esse

Security for Systems Engineering – VO 05: IT-Risikomanagement und IT-Grundschutz

Florian Fankhauser, Christian Brem

Agenda

IT-Risikomanagement

Begriffsdefinition: Risiko aus etymologischer Sicht

- Duden: *„Wagnis, Gefahr“*: Das Fremdwort wurde im 16. Jh. als kaufmännischer Terminus aus gleichbed. *it.* risico, risco (heute 'rischio') entlehnt, dessen weitere Herkunft unsicher ist. Aus dem *It.* stammt auch entsprechend *frz.* risque „Gefahr, Wagnis“. Davon abgeleitet ist das Verb *frz.* risquer *„in Gefahr bringen, aufs Spiel setzen, wagen“*, aus dem im 17. Jh. riskieren übernommen wurde.
- *Span.* risco *„steiler Felsen“*
- Bernstein: Risiko begreifen, messen und in Konsequenzen abschätzen
- Bernstein: Bereitschaft zum Risiko wesentlicher Katalysator des Fortschritts der modernen westlichen Gesellschaft

Begriffsdefinition: Risiko aus IT-Sicht

- „Projekte ohne echte Risiken sind Loser – wenn ein Projekt kein Risiko birgt, lassen Sie die Finger davon!“ (DeMarco)
  „Risikomanagement ist Projektmanagement für Erwachsene.“ (DeMarco)
- BSI: Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab.

- In der IT-Sicherheit häufig definiert als:
  - Risiko = Eintrittswahrscheinlichkeit $*$ Schadenshöhe
- Grenzrisiko, Restrisiko

Risiko im Alltag, Risiko in Relation

- Nahezu keine Erfahrung erforderlich
- Nahezu keine Gefahren

- Kenntnisse und Erfahrung erforderlich
- Eigenes Einschätzungsvermögen
- Gefahren vorhanden

Alltägliches Risikomanagement

- Risiken sind subjektiv – jeder/jede empfindet eine Situation oder eine Gefahr anders
- Alltägliches Risikomanagement
  - Freizeit, Sport
  - Autofahren etc.
- (Un-)bewusstes Risikomanagement, z.B. durch
  - Versicherungen (Lebens-, Kranken-, Unfall-,...)
  - Altersvorsorge
- Risikobewusstsein erfordert Verantwortungsbewusstsein

Risiko in der IT: Beispiele für Standards und Normen

Norm	Beschreibung
ISO/IEC Guide 73:2009	Risk management – Vocabulary – Guidelines for use on standards
AS/NZS 4360:2004	Risk management (Australian/New Zealand Standard)
HDB 4360:2004	Handbook Risk Management Guidelines Companion to AS/NZS 4360 : 2004
ISO/IEC 17799:2005	Information technology – Security techniques – Code of practice for information security management
ISO 14971:2012	Medical devices. Application of risk management to medical devices
ISO 27005:2018	Information security risk management
ISO/IEC 31000:2018	Risk Management
BSI-Standard 200-3	Risikoanalyse auf der Basis von IT-Grundschutz

Charakteristik von Risiken und Risikomanagement in der IT

- IT-Risiken sind Bedrohungen, die sich nachteilig
  - auf den Betrieb und die Verfügbarkeit von Prozessen,
  - eingesetzten Systemen,
  - bis hinunter zu den einzelnen Daten und Informationen

  im Unternehmen auswirken können

- IT-Risikomanagement beinhaltet
  - frühzeitige Erkennung solcher Bedrohungen
  - Erarbeitung von entsprechenden Gegenmaßnahmen

IT-Risikomanagement-Prozess

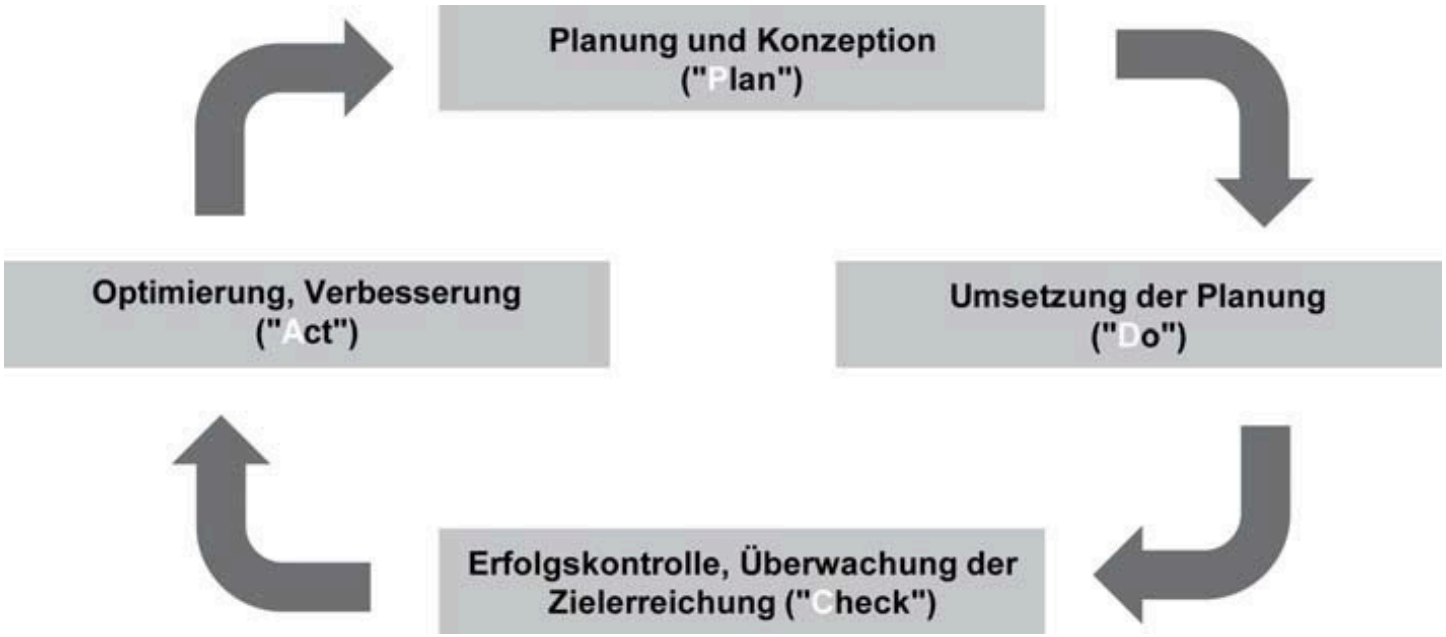
- Schlussendlich sind alle Ansätze ähnlich aufgebaut
  - Risikoidentifikation/Gefährdungsübersicht
  - Einstufung des Risikos
    - Einschätzung des Risikos
    - Bewertung des Risikos
  - Risikobehandlung/-steuerung
  - Risikokonsolidierung

- Wiederholter, immer wiederkehrender Durchlauf der Phasen!

(Vergleiche BSI Standard 200-3)

Informationssicherheitsprozess

Sicherheitsprozess unterliegt einem Lebenszyklus; Darstellung z.B. als PDCA-Modell



(Vergleiche BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS))

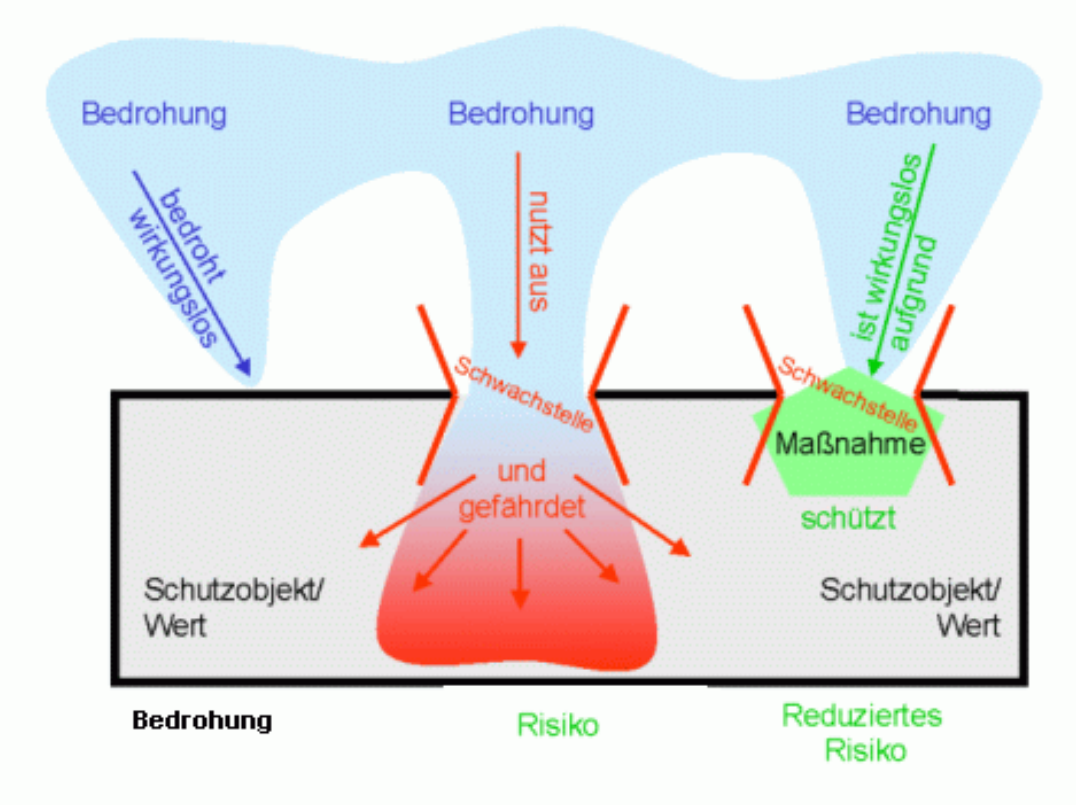
Vorarbeiten zur Risikoanalyse

- Initiierung eines systematischen Informationssicherheitsprozesses
- Festlegung der Verantwortlichkeiten
- Definition eines Geltungsbereichs der Sicherheitskonzeption
- Schutzbedarfsfeststellung
- Beschreibung geeigneter Methoden für
  - Analyse von Risiken
  - Bewertung von Risiken
  - Behandlung von Risiken
- Dies bedeutet beispielsweise
  - Festlegung der Schutzklassen und Kriterien (Schadenshöhe, Eintrittswahrscheinlichkeit, Risikoakzeptanz)
  - Festlegung der Review-Zyklen

Risikoidentifikation

- Erkennung von Risiken
- Eindeutige Beschreibung des Risikos
- Eingangsparameter wie Schwachstellen und Bedrohungen
- Erfassung geplanter und realisierter Sicherheitsmaßnahmen
- Beispiele für Methoden
  - Brainstorming
  - Angriffsbäume
  - Failure Modes and Effects Analysis (FMEA)
  - Fault Tree Analysis (FTA)

Entstehung von Risiken



Risiken können nur entstehen, wenn eine Bedrohung auf ein Schutzobjekt wirkt und durch eine Schwachstelle zu einem Schaden führen kann.

(Vergleiche BSI)

Risikobewertung

- Basiert auf der Risikoidentifikation

- Schätzung der Schadensschwere
- Schätzung der Eintrittshäufigkeit

- Sollte von ExpertInnen mit entsprechendem Know-How durchgeführt werden
- Ergebnis ist das Risikolevel für ein Risiko

Risikobewertung: Festlegung der Schadensschwere

- Bestimmt durch Einordnung des Schadens in eine Schadenskategorie und Bestimmung der anzunehmenden maximalen Schadensklasse
- Schadenskategorien, z.B.
  - Verstoß gegen Gesetze, Verträge oder Vorschriften
  - Beeinträchtigung der Aufgabenerfüllung
  - Negative Innen- bzw. Außenwirkung
  - Finanzielle/Wirtschaftliche Schäden
- Schadensklasse, z.B.
  - Festlegung der Klassen für jede Kategorie
  - Einteilung z.B. in Klein, Niedrig, Mittel, Hoch...

Risikobewertung: Festlegung der Eintrittshäufigkeit

- Die Eintrittshäufigkeit bestimmt welche Häufigkeit für den Eintritt eines Risikos und somit eines Schadensereignisses angenommen wird
- Einteilung in Eintrittshäufigkeitsklassen
  - z.B. Niemals, Selten, Gelegentlich, Häufig...
  - entspricht der erwarteten Anzahl des Auftretens pro Zeiteinheit

Risikobewertung: Festlegung der Risikobereiche

Der Risikobereich eines Risikos ergibt sich aus der Kombination der festgelegten Schadensschwere und der Eintrittshäufigkeit.

Eintrittshäufigkeit	Risikobereich				
Sehr Häufig (5)					
Häufig (4)					
Gelegentlich (3)					
Selten (2)					
Sehr Selten (1)					
nicht möglich (0)					
	kein Schaden (0)	Niedrig (1)	Mittel (2)	Hoch (3)	Sehr Hoch (4)
	Schadensschwere (Schadensklasse)				

(Vergleiche BSI)

Risikobehandlung/-steuerung: Mögliche Optionen

- Risikoakzeptanz
- Risikovermeidung
- Risikoverminderung/-mitigierung
- Risikotransferierung

- Risikoakzeptanz auf Management-Ebene
- Setzen von anderen Maßnahmen als Risikoakzeptanz $\rightarrow$ Risiko muss erneut betrachtet werden
- Restrisiko bleibt erhalten und muss jedenfalls akzeptiert werden

Risikokontrolle: Risiko-Reporting

- Wichtig ist die Bereitstellung entscheidungsrelevanter Risikoinformationen für die Projektleitung
- Das beinhaltet
  - die Ergebnisse der operativen und strategischen Kontrollen fortlaufend auszuwerten
  - eine transparente und nachvollziehbare Dokumentation der Risikoentwicklung
- IT-Risikomanagement ist ein Prozess, d.h., Risiken müssen laufend erkannt und behandelt werden
- Risiko-Reporting muss laufend, am besten Tool-gestützt, fortgeschrieben werden

IT-Grundschutz

Zentrale Frage der IT-Sicherheit

Was muss ich in meinem Projekt wie schützen?

Teilaspekte dieser zentralen Frage der IT-Sicherheit

- Welche Daten/Komponenten sind in meinem Projekt schützenswert?
- Welche konkreten Aspekte davon müssen geschützt werden?
- Wie werden Sicherheitsmaßnahmen umgesetzt?
- Wie erfahre ich dies effizient?
- Was ist Best-Practice?
- Wie sicher sind andere Systeme, mit denen ich zusammenarbeite?
- Wie weise ich anderen nach, dass meine Infrastruktur sicher ist?

Beurteilung von IT-Sicherheit

- Standards; Allgemein gültige Aussagen, Empfehlungen
  - Common Criteria for Information Technology Security Evaluation (CC, ISO/IEC 15408)
  - International Standard for an Information Security Management System (ISO 27k-Reihe)
  - COBIT
  - ITIL
  - ...
- IT-Grundschutz

Grundlagen zu IT-Grundschutz – Recap

- Herausgegeben vom BSI, Deutschland
- „Kochbuch“ für normales Schutzniveau
- Praktikable Durchführung von IT-Sicherheitsanalysen
- Kosteneffektive Erhöhung des IT-Sicherheitsniveaus
  - Schnelle Identifizierung von Sicherheitsmaßnahmen
  - Schnelle Umsetzung von Sicherheitsmaßnahmen
- Angemessener Schutz durch Kombination von organisatorischen, personellen, infrastrukturellen und technischen Maßnahmen
- Verwendung eines Baukastenprinzips: Bausteine, Gefährdungen, Maßnahmen
- Soll-Ist-Vergleich empfohlene und realisierte Maßnahmen
- Einfache und arbeitsökonomische Erstellung von IT-Sicherheitskonzepten

IT-Grundschutz – Standards

- BSI-Standards
  - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)
  - BSI-Standard 200-2: IT-Grundschutz-Methodik
  - BSI-Standard 200-3: Risikomanagement Leitfaden Basis-Absicherung
  - BSI-Standard 200-4: Notfallmanagement
- IT-Grundschutzkataloge

Aufbau des IT-Grundschutz-Kompendiums

- Einführung
- IT-Grundschutz – Basis für Informationssicherheit
- Schichtenmodell und Modellierung
- Rollendefinitionen
- Übersicht der elementaren Gefährdungen
- Bausteine:
  - ISMS: Sicherheitsmanagement
  - ORP: Organisation und Personal
  - CON: Konzeption und Vorgehensweise
  - ...

(Vergleiche IT-Grundschutz-Kompendium)

Der IT-Sicherheitsprozess laut IT-Grundschutz

- *Initiierung des Sicherheitsprozesses*
- *Organisation des Sicherheitsprozesses*
- Dokumentation im Sicherheitsprozess
- Sicherheitskonzeption gemäß IT-Grundschutz
  - Sicherheitskonzeption nach Basis-Absicherung
  - Sicherheitskonzeption nach Kern-Absicherung
  - Sicherheitskonzeption nach Standard-Absicherung
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und Verbesserung

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Initiierung und Organisation des Sicherheitsprozesses

- Initiierung des Sicherheitsprozesses
  - Verantwortung der Leitungsebene
  - Konzeption und Planung, Festlegung der Vorgehensweise
  - Erstellung einer Leitlinie zur Informationssicherheit
- Organisation des Sicherheitsprozesses
  - Integration der Informationssicherheit in Prozesse
  - Aufbau einer Informationssicherheitsorganisation
  - Vergabe von Aufgaben und Verantwortungen, u.a.
    - Informationssicherheitsbeauftragte/r und IS-Management Team
    - Datenschutzbeauftragte/r
    - Einbindung externer SicherheitsexpertInnen

Der IT-Sicherheitsprozess laut IT-Grundschutz

- Initiierung des Sicherheitsprozesses
- Organisation des Sicherheitsprozesses
- *Dokumentation im Sicherheitsprozess*
- Sicherheitskonzeption gemäß IT-Grundschutz
  - Sicherheitskonzeption nach Basis-Absicherung
  - Sicherheitskonzeption nach Kern-Absicherung
  - Sicherheitskonzeption nach Standard-Absicherung
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und Verbesserung

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Auszug Ablauf Dokumentation im Sicherheitsprozesses

- Klassifikation von Informationen
- Informationsfluss im Informationssicherheitsprozess
  - Berichte an Leitungsebene
  - Dokumentation im Informationssicherheitsprozess
  - Anforderungen an die Dokumentation
  - Informationsfluss und Meldewege

Der IT-Sicherheitsprozess laut IT-Grundschutz

- Initiierung des Sicherheitsprozesses
- Organisation des Sicherheitsprozesses
- Dokumentation im Sicherheitsprozess
- *Sicherheitskonzeption gemäß IT-Grundschutz*
  - Sicherheitskonzeption nach Basis-Absicherung
  - Sicherheitskonzeption nach Kern-Absicherung
  - Sicherheitskonzeption nach Standard-Absicherung
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und Verbesserung

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Auswahl einer Sicherheitskonzeption

Erfolgt nach Erfüllung folgender Voraussetzungen:

- Initiierung eines Informationssicherheitsprozesses
- Sicherheitsleitlinie und -organisation wurde definiert
- Asset-Übersicht der Institution wurde erstellt
- Schutzbedarfsanalyse

Entsprechend der Situation der abzusichernden Institution wird anschließend eine Sicherheitskonzeption ausgewählt

Schutzbedarfsfeststellung

- Ermittlung eines angemessenen Schutzbedarfs für Informationen und Geschäftsprozesse
- Betrachtung von zu erwartenden Schäden, die bei Beeinträchtigung der Schutzziele (z.B. CIA) entstehen können
- wichtig: Abschätzung von Folgeschäden einbeziehen!
- Definition der Schutzbedarfskategorien
- Schutzbedarfsfeststellung für Prozesse und Anwendungen
- Schutzbedarfsfeststellung für IT-, ICS- und IoT-Systeme
- Schutzbedarfsfeststellung für Räumlichkeiten und Gebäude
- Schutzbedarfsfeststellung für Kommunikationsverbindungen
- Schlussfolgerungen aus den Ergebnissen der Feststellungen
- für alle 3 Formen der Sicherheitskonzeption jeweils (erneut) durchzuführen

Sicherheitskonzeptionstypen

- Basis-Absicherung
  - Flächendeckende Umsetzung der „Basis-Anforderungen“
- Kern-Absicherung
  - Fokus auf den Schutz der essenziellen Assets
  - Sinnvoll bei großem Handlungsbedarf im Bereich der IT-Sicherheit
  - Zuerst essenzielle Assets absichern, danach breite Strategie umsetzen
- Standard-Absicherung
  - „Vollständige“ Umsetzung des IT-Grundschutz
  - Ziel ist pragmatische und effektive Vorgehensweise zur Erzielung eines normalen Sicherheitsniveaus

Sicherheitskonzeption: IT-Grundschutz-Check

- Organisatorische Vorbereitungen
  - Auswahl der AnsprechpartnerInnen
  - Vorbereitung Checklisten
- Soll-Ist-Vergleich mittels Interviews sowie exemplarischer Kontrolle
  - Erläuterung der Zielsetzung des Basis-Sicherheitschecks für InterviewpartnerInnen
  - Umsetzungsstatus der einzelnen Maßnahmen erfragen
  - Verantwortlichkeiten erfragen
- Dokumentation der Ergebnisse des Soll-Ist-Vergleichs einschließlich der erhobenen Begründungen und eventueller weiterer Anmerkungen
  - Ergebnisse den Befragten mitteilen

Der IT-Sicherheitsprozess laut IT-Grundschutz

- Initiierung des Sicherheitsprozesses
- Organisation des Sicherheitsprozesses
- Dokumentation im Sicherheitsprozess
- *Sicherheitskonzeption gemäß IT-Grundschutz*
  - *Sicherheitskonzeption nach Basis-Absicherung*
  - Sicherheitskonzeption nach Kern-Absicherung
  - Sicherheitskonzeption nach Standard-Absicherung
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und Verbesserung

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Sicherheitskonzeption nach Basis-Absicherung

- Festlegung des Geltungsbereichs
- Auswahl und Priorisierung
- IT-Grundschutz-Check
- Realisierung
- Auswahl einer folgenden Vorgehensweise
  - Kern-Absicherung
  - Standard-Absicherung

Der IT-Sicherheitsprozess laut IT-Grundschutz

- Initiierung des Sicherheitsprozesses
- Organisation des Sicherheitsprozesses
- Dokumentation im Sicherheitsprozess
- *Sicherheitskonzeption gemäß IT-Grundschutz*
  - Sicherheitskonzeption nach Basis-Absicherung
  - *Sicherheitskonzeption nach Kern-Absicherung*
  - Sicherheitskonzeption nach Standard-Absicherung
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und Verbesserung

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Sicherheitskonzeption nach Kern-Absicherung

- Fokus auf Absicherung besonders schützenswerter Assets
- Nach Auswahl im Anschluss an Durchführung der Basis-Absicherung
- Festlegung des Geltungsbereichs
- Identifikation und Festlegung der kritischen Assets
- Strukturanalyse
- Schutzbedarfsfeststellung, gegebenenfalls Prüfung / Fokussierung / Erweiterung von Task bei Auswahl einer Sicherheitskonzeption
- Modellierung
- IT-Grundschutz-Check (Erfüllungsstatus der Anforderungen feststellen,. . . – siehe Basis-Absicherung)
- Risikoanalyse und weiterführende Sicherheitsmaßnahmen
- Umsetzung (Verbesserung, Erweiterung, Zertifizierung,. . .)

Kern-Absicherung: Identifikation/Charakteristika kritischer Assets

- Kritische Assets sind nur Informationen oder Prozesse, keine Anwendungen, System
- Anzahl dieser Assets ist überschaubar bzw. umfasst nur kleinen Anteil aller Informationen/Prozesse
- Schutzbedarf solcher kritischer Assets sind mindestens als „hoch“ einzustufen
- Schutzbedarf kann so hoch sein, dass noch nicht einmal Sicherheitsbeauftragte Einsicht haben dürfen
- Schutzbedarf kann sich mit Zeit verändern

Kern-Absicherung: Beispiele kritischer Assets

- Zu *besonders schützenswerten Assets* gehören üblicherweise:
  - Informationen zur Bereitstellung essenzieller Geschäftsprozesse
  - Informationen und Geschäftsprozesse mit deutlich erhöhtem Informationssicherheitsbedarf (z.B. gemäß CIA-Triade)
  - Informationen und Geschäftsprozesse mit existenziell bedrohlichem Schaden bei Verlust der Vertraulichkeit, Zerstörung, Veränderung etc.

Kern-Absicherung: Strukturanalyse

- Erhebung von Informationen für die weitere Vorgehensweise
- Analyse der Interaktion von Geschäftsprozessen, Anwendungen und Systemen
- Komplexitätsreduktion durch Gruppenbildung
- Teilaufgaben:
  - Erfassung von Geschäftsprozessen, Anwendungen und Informationen
  - Netzplanerhebung
  - Erhebung von IT-, ICS- und IoT-Systemen
  - Erfassung der Räumlichkeiten und Gebäude

Sicherheitskonzeption nach Kern-Absicherung: Komplexitätsreduktion durch Gruppenbildung

- Gruppierung von Objekten
  - Gleicher Typ
  - Ähnliche Konfiguration
  - Ähnliche Einbindung in das Netz (im Fall von IT-Systemen z.B. am gleichen Switch)
  - Ähnliche administrative und infrastrukturelle Rahmenbedingungen
  - Bedienung ähnlicher Anwendungen

- Wichtig: *Alle gruppierten Objekte müssen den gleichen Schutzbedarf aufweisen! – Siehe nächster Schritt.*

Schutzbedarfsfeststellung für IT-Systeme

- Betrachtung der Anwendungen, die in direktem Zusammenhang mit dem IT-System stehen

- *Beachtung von Abhängigkeiten*: Übertragung von Anforderungen
- *Maximumprinzip*: aufgrund schwerwiegendster Auswirkung
- *Kumulationseffekt*: mehrere kleine Schäden führen zu einem Großen
- *Verteilungseffekt*: Aufteilung des Schutzbedarfs, z.B. Redundanzen

Schutzbedarfsfeststellung: Schutzbedarfskategorien

Gemäß BSI IT-Grundschutz haben sich die folgenden Kategorien in der Praxis bewährt:

Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Schutzbedarfskategorien: Beispiel

Exemplarisch eine Ausarbeitung für die Kategorie „Sehr Hoch“

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Schutzbedarfsfeststellung: Schutzwirkung

Aus der Schutzbedarfsfeststellung lässt sich die Schutzwirkung der Anforderungen nach IT-Grundschutz wie folgt angeben:

Schutzwirkung von Sicherheitsanforderungen nach IT-Grundschutz	
Schutzbedarfskategorie „normal“	Sicherheitsanforderungen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
Schutzbedarfskategorie „hoch“	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen sollten auf Basis einer Risikoanalyse ermittelt werden.
Schutzbedarfskategorie „sehr hoch“	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, reichen aber alleine im Allgemeinen nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer Risikoanalyse ermittelt werden.

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Sicherheitskonzeption nach Kern-Absicherung: Modellierung

- Basis Strukturanalyse und Schutzbedarfsfeststellung
- Abbildung des betrachteten/analysierten IT-Verbunds auf IT-Grundschutz-Bausteine
- Zusammentragen der relevanten Sicherheitsmaßnahmen aus den Maßnahmenkatalogen
- Ergebnis ist ein IT-Grundschutz-Modell des IT-Verbundes

IT-Grundschutz-Bausteine

- Gruppierung der Sicherheitsaspekte nach bestimmten Themen
- Vereinfachte Abbildung auf den IT-Verbund

- B 1: Übergreifende Aspekte; z.B. Datensicherungskonzept, Krypto-Konzept
- B 2: Infrastruktur; z.B. Serverraum, Schutzschränke
- B 3: IT-Systeme; z.B. Laptop, Windows 7-Client, TK-Anlage
- B 4: Netze; z.B. WLAN, VoIP
- B 5: Anwendungen; z.B. Webserver, Datenbanken

(Vergleiche IT-Grundschutz-Bausteine)

Maßnahmenkataloge

- Den einzelnen Bausteinen sind Sicherheitsmaßnahmen zugeordnet
- Maßnahmenkataloge
  - M 1: Infrastruktur
  - M 2: Organisation
  - M 3: Personal
  - M 4: Hardware und Software
  - M 5: Kommunikation
  - M 6: Notfallvorsorge
- Anschließend Durchführung IT-Grundschutz-Check (Soll-Ist-Vergleich)

Der IT-Sicherheitsprozess laut IT-Grundschutz

- Initiierung des Sicherheitsprozesses
- Organisation des Sicherheitsprozesses
- Dokumentation im Sicherheitsprozess
- *Sicherheitskonzeption gemäß IT-Grundschutz*
  - Sicherheitskonzeption nach Basis-Absicherung
  - Sicherheitskonzeption nach Kern-Absicherung
  - *Sicherheitskonzeption nach Standard-Absicherung*
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und Verbesserung

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Erstellung einer Sicherheitskonzeption nach Standard-Absicherung Vorgehensweise

Ziel ist eine pragmatische und effektive Vorgehensweise zur Erzielung eines normalen Sicherheitsniveaus:

- *Festlegung des Geltungsbereichs*
- *Strukturanalyse* (siehe Kern-Absicherung)
- *Schutzbedarfsfeststellung* (siehe Kern-Absicherung)
- *Modellierung* (siehe Kern-Absicherung)
- *IT-Grundschutz-Check (Teil 1)* (Soll-Ist-Vergleich)
- *Optional: Risikoanalyse*
- *Konsolidierung*
- *IT-Grundschutz-Check (Teil 2)*
- *Realisierung der Maßnahmen*
- *Kontinuierliche Verbesserung*

Der IT-Sicherheitsprozess laut IT-Grundschutz

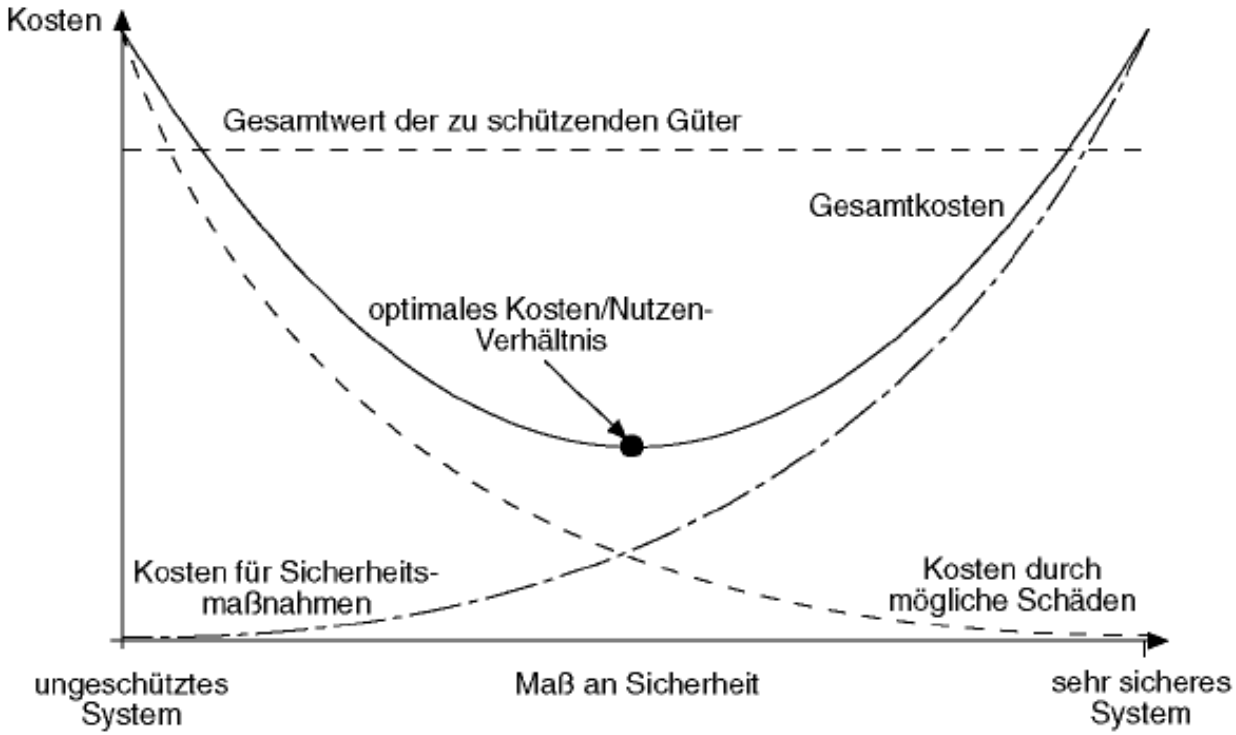
- Initiierung des Sicherheitsprozesses
- Organisation des Sicherheitsprozesses
- Dokumentation im Sicherheitsprozess
- Sicherheitskonzeption gemäß IT-Grundschutz
  - Sicherheitskonzeption nach Basis-Absicherung
  - Sicherheitskonzeption nach Kern-Absicherung
  - Sicherheitskonzeption nach Standard-Absicherung
- *Umsetzung der Sicherheitskonzeption*
- Aufrechterhaltung und Verbesserung

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Umsetzung der Sicherheitskonzeption

- Sichtung der Untersuchungsergebnisse
- Kosten- und Aufwandsschätzung
- Festlegung der Umsetzungsreihenfolge der Maßnahmen
- Festlegung der Aufgaben und der Verantwortung (siehe Kern-Absicherung)
- Realisierungsbegleitende Maßnahmen (z.B. Schulungen)

Wiederholung: Kosten-/Nutzenanalyse



(Vergleiche M. Raepple: Sicherheitskonzepte für das Internet)

Der IT-Sicherheitsprozess laut IT-Grundschutz

- Initiierung des Sicherheitsprozesses
- Organisation des Sicherheitsprozesses
- Dokumentation im Sicherheitsprozess
- Sicherheitskonzeption gemäß IT-Grundschutz
  - Sicherheitskonzeption nach Basis-Absicherung
  - Sicherheitskonzeption nach Kern-Absicherung
  - Sicherheitskonzeption nach Standard-Absicherung
- Umsetzung der Sicherheitskonzeption
- *Aufrechterhaltung und Verbesserung*

(Vergleiche BSI-Standard 200-2: IT-Grundschutz-Vorgehensweise)

Aufrechterhaltung und Verbesserung

- Aufarbeitung der Ergebnisse und Einbindung in die Informationssicherheitsstrategie im Fokus
- Überprüfung des Informationssicherheitsprozesses auf allen Ebenen
- Eignung der Informationssicherheitsstrategie
- Übernahme der Ergebnisse in den Informationssicherheitsprozess
- Weiterführende Zertifizierungen

Zertifizierung nach ISO 27001

- Zertifizierung optional möglich

- Nachweis, dass Maßnahmen gemäß IT-Grundschutz realisiert wurden
- Zusicherung von Informationssicherheit an KooperationspartnerInnen
- Nachweis, dass durch Vernetzung keine untragbaren Risiken entstehen
- Bemühungen zu Informationssicherheit verdeutlichen

Literatur – 1/3

- Günther Drosdowski und Paul Grebe, (Hrsg.). *Der große Duden : in 9 Bänden. 7. Duden - Etymologie : Herkunftswörterbuch der deutschen Sprache*. Bibliographisches Institut, 2013
- Peter L. Bernstein. *Wider die Götter*. Murmann, 2004. ISBN 3938017139. Against the Gods, 1996
- Tom DeMarco. *The deadline : a novel about project management*. Dorset House Publishing, New York, 1997. ISBN 0932633390
- George Cybenko. Why Johnny Can't Evaluate Security Risk. *Security & Privacy, IEEE*, 4(1):5–5, Januar/Februar 2006. ISSN 1540-7993. doi: 10.1109/MSP.2006.30

Literatur – 2/3

- Daniel Jr. Geer, Kevin S. Hoo, und Andrew Jaquith. Information security: why the future belongs to the quants. *IEEE Security & Privacy Magazine*, 1(4):24–32, 2003. ISSN 1540-7993. doi: 10.1109/MSECP.2003.1219053
- Bruce Schneier. Hacking the business climate for network security. *Computer*, 37(4):87–89, April 2004. ISSN 0018-9162. doi: 10.1109/MC.2004.1297316

Literatur – 3/3

- BSI. Grundschutz, 2020. https://www.bsi.bund.de/grundschutz
- Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz-Standards, 2020. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html
- derStandard. Gefahrenzonen in Zeiten von Corona-Lockerungen, 2020. https://www.derstandard.at/story/2000117522057/gefahrenzonen-in-zeiten-von-corona-lockerungen

- Hinweis: Die Slides enthalten Teile von Slides von (früheren) ESSE-KollegInnen

Zusammenfassung

- IT-Risikomanagement
  - Risiko als Chance und Gefahr
  - (IT-)Risiko im Alltag und in der IT
  - Risikomanagement-Prozess, u.a. Risikoidentifizierung, -bewertung, -behandlung
- IT-Grundschutz
  - Motivation für IT-Grundschutz
  - Grundlagen und Anwendung des IT-Grundschutz
  - Organisation und Dokumentation nach IT-Grundschutz
  - Basis-, Kern- und Standard-Absicherung
  - Umsetzung, Aufrechterhaltung und Verbesserung des Sicherheitsprozesses

Vielen Dank!

https://security.inso.tuwien.ac.at/