Nachweisbare Sicherheit durch Zertifizierung nach BSI Grundschutz

DECUS Symposium
8.-10. April 2003

Jürgen Bachinger
Senior Consultant
HP Services - Consulting & Integration
BSI-Auditor: BSI-GSL-0001-2002

Agenda

- Einführung
  - Definition Grundschutz
  - Ziele
  - Stufen und Ausprägungen
- Ablauf einer Qualifizierung
  - Erhebungsphase
  - Qualifizierungsphase
- Bisherige Erfahrungen / Ausblick
  - Aufwand und Kosten
  - ISO 17799 oder BSI Grundschutz
  - Tendenzen im Markt

Was ist IT-Grundschutz?

- Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten
- Standard für IT-Sicherheit
- Maßnahmensammlung
- Nachschlagewerk
- Quelle: *www.bsi.de/gshb*

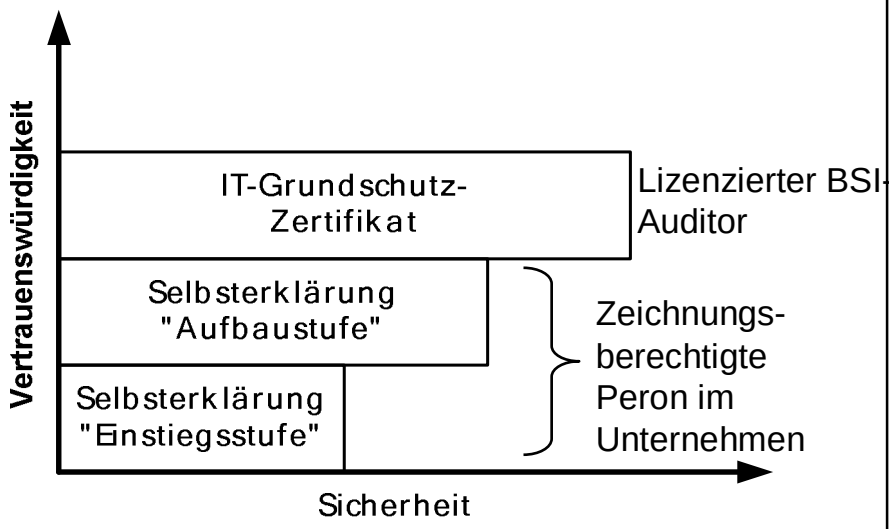
Ziel IT-Grundschutz

Durch geeignete Anwendung von infrastrukturellen, organisatorischen, personellen und technischen Standardsicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den mittleren Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Anwendungen dienen kann.

Warum IT-Grundschutz-Qualifizierung?

- Unternehmen und Behörden wollen Sicherheitsniveau dokumentieren
  - intern
  - nach außen
- Wie sicher sind meine Geschäftspartner?
- Maßstab für Umsetzung von Standard-Sicherheits-Maßnahmen

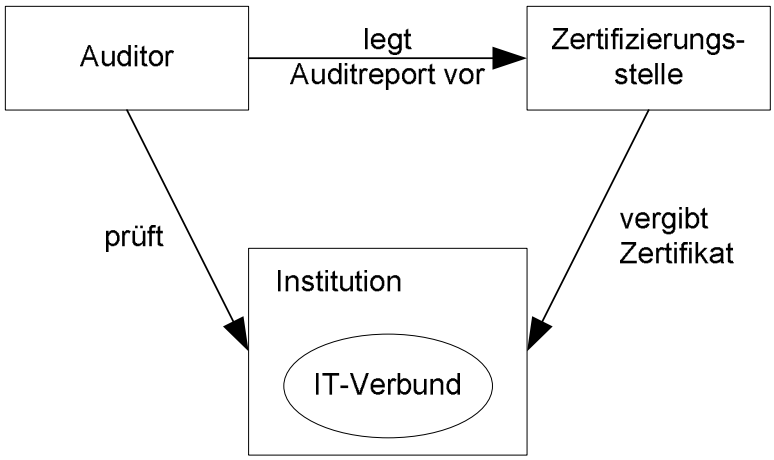
Ausprägungen



IT Grundschutz-Zertifikat

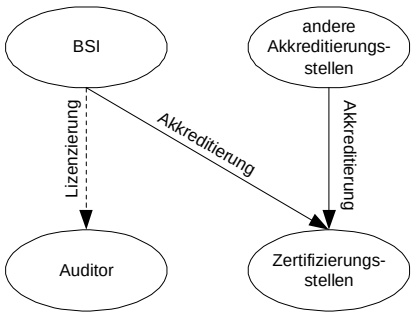
- Vollständige Umsetzung des „IT-Grundschutz“
- Zertifizierung durch akkreditierte Dritte
- 2 Jahre Gültigkeit
- Referenz zur Version des Handbuchs

Zertifizierungsschema



Akkreditierung

Grundlage für Akkreditierung ist EN 45011 oder EN 45012



Akkreditierungsanforderungen:

- organisatorische Anforderungen
- Nachweis der Kompetenz des Personals

IT-Grundschutz-Selbsterklärung

- Kernaussage: Man ist „im IT-Grundschutzprozess!“
- Keine Verlängerung, sondern nächste Stufe notwendig
- Ausprägungen
  - Einstiegstufe
  - Aufbaustufe
- Qualifizierung
  - als Selbsterklärung des Unternehmens
  - durch „unabhängige“ Interne

Stufen

Zuordnung der Maßnahmen:

"A": Umsetzung ist für alle drei Stufen erforderlich

"B": Umsetzung ist für Aufbaustufe und für Zertifikat erforderlich

"C": Umsetzung ist nur für das IT-Grundschutz-Zertifikat erforderlich

Agenda

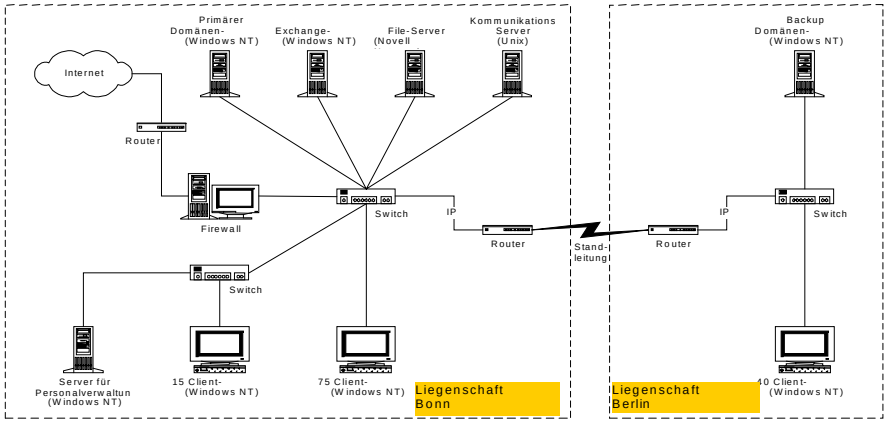
- Einführung
  - Definition Grundschutz
  - Ziele
  - Stufen und Ausprägungen
- Ablauf einer Qualifizierung
  - Erhebungsphase
  - Qualifizierungsphase
- Bisherige Erfahrungen / Ausblick
  - Aufwand und Kosten
  - ISO 17799 oder BSI Grundschutz
  - Tendenzen im Markt

Erhebungsphase

- Schritt 1: Definition des Untersuchungsgegenstands
- Schritt 2: Vorarbeiten
- Schritt 3: Basis-Sicherheitscheck
- Schritt 4: Festlegung der weiteren Vorgehensweise

Schritt 1: Definition des Untersuchungsgegenstands

Abgrenzung Untersuchungsgegenstand / IT-Verbund



Schritt 2: Vorarbeiten (1)

IT-Strukturanalyse (Kapitel 2.1 GSHB)

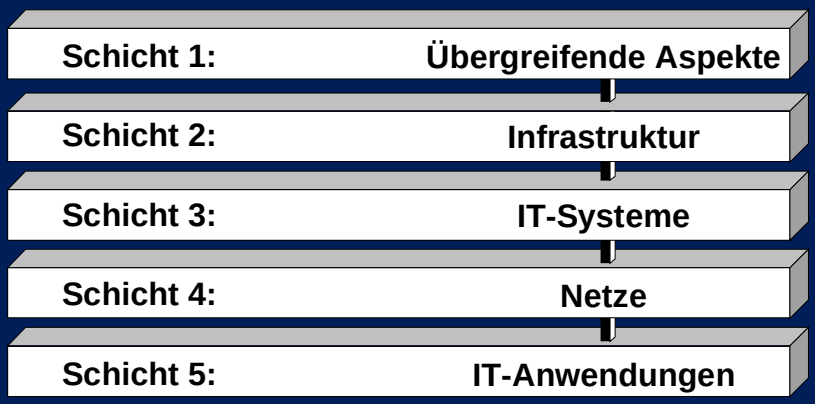
- Bereinigter Netzplan
- Liste der IT-Systeme
- Liste der IT-Anwendungen

Schutzbedarfsfeststellung (Kapitel 2.2)

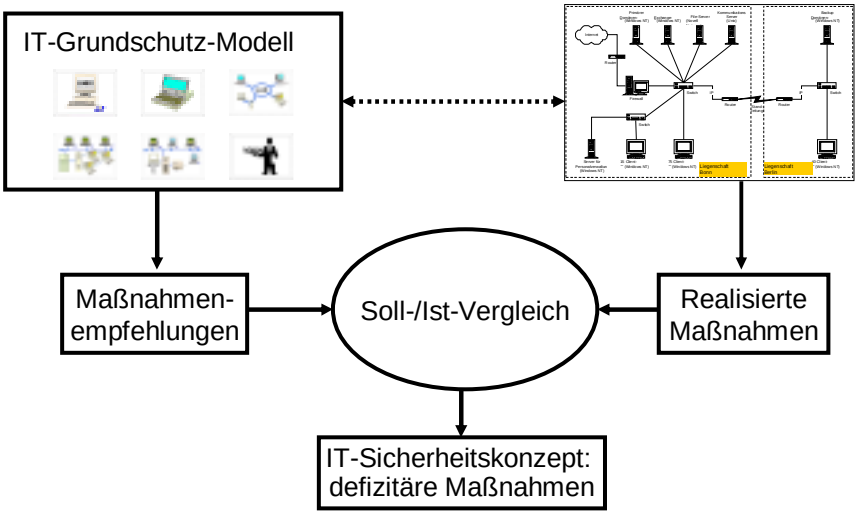
- "niedrig bis mittel"
- "hoch"
- "sehr hoch"

Schritt 2: Vorarbeiten (2)

Modellierung des IT-Verbunds (Kapitel 2.3)



Schritt 3: Basis-Sicherheitscheck



Schritt 4: Festlegung der weiteren Vorgehensweise

- Was wurde erreicht?
  - IT-Grundschutz-Zertifikat
  - Selbsterklärung „IT-Grundschutz Aufbaustufe“
  - Selbsterklärung „IT-Grundschutz Einstiegsstufe“
- Nachbesserungen?

Qualifizierungsphase

- Schritt 5: Plausibilitätsprüfung
- Schritt 6: Realisierungsprüfung
- Schritt 7: Selbsterklärung/Zertifizierung
- Schritt 8: Re-Qualifizierung.

Schritt 5: Plausibilitätsprüfung

Qualifizierer prüft:

- Hat der IT-Verbund eine sinnvolle Mindestgröße?
- Sind die IT-Strukturanalyse und Schutzbedarfsfeststellung plausibel?
- Ist die Modellierung des IT-Verbundes ordnungsgemäß?
- Ist der Basis-Sicherheitscheck vollständig und sind die Ergebnisse plausibel?

Schritt 6: Realisierungsprüfung

Die Prüfung erfolgt

- stichprobenartig und
- umfasst mindestens den Baustein "IT-Sicherheits-Management",
- zufällig aus jeder der fünf Schichten jeweils einen Baustein und
- vier weitere Bausteine nach eigenem Ermessen

Schritt 7: Selbsterklärung/ Zertifizierung

- Plausibilitätsprüfung und Realisierungsprüfung waren erfolgreich
- sämtliche Maßnahmen der angestrebten Ausprägung der IT-Grundschutz-Qualifizierung sind erfüllt

- Selbsterklärung (durch zeichnungsbefugten Vertreter der Institution) oder
- Zertifizierung (durch unabhängige akkreditierte Zertifizierungsstelle)

Schritt 8: Re-Qualifizierung

Re-Qualifizierung
- spätestens nach zwei Jahren oder
- bei sicherheitsrelevanten Veränderungen

Ein (nachweislich) gutes IT-Sicherheitsmanagement meistert auch neue Aufgaben!

Agenda

- Einführung
  - Definition Grundschutz
  - Ziele
  - Stufen und Ausprägungen
- Ablauf einer Qualifizierung
  - Erhebungsphase
  - Qualifizierungsphase
- Bisherige Erfahrungen / Ausblick
  - Aufwand und Kosten
  - ISO 17799 oder BSI Grundschutz
  - Tendenzen im Markt

Aufwand und Kosten

- Review bestehender Unterlagen und Plausibilitätsprüfung: 2 - 3 PT
- Verifikation der Umsetzung: 12 – 20 PT
- Abschlussbericht: 1 – 2 PT
- Gesamtaufwand: 15 – 25 PT

Einflussfaktoren:

- Größe und Komplexität des Untersuchungsgegenstand
- Status (Planung, Entwicklung, Produktion)
- Detaillierungsgrad (Desktop Review vs. Inspektion)

ISO 17799 vs. BSI Grundschutz

ISO 17799

☺ International bekannt und akzeptiert
☺ Große Freiheit bei der Umsetzung
☹ Für Außenstehende ist das erreichte Sicherheitsniveau nicht transparent

BSI Grundschutz

☺ Referenz für Aufsichtsbehörden (z.B. BAFin)
☺ Einfache und strukturierte Vorgehensweise
☹ Umsetzung kann hohen Aufwand nach sich ziehen

Tendenzen im Markt

- Verstärkte Nachfrage nach umfassenden Sicherheitskonzepten
- Grosses Interesse an Zertifizierungen
- Industrieunternehmen legen bei Zulieferern großen Wert auf Zertifizierungen
- Internationale Unternehmen tendieren zu ISO 17799
- Behörden, Banken und Versicherungen: BSI Grundschutz

Prognose

- In den nächsten 2 Jahren werden Zertifikate einen Wettbewerbsvorteil darstellen
- In 3-5 Jahren werden Zertifikate Standard sein!