esse

Security for Systems Engineering – VO 04: IT-Risikomanagement und IT-Grundschutz

Florian Fankhauser

Agenda

IT-Risikomanagement

- Begriffsdefinition: Risiko
- Risiko im Alltag
- Risiko in der IT
- IT-Risikomanagement-Prozess

IT-Grundschutz

- Motivation
- Grundlagen
- Aufbau und Anwendung
- Erstellung eines Sicherheitskonzepts

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

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

Risiko in der IT: Beispiele für Standards und Normen

Norm	Beschreibung
ISO/IEC Guide 73:2002	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 14971:2001	Medical devices. Application of risk management to medical devices
ISO 14300-1	Space systems – Programme management – Part 1: Structuring of a programme
ISO 27005	Risk Management
BSI-Standard 100-3	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

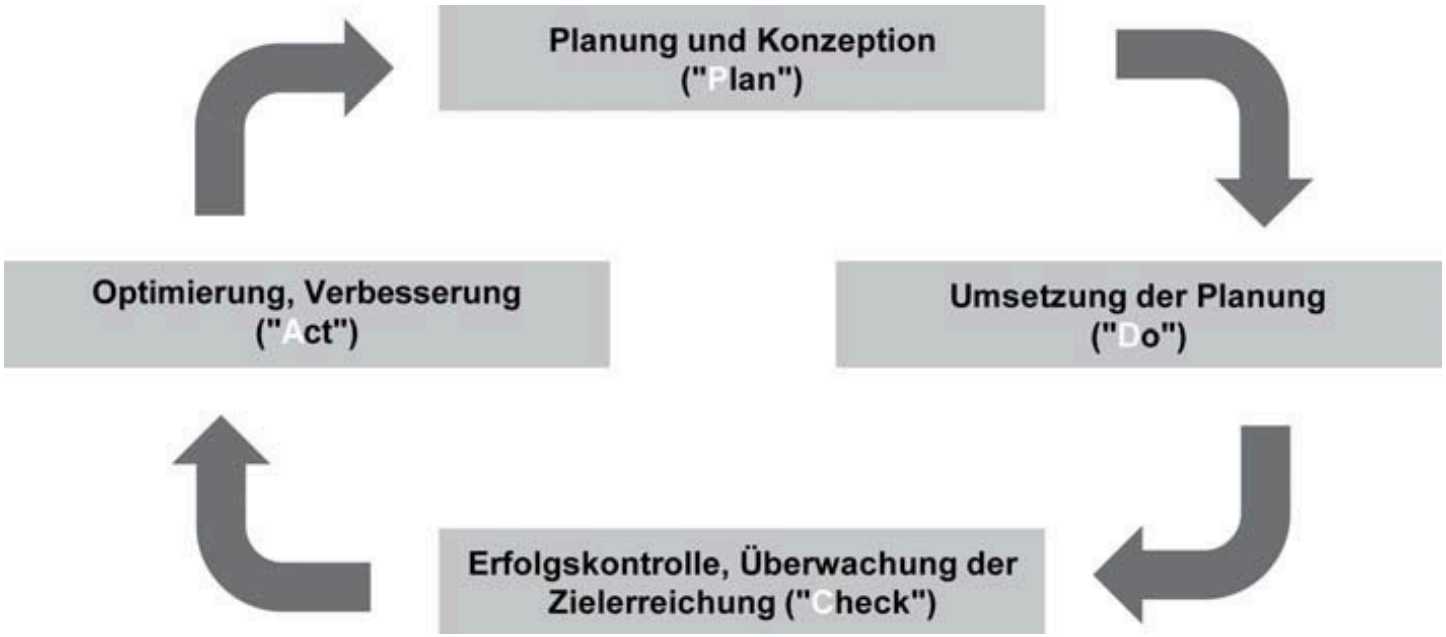
IT-Risikomanagement-Prozess

- Schlussendlich sind alle Ansätze ähnlich aufgebaut
  - Risikoidentifikation
  - Risikobewertung
  - Risikobehandlung/-steuerung
  - Risikokontrolle

- Wiederholter, immer wiederkehrender Durchlauf der Phasen!

Informationssicherheitsprozess

Sicherheitsprozess unterliegt einem Lebenszyklus; Darstellung als PDCA-Modell



(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

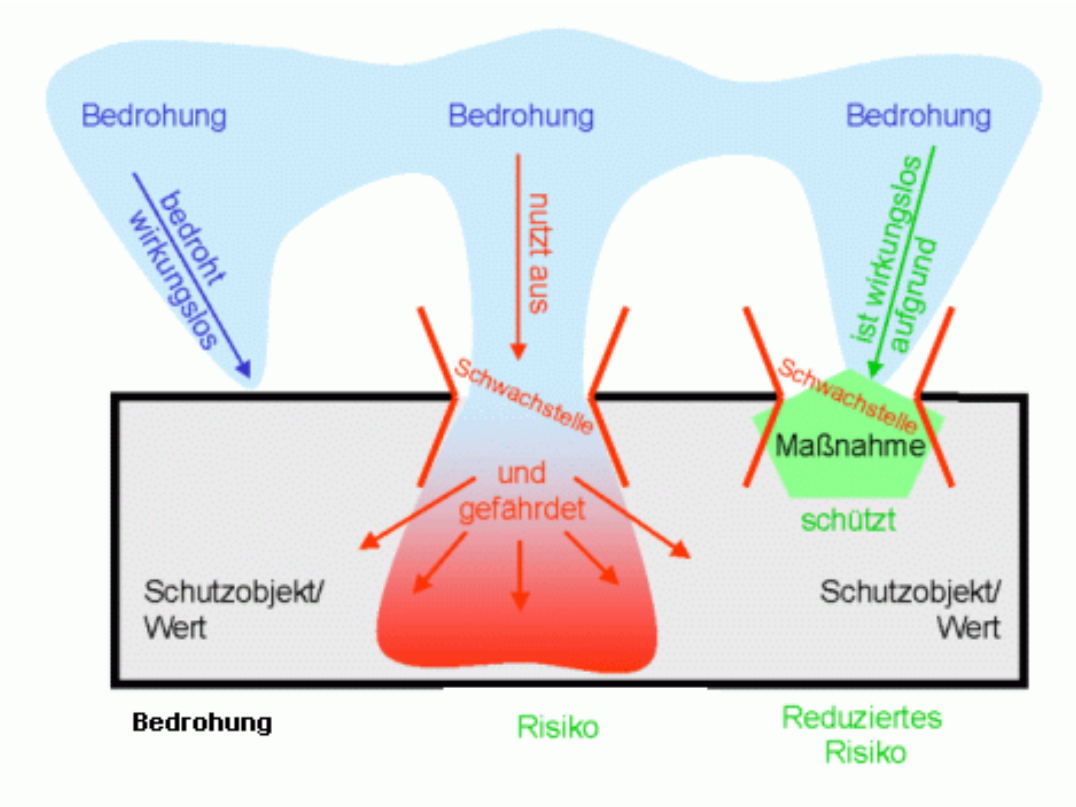
Vorarbeiten zur Risikoanalyse

- 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 Verantwortlichkeiten
  - Festlegung der Review-Zyklen

Risikoidentifikation

- Erkennung von Risiken
- Eindeutige Beschreibung des Risikos
- Eingangsparameter wie Schwachstellen und Bedrohungen
- Erfassung geplanter oder realisierter Maßnahmen
- 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 Risikoidentifkation

- 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 erwarteteten 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 Unternehmensleitung
- Das beinhaltet
  - die Ergebnisse der operativen und strategischen Kontrollen fortlaufend auszuwerten
  - eine transparante 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 meiner Organisation wie schützen?

Teilaspekte dieser zentralen Frage der IT-Sicherheit

- Welche Daten/Komponenten sind in meiner Organisation schützenswert?
- Welche Aspekte davon müssen geschützt werden?
- Wie werden Sicherheitsmaßnahmen umgesetzt?
- Wie erfahre ich dies effizient?
- Was ist Best-Practise?
- 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

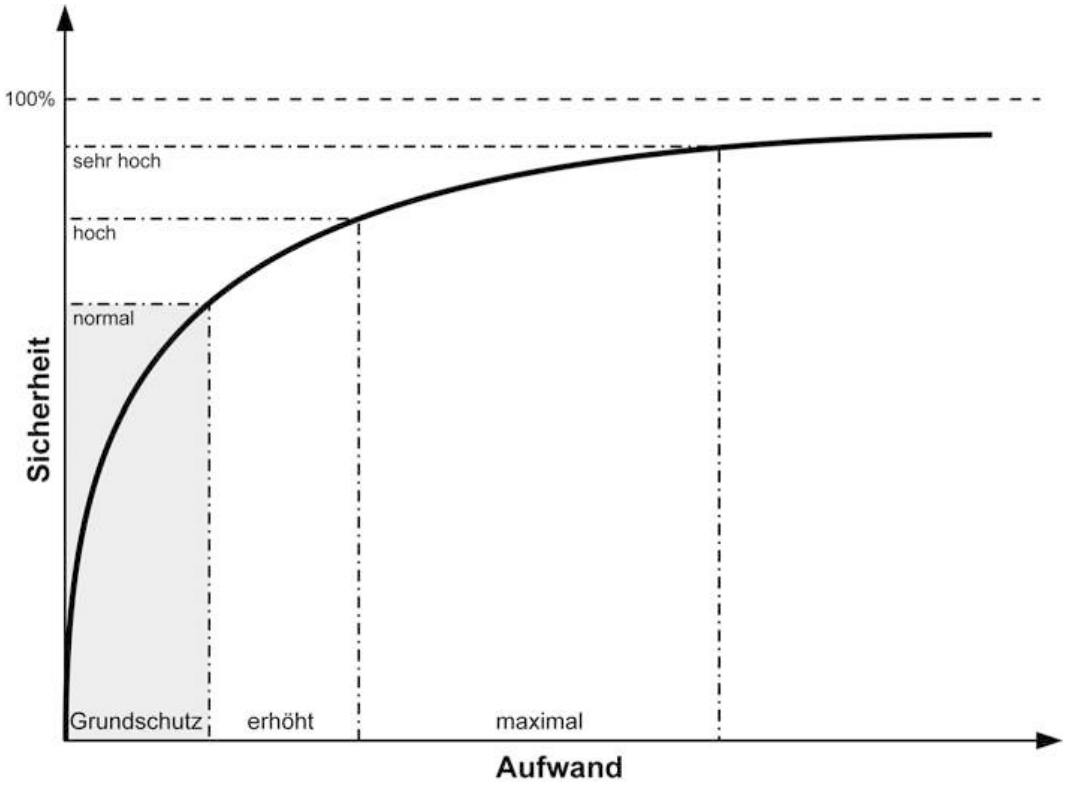
- Herausgegeben vom BSI, Deutschland
- „Kochbuch“ für normales Schutzniveau
- Praktikable Durchführung von IT-Sicherheitsanalysen
- Kosteneffektive Erhöhung des IT-Sicherheitsniveaus
  - Schnelle Identifizierung von Sicherheitsmaßnahmen
  - Schnelle Umsetzung von Sicherheitsmaßnahmen
- Angemessener Schutz durch Kombination von organisatorischen, personellen, infrastrukturellen & 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 100-1: Managementsysteme für Informationssicherheit (ISMS)
  - BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
  - BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
  - BSI-Standard 100-4: Notfallmanagement
- IT-Grundschutzkataloge

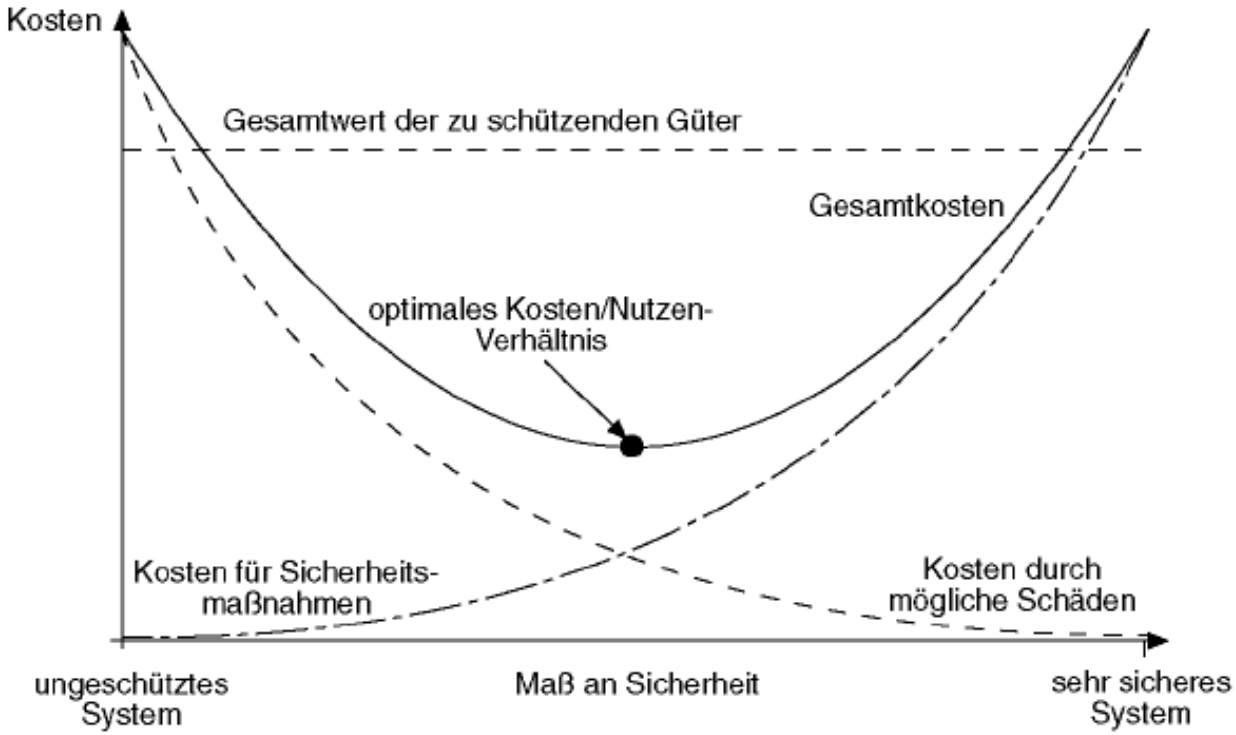
Aufwand-Nutzen-Relation

Verhältnis zwischen Aufwand zur Erhöhung des Sicherheitsniveaus und erreichtem Sicherheitsgewinn wird immer ungünstiger



(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Wiederholung: Kosten-/Nutzenanalyse



(Vergleiche M. Raepple: Sicherheitskonzepte für das Internet)

Aufbau der IT-Grundschutzkataloge

- Einführung
- IT-Grundschutz – Basis für Informationssicherheit
- Schichtenmodell und Modellierung
- Bausteine
- Gefährdungskataloge
- Maßnahmenkataloge
- Hilfsmittel

`https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html`

Der IT-Sicherheitsprozess laut IT-Grundschutz

- Initiierung des Sicherheitsprozesses
  - Verantwortung der Leitungsebene
  - Konzeption und Planung
  - Aufbau einer Informationssicherheitsorganisation
  - Bereitstellung von Ressourcen
  - Einbeziehung aller MitarbeiterInnen
- Erstellung einer Sicherheitskonzeption
- Umsetzung der Sicherheitskonzeption
- Aufrechterhaltung und Verbesserung

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Auszug Ablauf Erstellung eines IT-Sicherheitskonzepts

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung des Verbunds (Auswahl der Maßnahmen)
- Basis-Sicherheitscheck (Soll-Ist-Vergleich)
- Ergänzende Sicherheitsanalyse

Ablauf Erstellung eines IT-Sicherheitskonzepts

- *Strukturanalyse*
- Schutzbedarfsfeststellung
- Modellierung des Verbunds (Auswahl der Maßnahmen)
- Basis-Sicherheitscheck (Soll-Ist-Vergleich)
- Ergänzende Sicherheitsanalyse

IT-Strukturanalyse

„Erfassung der Bestandteile (Informationen, Anwendungen, IT-Systeme, Räume, Kommunikationsnetze), die zur Erfüllung der im Geltungsbereich festgelegten Geschäftsprozesse oder Fachaufgaben benötigt werden.“

- Erfassung der Anwendungen und der zugehörigen Informationen; z.B. Personaldatenverarbeitung
- Netzplanerhebung; z.B. Switches, Router
- Erhebung der IT-Systeme; z.B. Server für Personalverwaltung
- Erfassung der Räume; z.B. Serverraum
- Komplexitätsreduktion durch Gruppenbildung

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.*

Erfassung der Anwendungen

Erfassung von Anwendungen und Informationen, die für die betrachteten Geschäftsprozesse oder Fachaufgaben erforderlich sind

Nr	Anwendung	Art der Information	Verantwortlich	Benutzer	Geschäftsprozess
A1	Personaldatenverarbeitung	P	Z1	Z1	GP0-1, GP0-2
A2	Beihilfeabwicklung	P	Z2	alle	GP0-2
A3	Reisekostenabrechnung	P/V/F	Z2	alle	GP0-1, GP0-3
A4	Benutzer-Authentisierung	P/S	IT1	alle	GP0, GP5, GP6
A5	Systemmanagement	S	IT3	IT3	alle
A6	Bürokommunikation	P/V/F/S	IT3	alle	alle
A7	zentrale Dokumentenverwaltung	P/V/F/S	Z1	alle	GP0, GP5
A8	USB-Sticks zum Datenaustausch	P/V/F	IT3	IT3	GP0-1,GP0-3

P=personenbezogene D./V=verwaltungsspezifische D./F=fachliche Informationen,S=systemspezifische/technische Informationen

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Erhebung der IT-Systeme

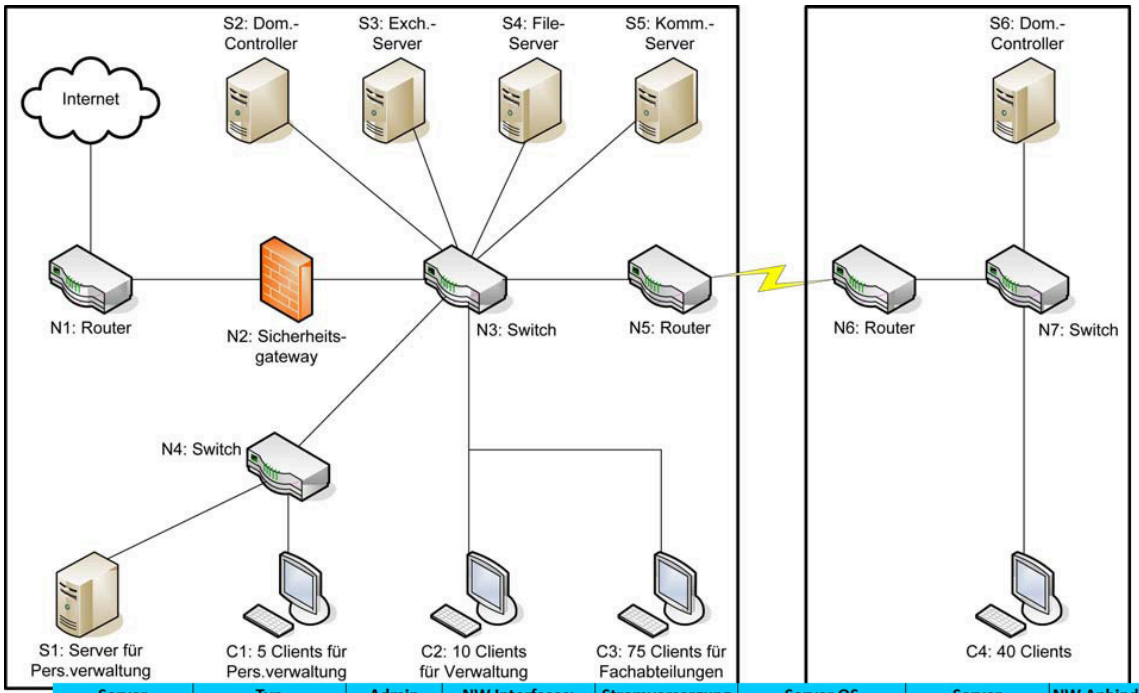
Erfassung von vernetzten als auch von nicht vernetzten IT-Systemen

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Anwender
S1	Server für Personalverwaltung	Windows Server 2003	1	Bonn,R 1.01	in Betrieb	Personalreferat
S2	Domänen-Controller	Windows Server 2008	1	Bonn,R 3.10	in Betrieb	alle IT-Anwender
C1	Gruppe von Clients der Personal-datenverarbeiung	Windows XP SP3	5	Bonn,R. 1.02.-1.06	in Betrieb	Personalreferat
C2	Gruppe von Clients in der Ver-waltungsabteilung	Windows 7	10	Bonn,R1.07-1.16	in Betrieb	Verwaltungs-abteilung
C6	Gruppe der Laptops für Berlin	Laptop unter Windows 7	2	Berlin,R 2.01	in Betrieb	alle IT-Anwender in Aussenstelle Berlin

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Netzplanerhebung

Graphische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung



Liege

Server	Typ	Admin	NW Interfaces; Anzahl, Typ	Stromversorgung Standard/USV	Server OS	Server Patchlevel	NW Anbindung über Switch/Router, Port	Standort/Raumnummer
S1	SRV für Pers.Verwaltg	A1	1, GB	Ja	WinServer 2003, SP2	Sep.08	N4/1/17	GER-BO/RO01-B06/CH01/01
S2	DOM Controller	A2	1, GB	Ja	WinServer 2003, SP2	Sep.08	N3/1/18	GER-BO/RO01-B06/CH01/02
S3	Exchange Server	A1	1, GB	Ja	WinServer 2003, SP2	Sep.08	N3/2/17	GER-BO/RO01-B06/CH01/03
S4	File Server	A3	1, GB	Ja	WinServer 2003, SP2	Sep.08	N3/2/18	GER-BO/RO01-B06/CH01/04

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Ablauf Erstellung eines IT-Sicherheitskonzepts

- Strukturanalyse
- *Schutzbedarfsfeststellung*
- Modellierung des Verbunds (Auswahl der Maßnahmen)
- Basis-Sicherheitscheck (Soll-Ist-Vergleich)
- Ergänzende Sicherheitsanalyse

Grundlagen zur Schutzbedarfsfeststellung

- Ermittlung welcher Schutz für Informationen und Informationstechnik ausreichend und angemessen ist
- Definition der Schutzbedarfskategorien
- Schutzbedarfsfeststellung für Anwendungen
- Schutzbedarfsfeststellung für IT-Systeme
- Schutzbedarfsfeststellung für Räume
- Schutzbedarfsfeststellung für Kommunikationsverbindungen
- Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Schutzbedarfskategorien

Qualitative Aussage des Schutzbedarfs durch Unterteilung in z.B. drei Kategorien

Schutzbedarf		Bsp. Verfügbarkeit
"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.	> 1 Tag
"hoch"	Die Schadensauswirkungen können beträchtlich sein.	1 Tag
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches,katastrophales Ausmaß erreichen.	< 1 Stunde

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Anwendung auf Schutzziele, z.B. Vertraulichkeit, Integrität und Verfügbarkeit

Beispiel-Dokumentation Schutzbedarfsfeststellung

Anwendungen

„Was wäre, wenn. . . ?“ – realistische Schadensszenarien werden aus Sicht der AnwenderInnen entwickelt

Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grundwert**	**Schutz-bedarf**	**Begründung**
A1	Personaldaten-verarbeitung	X	Vertrau-lichkeit	hoch	Personaldaten sind besonders schutz-bedürftige personenbezogene Daten, deren Bekanntwerden die Betroffenen erheblich beeinträchtigen können.
			Integrität	normal	Der Schutzbedarf ist normal, da Fehler rasch erkannt und die Daten nachträg-lich korrigiert werden können.
			Verfüg-barkeit	normal	Ausfälle bis zu einer Woche können mittels manueller Verfahren über-brückt werden.

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

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

Beispiel-Dokumentation Schutzbedarfsfeststellung IT-Systeme

IT-System		Schutzbedarfsfeststellung		
Nr	**Beschreibung**	**Grundwert**	**Schutz bedarf**	**Begründung**
S1	Server für Personal-verwaltung	Vertrau-lichkeit	hoch	Maximumprinzip
		Integrität	normal	Maximumprinzip
		Verfügbar-keit	normal	Maximumprinzip
S2	Domänen-Controller	Vertrau-lichkeit	normal	Maximumprinzip
		Integrität	hoch	Maximumprinzip
		Verfügbar-keit	normal	Gemäß der Schutzbedarfsfeststellung für Anwen-dung A4 ist von einem hohen Schutzbedarf für diesen Grundwert auszugehen. Zu berücksichti-gen ist aber, dass diese Anwendung auf zwei Rechnersysteme verteilt ist. Eine Authentisierung über den zweiten Domänen-Controller S6 in Berlin ist für die Mitarbeiter des Bonner Stan-dortes ebenfalls möglich. Ein Ausfall des Domä-nen-Controllers S2 kann bis zu 72 Stunden

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Beispiel-Dokumentation Schutzbedarfsfeststellung Räume

Ermittlung aufgrund der Ergebnisse der Schutzbedarfsfeststellung der Anwendungen und der IT-Systeme

Raum			IT / Informationen	Schutzbedarf		
Bezeich-nung	**Art**	**Lokation**	**IT-Systeme / Datenträger**	**Vertrau lichkeit**	**Integri-tät**	**Verfüg-barkeit**
R U.02	Datenträger-archiv	Gebäude Bonn	Backup-Datenträger (Wochensicherung der Server S1 bis S5)	hoch	hoch	normal
R B.02	Technikraum	Gebäude Bonn	TK-Anlage	normal	normal	hoch
R 1.01	Serverraum	Gebäude Bonn	S1, N4	hoch	hoch	normal
R 1.02 - R 1.06	Büroräume	Gebäude Bonn	C1	hoch	normal	normal
R 3.11	Schutzschrank im Raum R 3.11	Gebäude Bonn	Backup-Datenträger (Tagessicherung der Server S1 bis S5)	hoch	hoch	normal
R E.03	Serverraum	Gebäude Berlin	S6, N6, N7	normal	hoch	hoch
R 2.01 - R 2.40	Büroräume	Gebäude Berlin	C4, einige mit Faxgeräten	normal	normal	normal

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Schutzbedarfsfeststellung für Kommunikationsverbindungen

- Netzplan als Grundlage
- Untersuchung ausgewählter Kommunikationsverbindungen
  - Außenverbindungen
  - Übertragung hochschutzbedürftiger Informationen
  - Verbot der Übertragung bestimmter hochschutzbedürftiger Informationen

Schlussfolgerungen aus der Schutzbedarfsfeststellung

- Ergebnisse der Schutzbedarfsfeststellung bieten Anhaltspunkt für weitere Vorgehensweise

Schutzbedarf normal Standard-Sicherheitmaßnahmen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.

Schutzbedarf hoch Standard-Sicherheitmaßnahmen bilden einen Basisschutz, sind aber u.U. alleine nicht ausreichend. Weitergehende Maßnahmen können auf Basis einer ergänzenden Sicherheitsanalyse ermittelt werden.

Schutzbedarf sehr hoch Standard-Sicherheitmaßnahmen bilden einen Basisschutz, reichen aber alleine i.A. nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer ergänzenden Sicherheitsanalyse ermittelt werden.

Ergänzende Sicherheitsanalyse bei erhöhtem Schutzbedarf!

Ablauf Erstellung eines IT-Sicherheitskonzepts

- Strukturanalyse
- Schutzbedarfsfeststellung
- *Modellierung des Verbunds (Auswahl der Maßnahmen)*
- Basis-Sicherheitscheck (Soll-Ist-Vergleich)
- Ergänzende Sicherheitsanalyse

Modellierung laut IT-Grundschutz – Auswahl der Maßnahmen

- 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 `https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Bausteine/bausteine_node.html`)

Abbildung des IT-Verbundes: Zuordnung Bausteine zu Zielobjekten

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Ansprechpartner	Hinweise
B 1.1	Organisation	Standort Bonn		Der Baustein Organisation muss für die Standorte Bonn und Berlin separat bearbeitet werden, da in Berlin eigene organisatorische Regelungen gelten.
B 1.1	Organisation	Standort Berlin		
B 1.2	Personal	gesamtes BOV		Die Personalverwaltung des BOV erfolgt zentral in Bonn.
B 2.5	Datenträgerarchiv	R U.02 (Bonn)		In diesem Raum werden die Backup-Datenträger aufbewahrt.
B 3.203	Laptop	C5		Die Laptops in Bonn bzw. Berlin werden jeweils in einer Gruppe zusammengefasst.
B 3.203	Laptop	C6		
B 5.4	Webserver	S5		S5 dient als Server für das Intranet.
B 5.7	Datenbanken	S5		Auf dem Server S5 kommt eine Datenbank zum Einsatz.

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

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

Ablauf Erstellung eines IT-Sicherheitskonzepts

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung des Verbunds (Auswahl der Maßnahmen)
- *Basis-Sicherheitscheck (Soll-Ist-Vergleich)*
- Ergänzende Sicherheitsanalyse

Basis-Sicherheitscheck – Soll-Ist-Vergleich der Maßnahmen

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

Beispiel für Dokumentation Basis-Sicherheitscheck

4.4 Schutzschrank (Serverraum, Hauptstrasse 1, 1. Stock)						
Maßnahme (Priorität)	**Baustein**	**E**	**J**	**T**	**N**	**Bemerkung/ Begründung für Nicht-Umsetzung**
M 1.7 (2)	Handfeuerlöscher		X			
M 1.8 (2)	Raumbelegung unter Berücksichtigung von Brandlasten				X	Unterhalb des Serverraums befindet sich das Lager für Büromaterialien (u.a. Papier)
M 1.15 (1)	Geschlossene Fenster und Türen		X			Außenfenster ist immer geschlossen;
M 2.6 (1)	Vergabe von Zutrittsberechtigungen			X		Zutrittsberechtigung erfolgt über die Zutrittsberechtigung für den Serverraum selbst; Zutrittsregelung erfolgt durch Schlüsselvergabe; Zutrittsregelung ist an der Tür gekennzeichnet; Der Schutzschrank selbst ist aber unverschlossen;

(Vergleiche BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise)

Ablauf Erstellung eines IT-Sicherheitskonzepts

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung des Verbunds (Auswahl der Maßnahmen)
- Basis-Sicherheitscheck (Soll-Ist-Vergleich)
- *Ergänzende Sicherheitsanalyse*

Ergänzende Sicherheitsanalyse

- Gegebenenfalls ist Durchführung einer ergänzenden Sicherheitsanalyse erforderlich
- Siehe Schlussforderungen aus Schutzbedarfsanalyse
- Aber auch, wenn z.B. kein Baustein vorhanden ist

Zertifizierung nach ISO 27001

- Zertifizierung optional möglich

- Nachweis, dass Maßnahmen gemäß IT-Grundschutz realisiert wurden
- Zusicherung von Informationssicherheit an Kooperationspartner
- 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: http://doi.ieeecomputersociety.org/10.1109/MC.2004.1297316

Literatur – 3/3

- BSI. Grundschutz, 2013. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz-Standards, 2013. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html
- 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
  - Erstellung eines Sicherheitskonzepts nach IT-Grundschutz
  - IT-Sturkturanalyse, Schutzbedarfsfeststellung, Modellierung des Verbunds, Basis-Sicheheitscheck, Ergänzende Sicherheitsanalyse

Vielen Dank!

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