IT-Grundschutz Profile:
Beispiele zur Anwendung des IT-Grundschutzes für ein effektives IT-Sicherheitsmanagement

Dr. Lydia Tsintsifa

Bundesamt für Sicherheit in der Informationstechnik

IT-Symposium 2005
07.04.2005

Agenda

- IT-Sicherheitsmanagement mit IT-Grundschutz
- IT-Grundschutz Profile: Motivation und Überblick
- Vorstellung der einzelne Profile
  - Rahmenbedingungen
  - Vorgehen und Inhalt
- Zusammenfassung

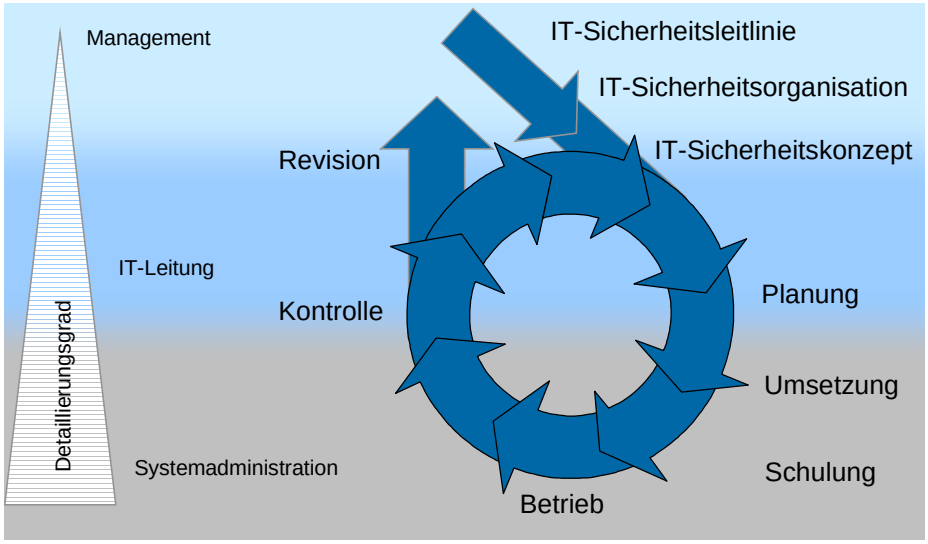
IT-Sicherheitsmanagement mit IT-Grundschutz (1)

- **IT-Sicherheitsmanagement** (=Systematisches Vorgehen zum Erreichen eines angemessenen IT-Sicherheitsniveaus in Bezug auf Verfügbarkeit, Integrität, Vertraulichkeit)
- Optimaler Einsatz der Ressourcen für IT-Sicherheit
- Optimierung der internen Prozesse führt zu einem geordneten, effektiven und effizienten IT-Betrieb --> mittelfristige Kosteneinsparungen
- Attraktivität für Kunden und Geschäftspartner durch Vertrauen
- Versicherungen honorieren zunehmend IT-Sicherheit

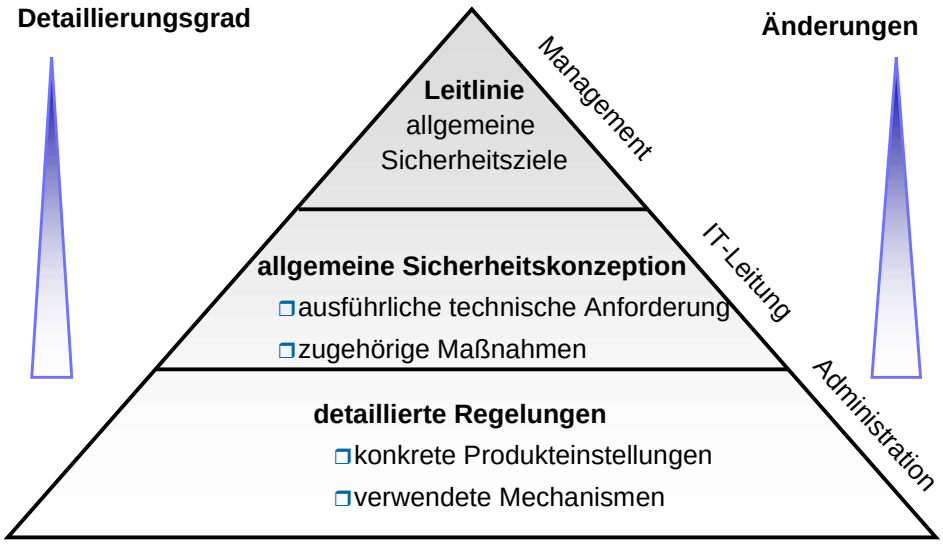
IT-Sicherheitsmanagement mit IT-Grundschutz (2)

- **Aus den Unternehmenszielen werden die Sicherheitsziele festgelegt**
  - Schutz der unternehmenskritischen Werte in Bezug auf:
    - Verfügbarkeit
    - Integrität
    - Vertraulichkeit
- Welches Schutzniveau ist für jeden dieser Aspekte angemessen? (Kosten - Nutzen Verhältnis)
- Hier bedarf es einer verbindlichen Aussage der **Geschäftsführung!**
- Nutzung von Referenzwerken und Standards erhöht die Effizienz

IT-Grundschutz
Der Sicherheitsprozess

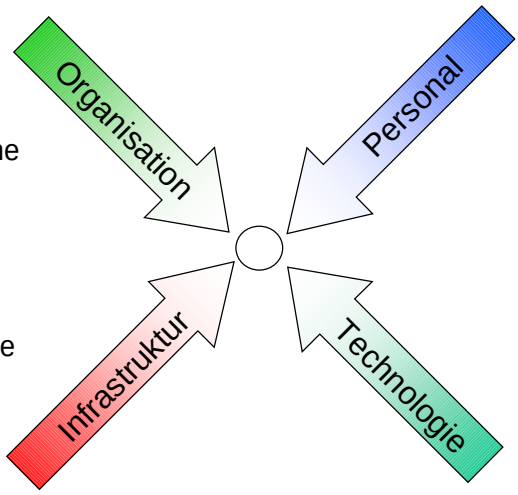


IT-Sicherheitsmanagement
Dokumente und Richtlinien

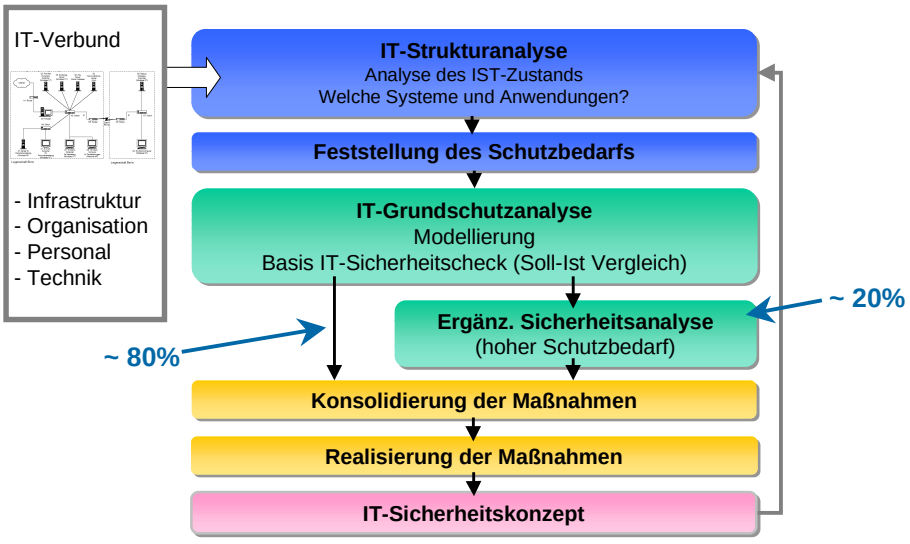


IT-Grundschutz
Erstellung des IT-Sicherheitskonzeptes

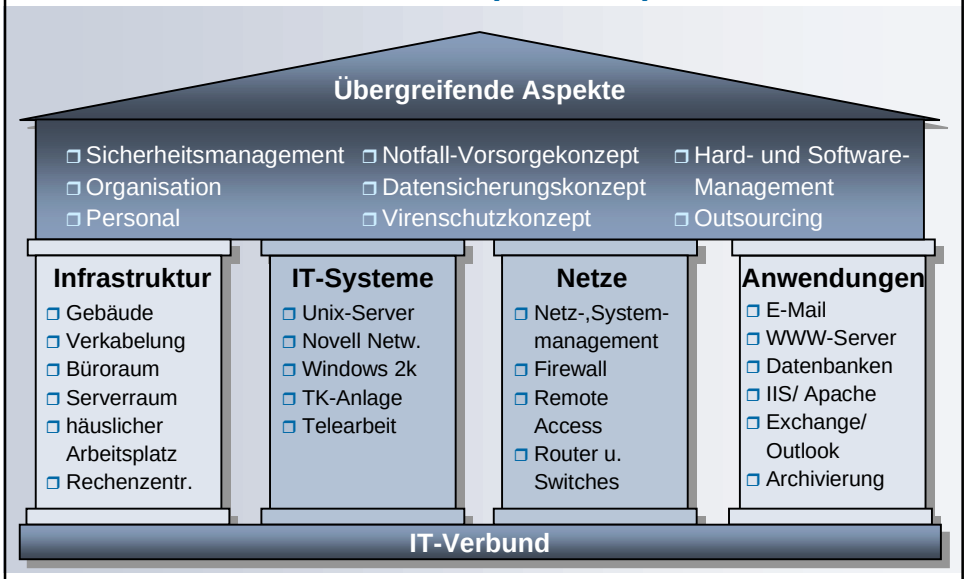
- Aufbau eines **Standard-Sicherheitsniveaus**, das auch für sensiblere Bereiche **ausbaufähig** ist
- Infrastrukturelle, organisatorische, personelle und technische **Standard-Sicherheitsmaßnahmen**



IT-Grundschutz
Erstellung des IT-Sicherheitskonzeptes



IT-Grundschutzhandbuch
Bausteine (Auswahl)



IT-Grundschutz Zertifizierung

Was kann zertifiziert werden?

- Ein oder mehrere Geschäftsprozesse
- Eine oder mehrere Fachaufgaben
- Eine oder mehrere Organisationseinheiten

- Es braucht nicht gleich das gesamte Unternehmen zu sein!

Bedingung:

- IT-Verbund muss eine sinnvolle Mindestgröße haben!

IT-Grundschutz Zertifizierung
Aktuell

Stand Februar 2005

- 11 Zertifikate erteilt
  - Sehr unterschiedliche Unternehmensgrößen
  - Von "10 Server, 4 Gruppen von Clients" bis "Rechenzentrum mit 800 Servern"
  - Branchen: IT-Firmen, Dienstleister, Banken

Materialien und Tools

- IT-Grundschutzhandbuch
- Webkurs IT-Grundschutz
- Leitfaden IT-Sicherheit
- GSTOOL
- Risikoanalyse auf der Basis von IT-Grundschutz
- Musterrichtlinien
- IT-Grundschutz Profile

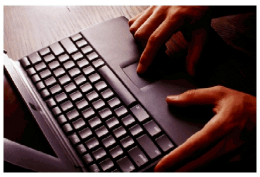
- **www.bsi.de**

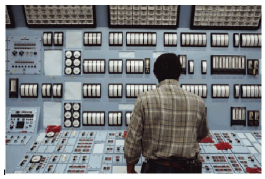
IT-Grundschutz Profile
Motivation

- Umfrage unter allen IT-Grundschutz-Anwendern (2003)
- Großes Interesse für die IT-Grundschutz Zertifizierung
- Viele Fragen an der Grundschutz-Hotline, insbesondere zu den Themen:
  - Modellierung eines konkreten IT-Verbundes
  - Einsatz des GSTOOL
  - Zertifizierung eines konkreten IT-Verbundes nach IT-Grundschutz

IT-Grundschutz Profile
Überblick

- **IT-Grundschutz Profile:** Beispiele für die Anwendung der Vorgehensweise nach IT-Grundschutzhandbuch
- Veröffentlicht seit November 2004





- 3 Beispiele: kleine, mittlere, große Institution
- Download unter: www.bsi.bund.de/gshb/

Profil für eine kleine Institution

- Anwendergruppe: Steuerberaterbüro, Anwaltskanzlei, kleine Behörde,...
- Voraussetzungen: Wenige IT-Systeme, geringes IT-Sicherheitswissen
- „einfache“ Vorgehensweise, Verwendung von Checklisten und Beispielen
- Geschäftsinteresse steht im Vordergrund

Profil für eine kleine Institution

- GSHB-Methodik anhand eines durchgehenden Beispiels :
  - Kleiner Familienbetrieb mit 3 Angestellten
  - Einsatz von PCs und Laptops
  - Führung der Kundenkartei, Erstellung von Angeboten & Rechnungen
- Vorgehen bei der Erstellung des IT-Sicherheitskonzeptes
- Maßgeschneiderte Umsetzung
- Geringer Umfang (ca. 35 Seiten)

Kleine Institution
Verantwortlichkeit

- Leitung trägt die gesamte Verantwortung für IT-Sicherheit
- Verantwortung der Leitung auch für konkrete Aufgaben:
  - Sicherheitsleitlinie erstellen
  - Risikobewertung durchführen
  - PC Pass erstellen
  - Sicherheitsmaßnahmen umsetzen
  - Alle Vorgänge und Maßnahmen dokumentieren
- Hilfsmittel im Dokument: IT-Sicherheitsleitlinie, PC-Pass, Definition von Schutzbedarfsklassen, Checkliste, Maßnahmenlisten

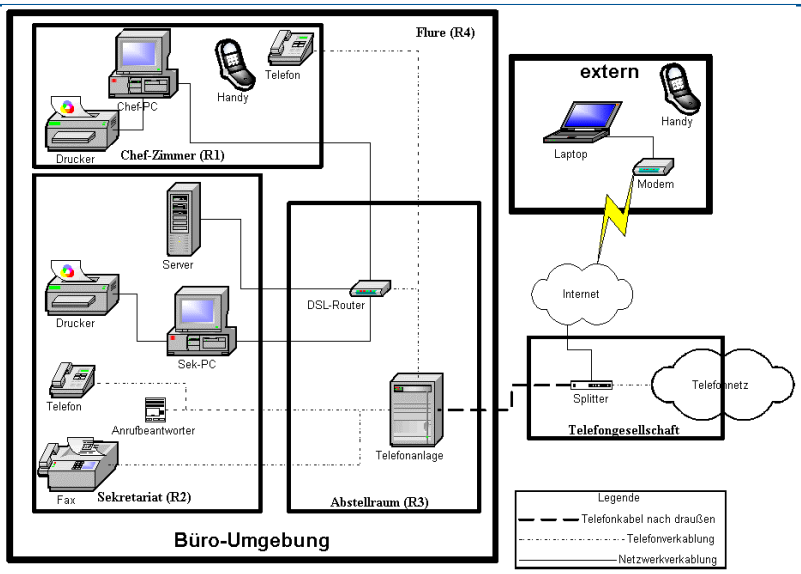
Kleine Institution
IT-Sicherheitsleitlinie

- Umfang von 1,5 Seiten
- Bedeutung von
  - Ausfall der IT (keine bzw. geringe Beeinträchtigung des Geschäftsbetriebs)
  - Verfügbarkeit (Ausfälle nur in geringem Maße tolerierbar)
  - Vertraulichkeit (höchste Ansprüche)
- Institutsleiter übernimmt Rolle des IT-Sicherheitsbeauftragten
- Schulung von Mitarbeitern zu IT-Sicherheitsmaßnahmen
- Hinweise auf Datenschutzgesetz

Kleine Institution
IT-Strukturanalyse

- PC-Pass:
  - Betriebssystem, installierte Software, Administrator
  - Hinweise auf Hardware-, Installations- und Konfigurationsdokumentation
  - Ansprechpartner, Hotline-Nummern
- PC-Pass Einsatz für:
  - alle Systeme
  - weitere Geräte: Telefonanlage, Mobiltelefon, Kopierer, Anrufbeantworter, etc.

Kleine Institution
Netzplan



Kleine Institution
Schutzbedarfsfeststellung

Definition Schutzbedarfskategorien:

- Zwei Schutzbedarfsklassen: normal und hoch
- Beispiel für die Einstufung finanzieller Schäden
- Mögliche Gefahren werden erläutert
- Vorgaben für Schutzbedarfskategorien sind leicht adaptierbar

Vorgehen Schutzbedarfsfeststellung:

- Der Schutzbedarf der Anwendungen wird in den PC-Pass eingetragen
- Der Schutzbedarf für die Systeme wird daraus abgeleitet
- Kommunikationsverbindungen: kritische Internetanbindung des Verbundes
- Schutzbedarf für Räume durch „Vererbung“

Kleine Institution
Modellierung

Nr.	Baustein	anzuwenden auf
Übergeordnete Komponenten		
B 3.0	IT-Sicherheitsmanagement	gesamten IT-Verbund
B 3.1	Organisation	gesamten IT-Verbund
B 3.2	Personal	gesamten IT-Verbund
B 3.4	Datensicherungskonzept	gesamten IT-Verbund
B 3.6	Computer-Virenschutzkonzept	gesamten IT-Verbund
B 3.9	Hard- und Software-Management	gesamten IT-Verbund
B 9.1	Standardsoftware	gesamten IT-Verbund

Kleine Institution
Basis-Sicherheitscheck

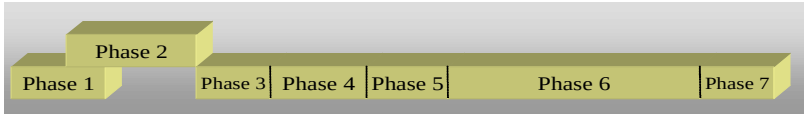
- Welche Standard-Sicherheitsmaßnahmen sind bereits umgesetzt und wo ist noch Handlungsbedarf?
- Erläuterungen zu den Bausteinen:
  - Datensicherungskonzept
  - E-Mail
  - Windows 200 Client
  - Servergestütztes Netz
- direkt verwendbare Checkliste für alle Maßnahmen

Profil für eine mittlere Institution

- Hilfe für IT-Sicherheitsbeauftragte einer mittelgroßen Institution
- Repräsentation eines Unternehmens mit mehreren Servern und wenig IT-Grundschutz Erfahrung
- Ausführliche Erläuterung der Anwendung des IT-Grundschutzhandbuchs
- Beispielhafte Anwendung des GSTOOL

Profil für eine mittlere Institution

- IT-Grundschutz Vorgehensweise in 7 Phasen



- Phase 1: Initiierung des IT-Sicherheitsprozesses
- Phase 2: Durchführung einer IT-Strukturanalyse
- Phase 3: Durchführung einer Schutzbedarfsfeststellung
- Phase 4: Modellierung nach IT-Grundschutz
- Phase 5: Durchführung des Basis-Sicherheitsschecks
- Phase 6: Realisierung von IT-Sicherheitsmaßnahmen
- Phase 7: Zertifizierung

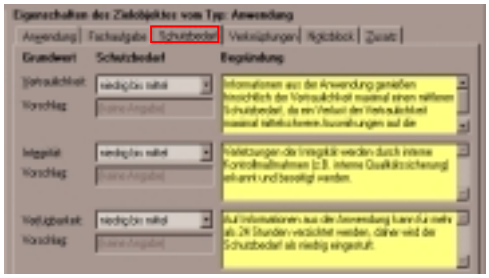
Profil für eine mittlere Institution

- Zu jeder Phase: detaillierte Erläuterung der IT-Grundschutz Vorgehensweise
- Hervorhebung der Schritte, die

durch das GSTOOL unterstützt werden

die bei einer nicht tool-gestützten Vorgehensweise zu beachten sind

- Anwendung des GSTOOL, dargestellt durch Screenshots



Profil für eine mittlere Institution

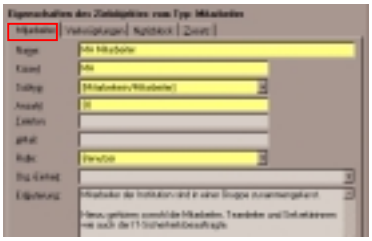
- Institution mit 4 Abteilungen (Finanzen, IT, Produktion, Labor)
- Stabstelle für QM und IT-Sicherheit
- Größe des IT-Verbundes: ca. 20 Clients und 4 Server
- Anbindung an das Internet über DSL
- Existenz interner Teilnetze
- IT-Anwendungen/Systeme eines Projektteams haben erhöhten Schutzbedarf und werden gesondert gruppiert

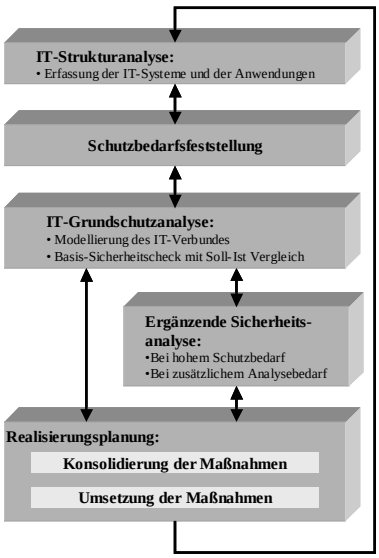
Mittlere Institution
IT-Sicherheitsleitlinie

- Umfang von 4 Seiten
- Bedeutung von
  - Verfügbarkeit (Ausfälle nur in geringem Maße tolerierbar)
  - Vertraulichkeit (höchste Ansprüche)
- Benennung eines IT-Sicherheitsbeauftragten
- Festlegung von Verantwortlichkeiten
- Schulung von Mitarbeitern zu IT-Sicherheitsmaßnahmen
- Revision der IT-Sicherheitskonzeption

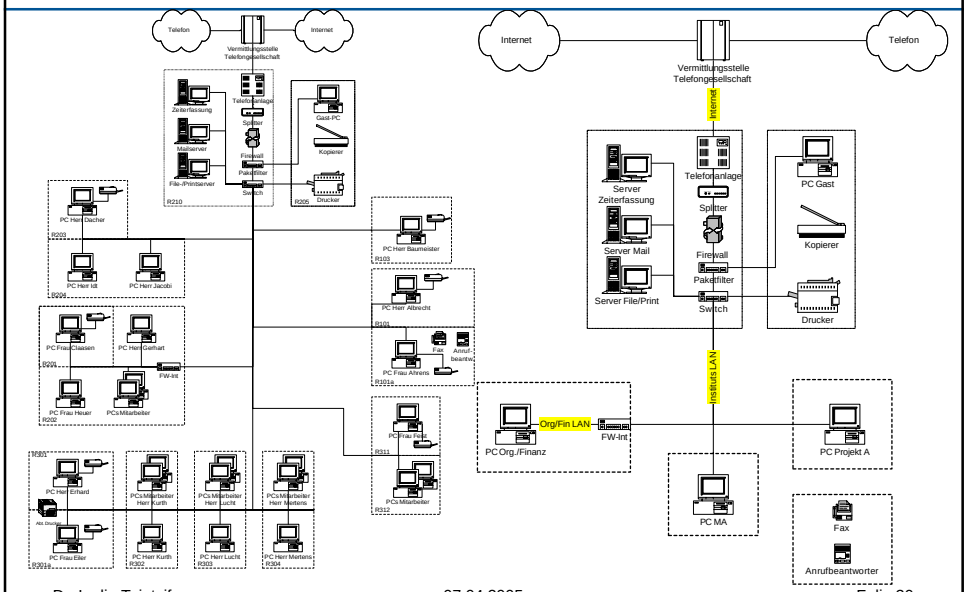
Mittlere Institution
IT-Strukturanalyse

- Tabellarische Übersichten
- Beispiele zur Gruppenbildung
- Anwendung des GSTOOL
- Beispiel-Datenbank wird zur Verfügung gestellt





Mittlere Institution
Netzplan

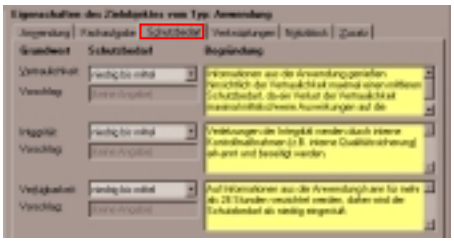


Mittlere Institution
Schutzbedarfsfeststellung

- Drei Kategorien: normal, hoch und sehr hoch
- Beispiele für Schadensszenarien anhand des Beispiel IT-Verbunds

> *In der beispielhaften Institution würde z. B. ein Ausfall des internen Fileservers die Aufgabenerfüllung beeinträchtigen. Eine Folge könnte die verspätete Auslieferung von Dokumenten an die Kunden der Institution sein. Dies ist in Abhängigkeit von evtl. vereinbarten Vertragsstrafen bei der Schutzbedarfsfeststellung zu berücksichtigen.*

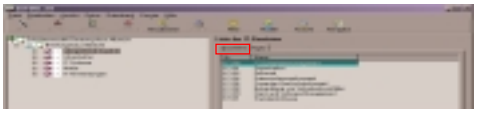
- Detaillierte Beispiele der durchgeführten Schutzbedarfsfeststellung anhand des GSTOOL



Mittlere Institution
IT-Grundschutzanalyse

Modellierung:

- IT-Grundschutz Schichtenmodell
- Modellierung mit dem GSTOOL



- Hinweise für eine Modellierung ohne das GSTOOL

Basis-Sicherheitscheck:

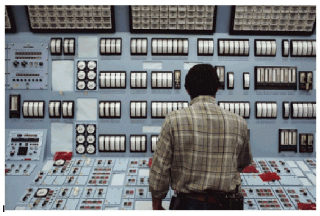
- Fokussierung auf organisatorische Aspekte
- Hilfestellung bei
  - Vorbereitung der Interviews
  - Durchführung der Interviews

Mittlere Institution
Realisierung

- Erläuterung und Hinweise innerhalb der Schritte:
  - *Schritt 1* ***Sichtung der Untersuchungsergebnisse***
  - *Schritt 2* ***Konsolidierung der Maßnahmen***
  - *Schritt 3* ***Kosten- und Aufwandsschätzung***
  - *Schritt 4* ***Festlegung der Umsetzungsreihenfolge der Maßnahmen***
  - *Schritt 5* ***Festlegung der Verantwortlichkeit***
  - *Schritt 6* ***Realisierungsbegleitende Maßnahmen***

  Die Mitarbeiter sollten möglichst frühzeitig in die Planungen mit einbezogen werden: Sie sind es, die mit den neuen Maßnahmen „leben“ müssen.
- Besonderer Hinweis auf die Aufrechterhaltung der IT-Sicherheit

Profil für eine große Institution



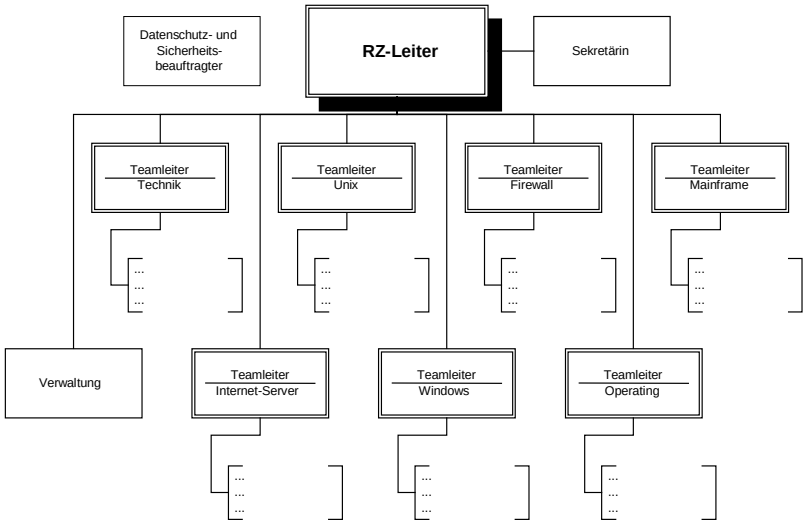
- Zugrunde gelegtes Beispiel: Rechenzentrum (ca. 100 Server)
- IT-Sicherheitserfahrung und IT-Grundschutzkenntnis sind vorhanden
- Ziel: Unterstützung des IT-Sicherheitsbeauftragten
  - Erläuterungen zu den einzelnen Phasen des IT-Grundschutzhandbuchs
  - Darstellung der Nutzungsmöglichkeiten und Grenzen des GSTOOL
  - Lösungsvorschläge für phasenbezogenen Problemstellungen

Profil für eine große Institution

- Darstellung der *üblichen* Probleme innerhalb der jeweiligen Umsetzungsphase

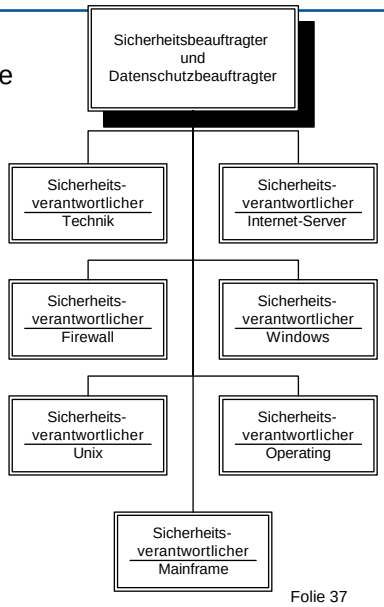
- Hinweise und Lösungsansätze zu diesen Problemen

Große Institution
Das Organigramm



Große Institution
Das Sicherheitsmanagement-Team

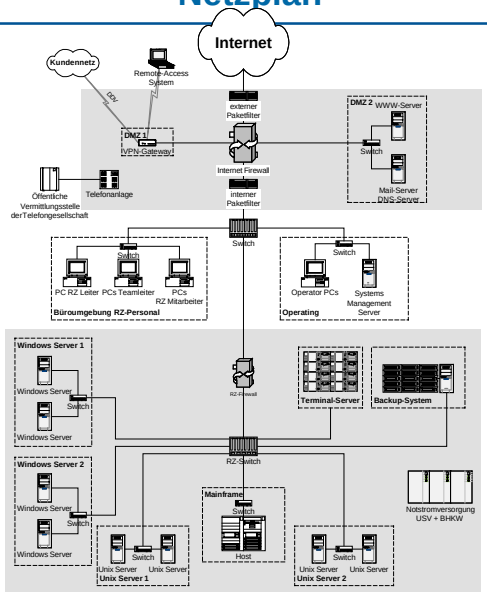
- Der IT-Sicherheitsbeauftragte als oberste Instanz
- Technische und organisatorische Unterstützung durch die einzelnen Bereiche



Profil für eine große Institution

- Anbindung an das Internet
- Anbindung an verschiedene Kunden per DDV
- Definition des Rechenzentrums als IT-Verbund
  - Bereiche Operating und Büroumgebung sind *nicht* Teil des IT-Verbunds
- Einsatz eines Mainframes

Große Institution
Netzplan



Große Institution
IT-Sicherheitsleitlinie

- Umfang von 6 Seiten
- Basis für eine IT-Sicherheitsleitlinie eines Rechenzentrums
- Berücksichtigung der Kundenanforderungen
- Benennung eines IT-Sicherheitsbeauftragten und Definition eines IT-Sicherheitsmanagement-Teams
- Festlegung von Verantwortlichkeiten
- Allgemeine IT-Sicherheitsstrategien
- Schulung von Mitarbeitern zu IT-Sicherheitsmaßnahmen
- Revision von IT-Sicherheitsmaßnahmen

Große Institution
Modellierung

- Detaillierte Erläuterung des Prinzips
- Modellierung anhand des GSTOOL

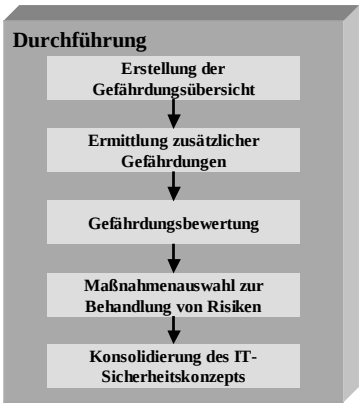
Große Institution
Sicherheitsscheck, Zertifizierung

Basis-Sicherheitscheck

- Erläuterung der ergänzenden Sicherheitsanalyse
- Darstellung von Problemen in allen Phasen

Zertifizierung

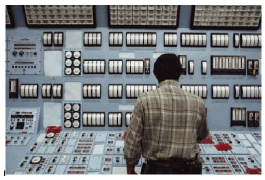
- Darstellung der Ausbaustufen
- Erläuterung von Problemen bei der Vorbereitung



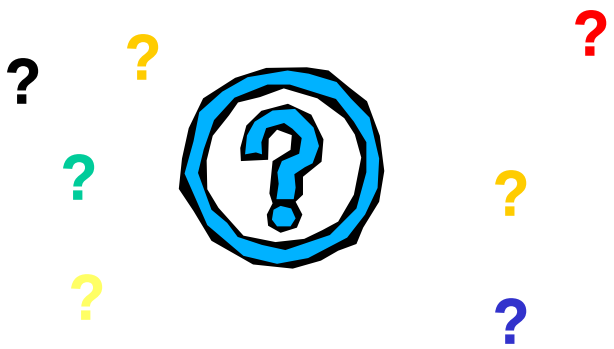
IT-Grundschutz Profile
Zusammenfassung

- Praxis-orientierte Hilfestellung für die Implementierung des IT-Grundschutzes
- Hilfestellung, Beispiel-Dokumente und Tipps
- Beispiele für den Einsatz des GSTOOL





Fragen und Diskussion



Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Lydia Tsintsifa
IT-Sicherheitsmanagement, IT-Grundschutz
Tel: +49 (0)1888-9582-240
Fax: +49 (0)1888-9582-90240
lydia.tsintsifa@bsi.bund.de

IT-Grundschutz Hotline:
Tel: +49 (0)1888-9582-369
gshb@bsi.bund.de

GSTOOL Hotline:
Tel: +49 (0)1888-9582-299
gstool@bsi.bund.de