IT-Symposium 2004

1B08 – 20. April 2004

Praxisbericht Grundschutzzertifizierung

Frank Reiländer, Berater IT-Sicherheit
- Lizenzierter IT-Grundschutz-Auditor des BSI -
Infodas GmbH, Rhonestr. 2, 50765 Köln
☎(0221) 70912-85 f.reilaender@infodas.de
www.save-infodas.de

SAVe® Security Services

Innovative Beratung und Lösungen

- Security Management
- Security Policies
- Sicherheitskonzepte
- Sicherheitsanalysen
- Business Continuity Planning
- SAVe IT-Sicherheitsdatenbank
- Sicherheitszertifizierungen

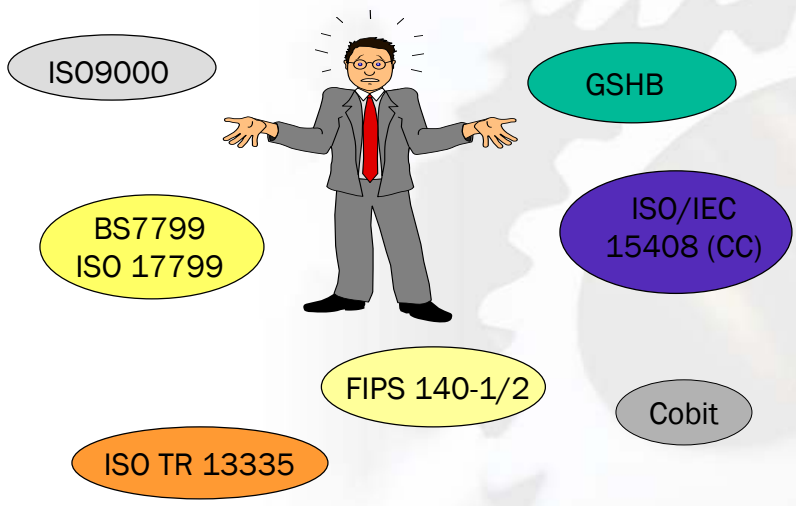
Inhalt

IT-Symposium 2004

- Idee der Grundschutz-Zertifizierung
  - Idee des IT-Grundschutzes
  - Sinn und Nutzen eines Grundschutz-Zertifikats
- Voraussetzungen und Vorbereitung
  - Basis-Sicherheitscheck als Vorprüfung
  - Zertifizierung TDS AG
- Ablauf der Prüfung
- Erfahrungen und Empfehlungen

 3

Standards für IT-Sicherheit und Qualitätsmanagement



 4

IT-Grundschutz ...die Anfänge 1995


Bundesanzeiger

G 1990 A

IT-Grundschutzhandbuch

Maßnahmenempfehlungen
für den mittleren Schutzbedarf

Schriftenreihe zur IT-Sicherheit

- Band 3 -

Stand: 1995

- komplette Erstellung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Beratungsauftrag des BSI für die Bundesbehörden
- kein integraler Sicherheitsprozess

IT-Grundschutzhandbuch 1995
- 18 Bausteine
- 200 Maßnahmen
- 150 Seiten

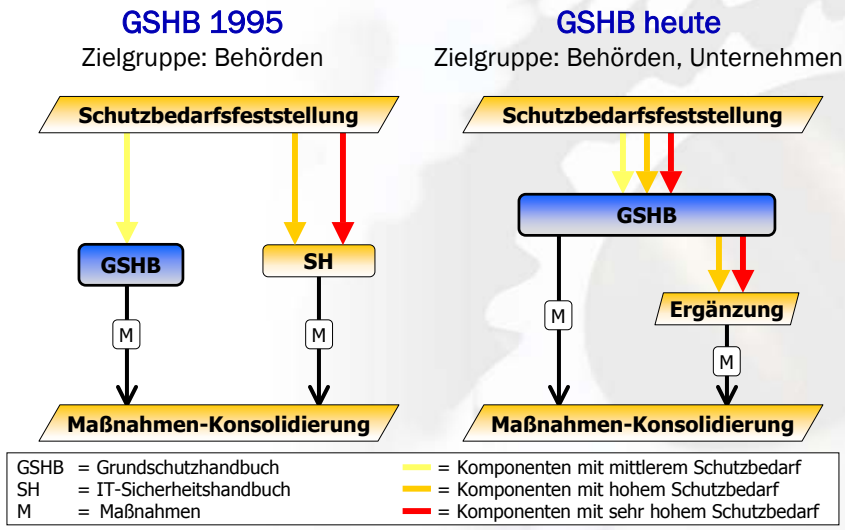
IT-Grundschutz Standard für IT-Sicherheit

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

BSI Bundesamt für Sicherheit in der Informationstechnik

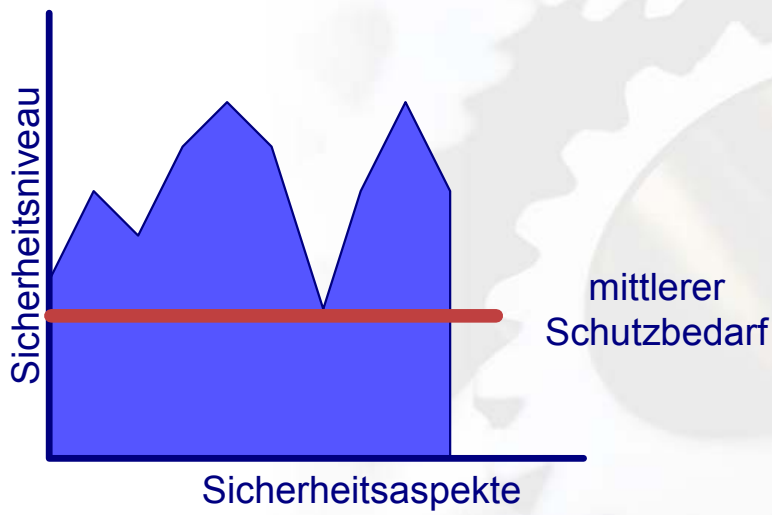
IT-Grundschutzhandbuch 2003
- 65 Bausteine
- 335 Gefährdungen
- 772 Maßnahmen
- 2525 Seiten

IT-Grundschutz
Ablauf Basis-Sicherheitscheck



 7

IT-Grundschutz
Erreichbares Sicherheitsniveau



 8

Methodik IT-Grundschutz

- Charakteristika (Auswahl)
  - Baukastenprinzip
  - Implizite Risikoanalyse
  - Konkrete standardisierte Maßnahmen
  - Fokussierung auf den Anwendungsbereich
  - Einheitliche Prüftiefe
  - Prozessunterstützung des IT-Sicherheitsmanagements
- Bewertung
  - Leichte Anwendbarkeit
  - Unterstützung bei Implementierung und Auditierung
  - Einheitliches Bewertungsschema (Kategorien)
  - Eignung zur standardisierten und Tool-unterstützten Erfassung

Inhalt

- Idee der Grundschutz-Zertifizierung
  - Idee des IT-Grundschutzes
  - Sinn und Nutzen eines Grundschutz-Zertifikats
- Voraussetzungen und Vorbereitung
  - Basis-Sicherheitscheck als Vorprüfung
  - Zertifizierung TDS AG
- Ablauf der Prüfung
- Erfahrungen und Empfehlungen

IT-Grundschutz-Zertifikat

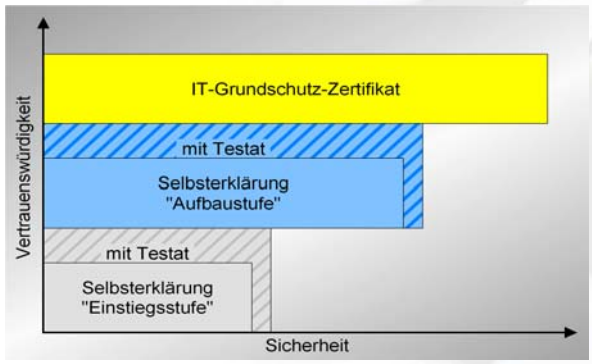
- Kein international standardisiertes Verfahren (ISO)
  - British Standard Institut war mit BS 7799 -> ISO 17799 schneller
  - Standardisierung langwierig
  - Verfahren ist (noch) flexibel
- Zertifizierung
  - Seit Frühjahr 2002
  - Durch das BSI lizenzierte Auditoren (Personenlizenz)
- Qualifizierung und Zertifizierung
  - Dokumente http://www.bsi.bund.de/gshb/zert/schema.htm
  - Auditoren http://www.bsi.bund.de/gshb/zert/auditor.htm

IT-Grundschutz-Zertifikat

- Migrationspfad des IT-GSHB wird fortgeführt
  - „Alte“ Einstufungen
    - Priorität 1
    - Priorität 2
    - Priorität 3
    - optional
  - „Neue“ Einstufungen
    - A Einstiegsstufe
    - B Aufbaustufe
    - C Zertifikatsstufe
    - Z zusätzlich
- Sinn des Zertifikats = Überprüfung und Transparenz ohnehin realisierter Maßnahmen

GS-Siegel (Zertifizierung) Arten der Qualifizierung

- Selbsterklärung „IT-Grundschutz Einstiegsstufe“
- Selbsterklärung „IT-Grundschutz Aufbaustufe“
- IT-Grundschutz-Zertifikat



Selbsterklärung

Die Selbsterklärung muss mindestens folgende Informationen umfassen:

- Name und Adresse der Institution
- Name und Adresse des Auditors (ggf. Unternehmen)
- Beschreibung des Untersuchungsgegenstandes
- Stufe der Selbsterklärung (Einstiegs- bzw. Aufbaustufe)
- Version des GS-Handbuches
- Beginn der Gültigkeit der Selbsterklärung (Ausstellungsdatum)
- Ende der Gültigkeit der Selbsterklärung (2 Jahre nach Ausstellung)

Selbsterklärung mit Testat

Die Selbsterklärung mit Testat muss mindestens folgende Informationen umfassen:

- Die Voraussetzungen einer Selbsterklärung (Einstiegsstufe oder Aufbaustufe) müssen erfüllt werden.
- Die Auditierung wird von einem externen, vom BSI lizenzierten Auditor durchgeführt.
- Das Testat ist ein zusätzlicher Absatz des Antrags, in dem der Auditors die ordnungsgemäße Durchführung eines IT-Grundschutz-Audits bestätigt.

Gültigkeitsdauer und Kosten einer Selbsterklärung

- Die Gültigkeit von einer Selbsterklärung ist auf 2 Jahre beschränkt.
- Eine Verlängerung der Gültigkeit einer Selbsterklärung ist nicht möglich. Es kann ein neuer Antrag für denselben IT-Verbund für eine höhere Sicherheitsstufe gestellt werden.
- Für jegliche Selbsterklärung wird vom BSI eine Pauschalgebühr von 20 Euro erhoben.

Arten der Qualifizierung

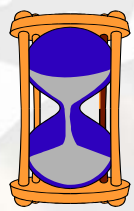
Das Zertifizierungsverfahren ist ein Antragsverfahren.

Der Antrag enthält folgende Informationen

- Name und Adresse der Institution
- Name und Funktion des Unterzeichners
- Ansprechpartner
- Art der Zertifizierung
- Veröffentlichung
- Erklärungen
- Beschreibung des Untersuchungsgegenstandes
- Beschreibung des IT-Verbunds

Gültigkeitsdauer und Kosten eines Zertifikats

- Die Gültigkeit eines IT-Grundschutz-Zertifikats ist auf **2 Jahre** beschränkt.
- Nach Ablauf der Gültigkeit eines IT-Grundschutz-Zertifikats muss ein Re-Zertifizierungsantrag gestellt werden.



- Für eine Zertifizierungsverfahren wird vom BSI eine Pauschalgebühr von **2500 Euro** erhoben.

Inhalt

- Idee der Grundschutz-Zertifizierung
  - Idee des IT-Grundschutzes
  - Sinn und Nutzen eines Grundschutz-Zertifikats
- Voraussetzungen und Vorbereitung
  - Basis-Sicherheitscheck als Vorprüfung
  - Zertifizierung TDS AG
- Ablauf der Prüfung
- Erfahrungen und Empfehlungen

 19

Schritte zum Zertifikat

- Erstkontakt – Vorplanung
- Abschätzung der Erfolgsaussichten
- Projektdefinition → Vertrag
- Vorprüfung
  - IT-Strukturanalyse + Schutzbedarfsfeststellung
  - Modellierung
  - Basis-Sicherheitscheck
- Umsetzung defizitärer Maßnahmen
- Nachkontrolle
- Zertifizierungs-Audit
- Zertifizierung

 20

Übernahme und Überprüfung von Ergebnissen der Vorprüfung

- Manuelle Überprüfung
  - Prüfung auf Vollständigkeit der Dokumente
  - Prüfung auf inhaltliche Konsistenz
  - Prüfung auf Plausibilität der Inhalte
  - Prüfung auf Übereinstimmung mit der Realität (Stichproben)
- Werkzeugunterstützung
  - Werkzeug sollte alle geforderten Dokumente bereitstellen
  - Werkzeug sollte Konsistenzkontrolle erleichtern
    - durch Erzwingen konsistenter Strukturen
    - durch Hervorheben von Inkonsistenzen
  - Plausibilitätsprüfung muss weiter manuell erfolgen
  - Werkzeug sollte die Markierung von Abweichungen erlauben

Unabhängigkeit des Zertifizierungs-Audits

- Das Zertifizierungs-Audit ist **nicht** der Basis-Sicherheitscheck, sondern eine unabhängige Prüfung!
- Die Unabhängigkeit der Prüfung durch den lizenzierten Auditor muss gewährleistet sein.
  - keine Beratung durch den Auditor
  - keine Durchführung des Basis-Sicherheitschecks durch den Auditor
  - weisungsfreies Arbeiten des Auditors muss gewährleistet sein
- Strikte Trennung zwischen den zu prüfenden Dokumenten und dem Zertifizierungsbericht

Inhalt

- Idee der Grundschutz-Zertifizierung
  - Idee des IT-Grundschutzes
  - Sinn und Nutzen eines Grundschutz-Zertifikats
- Voraussetzungen und Vorbereitung
  - Basis-Sicherheitscheck als Vorprüfung
  - Zertifizierung TDS AG
- Ablauf der Prüfung
- Erfahrungen und Empfehlungen

TDS Informationstechnologie AG

- Unternehmenskennzahlen
  - Gründung 1975 (Günter Steffen, Aufsichtsratvorsitzender)
  - Rund 630 Mitarbeiter
  - Hauptsitz Neckarsulm bei Heilbronn
- IT-Verbund
  - Geschäftsbereich Application Hosting
  - 800 Server
  - 450 SAP Systeme
  - 350 Client/Server Systeme
  - 330 Router und Switches
  - 30 Firewalls und Load Balancer

Fragen zum Projektbeginn

- Bestehende Selbsterklärung SOE-0004-2002
- Abbildung des IT-Verbunds auf das IT-GSHB
  - Der IT-Verbund ist sinnvoll abgegrenzt und besitzt die notwendige Mindestgröße, aber es gibt einen
- Anwendbarkeit des IT-GSHB
  - Hoher Anteil an SAP-Systemen
  - Hoher Anteil an Router und Switches
  - Kann das IT-GSHB für eine ausreichende Abbildung sorgen?
  - Bestehen sehr hohe Schutzanforderungen in diesen Bereichen?
- Klärung mit dem Grundschutz-Referat herbeigeführt
  - Schnell, unproblematisch und unbürokratisch
    ...wie auf dem letzten Auditorentreffen versprochen

Vor der Zertifizierung

- Aufbau des Sicherheitsmanagements aus dem Qualitätsmanagement heraus
  - Projektleitung TDS: Knut Krabbes
  - Quality und Facility Security Manager
  - ISO 9000 und IT-Grundschutz-Auditor
- Stärken
  - Bauliche Sicherheit
  - Notfallvorsorge
- Update der Dokumentenlage im Unternehmen
  - Formale Regelungen gut funktionierender, adäquater Prozesse
  - Schaffung von Awareness

Prüfgrundlage Basis-Sicherheitscheck

- Die „Generalprobe“
  - Anlegen des Zertifizierungsmaßstabs
  - Vermeidung von Nachprüfungen
  - Reibungsloser Ablauf der Zertifizierung
  - Ziel: Erstes Zertifikat für einen solchen IT-Verbund
- Durchgängiger Einsatz der Werkzeugunterstützung (SAVe®)
  - Schnelle Erfassung
  - Transparente Darstellung
  - To Do – Liste mit Fälligkeiten und Verantwortlichkeiten
  - Projektstand darstellbar

Ergebnisse der Vorprüfung

Filter: Baustein: 4.2 Verkabelung
Nur bearbeitete Maßnahmen

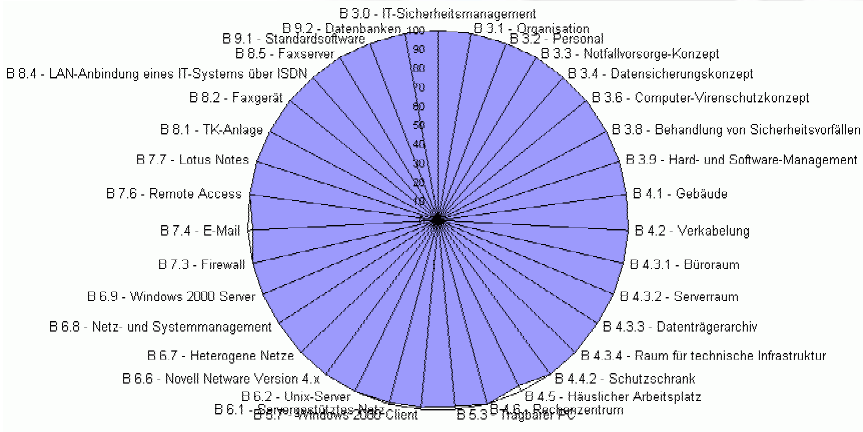
Basis-Sicherheitscheck — **Datenbestand:** Daten für Zertifikats-Audit

Bundesamt für Organisation und Verwaltung (BOV) — **Gültigkeitsbereich / IT-System:** Gesamtnetz; **Standort:** Keller; **Benutzer:** Netzverwaltung

Nr.	Prio Zertifikat	Opt.	Beschreibung	ja	z.T.	Nein	n/a	fällig	verantwortlich	Begründung für Nicht-Umsetzung / Bemerkungen	Kosten
4.2			**Verkabelung**								
M 1.9	1 Einstieg	☐	Brandabschottung von Trassen	◉	○	○	○				
M 1.20	3 Einstieg	☐	Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht	◉	○	○	○				
M 1.21	2 Einstieg	☐	Ausreichende Trassendimensionierung	◉	○	○	○				
M 1.22	3 zusätzlich	☑	Materielle Sicherung von Leitungen und Verteilern	○	○	◉	○	30.04.2004	Hr. Gebhart		€ 2.500,-
M 1.39	3 zusätzlich	☐	Verhinderung von Ausgleichsströmen auf Schirmungen	○	○	◉	○			zurückgestellt - bisher keine Probleme	
M 2.19	2 Aufbau	☐	Neutrale Dokumentation in den Verteilern	◉	○	○	○				
M 2.20	3 zusätzlich	☑	Kontrolle bestehender Verbindungen	○	◉	○	○	31.03.2004	Hr. Schneffke		€ 400,- / Monat
M 5.1	3 Aufbau	☐	Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen	◉	○	○	○				
M 5.2	2 Einstieg	☐	Auswahl einer geeigneten Netz-Topographie	○	○	○	◉			durch Gebäudeverkabelung vorgegeben	

Legende zur Maßnahmenumsetzung: "Ja": vollständig umgesetzt - "z.T.": teilweise umgesetzt - "Nein": nicht umgesetzt - "n/a": entbehrlich

Maßnahmenumsetzung Basis-Sicherheitscheck TDS AG



- Basis: alle Maßnahmen IT-GSHB (inkl. zusätzlicher Maßnahmen)

Inhalt

IT-Symposium 2004

- Idee der Grundschutz-Zertifizierung
  - Idee des IT-Grundschutzes
  - Sinn und Nutzen eines Grundschutz-Zertifikats
- Voraussetzungen und Vorbereitung
  - Basis-Sicherheitscheck als Vorprüfung
  - Zertifizierung TDS AG
- Ablauf der Prüfung
- Erfahrungen und Empfehlungen

Ablauf des Zertifizierungsaudits

- Sichtung der Referenzdokumente
- Verifikation des Basis-Sicherheitschecks
- Erstellung des Auditreports
  - Umfang: 170 Seiten
- Prüfung durch das BSI
  - Fachlich: IT-Grundschutzreferat
  - Formell: Zertifizierungsstelle
- Ausstellung und Übergabe des Zertifikats

Überprüfung der IT-Strukturanalyse

- Definition des Untersuchungsgegenstands
  - Abgrenzung / Umfang des IT-Verbunds
  - Firmen-/Behördenprofil / Beschreibung der Tätigkeitsfelder
- Bereinigter Netzplan
- Liste der IT-Systeme
  - Konformität mit dem Netzplan
- Liste der IT-Anwendungen
  - Software-Produkte
  - Einzelaufgaben
  - Geschäftsprozesse
- Liste der Räume ???
- Liste der Kommunikations-verbindungen ???

sinnvoll? nachvoll-ziehbar?

identifizierbare Komponenten?

vollständige Informationen?

eindeutig? Zuordnung zu den IT-Systemen?

Warum fehlen diese Listen?

Überprüfung der Schutzbedarfsfeststellung

- Definition der Schutzbedarfskategorien — plausibel?
  - i.a. mit Bezug auf die Definitionen des GSHB — vollständig?
- Schutzbedarf der IT-Anwendungen
  - mit stichhaltiger, nachvollziehbarer Begründung — vollständig? plausibel?
- Schutzbedarf der IT-Systeme — begründet?
- Kritikalität der Kommunikationsverbindungen
  - Unterscheidung in kritische / nicht-kritische Verbindungen
  - Liste der kritischen Verbindungen oder Hervorhebung im Netzplan
- Schutzbedarf der IT-Räume — plausibel?
  - aus dem Schutzbedarf der IT-Systeme/Datenträger abgeleitet

Überprüfung der Modellierung

- Jeder Baustein muss auf **alle** Zielobjekte im IT-Verbund angewandt werden, für die er relevant ist: — vollständig?
  - alle IT-Systeme (siehe Liste der IT-Systeme)
  - alle Räume, in denen diese IT-Systeme betrieben werden
- Anwendbarkeit des Grundschutzhandbuchs — korrekt?
  - direkte Modellierung des überwiegenden Teils des IT-Verbunds
  - Schutzbedarf der nicht direkt modellierbaren Komponenten darf nicht „sehr hoch“ sein
  - korrekte Anwendung ähnlicher oder generischer Bausteine
- Korrektheit der Gruppenbildung — korrekt?
  - Komponenten vom gleichen Typ
  - gleich oder nahezu gleich konfiguriert / in das Netz eingebunden
  - gleiche administrative, infrastrukturelle Rahmenbedingungen
  - Bedienung gleicher Anwendungen

Überprüfung des Basis-Sicherheitschecks

- Baustein-Auswahl
  - dieselben Bausteine wie in der Modellierung
- Transparenz der Interview-Partner
  - befragte Personen mit Name und Funktion gekennzeichnet
  - ggf. Funktionsbezeichnung in der Institution
  - Abbildung auf die im GSHB definierten Rollen kann hilfreich sein
- Umsetzungsgrad der IT-Grundschutz-Maßnahmen
  - **alle** Maßnahmen der Stufen A, B und C behandelt
  - Begründung für entbehrliche Maßnahmen
  - maximal eine Maßnahme nicht / teilweise umgesetzt
- Prüfung der Umsetzung beschränkt sich auf definierte Stichprobe (i.a. 10 ausgewählte Bausteine)

korrekt?

verständlich?

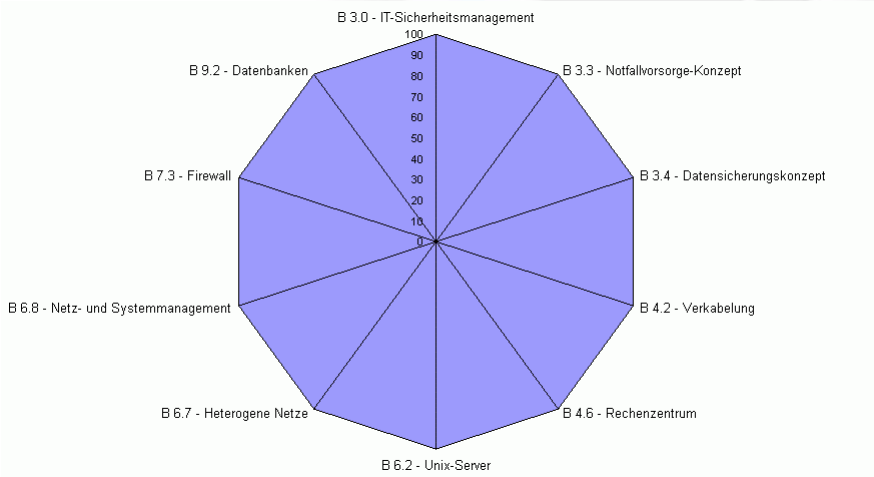
korrekt dokumentiert?

Auswahl der Stichproben

- 3.0 IT-Sicherheitsmanagement
- 3.3 Notfallvorsorgekonzept
- 4.6 Rechenzentrum
- 6.2 UNIX-Server
- 6.7 Heterogene Netze
- 9.2 Datenbanken
- 3.4 Datensicherungskonzept
- 4.2 Verkabelung
- 6.8 Netz- u.Systemmanagement
- 7.3 Firewall

- Begründungen für die Bausteinauswahl
  - Vernachlässigung der Zufälligkeitsprinzips
  - Anwendung einer angenommenen Kundensicht
  - Prüfung charakteristischer Aspekte des IT-Verbunds
  - Transparenz des Audits (und des Zertifikats)
  - Vorbeugung vor Kritik „nicht den Kern getroffen zu haben“

Maßnahmenumsetzung Zertifizierungs-Audit



Inhalt

IT-Symposium 2004

- Idee der Grundschutz-Zertifizierung
  - Idee des IT-Grundschutzes
  - Sinn und Nutzen eines Grundschutz-Zertifikats
- Voraussetzungen und Vorbereitung
  - Basis-Sicherheitscheck als Vorprüfung
  - Zertifizierung TDS AG
- Ablauf der Prüfung
- Erfahrungen und Empfehlungen

Erfolgsfaktoren

- Abstrahierung des Schutzbedarfs der Anwendungen
  - Klassifizierung anhand der Verfügbarkeitsanforderungen (SLA's)
  - Klassifizierung anhand der Vertraulichkeit (z.B. SAP HR Module)
- Konsequente Anwendung der Gruppenbildung
  - Anwendungen und Server
  - Netzkomponenten und Managementkomponenten
  - Und: Zusammenfassung der vier Rechenzentren als Gruppe
- Durchgängiger Einsatz einer Werkzeugunterstützung
  - Erläuterungen zur Maßnahmenumsetzung (10 Stichproben)
  - Leichte Prüfung der Vollständigkeit
  - Filterung auf Prüfkriterien (z.B. Begründung der Entbehrlichkeit)

Erfahrungen aus dem Audit

- Gute Anwendbarkeit des Prüfschemas
- Hauptsächlicher Knackpunkte
  - Der „bereinigte Netzplan"
  - Kritikalität der Kommunikationsverbindungen
- Optimierung des Werkzeugs
  - Unterstützung des Auditreports
  - Neues Objekt: Kommunikationsverbindungen (inkl. Kritikalität)
- Resonanz
  - Überreichung des Zertifikats durch Dr. Helmbrecht (Systems 2003)
  - Zwei Presseerklärungen durch das BSI
  - Beteiligung von Pressevertretern
- Hervorragende Unterstützung durch das BSI

Empfehlungen für die Vorprüfung

- Vorprüfung sollte mit demselben Maßstab wie bei einer Zertifizierung erfolgen
  - schärfere Prüfung schreckt vor der Zertifizierung ab
  - schwächere Prüfung bringt Risiko, dass Mängel erst in der Zertifizierung erkannt werden
- Prüfer sollte das Zertifizierungsschema beherrschen
  - **auch die Vorprüfung sollte durch einen lizenzierten Auditor erfolgen**
- Realistische, vollständige Modellierung des IT-Verbunds
- Basis-Sicherheitscheck sollte die Zertifizierung vorbereiten
  - alle Entscheidungen über die Maßnahmenumsetzung begründen
  - Vorgaben für die Umsetzung defizitärer Maßnahmen machen
    - Termine
    - Verantwortliche

Nachbesserungen

- Unterstützung bei der Umsetzung defizitärer Maßnahmen
  - Vorprüfer kennt die Defizite
  - Vorprüfer kennt die Anforderungen für die Zertifizierung
- Hilfe bei der Erstellung fehlender Dokumentation
  - auf der Basis der Maßnahmen im GSHB
  - mit Hilfe vorhandener Templates in den Hilfsmaterialien zum GSHB
  - Anpassung an lokale Gegebenheiten / Organisationsstrukturen
    - vor allem bei der Erstellung von Security Policy / Notfallhandbuch
- Überprüfung auf Vollständigkeit der Nachbesserungen
  - damit nicht erst beim Zertifizierungs-Audit Lücken auffallen
  - überarbeitete Ergebnisse des Basis-Sicherheitschecks bilden die Grundlage für das Zertifizierungs-Audit

Das Zertifizierungs-Audit

- Anforderungen ergeben sich aus dem Prüfschema für Auditoren
- Prüfung kann relativ schnell erfolgen, wenn
  - die Vorprüfung sorgfältig durchgeführt wurde
  - alle Ergebnisse der Vorprüfung sauber dokumentiert sind
  - die Dokumentation der Vorprüfung in einer direkt für die Zertifizierung nutzbaren Form erfolgt ist
  - der IT-Verbund nach der Vorprüfung nicht mehr verändert wurde
    - Zertifizierungs-Audit sollte zeitnah nach der Vorprüfung erfolgen
    - Zeitraum für die Nachbesserungen wird hierdurch eingeschränkt
- Vollständigkeit der Dokumente muss gegeben sein
- Verifikation beschränkt sich auf Stichproben

Presseberichte Zertifizierung

- Übergabe des TDS-Zertifikats, Systems 2003

BSI-Präsident Dr. Udo Helmbrecht, TDS CIO Thomas Gebhardt und QM Knut Krabbes, Auditor Frank Reiländer und Geschäftsführer Holger Henn (beide INFODAS) stoßen auf das IT-Grundschutz-Zertifikat und das erfolgreiche Projekt an.

Pressebeispiel zur Übergabe des SAP SI-Zertifikats, CeBIT 2004

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn
Telefon: 01888 95820
Telefax: 01888 9582-400
E-Mail: bsi@bsi.bund.de

suche | Home | Kontakt | Impressum | Datenschutz |

Über das BSI | Aktuelles | Jobs/Einkauf | Veranstaltungen | Publikationen | English
Schwerpunkte | Fachthemen | Projekte | Produkte/Tools | Presse | FAQ/Links

Presse

- Aktuell
- Archiv
- Newsletter

Pressemitteilung

Bundesamt für Sicherheit in der Informationstechnik überreicht IT-Grundschutz-Zertifikat an SAP SI Hosting

Bonn, 19. März 2004 – Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), überreicht heute Uwe Ripprich, Leiter Hosting bei SAP Systems Integration AG (SAP SI), das IT-Grundschutz-Zertifikat. Dieses Zertifikat bestätigt die Umsetzung aller notwendigen IT-Sicherheitsmaßnahmen im Geschäftsbereich Hosting des IT-Service-Unternehmens und gilt zwei Jahre.

„Mit dem IT-Grundschutz-Zertifikat dokumentiert das Unternehmen, dass es die im IT-Grundschutzhandbuch des BSI (GSHB) empfohlenen Sicherheitsmaßnahmen umgesetzt hat", erklärte Dr. Udo Helmbrecht. Die Überprüfung erfolgte im Rahmen eines Audits. Bei der SAP SI waren Dr. Gerhard Weck und Frank Reiländer (INFODAS) als Auditoren tätig. Weck und Reiländer sind zwei von rund einhundert lizenzierten IT-Grundschutz-Auditoren des BSI. Die Ergebnisse der Zertifizierung können im Internet unter www.bsi.bund.de/gshb/zert/t_zert.htm eingesehen werden.

Zum zertifizierten IT-Verbund zählt das Outsourcing Netz mit der gesamten Netzwerktechnik, die unter vollständiger Kontrolle des Geschäftsbereichs Hosting betrieben wird. Das reicht von den Kundenschnittstellen (Routern) über Firewall-Systeme, Backbone Switches bis zu den über 400 Windows- und Unix-basierten Kundenservern zum Hosten der SAP-Anwendungen in drei hochverfügbaren Serverzentren am Standort Dresden.

Zertifikatsübergabe auf dem SAP-Messestand
v.l.n.r.: Dr. Udo Helmbrecht (BSI), Uwe Ripprich (SAP), Dr. Gerhard Heck (INFODAS)

Weitere Informationen

BSI Forum
2003*6 11. Jahrgang

BSI Forum
Organ des Bundesamtes für Sicherheit in der Informationstechnik

Inhalt

Erstes IT-Grundschutz-Zertifikat für ein Rechenzentrum 35
Kritische Infrastrukturen 43
Amtliche Mitteilungen 47

IT-Grundschutz

Erstes IT-Grundschutz-Zertifikat für ein Rechenzentrum

Am 22. Oktober 2003 hat die TDS Informationstechnologie AG, Neckarsulm, ein IT-Grundschutz-Zertifikat für den Geschäftsbereich Application Hosting erhalten. Basierend auf einer Sachstandsbeschreibung des IT-Grundschutzes zeigt dieser Beitrag aus Sicht des durchführenden Auditors, wie sich das Zertifizierungsschema für ein Outsourcing-Rechenzentrum anwenden lässt. IT-Grundschutz-Interessenten finden Tipps und einen Ausblick auf die weitere IT-Grundschutz-Entwicklung.

Von Frank Reiländer, INFODAS GmbH, Köln

Bei der Überreichung des IT-Grundschutz-Zertifikats an die TDS Informationstechnologie AG, Neckarsulm, vertreten durch Thomas Gebhardt, CIO und Geschäfts- Grundschutz-Handbuch (IT-GSHB) schon beschritten hat. In vielen Behörden und Unternehmen bildetes – oft seit langem – die Basis für eine kontinuierliche Umsetzung von

Impressum

Redaktion:
Michael Dickopf (verantwortlich)
Pressesprecher
E-Mail: Michael.Dickopf@bsi.bund.de

Anja Hartmann
Referatsleiterin Marketing, Öffentlichkeitsarbeit
E-Mail: Anja.Hartmann@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Postfach 20 03 63

- Erfahrungsbericht zur Grundschutz-Zertifizierung
- Gedanken zur Anwendbarkeit des IT-GSHB
- Trends in der Zertifizierung

- BSI Forum <kes> 2003#6
- www.infodas.de/download/KES6-35-42.pdf

Erfolg mit Sicherheit
Lizenzierte Grundschutz-Auditoren

- Dr. Gerhard Weck
  - Lizenz-Nr.BSI-GSL-0021-2002
  - Gültigkeitsdauer 01.01.2002 – 31.12.2006
  - Zertifizierung SAP SI AG, Dresden BSI-GSZ-005-2004

- Frank Reiländer
  - Lizenz-Nr. BSI-GSL-0059-2003
  - Gültigkeitsdauer 03.04.2003 – 02.04.2008
  - Zertifizierung TDS AG BSI-GSZ-003-2003

* GSL = IT-Grundschutz-Lizenz
GSZ = IT-Grundschutz-Zertifikat

 47

IT-Symposium 2004
1B08 – 20. April 2004

Praxisbericht Grundschutzzertifizierung

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf Ihre Fragen und Anforderungen:

INFODAS GmbH, Rhonestraße 2, D-50765 Köln
info@save-infodas.de oder www.save-infodas.de