IT-Grundschutz für große Institutionen
- Ein Profil -

Manuel Atug

SRC Security Research & Consulting GmbH

Bonn - Wiesbaden

Ziel des Projektes

- Erstellung von drei „Profilen“
  - Profil 1: Kleiner IT-Verbund
    - Repräsentation einer Anwaltskanzlei, kleinen Behörde
    - Wenige IT-Systeme, keine Kenntnis der GSHB-Methodik
    - Umgangssprachliche Formulierung, konkrete Anleitung
  - Profil 2: Mittlerer IT-Verbund
    - Repräsentation eines Unternehmens mit mehreren Servern
    - Anwendung und Hinweis auf das GSTOOL, GSHB-Methodik bekannt
  - Profil 3: Großer IT-Verbund (Rechenzentrum)
    - Repräsentation eines Rechenzentrums
    - Als FAQ aufgebaut
    - GSHB-Methodik wird als bekannt vorausgesetzt

Generelles Vorgehen 1

- **Erläuterung der GSHB-Vorgehensweise zu Beginn eines jeden Kapitels**

4.1 Generelle Vorgehensweise bei der Erstellung der Sicherheits-Leitlinie

Die Sicherheits-Leitlinie definiert das innerhalb des Geltungsbereiches (IT-Verbundes) angestrebte Sicherheitsniveau. In ihr werden daher der Geltungsbereich, in dem die Sicherheits-Leitlinie gültig ist und die von der Institution angestrebten Sicherheitsziele sowie die verfolgte Sicherheitsstrategie festgehalten. Die Sicherheits-Leitlinie ist somit Anspruch und Aussage zugleich. Über die Sicherheits-Leitlinie wird das zu erreichende „Ziel“ (Sicherheitsniveau) der Institution festgelegt. Die Leitung der Institution unterrichtet alle Mitarbeiter über diese Sicherheits-Leitlinie und weist auf die verpflichtende Einhaltung und Verbindlichkeit innerhalb der Institution hin.

Die Sicherheits-Leitlinie kann auf unterschiedliche Arten erstellt werden. Ausgehend von den oben genannten Aspekten bietet es sich an, Workshops zu den einzelnen Themen zu veranstalten und mit den Verantwortlichen die Formulierung eines Entwurfs der Sicherheits-Leitlinie zu erarbeiten. Als Grundlage für die Sicherheits-Leitlinie bietet es sich an, die durch das BSI veröffentlichte Dokumente [MURI] zu nutzen.

Generelles Vorgehen 2

- **Darstellung der *üblichen* Probleme innerhalb der jeweiligen Umsetzungsphase**

4.2 Häufige Probleme bei der Erstellung der Sicherheits-Leitlinie
- 4.2.1 Personelle Probleme
  - 4.2.1.1 Benennung des IT-Sicherheitsbeauftragten
  - 4.2.1.2 Fehlende personelle Ressourcen
  - 4.2.1.3 Fehlendes Bewusststein bei der Institutsleitung
- 4.2.2 Inhaltliche Probleme
  - 4.2.2.1 Detaillierungsgrad der Sicherheits-Leitlinie
  - 4.2.2.2 Nutzung vorhandener Dokumente
  - 4.2.2.3 Berücksichtigung von Kundenanforderungen
  - 4.2.2.4 Definition des IT-Sicherheitsmanagement-Teams

Generelles Vorgehen 1

- **Verdeutlichung der Erläuterungen und Probleme durch**
  - **Beispiele**

Im Laufe der Jahre hat die Institutsleitung verschiedene verbindliche Hausmitteilungen veröffentlicht. Hierunter fällt auch eine Hausmitteilung zur generellen Nutzung von Passworten und zum Virenschutz. Der IT-Sicherheitsbeauftragte nutzt Aussagen dieser Hausmitteilungen um einen ersten Entwurf für die Sicherheits-Leitlinie zu erstellen.

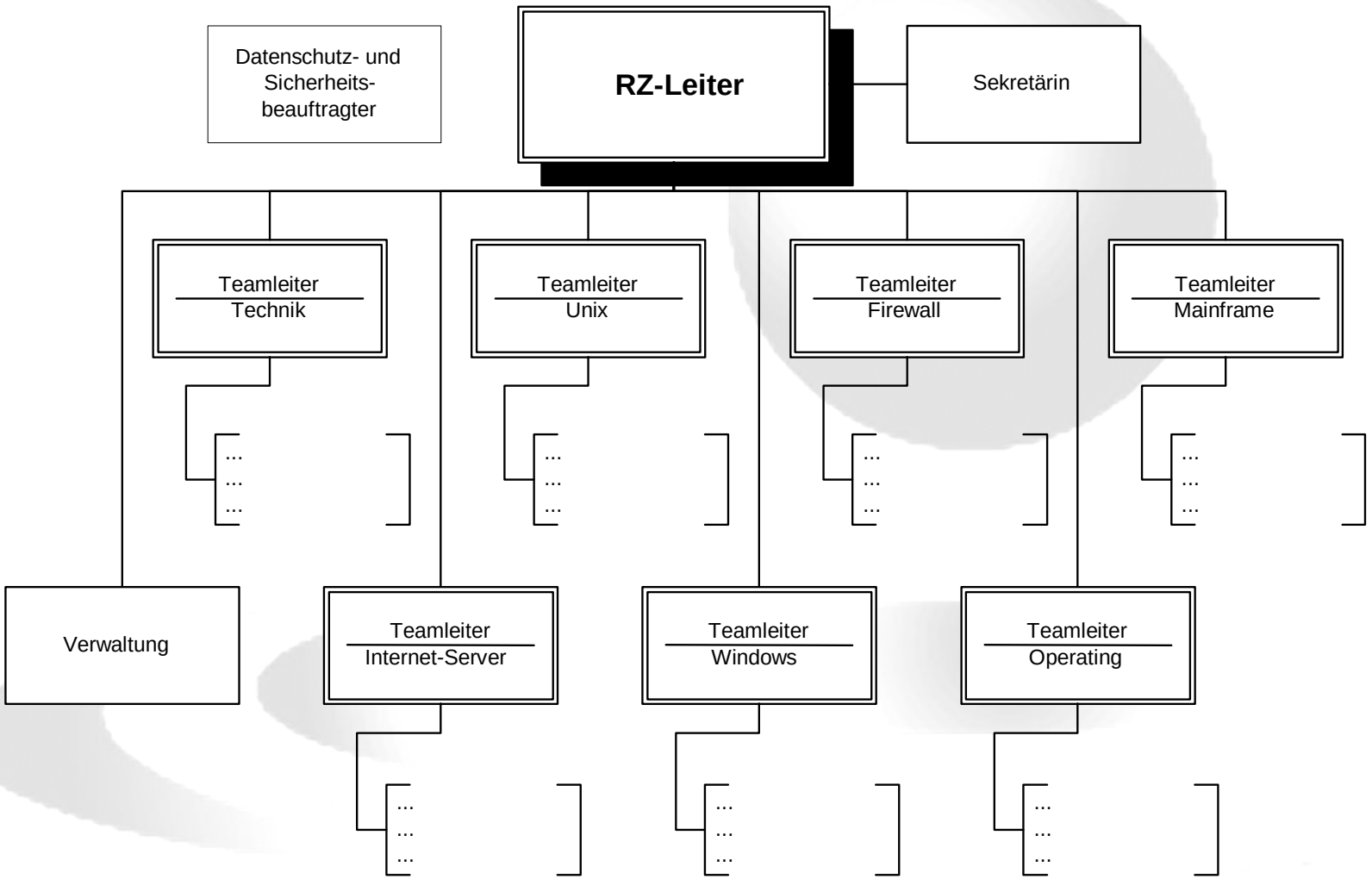
und

  - **Tipps**

Häufig sind in Rechenzentren interne Richtlinien vorhanden und Hausmitteilungen erlassen worden. Derartige Dokumente spiegeln das Sicherheitsempfinden sehr gut wieder und enthalten teilweise Aussagen, die Bestandteil einer Sicherheits-Leitlinie sein müssen. Derartige Dokumente sollten daher in die Erstellung der Sicherheits-Leitlinie mit einbezogen werden. Dies ist vorteilhaft, da hierdurch bereits etablierte und bekannte Aspekte in die Sicherheits-Leitlinie einfließen.

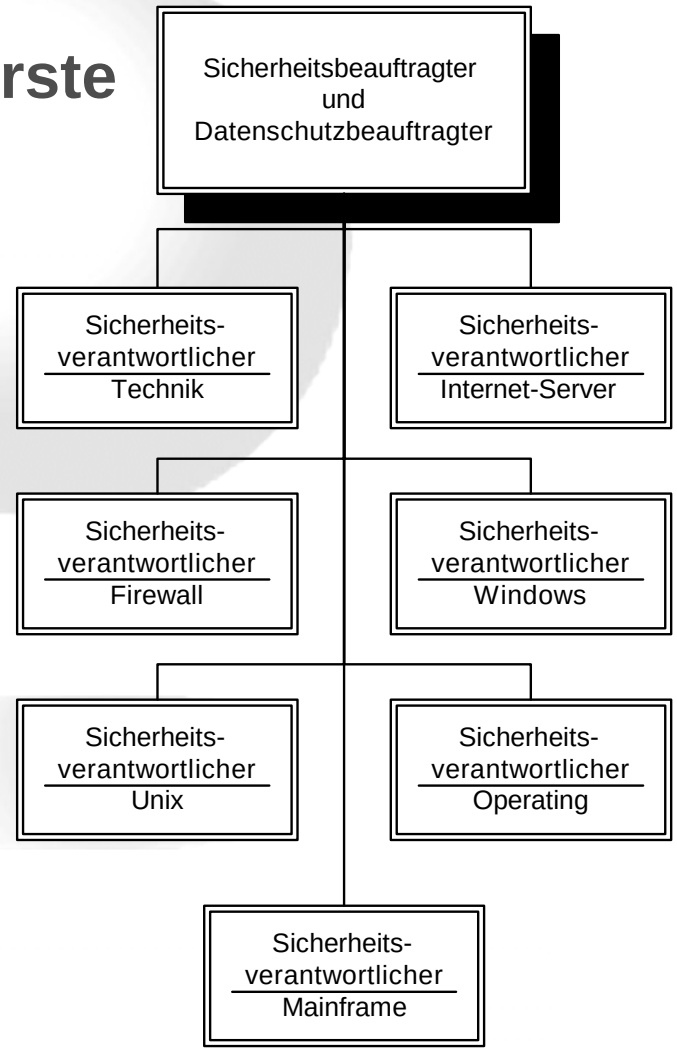
Das Beispiel

- **Das Organigramm**



Das Beispiel

- **Das Sicherheitsmanagement-Team**
  - **Sicherheitsbeauftragter als oberste Instanz**
  - **Unterstützung durch die einzelnen Bereiche**
    - **Technische und organisatorische**



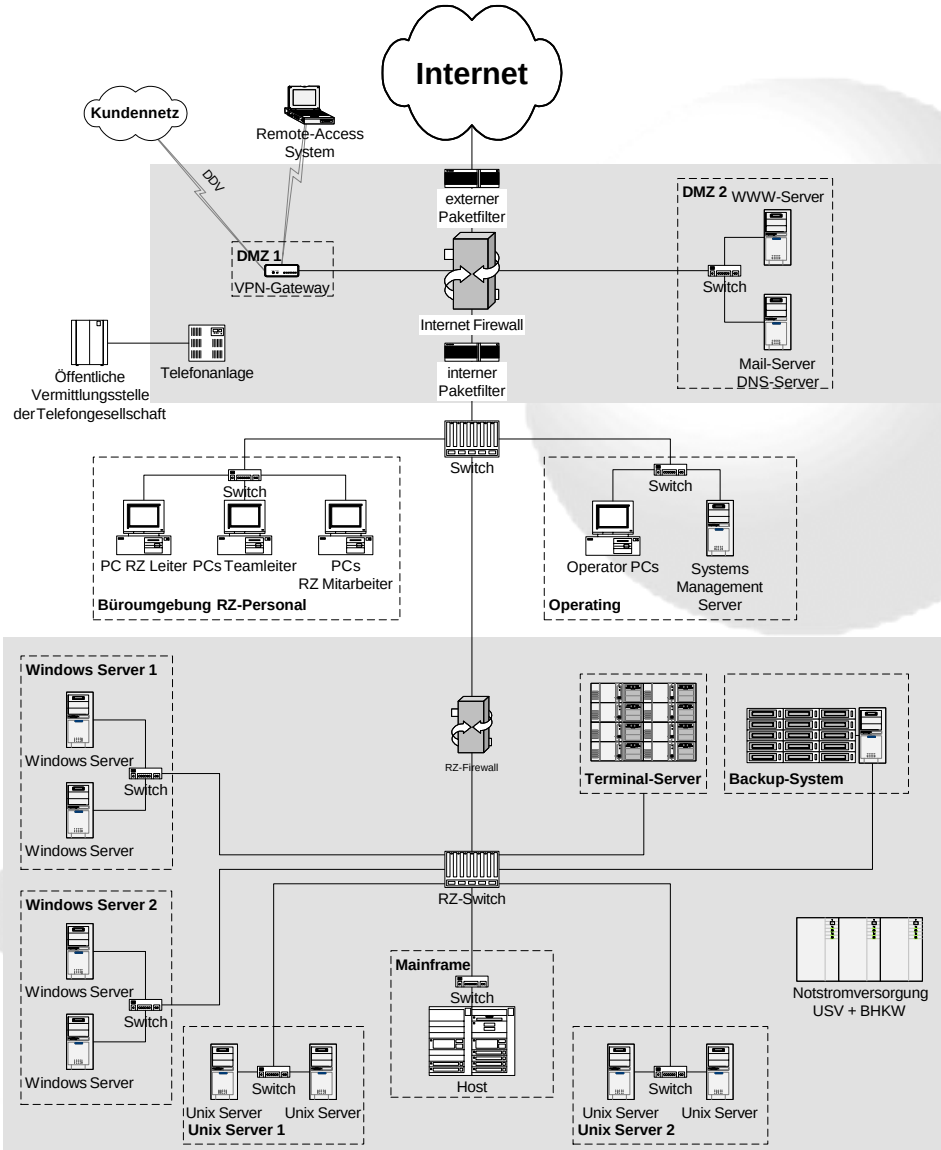
Verantwortlichkeit

- *Zielperson:* Der IT-Sicherheitsbeauftragte
- Unterstützung bei auftretenden Fragestellungen während der Umsetzung des GSHB
- Darstellung der Nutzungsmöglichkeiten und Grenzen des GSTOOL

Der „große IT-Verbund“

- 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

Der „große IT-Verbund“



Parallelen

- Betrachteter Verbund dient auch hier als Beispiel
- Abweichungen möglich
  - Betriebssystem
  - Anzahl der Rechner
  - Art des Internetanschlusses
  - Server
  - Räume / Verkabelung
- Ziel: Mögliche Probleme und Lösungen verdeutlichen

Vorgabe einer Sicherheits-Leitlinie

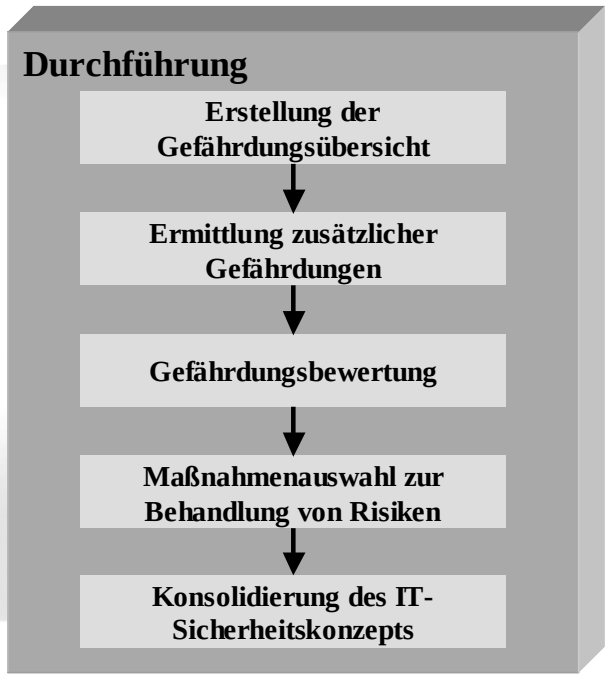
- Sechs Seiten
- Abgeleitet aus den Musterrichtlinien und Beispielkonzepten des BSI
- Basis für eine Sicherheits-Leitlinie eines Rechenzentrums
- Berücksichtigung der Kundenanforderungen
- Definition eines IT-Sicherheitsmanagement-Teams
- Schulung von Mitarbeitern bzgl. Sicherheitsmaßnahmen
- Revision von Sicherheitsmaßnahmen

Modellierung

- Detaillierte Erläuterung des Prinzips
- Modellierung anhand des GSTOOL

Basissicherheitscheck

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



Zertifizierung

- Zertifizierung ist das Ziel der Umsetzung des GSHB
- Darstellung der Ausbaustufen
- Erläuterung von Problemen bei der Vorbereitung

Ergebnis

- Unterstützung eines IT-Sicherheits-beauftragten, der mit der Umsetzung des GSHB beauftragt ist
- Darstellung üblicher Probleme und Lösungsansätze

Kontakt

SRC
Security Research & Consulting GmbH
Graurheindorfer Str. 149a
53117 Bonn

Tel. **+49-(0)228-2806-0**
Fax: **+49-(0)228-2806-199**
E-mail: **info@src-gmbh.de**
WWW: **www.src-gmbh.de**