

Verankerung und Umsetzung der IT-Sicherheit in der Hochschule

3. Arbeitstreffen der G-WiN Kommission des ZKI
Berlin, den 27.10.2003

Dipl.-Inform. W. Moll
Institut für Informatik IV der Universität Bonn

1. Kriterien für IT-Sicherheitsstandards
2. Der IT-Sicherheitsprozess
3. Management der IT-Sicherheit
4. Umsetzung der IT-Sicherheit

Kriterien für die IT - Sicherheitsstandards

Technischer Fokus (Schichten)

- IT-Organisation
- Infrastruktur
- IT-Systeme
- Netze
- IT-Anwendungen

Ganzheitlicher Ansatz (Prozesse)

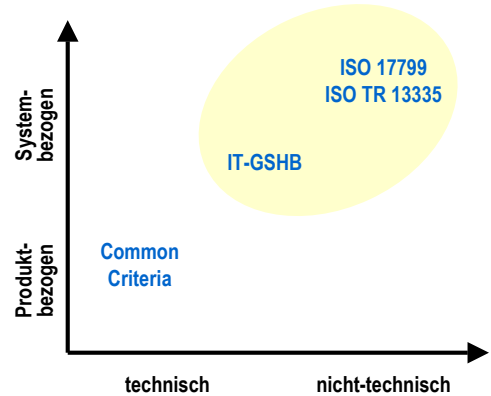
- Geschäftsprozesse
- Management der IT-Sicherheit
- Wirtschaftlichkeit der Maßnahmen
- Bewusstsein für IT-Sicherheit

Kriterien für die IT - Sicherheitsstandards

National (BSI): Das IT-Grundschutzhandbuch (IT-GSHB)

International (ISO) :

1. BS 7799-1 als ISO-Standard 17799
2. BS 7799-2 (auf dem Weg zum Standard)
3. ISO/IEC TR 13335
4. Common Criteria, CobiT, ...

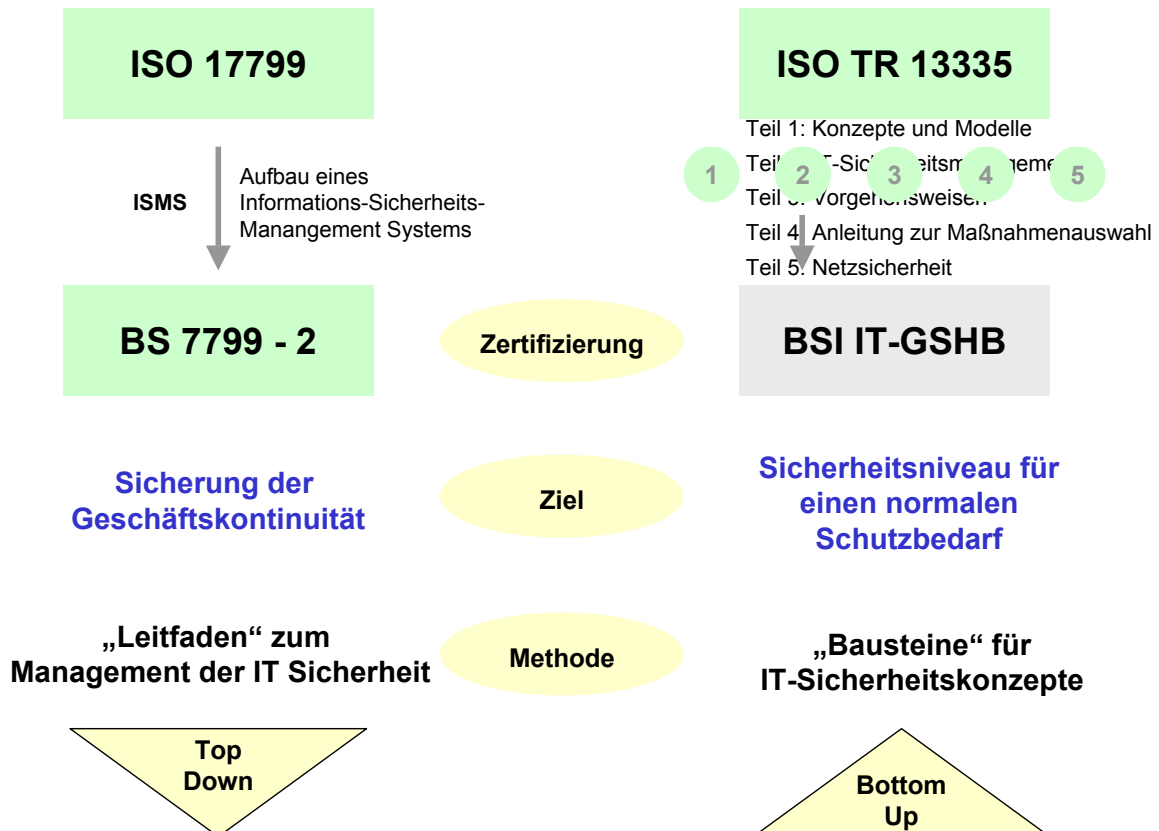


Kriterien *)

1. Zielsetzung und Zielgruppen
2. Vorgehensweise
3. Skalierbarkeit und Aktualisierbarkeit
4. Angestrebtes Sicherheitsniveau
5. Anwendbarkeit, Kosten

*) siehe Initiative D21 – IT-Sicherheitskriterien im Vergleich, 2001

Kriterien für die IT - Sicherheitsstandards



Der IT - Sicherheitsprozess

Kritische Erfolgsfaktoren

- ▶ Leitlinien, Ziele und Maßnahmen spiegeln die **Geschäftsziele** der Hochschule wider
- ▶ Die Umsetzung des Sicherheitskonzeptes entspricht der **Universitätskultur**
- ▶ **Sichtbare Unterstützung** und **Verbindlichkeit** durch die Hochschulleitung
- ▶ Effektives „**Marketing**“ der IT-Sicherheit innerhalb der Hochschule (Sicherheitsbewusstsein)
- ▶ Ein klares **Verständnis** für Sicherheitsanforderungen, Risikobewertung und Risikobehandlung
- ▶ Entwicklung von **Schulungsangeboten**
- ▶ **Messbare Überprüfung** der erreichten IT-Sicherheit

System von Verfahren und Regeln zur **dauerhaften** Steuerung und Kontrolle der Informationssicherheit

Der IT - Sicherheitsprozess



Der IT - Sicherheitsprozess

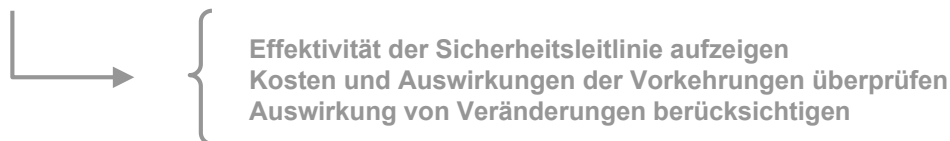
Sicherheitsleitlinie

Zielrichtung und Unterstützung der Leitung für die IT-Sicherheit

- Stellenwert der IT-Sicherheit und Bedeutung der IT aufzeigen
- Sicherheitsziele und Geltungsbereich definieren
- Zusicherung, dass IT-Sicherheitsrichtlinie durchgesetzt wird
- Grundzüge der Sicherheitsstrategie festlegen
- Beschreibung der Organisationsstruktur für IT-Sicherheit
- Zuweisung allgemeiner und spezifischer Verantwortlichkeiten
- Darstellung der Durchsetzung, etwa Vorgehensweise bei Verstößen
- Überblick über die Dokumentation des IT-Sicherheitsprozesses
- Aussagen zu Programmen für Schulungs- und Sensibilisierungsmaßnahmen
- Aussagen zur **periodischen Überprüfung** der IT-Sicherheitsmaßnahmen



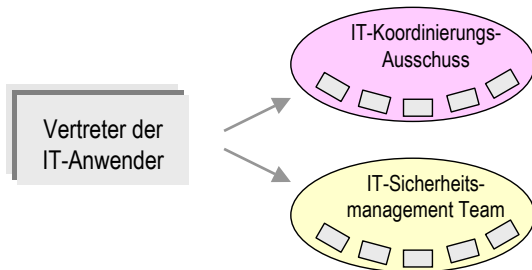
- ✓ Geltungsbereich
- ✓ **Sicherheitsleitlinie**
- ✓ Organisationsstruktur



Der IT - Sicherheitsprozess

Organisationsstruktur

Aufbauorganisation des IT-Sicherheitsmanagement



Leitung des Unternehmens

IT-Sicherheitsbeauftragter

Bereichs-IT-Sicherheitsbeauftragte

Projekt/System-IT-Sicherheitsbeauftragte



- **Koordinierung**
- **Informationsfluss**
- **Anlaufstelle**
- **Konzepte erstellen**

- IT-Sicherheitsziele, Strategie und Leitlinien definieren
- Ressourcen bereitstellen
- Umsetzung der IT-Sicherheitsleitlinie überprüfen
- Sicherheitsprozess initiieren, steuern und koordinieren
- Realisierungsplan IT-Sicherheitskonzept genehmigen
- Überprüfung des IT-Sicherheitskonzeptes
- Schulungs- und Sensibilisierungsprogramme erstellen
- IT-Koordinierungsausschuss und Unternehmensleitung beraten

Der IT - Sicherheitsprozess

Risiken
Systematischer Ansatz zur Beurteilung von Risiken

Definition:

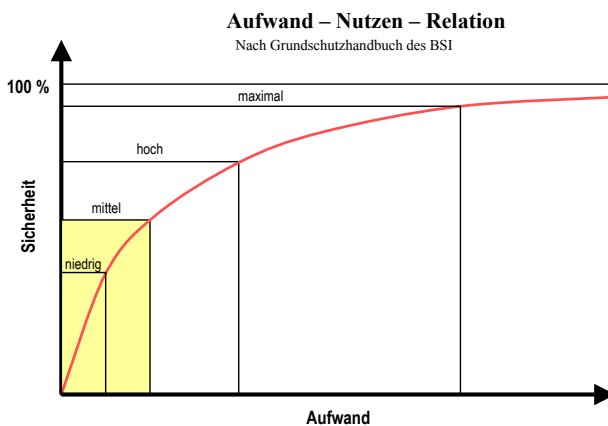
Ein Risiko ist die Möglichkeit (Potential), dass eine gegebene Bedrohung eine Schwachstelle ausnutzt und einen Schaden anrichtet.

Ein Risiko wird charakterisiert durch zwei Faktoren:
Die Wahrscheinlichkeit des Auftretens sowie seine Auswirkung.



Der IT - Sicherheitsprozess

Mythos:
Mit geringem Aufwand kann bereits ein befriedigendes Sicherheitsniveau erzielt werden



Problem

1. Hoher Schaden
2. Hohe Wahrscheinlichkeit
3. Hoher Aufwand zur Vermeidung



Ausgewogenheit, Durchgängigkeit, Angemessenheit

Umsetzung der IT-Sicherheit

Was

Wofür

Wer

Sicherheitsleitlinie

„Gesetze“

Rektorat
IT-Vorstand

**Geschäftsprozesse
Rollenkonzepte**

Schutzbedarf der
Geschäftsprozesse

Fachbereiche
Verwaltung

**Bedrohungs- und Risikoanalyse
Maßnahmenkatalog**

Gefährdungen und
Bewertung der
Risiken und Maßnahmen

Sicherheitsbeauftragte
und lokales IT-Personal

© Wolfgang Moll, Institut für Informatik der Universität Bonn, 2003

11

Umsetzung nach ISO 17799 (BS 7799-1)

Management des kontinuierlichen Geschäftsbetriebs

Aspekte zur Aufrechterhaltung
des Geschäftsbetriebs
Einhaltung der Verpflichtungen

Einhaltung gesetzlicher Verpflichtungen

Überprüfung der Sicherheitspolitik und
technischen Normerfüllung
Überlegungen zum Systemaudit

Physische und umgebungsbezogene Sicherheit

Sicherheitszonen
Sicherheit der Geräte
Allgemeine Maßnahmen

Einstufung und Kontrolle der Werte

Zurechenbarkeit der Werte
Einstufung von Informationen

Management der Kommunikation und des Betriebs

Betriebsverfahren und -verantwortlichkeiten
Systemplanung und -abnahme
Schutz vor bösartiger Software
Haushaltsorganisation
Netzwerkmanagement
Umgang mit und Sicherheit von Datenträgern
Austausch von Informationen und Software

Systementwicklung und -wartung

Sicherheitsanforderungen an Systeme
Sicherheit in Anwendungssystemen
Kryptographische Maßnahmen
Sicherheit von Systemdateien
Sicherheit bei Entwicklungs- und
Supportprozessen

Organisation der Sicherheit

Infrastruktur der
Informationssicherheit
Sicherheit bei dem Zugang
durch Fremdunternehmen
Outsourcing

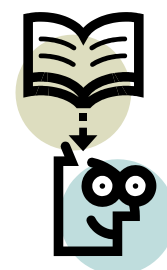
Personelle Sicherheit

Sicherheit bei der Stellenbeschreibung
und Bereitstellung von Ressourcen
Benutzerschulung
Verhalten bei Sicherheitsvorfällen
und -störungen

Zugangskontrolle

Geschäftsanforderungen an die Zugangskontrolle
Verwaltung der Zugriffsrechte der Benutzer
Verantwortung der Benutzer
Netzzugriffskontrolle
Kontrolle des Betriebssystemzugriffs
Zugriffskontrolle für Anwendungen
Überwachung des Systemzugriffs
und der Systembenutzung
Mobile Computing und Telearbeit

Interviews Checkliste



© Wolfgang Moll, Institut für Informatik der Universität Bonn, 2003

12

Blaupause

- **Übertragung eines gemäß BS 7799 "standardmäßigen" Vorgehens auf die Verhältnisse einer Hochschule.**
- **Aufbau organisatorischer IT Sicherheitsstrukturen**
- **Entwicklung eines gemeinsamen Vorgehensmodells**
 - **Analyse von Prozessabläufen (Verwaltung, Institute)**
 - **Definition von Rollenkonzepten, Verantwortlichkeiten**
 - **Erstellen einer Blaupause für ein Sicherheitskonzept**
 - **Etablierung des Sicherheitsmanagements**
 - **Erarbeiten von Sicherheitskonzepten an den einzelnen Hochschulen anhand der „Blaupause“**
 - **Kontrolle, d.h. Analyse der erzielten Effektivität**