



Informationssicherheitsmanagement
nach ISO 27001
Herkunft, Anforderungen, Chancen
DGO-Regionalkreis Darmstadt

Jürgen Reuter, 06.02.2007

Zur Person

- Kontakte:

Tel.: 06151-9371229

E-mail: juergen.reuter@t-systems.com

- Tätigkeiten:

Information Security Consultant am Standort Darmstadt

Seit über 25 Jahren tätig auf den Gebieten

Prozessmanagement, Sicherheit und Qualität

Auditor der DQS

Vom Bundesamt für Sicherheit in der Informationstechnik

lizenzierter Auditor

Übersicht

- Ausgangssituation
- Motivationsgründe einer Organisation
- Regulatorische Forderungen
- Marktbedingte Herausforderungen
- Chancen
- Modellwahl
- Vorgehensmodell
- Risk Assessment
- Ebene der Requirements
- Maßnahmen-Auswahl

Ausgangssituation - 1

- Tradierter Aufgabenfokus der Sicherheit
 - Objektschutz
 - Personen- und Veranstaltungsschutz
 - Verfolgung von Delikten
- In anderen Bereichen wird Sicherheit intuitiv gewährleistet.
- Unsicherheit wird erkannt, wenn Schäden auftreten.
- Gestiegene Bedeutung von Informationstechnik und Vernetzung für operative Prozesse und Finanzbereich
- Zunehmend unüberschaubares und komplexes Aufgabenfeld der Sicherheit

Ausgangssituation - 2

- Unerkannte und kaum kalkulierbare neue operative Risiken
- Sicherheitsmaßnahmen halten mit gesteigener Bedrohung nicht Schritt.
- Steigende Risikotoleranz führt zur Hinnahme von vermeidbaren Verwundbarkeiten.
- Mangelhafte Risikokommunikation

Motivationsgründe einer Organisation - 1

- Transparente Risikolage
 - Risiken, die man nicht kennt, sind trotzdem vorhanden.
 - Basis für gezielte risikomindernde Allokation von Mitteln
- Angemessenes Sicherheitsniveau
 - Berücksichtigung von Nutzerakzeptanz und Geschäftserfordernissen
 - Vorhandenes Budget wird wirkungsvoller eingesetzt.
 - Dokumentierte Behandlung von Risiken (einschließlich Akzeptanz)

Motivationsgründe einer Organisation - 2

- Nachhaltigkeit von Sicherheitsmaßnahmen
 - Unwirksame Sicherheitsmaßnahmen erkennen
 - Nachregelungsbedarf erkennen im Sinne eines KVP
- Sicherheitsbewusstsein in sicherheitsbewusstes Handeln umsetzen
 - Management Commitment herstellen
 - Mitarbeiter involvieren

Regulatorische Forderungen

- Basel II verlangt von Banken die risikoabhängige Eigenkapitalunterlegung von Krediten.
 - Neu ist vor Allem die Berücksichtigung von "Operational Risks".
 - Hierzu gehören die Risiken im Zusammenhang mit IT und Information.
- Sarbanes-Oxley verlangt die nachhaltige Kontrolle der Finanzberichterstattung.
 - Zuverlässige IT ist notwendige Voraussetzung hierfür.
 - Bei der IT-Sicherheit ist die Erfüllung des „Stand der Technik“ Mindestforderung.
 - Internes Kontrollsystem ist auch Gegenstand anderer Gesetze (z.B. GDPdU)

Marktbedingte Herausforderungen - 1

- Kunden verlangen in vielfältiger Weise Informations- und IT-Sicherheitsnachweise:
 - Grundschnachweis für den IVBB
 - ISO 17799 oder Grundschnachweis durch die Deutsche Bundesbank
 - CRAMM oder ISO 17799 in Ausschreibungen der Nato
 - Die Forderungen nach entsprechenden Nachweisen werden seit Verabschiedung der ISO 27001 stärker.

Marktbedingte Herausforderungen - 2

- Die Abwälzung von Risiken über Outsourcing wird nicht ohne Nachweis oder Überprüfung der Gegebenheiten beim Outsourcing-Partner anerkannt.
- Zertifizierte Informationssicherheit wird sich von einem marktdifferenzierenden Kriterium zu einer Selbstverständlichkeit entwickeln.

Chancen

- Qualitative Stärkung der Informationssicherheit steht im Vordergrund .
- Stärkung der Reputation im Bereich Informationssicherheit
- Systematische Verankerung der Informationssicherheit in den Geschäftsprozessen
- Vereinheitlichung der Managementsysteme und -handbücher
- Risikoadjustierte Zuweisung von Ressourcen für die Informationssicherheit
- Weniger Überraschungen durch Sicherheitsvorfälle
- Vereinfachung der Erbringung anderweitiger, ähnlicher Nachweise (S-Ox, GDPdU etc.)

Modellwahl - 1

- ISO 27001 bzw. 17799 zuvor BS 7799-2 bzw. BS 7799-1
 - hoher Bekanntheitsgrad, breiteste Anerkennung
 - zahlreiche Bezugnahmen in gesetzlichen Vorschriften
 - viele Gemeinsamkeiten mit vorhandenen Managementsystemen (Qualität- und Umwelt),
 - eine auf Vollständigkeit angelegte Systematik,
 - normiert kein ISMS, sondern bildet Grundlage für ein auf die Belange der Organisation ausgerichtetes Informationssicherheitsmanagementsystem.

Modellwahl - 2

- Formaler Zusatzaufwand lässt sich auf notwendiges Maß begrenzen.
- Zertifizierung ist unabhängig von technischen und Sicherheitsanforderungen möglich.
- Unter dem Dach von ISO 27001 lassen sich andere Modelle (z.B. Grundschutzmodell) abbilden.
- Die Nachweisführung bzgl. Forderungen verschiedenster Herkunft wird erbracht oder zumindest vereinfacht (S-Ox, GdPdU...). Ein Rechtsanspruch auf Anerkennung von Zertifikaten besteht jedoch nicht!

Vorgehensmodell - ISMS: Planung („Plan“)

- Scope-Definition (Geschäftszweig, Organisation, Standorte, Technologie und Inventar)
- ISMS-Rahmenkonzept auf Basis des Scope
 - Grundsätze hinsichtlich Informationssicherheit
 - Sicherheitspflichten (vertraglich, gesetzlich, geschäftsübliche)
 - Risikomanagementverfahren und Aufbauorganisation
 - Kriterien für die Klassifikation von Risiken aufstellen
- Verfahren für das Risk Assessment definieren
- Identifizieren der Risiken, Risk Assessment durchführen
- Maßnahmenoptionen ermitteln und auswählen
- Anwendbarkeitsstatement durch TOP-Management (SOA)
- Informationssicherheitskonzept

Vorgehensmodell - ISMS: Implementierung und Betrieb („Do“)

- Risk Treatment Plan formulieren und implementieren
- Implementierung der beschlossenen Maßnahmen
- Schulung und Sensibilisierung der Mitarbeiter
- Anpassung der betrieblichen Prozesse
- Verfahren zur Behandlung von Sicherheitsvorfällen einrichten

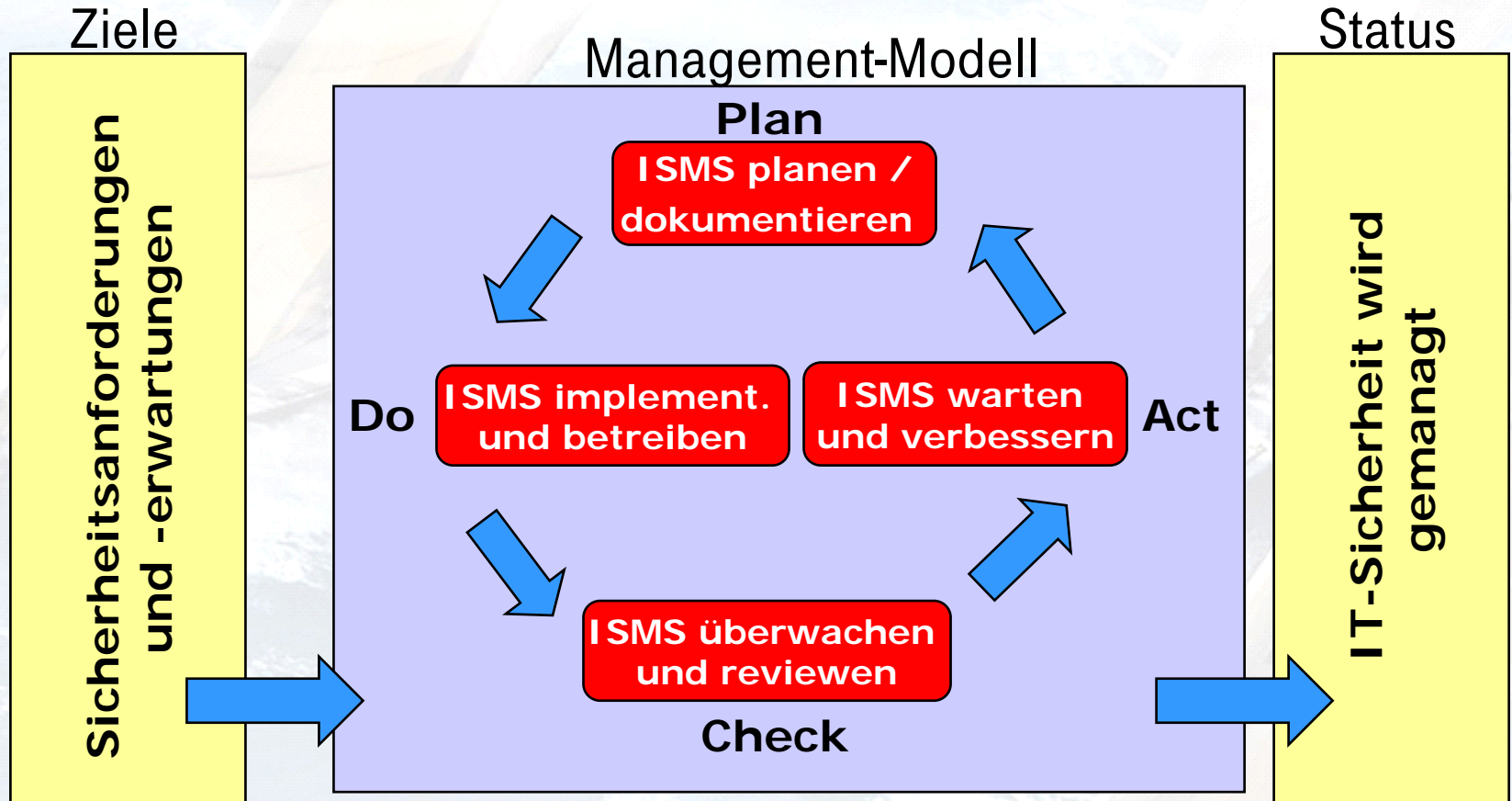
Vorgehensmodell - ISMS: Beobachten und Überprüfen („Check“)

- Beobachtungsprozeduren zur Erkennung von
 - Irrtümern, Sicherheitsvorfällen, Befolgung von Sicherheitsregeln
 - Verfolgung von Sicherheitsmaßnahmen im Lichte von geschäftlichen Prioritäten
- Reviews, Audits, Vorfallverfolgung, Vorschläge und Feedback
- Review des Risk Assessments im Zuge von Veränderungen
- Interne ISMS-Audits in festgelegter Frequenz
- Mindestens 1x jährlich Management-Review des ISMS
- Aufzeichnungen zu Maßnahmen und Vorfällen mit Wirkung auf ISMS
- Überprüfung der Wirksamkeit der Maßnahmen

Vorgehensmodell - ISMS: Pflege und Verbesserung („Act“)

- Entwickeln und dokumentieren von Korrektur- und Vorbeugemaßnahmen
- Kommunikation der Ergebnisse und Maßnahmen
- Einführung der identifizierten Verbesserungen (->Plan)

Vorgehensmodell - ISMS: Regelkreis

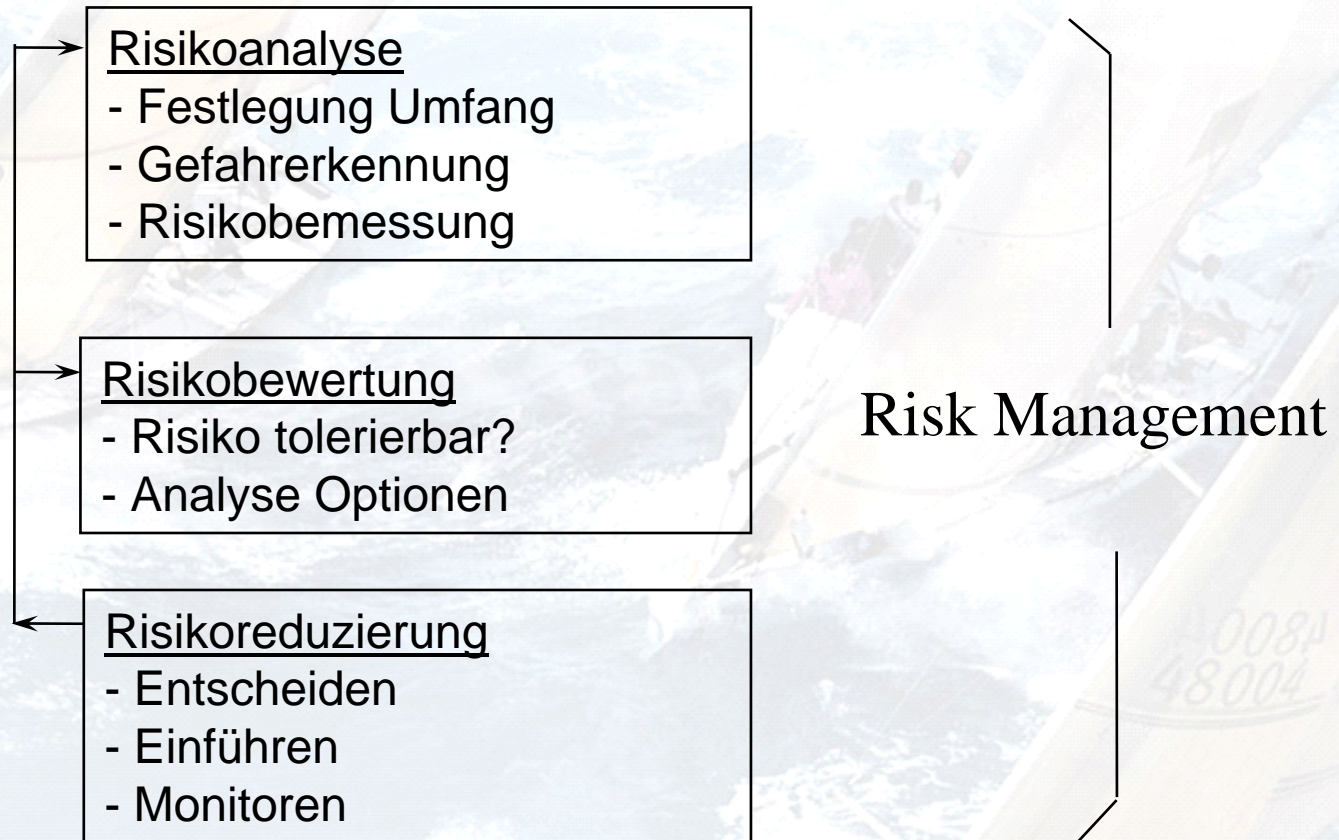


Dokumentation - ISMS

- Scope-Definition
- Risk Assessment
- Risk Treatment Plan
- Verfahren zu Planung, Betrieb und Überwachung der Informationssicherheitsprozesse
- Aufzeichnungen
- Statement of Applicability
- Security Policy / Sicherheitsleitlinie

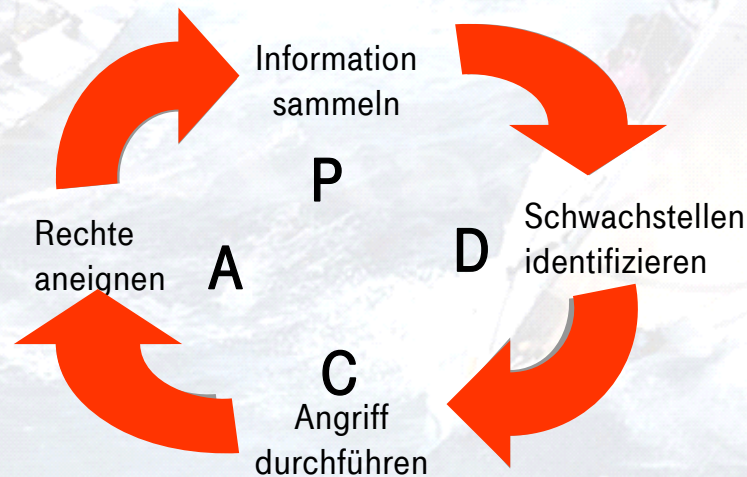
- In Verbindung mit den klassischen QM-Verfahren: Dokumentenlenkung, Freigabeverfahren, Change Management,...

Risk-Management - ISMS



Risiko-Analyse, den „PDCA-Zyklus“ des Angreifers unterbrechen!

Nach welchem Muster geht „der Angreifer“ vor?



Und was unternehmen wir?

Risiko-Analyse und -Bewertung - ISMS

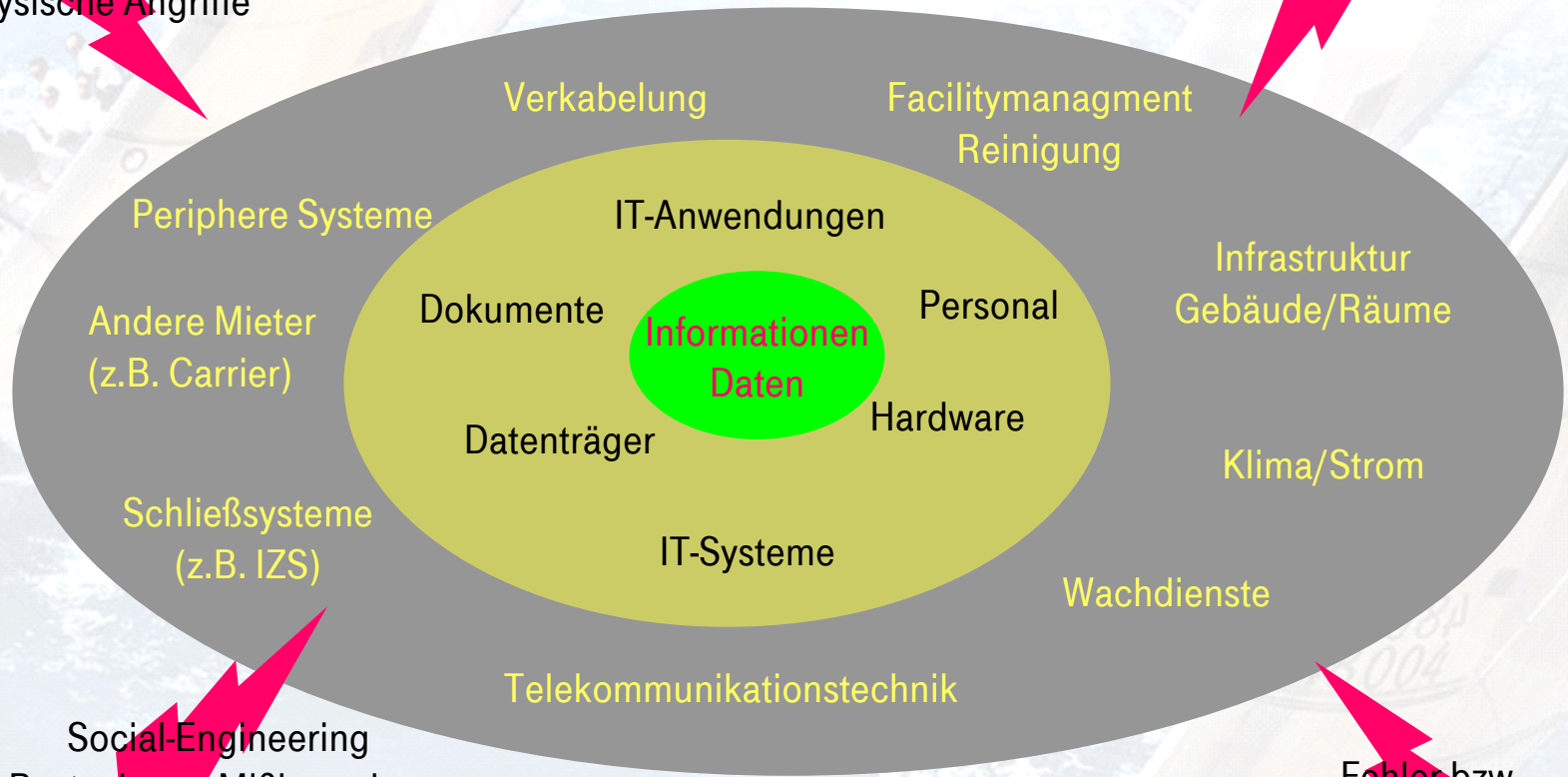
- Der Standard schreibt keine Methode vor.
- Bei der Vorgehensweise sind folgende Faktoren einzubeziehen:
 - Bedrohung: Wirkt von Außen auf das System ein!
 - Schwachstelle: Wohnt dem System selbst inne!
 - Schadensermwartung
 - Häufigkeitseinschätzung
 - Schadenshöhen

Informationssicherheitsmanagement nach ISO 27001

Infowerfassung

Physische Angriffe

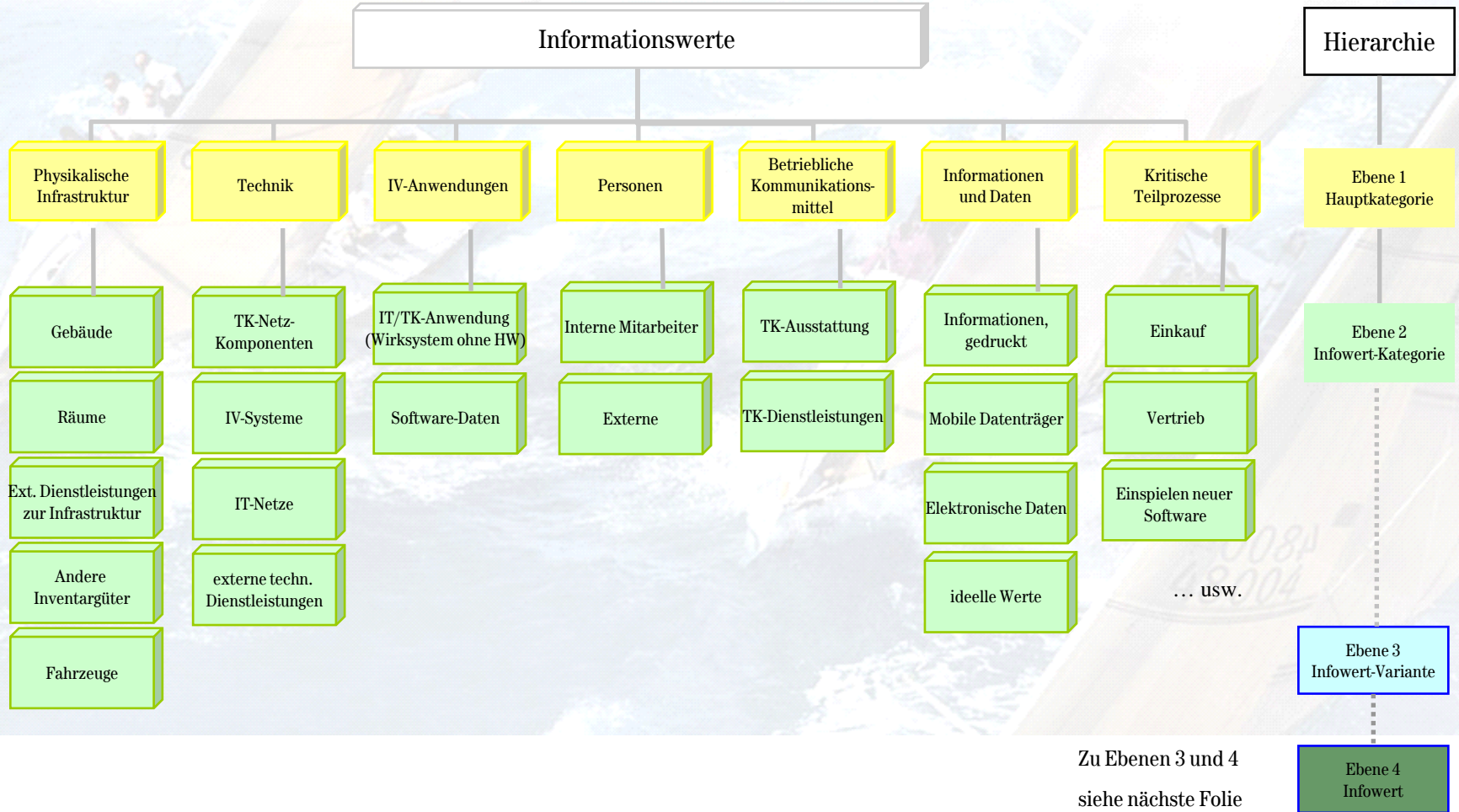
Logische Angriffe



Social-Engineering
Bestechung, Mißbrauch ...

Fehler bzw.
Irrtümer

Infowerterfassung



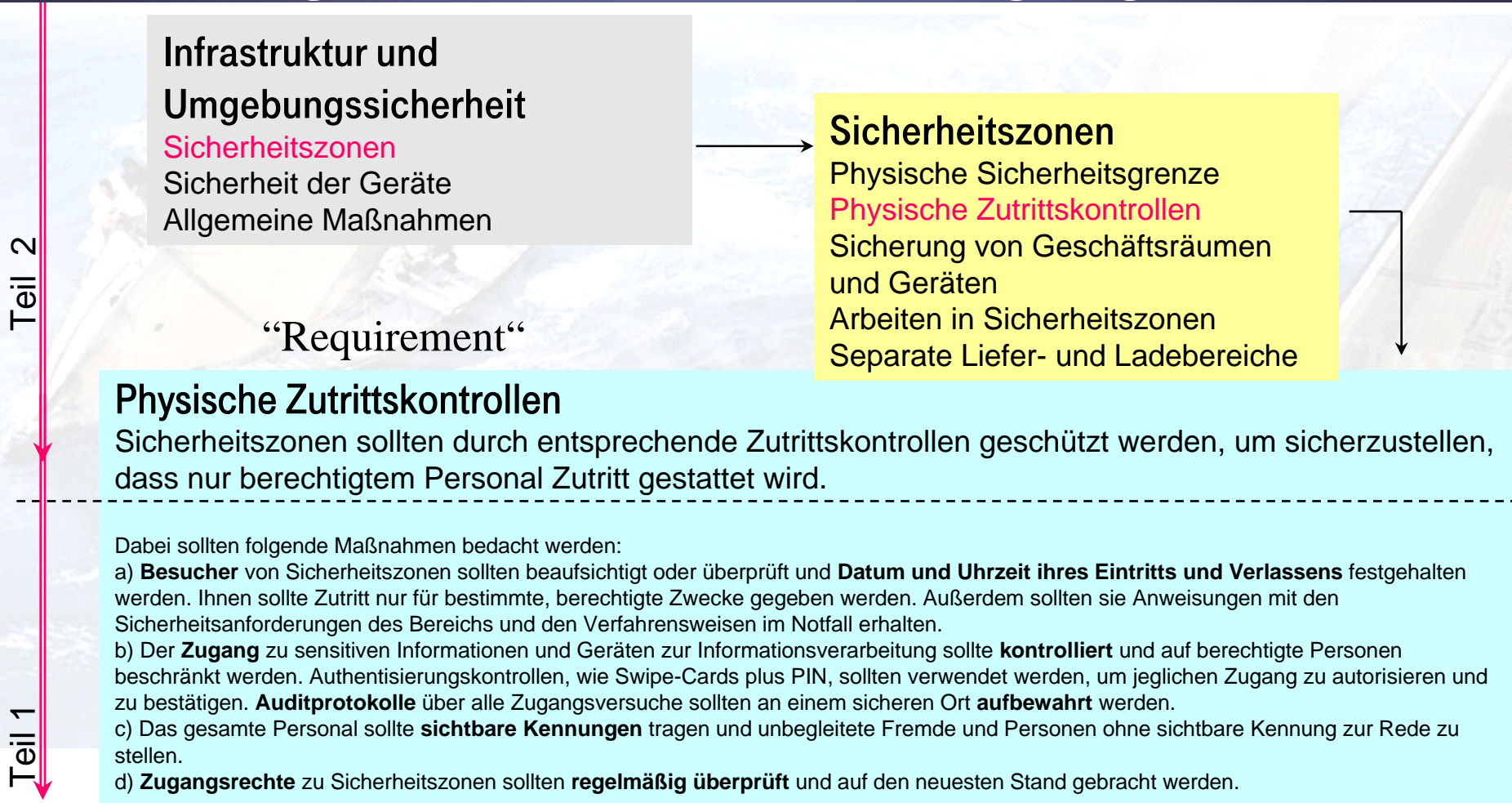
Risiko-Analyse (Beispiel)

Risikoanalyse eines Informationswertes:												Verantwortlich:				
Beschreibung:																
Bestehende Maßnahmen														Control Nr.		
Bedrohungen:																
Verwundbarkeiten:																
Schadenserwartung:																
<ul style="list-style-type: none"> - Vertraulichkeit - Unversehrtheit - Verfügbarkeit 																
Berechnung der Risikoprioritätszahl für den Ist-Zustand		RPZ	= B	* V	* S	Für B, V und S wird eine Zahl zwischen 1 (niedrig) und 40 (sehr hoch) gewählt. Miteinander multipliziert ergibt dies die RPZ.										
		36	3	4	3											
Control-Nr.:																
Anwendbar:																
Maßnahme Nr.:																
Lfd. Nr.	Maßnahmenbezeichnung	Kurze Beschreibung und Begründung der Maßnahme														
Berechnung der Risikoprioritätszahl nach Maßnahmenumsetzung		RPZ	= B	* V	* S	Für B, V und S wird eine Zahl zwischen 1 (niedrig) und 4 (sehr hoch) gewählt. Miteinander multipliziert ergibt dies die RPZ.										
		36	3	3	4											
Anwendbarkeitserklärung:		Die einschlägigen Controls der BS 7799-2 sind wie oben aufgeführt uneingeschränkt anwendbar bzw. es gelten die folgenden Einschränkungen:														
		<ol style="list-style-type: none"> 1. 2. 3. 														

Maßnahmenfindung: Aufbau von ISO 27001, Annex A

- Die Hauptüberschriften geben die Handlungsfelder für das Sicherheitsmanagement an.
 - Sicherheitspolitik
 - Organisatorische Sicherheit
 - Klassifikation und Überwachung der Informationswerte
 - Personelle Sicherheit
 - Infrastruktur und Umgebungssicherheit
 - Kommunikations- und Betriebsmanagement
 - Zugangüberwachung
 - Systementwicklung und -pflege
 - Management von Sicherheitsvorfällen
 - Notfallplanung
 - Compliance

Auszug zum Thema „Infrastruktur und Umgebungssicherheit“



Auswahl von Maßnahmen

- Welche Maßnahmen sind auszuwählen, um den „Requirements“ aus den 11 Hauptkapiteln zu genügen?
- ISO 17799 / BS7799-1 enthält Hinweise und Empfehlungen (Code of Practice).
- Maßnahmen können auch dem Grundschutzhandbuch des BSI entnommen werden.
- Es kann notwendig werden, eigene Sicherheitsmaßnahmen zu definieren.

Beispiel: fiktives Polizeipräsidium

Wert: Webserver (fiktiv)

Beschreibung: IIS-basierter Webserver (gehärtet) mit folgenden Aufgaben: Information der Bevölkerung bezüglich aktueller Fahndungen, allgemeine Öffentlichkeitsarbeit der Polizei, Informationsanlaufstelle der Bevölkerung bei Katastrophen, Notfällen, Bereitstellung eines Übermittlungsweges für vertrauliche Mitteilungen von Bürgern an die Polizei

Bedrohung: Faken der Webseite. Hacken der Webseite. Einbringen von unzulässigem Content. Überlastung der Webseite. Abfangen bzw. Veränderung vertraulicher Mitteilungen von Bürgern an die Polizei.

Schwachstelle: „polizeixystadt.de“ ist nicht für die Polizei reserviert, Eingabemasken nicht hinsichtlich der Absetzbarkeit von speziellen Kommandos gesichert, die vom Webserver bereitgestellten Inhalte unterliegen keiner besonderen Überwachung, Bürger können sich nicht über ein speziell abgesichertes Portal an die Polizei, angeboten wird nur eine gewöhnliche E-Mail Kontaktadresse

Schadenserwartung:

- Vertraulichkeit: Es könnten versehentlich vertrauliche Inhalte (Ermittlungsprotokolle oder dgl. auf der Seite eingestellt werden. Hieraus ergibt sich eine Verletzung von Persönlichkeitsrechten sowie ein Imageschaden für die Behörde. Der E-Mail Verkehr von Bürgern an die Polizei kann abgefangen werden.
- Integrität: Ein Imitieren der Webseite der Polizei durch Unbefugte ist leicht möglich. Durch das gezielte Ausstatten einer derartigen Webseite mit irreführenden Informationen könnten kriminelle Handlungen unterstützt werden. Schaden für die Opfer und Imageschaden für die Polizei.
- Verfügbarkeit: Keine besonderen Schadenspotentiale erkennbar, da von externem Dienstleister betrieben der nach neustem Stand der Technik arbeitet und die Berücksichtigung aller ihm obliegenden Aspekte der Informationssicherheit gewährleistet.
- Sonstiges: Keine erkennbaren weiteren Schäden.
- Schadenshöhe: Nachhaltige Imageschäden von gehörigem, allerdings nicht monetär messbarem, Ausmaß. Verstoß gegen das Bundesdatenschutzgesetz. Keine Konformität mit dem Grundschutz.
- Schadenshäufigkeit: Aufgrund der vorliegenden Situation keine eine beliebige Häufigkeit unterstellt werden.

Resultierende RPZ = $8 * 10 * 7 = 560 > \text{akzeptable RPZ} = 50$

Informationssicherheitsmanagement nach ISO 27001

Beispiel: fiktives Polizeipräsidium (Regeln nach ISO 27001 –Annex A)

Nr.	Regelinhalt	Mögliche Maßnahmen
5.1.1	Sicherheitskonzeption(Policy)	Aussage zur Klassifikation vertraulicher Unterlagen und zur Behandlung vertraulicher Informationen im Zusammenhang mit der Nutzung von Internet und E-Mail. Sowie Aussage zum Management der Contents.
7.2.1	Klassifizierung	Ermittlungsprotokolle einer Vertraulichkeitsklasse zuordnen
7.2.2	Kennzeichnung klassifizierter Informationen	Vertrauliche Dokumente kennzeichnen damit sie nicht versehentlich ins Internet kommen oder per normaler E-Mail verschickt werden.
10.1.1	Dokumentierte Betriebsverfahren	Definieren wie mit vertraulichen und wie mit für die Öffentlichkeit bestimmten Informationen zu verfahren ist.
10.1.2	Changemanagement	Contentmanagement für die Webseiten der Polizei festlegen.
10.1.3	Pflichtentrennung	Trennung zwischen Erstellung des einzelnen Webbeitrages, ggf. Redaktion, Freigabe und ggf. Einstellung durch den Administrator.
10.7.3	Verfahren zum Umgang mit Informationen	Definieren wie mit vertraulichen und wie mit für die Öffentlichkeit bestimmten Informationen zu verfahren ist.

Informationssicherheitsmanagement nach ISO 27001

Beispiel: fiktives Polizeipräsidium (Regeln nach ISO 27001 –Annex A)

Nr.	Regelinhalt	Mögliche Maßnahmen
10.8.1	Formale Verfahren für den sicheren Austausch von Informationen etablieren	Sicherstellen, dass keine sensitiven Informationen an offen zugänglichen Stellen liegen. Regelungen und Maßnahmen bzgl. des Weiterleitens von Mails oder sonstigen Informationen.
10.8.4	Regelungen zum Schutz von Informationen bei elektronischem Datentransfer treffen	Schutz vor unerlaubtem Zugriff, Veränderung oder Denial-of-service.
10.9.3	Schutz der öffentlich zugänglichen Info vor unerlaubter Veränderung oder Fälschung.	Einführen geeigneter Methoden zum Schutz der öffentlich zugänglichen Info vor unerlaubter Veränderung oder Fälschung. (z.B. digitaler Signaturen, vgl. 12.3) Durchführen entsprechender Tests. Formale Zulassung vor der Veröffentlichung. Einhalten der Datenschutzbestimmungen.
10.10	Überwachung des Systemzugriffs	Maßnahmen zum Logging und Auswerten der Protokolle. (versch. Sicherheitsregeln zu beachten)
11	Logische Zugangskontrolle	Diverse Sicherheitsregeln sind in Maßnahmen zum Schutz des logischen Zugriffs auf den Server umzusetzen.

Beispiel: fiktives Polizeipräsidium (Regeln nach ISO 27001 –Annex A)

Nr.	Regelinhalt	Mögliche Maßnahmen
12.3.1	Policy für den Einsatz kryptographischer Maßnahmen	Richtlinie zum Einsatz kryptographischer Methoden entwickeln und umsetzen.
14	Aspekte des Notfallmanagements	Festlegen gegen welche Notfälle hinsichtlich des Weiterbetriebs des Servers Vorsorge zu treffen ist und wie diese sich gestaltet. Überprüfen bzw. Testen der Wirksamkeit der Notfallvorsorge.
15.1.1	Identifikation der Rechtslage	Wenn datenschutzrelevante Informationen auf der Webseite vorgehalten werden ist z.B. das BDSG bzw. jew. LDSG zu beachten.
15.1.3	Schutz organisationseigener Aufzeichnungen	Festlegen wie z.B. Ermittlungsprotokolle zu behandeln sind.
15.1.4	Datenschutz	Aufstellen und Aufrechterhalten eines Datenschutzkonzepts.
15.2.1	Einhaltung von Sicherheitsverfahren	Überprüfung hinsichtlich des Umgangs mit vertraulichen Informationen sowie hinsichtlich der Einhaltung der für das Contentmanagement festgelegten Verfahren.
15.2.2	Überprüfung der Einhaltung technischer Bedingungen	Überprüfung ob das System technisch die Gewähr zur Erhaltung von Vertraulichkeit, Integrität und Verfügbarkeit bereitgestellter Informationen und Daten erfüllt.

Zusammenfassung

- Im Gegensatz zu anderen Vorgehensmodellen ist aus technischer Sicht die Methode
 - in ihrer Anwendungsbreite nicht beschränkt,
 - ganzheitlich, leicht durchschaubar und einfach umsetzbar,
 - leicht anpassbar (u.a. Risk Assessment, Maßnahmen-Auswahl) auf die speziellen Gegebenheiten,
 - Ressourcenschonend.

- Das Information Security Management System (ISMS) ist
 - erweiterbar und anschlussfähig sowie leicht wartbar,
 - entspricht dem Stand der Technik,
 - Ist national wie international anerkannt,
 - revisionsfähig wg. der erzeugten Sicherheitsnachweise.