



IT-Grundschutz – die Basis für ihre IT-Sicherheit

Grundschutz Analyse Herausforderungen & Vorgehen





IT-Sicherheit ist... gefährdet

- **Höhere Gewalt:** Feuer, Wasser, Blitzschlag, Krankheit, ...
- **Organisatorische Mängel:** Fehlende oder unklare Regelungen, fehlende Konzepte, ...
- **Menschliche Fehlhandlungen:** "Die größte Sicherheitslücke sitzt oft vor der Tastatur"
- **Technisches Versagen:** Systemabsturz, Plattencrash, ...
- **Vorsätzliche Handlungen:** Hacker, Viren, Trojaner, ...



IT-Sicherheit ist notwendig... Schadensbilanz

- **Anzahl** der Sicherheitsvorfälle steigt stetig:
 - 75 % aller Unternehmen hatten im letzten Jahr Vorfälle mit geschäftsschädigenden Auswirkungen.
- **Schadenshöhe** eines Einzelschadens:
 - Maximum: hohe zweistellige Mio-Beträge
 - Durchschnitt: 5-6-stellige Beträge
- **Art der Schäden:**
 - größtes Einzelproblem: Computerviren
 - überwiegend ist der Grundwert Verfügbarkeit betroffen.
 - Überwiegende Mehrheit aller Vorfälle ist kein gezielter Angriff.
 - Rangfolge der Ursachen: Mensch, Technik, Umwelt



Typische Probleme in der Praxis

... Wie gehe ich damit um

- Resignation, Fatalismus und Verdrängung
- Kommunikationsprobleme
- Sicherheit wird als technisches Problem mit technischen Lösungen gesehen
- Zielkonflikte: Sicherheit, Bequemlichkeit, Kosten
- unsystematisches Vorgehen bzw. falsche Methodik
- Management: fehlendes Interesse, schlechtes Vorbild
- Sicherheitskonzepte richten sich an Experten, der IT-Benutzer wird vergessen.



Konsequenzen fehlender Regelungen ...oder: Jeder tut, was er will!

- Konfusion im Notfall
 - Was ist zu tun? Wer hilft?
- lückenhafte Datensicherung
 - Notebooks, Heimarbeitsplätze, lokale Datenhaltung
- fehlende Klassifizierung von Informationen
 - Verschlüsselung, Weitergabe und Austausch von Informationen
- gefährliche Internetnutzung
 - Was alle machen kann doch nicht unsicher sein...?
- Disziplinlosigkeit
 - Ignoranz und Arroganz statt geregelter Prozesse
 - Konsequenzen bleiben aus, sind zu hart, sind willkürlich



Übersicht über den IT-Sicherheitsprozess (I/2)

1

Initiative der
Geschäftsführung

- Analyse: Geschäftsprozesse, Unternehmensziele
- IT-Sicherheitsleitlinie
- IT-Sicherheitsorganisation

2

Analyse der
Rahmen-
bedingungen

- Informationen, IT-Systeme, Anwendungen
- Schutzbedarf (Szenarien)

3

Sicherheitscheck

- Sicherheitsmaßnahmen
- Identifikation von Sicherheitslücken



Übersicht über den IT-Sicherheitsprozess (2/2)

4

Planung von
Maßnahmen

- Liste geeigneter Maßnahmen
- Kosten- und Nutzenanalyse
- Auswahl umzusetzender Maßnahmen
- Dokumentation des Restrisikos

5

Umsetzung von
Maßnahmen

- Implementierung
- Test
- Notfallvorsorge

6

Sicherheit im
laufenden Betrieb

- Sensibilisierung
- Schulung
- Audit, Kontrollen, Monitoring, Revision
- Notfallvorsorge



Methodik für IT-Sicherheit

Viele Wege führen zur IT-Sicherheit...



Welcher Weg ist der effektivste?



Risikoanalyse

Definition:

(engl. Risk Assessment/Analysis): Untersuchung, wie wahrscheinlich das Eintreten eines bestimmten Schadens ist und welche negativen Folgen der Schaden hätte.

Probleme:

- ungenaue Eingangsgrößen
- hoher Zeitaufwand
- teuer
- individuelle Betrachtung nötig



IT-Grundschutzhandbuch

Prinzipien

- Gesamtsystem enthält **typische** Komponenten (Server, Clients, Serverraum, E-Mail...)
- **Pauschalisierte** Gefährdungen und Eintrittswahrscheinlichkeiten, keine klassische Risikoanalyse
- Empfehlung von **Standard**-Sicherheitsmaßnahmen



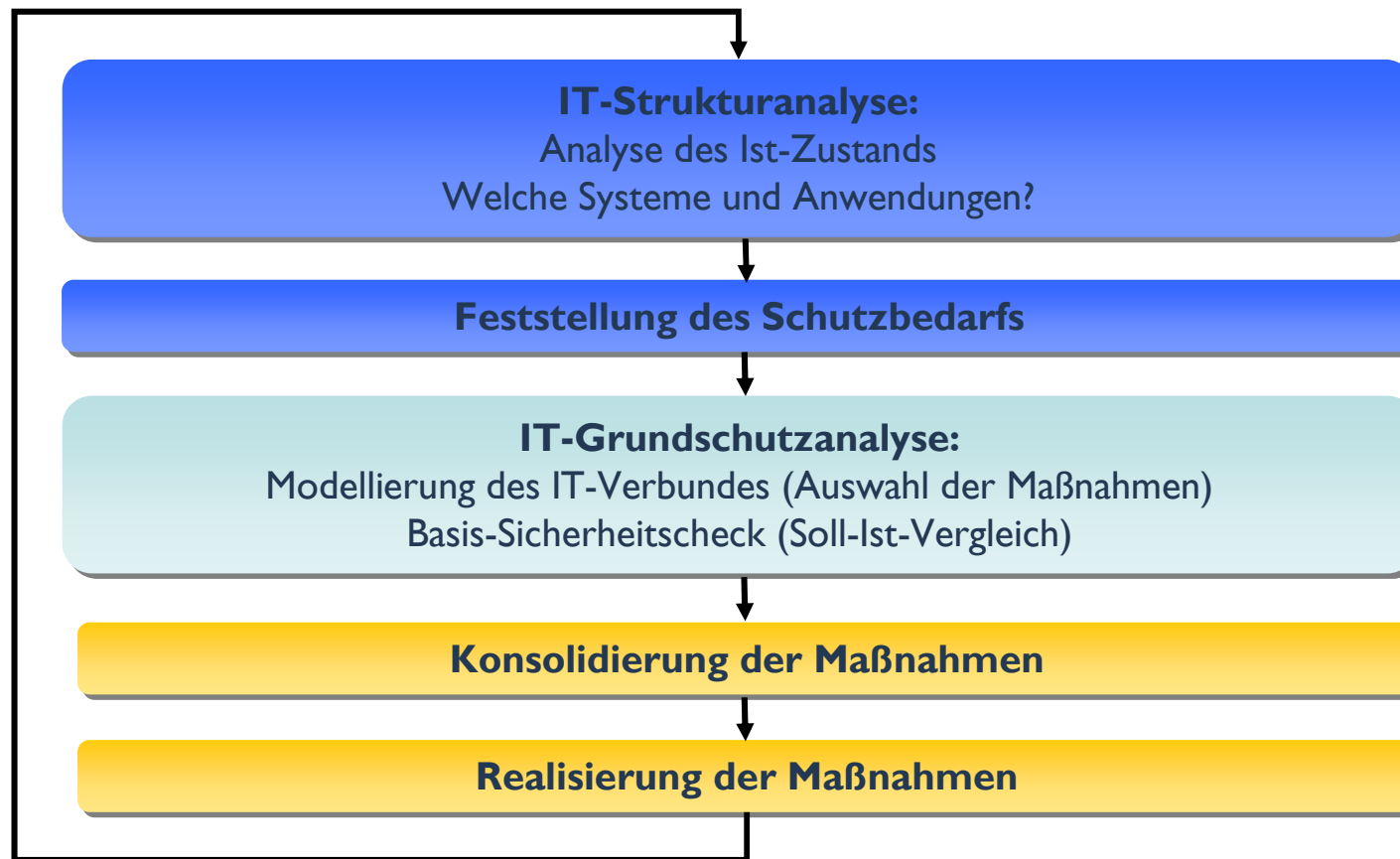
IT-Grundschutz

Vorteile

- arbeitsökonomische Anwendungsweise durch **Soll-Ist-Vergleich**
- kompakte IT-Sicherheitskonzepte durch Verweis auf **Referenzquelle**
- praxiserprobte, meist kostengünstige Maßnahmen mit hoher **Wirksamkeit**
- **Erweiterbarkeit** und **Aktualisierbarkeit**

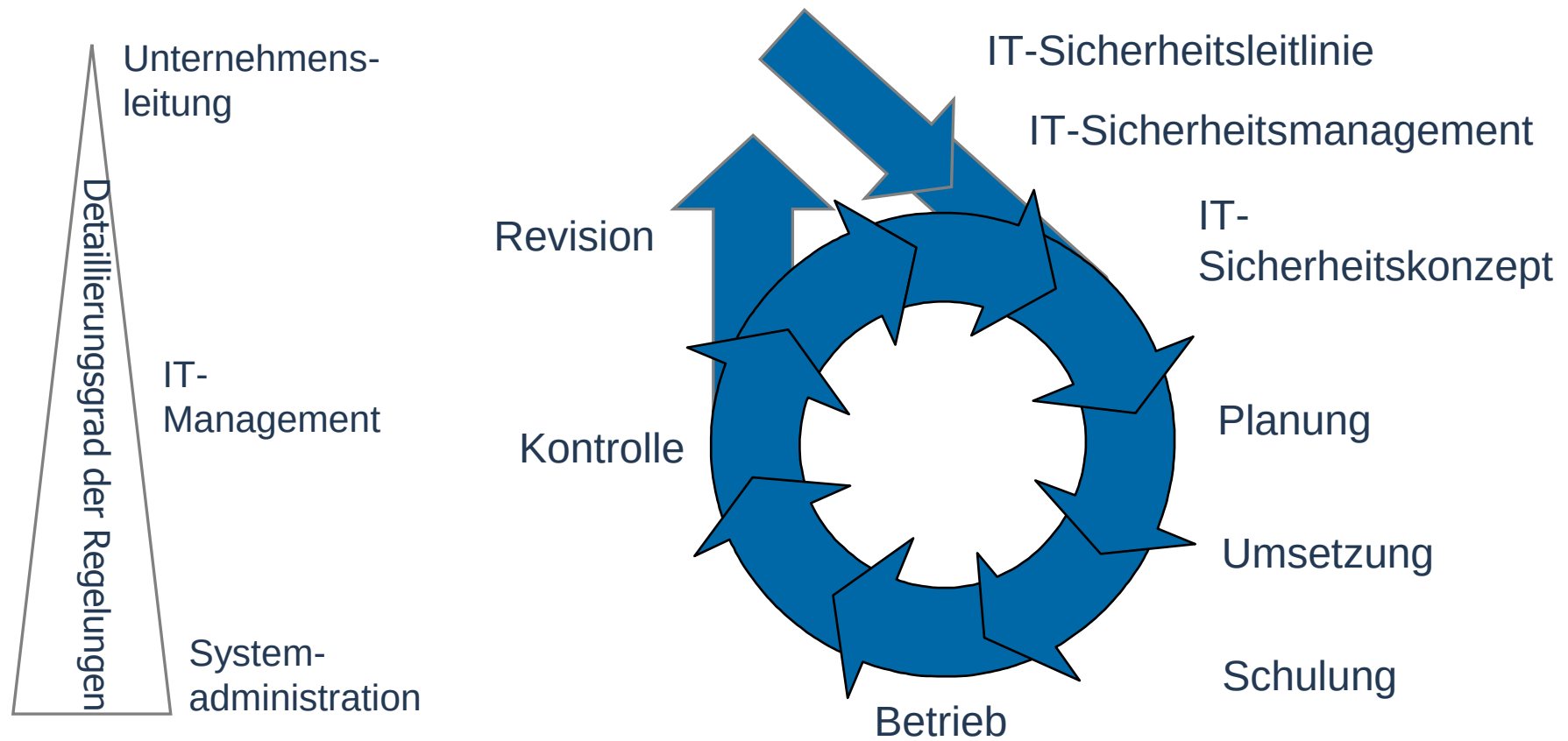


Erstellung und Realisierung eines IT-Sicherheitskonzepts





IT-Sicherheitsprozess





Vorgehen zur Durchführung eines IT Audits

- Festlegung des IT-Verbunds
- Durchführung der Erhebungsphase gemäß den Richtlinien des BSI Grundschutzhandbuchs
- Schutzbedarfsfeststellung
- Modellierung des IT-Verbunds und Durchführung des Sicherheitschecks
- Unterstützung bei der Umsetzung fehlender IT-Sicherheitsmaßnahmen



Referenzen



Freude am Fahren



Kabel Deutschland



Handwerkskammer
Braunschweig



Mercure
ACCOR hotels



mepha



HELVETIA
PATRIA



DIS AG
Viel mehr als Zeitarbeit.



ikk



BSAG Gut informiert ... bei uns zu Gast



Kontakt!

GEDS General Enterprise Data Systems

Waldweg 13

D-30900 Wedemark, Germany

Tel: +49 (0)5072 7726894

Fax: +49 (0)5072 770081

E-Mail: geds@kapur.eu

Homepage: www.geds.kapur.eu