenes Vorgehen
 - Seit 2008 auch DIN ISO/IEC 27001



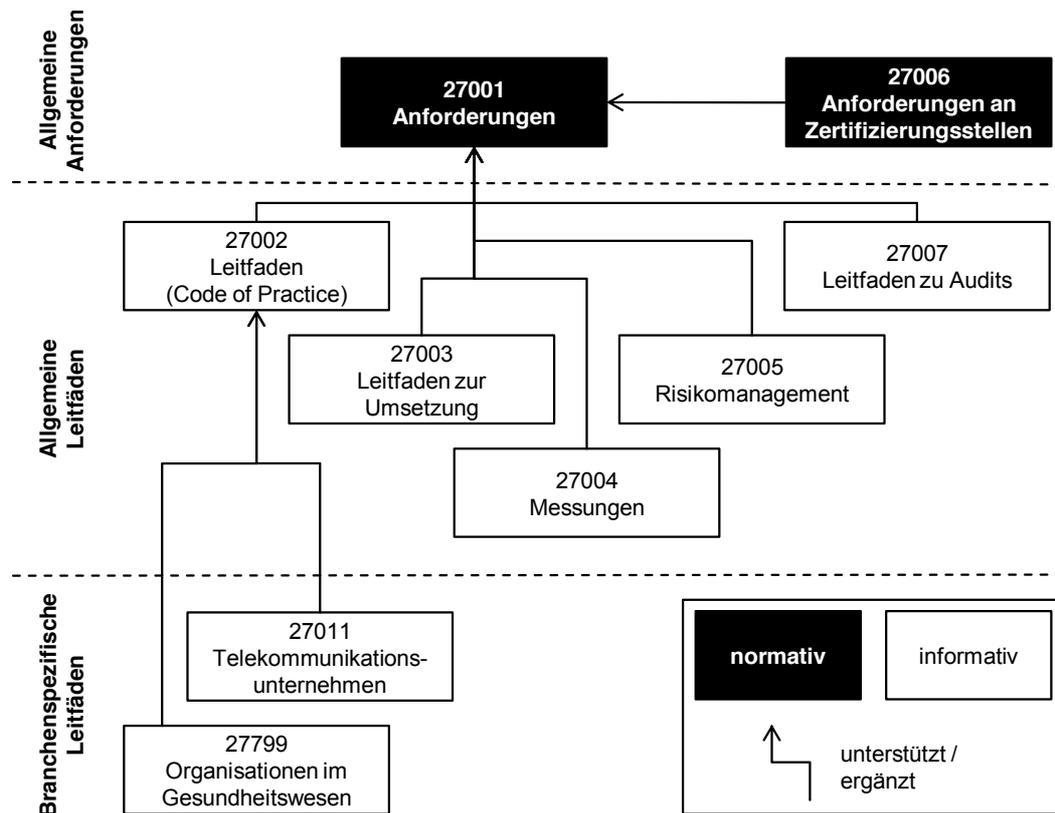
Informationssicherheits-Managementsystem (ISMS)

- Definition Managementsystem
 - System von Leitlinien, Verfahren, Anleitungen und zugehörigen Betriebsmitteln (inkl. Personal), die zur Erreichung der Ziele einer Organisation erforderlich sind.

- Definition ISMS:
 - Bestandteil des übergreifenden Managementsystems; es umfasst Einrichtung, Implementierung, Betrieb, Überwachung, Review, Wartung und Verbesserung der Informationssicherheit und stützt sich auf das Management von Geschäftsrisiken.

- Hinweis:
 - „System“ ist hier nicht im streng technischen Sinne, sondern als systematisches Rahmenwerk zu verstehen.

ISO/IEC 27000 im Überblick

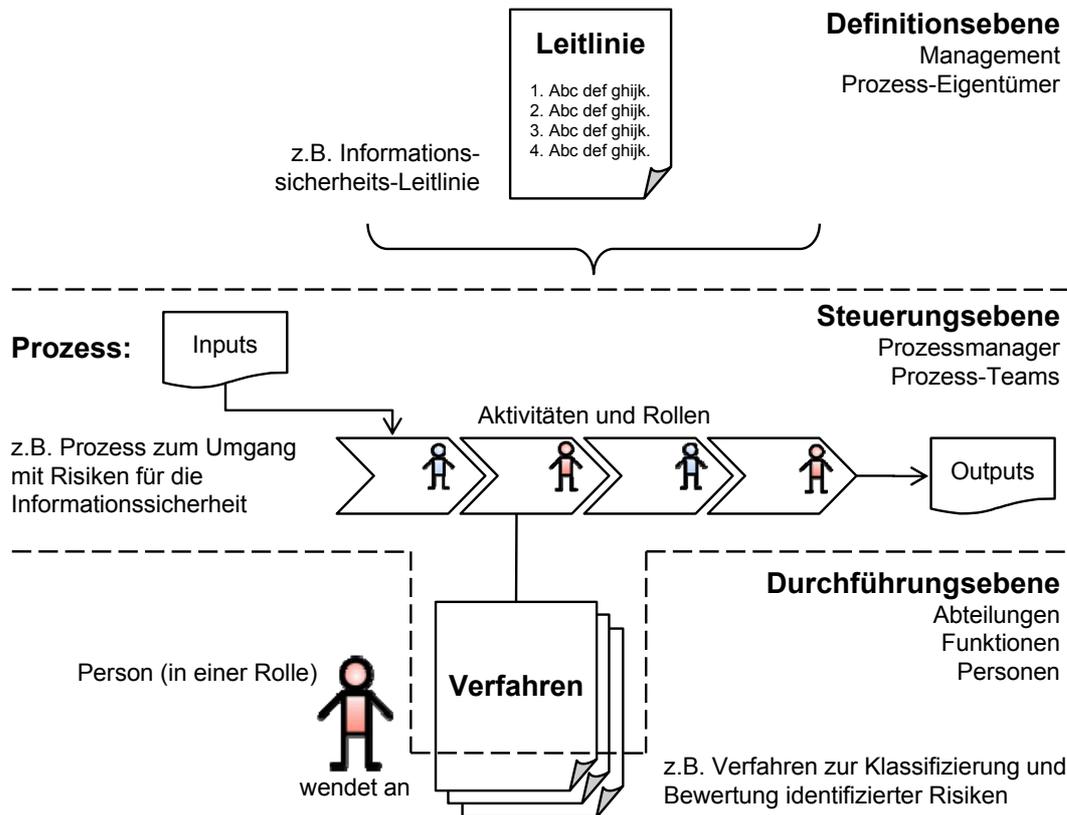


Wichtige Begriffe im Umfeld von ISMS

- (Informations-) Werte (engl. *assets*)
 - Alles, was für ein Unternehmen von Wert ist.
- Leitlinien
 - Anweisung, die formell durch das Management ausgesprochen wird.
- Prozesse
 - Ein Ablauf von zusammenhängenden oder wechselwirkenden Aktivitäten, die zu definierten Eingaben bestimmte Ergebnisse liefern.
- Verfahren
 - Vorgegebener Weg, eine Aktivität oder einen Prozess abzuwickeln.



Leitlinien, Prozesse, Verfahren



Kerninhalte von ISO/IEC 27001

- Begriffsdefinitionen
- PDCA-basierter Prozess zum Konzipieren, Implementieren, Überwachen und Verbessern eines ISMS
- Mindestanforderungen u.a. an Risikomanagement, Dokumentation und Aufgabenverteilung
- Normativer Anhang A enthält:
 - Definition von Maßnahmenzielen (control objectives)
 - Definition von Maßnahmen (controls)
- Umfang:
 - DIN ISO/IEC 27001:2008 - 45 Seiten
 - DIN ISO/IEC 27002:2008 - 144 Seiten



Maßnahmenziele und Maßnahmen: Überblick

A.5 Sicherheitsleitlinie (1/2) [= 1 Maßnahmenziel / 2 Maßnahmen (Controls)]			
A.6 Organisation der Informationssicherheit (2/11)			
A.7 Management von organisationseigenen Werten (2/5)			
A.8 Personelle Sicherheit (3/9)	A.9 Physische- und umgebungsbezogene Sicherheit (2/13)	A.10 Betriebs- und Kommunikationsmanagement (10/32)	A.12 Beschaffung, Entwicklung und Wartung von Informationssystemen (6/16)
A.11 Zugangskontrolle (7/25)			
A.13 Umgang mit Informationssicherheitsvorfällen (2/5)			
A.14 Sicherstellung des Geschäftsbetriebs (1/5)			
A.15 Einhaltung von Vorgaben (3/10)			



Beispiel: Maßnahmen in ISO/IEC 27001 A.8

Personelle Sicherheit (A.8)

Vor der Anstellung (A.8.1)

Aufgaben und Verantwortlichkeiten

Überprüfung

Arbeitsvertragsklauseln

Während der Anstellung (A.8.2)

Verantwortung des Managements

Sensibilisierung, Ausbildung, Schulung

Disziplinarverfahren

Beendigung oder Änderung der Anstellung (A.8.3)

Verantwortlichkeiten

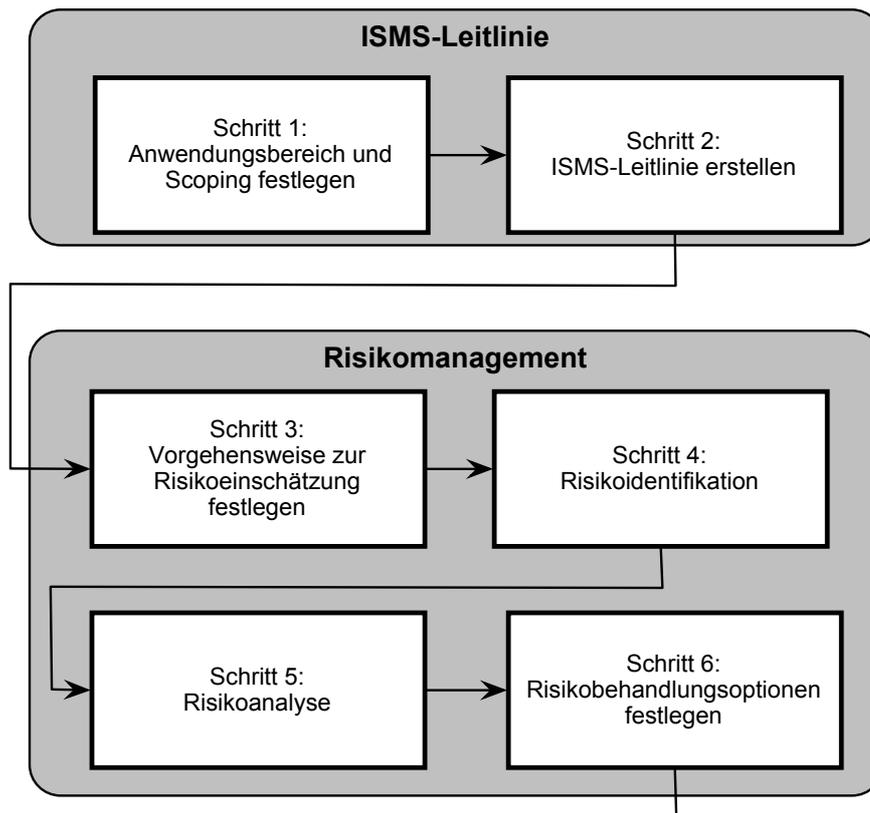
Rückgabe von Werten

Aufheben von Zugangsrechten

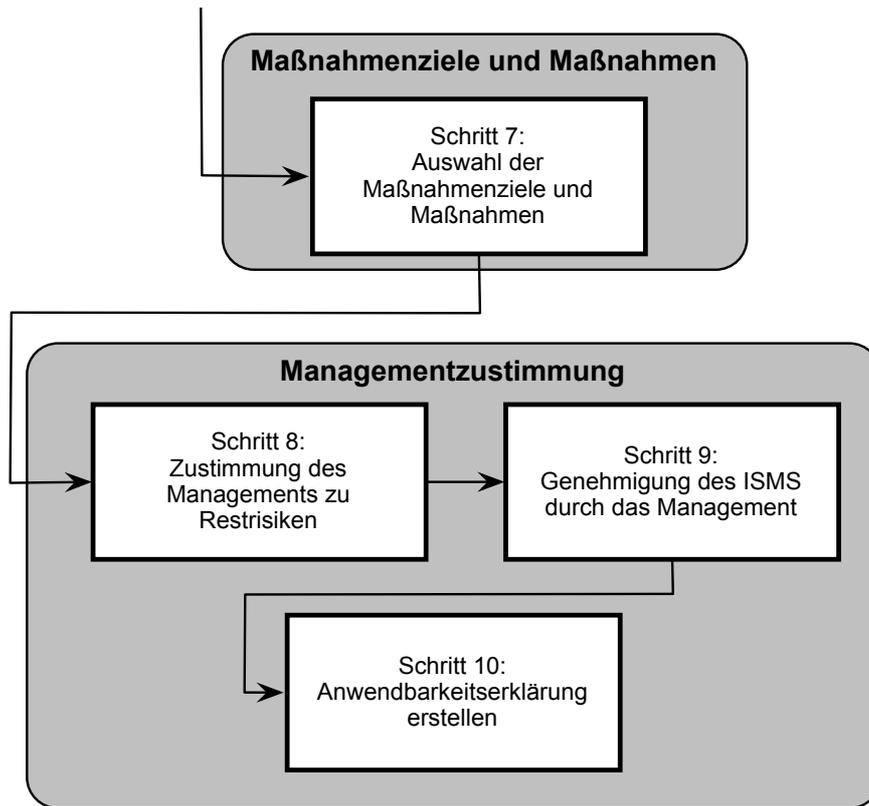




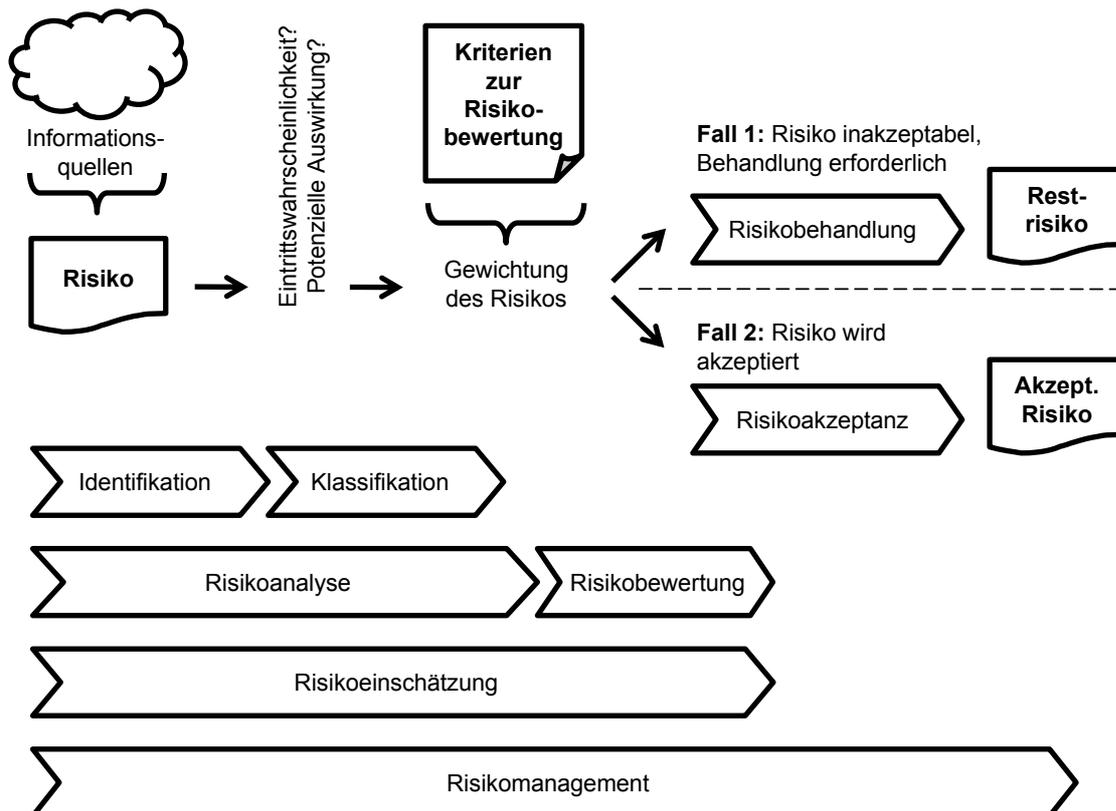
ISO/IEC 27001: Methode zum Aufbau eines ISMS



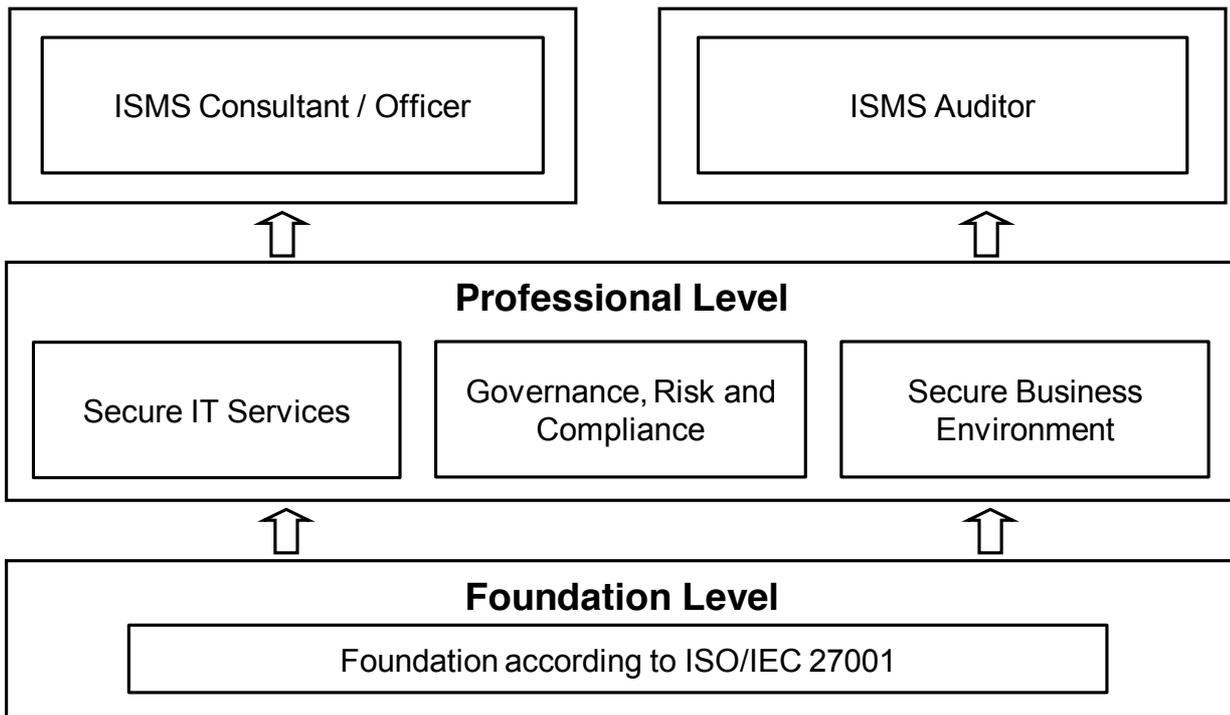
(Fortsetzung)



Grundlagen des Risikomanagements



Zertifizierungsprogramm für Personen



Kapitel 2: Inhalt

1. Überblick über die OSI-Sicherheitsarchitektur
2. ISO/OSI Referenzmodell
3. Grundlegende Begriffe und Vorgehensweisen
4. Relevante Standards
 - OSI Sicherheitsarchitektur
 - Sicherheitsdienste
 - Sicherheitsmechanismen
 - ISO/IEC 27000

5. Unterscheidung Security vs. Safety



Unterscheidung von Security und Safety

- Beide Begriffe werden oft mit „Sicherheit“ übersetzt
- Typische Themen der Safety („Funktionssicherheit“)
 - Betriebssicherheit für sicherheitskritische Programme, z.B. Steuerung und Überwachung von Flugzeugen oder Kraftwerken
 - Ausfallsicherheit (Reliability)
 - Gesundheitliche Sicherheit / Ergonomie
- Typische Themen der Security („Sicherheit“ i.S.d. Vorlesung)
 - Security Engineering
 - Security Policies
 - Sicherheitsanforderungen: Identifikation, Authentisierung, Autorisierung, Zugriffskontrolle, ...
 - Sicherheitsmechanismen realisieren Sicherheitsanforderungen
 - Verfügbarkeit (Availability) von Software und Hardware

Klassifikation nach Hartmut Pohl (1/2)

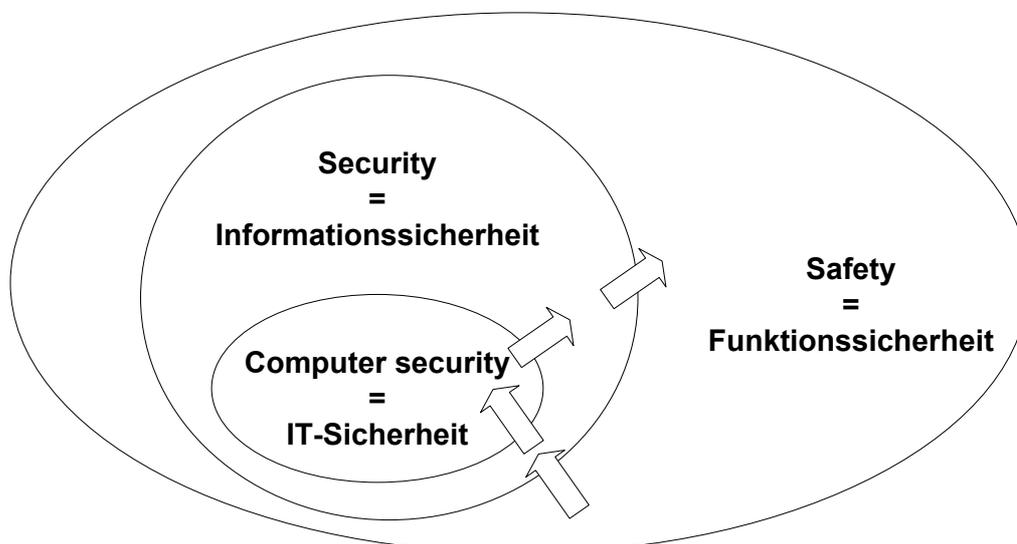
Legende:



„A ist als Teil von B zu betrachten“



„hat Einfluss auf“



Klassifikation nach Hartmut Pohl (2/2)

