# Neustrukturierung des IT-Grundschutzes

Dr. Gerhard Weck, INFODAS GmbH, Köln

27. DECUS Symposium 2004 in Bonn
Vortrag 1B07

## Inhalt

- Anforderungen
- Strukturierung nach dem Schichtenmodell
  - Neue Struktur des Handbuches
  - Aufbau von Teil B – Bausteine
- Entfernung von Redundanzen
  - Typen von Redundanzen: formal / inhaltlich
  - Entscheidungsfindung / Regeln zur Entfernung von Redundanzen
  - Sicherung der Konsistenz
  - Blick in den Werkzeugkasten
- Ersetzen der Prioritäten
- Lebenszyklus der Maßnahmen in den Bausteinen
- Überarbeitung generischer IT-System-Bausteine

## Anforderungen

- Konsequente Strukturierung nach dem Schichtenmodell
- Entfernung überflüssiger Redundanzen
  - formale Redundanzen durch Mehrfachreferenzierung von Maßnahmen
  - inhaltliche Redundanzen durch Überdeckung verschiedener Maßnahmen
- Ersetzen der Prioritäten durch Zertifizierungsstufen
- Lebenszyklusmodell für alle Bausteine
- Überarbeitung generischer IT-System-Bausteine
- Aktualisierung der Einleitungskapitel
  - Anpassung der Beschreibung an geänderte Struktur des IT-Grundschutzhandbuchs




## Strukturierung nach dem Schichtenmodell

- Bisherige Kapitelstruktur ist historisch gewachsen
  - Aufteilung entspricht nur zum Teil der Schichtenstruktur
  - Zuordnung einiger (älterer) Bausteine in die falsche Schicht
- Modellierung nach Schichten führt zur Zusammenfassung von Bausteinen aus verschiedenen Kapiteln
  - z.T. unübersichtlich
  - Aufwand / Fehleranfälligkeit bei der Zuordnung
- Ziel: Neustrukturierung der Bausteine gemäß Schichten
  - ändert die Kapitelaufteilung
  - erfordert neue Baustein-Numerierung
  - Numerierung von Maßnahmen / Gefährdungen unverändert

## Neue Struktur des Handbuches

- Kapitel 1 – Wegweiser durch das IT-Grundschutzhandbuch
- Kapitel 2 – Anwendung des IT-Grundschutzhandbuchs
- Kapitel 3 – IT-Sicherheitsmanagement
  - enthält den ehemaligen Baustein 3.0 als neuen Baustein B 1.0
- Teil B – Bausteine
  - aufgeteilt nach dem Schichtenmodell
  - mit neuer Numerierung der Bausteine
- Teil G – Gefährdungen
  - mit unveränderter Struktur
- Teil M – Maßnahmen
  - mit unveränderter Struktur



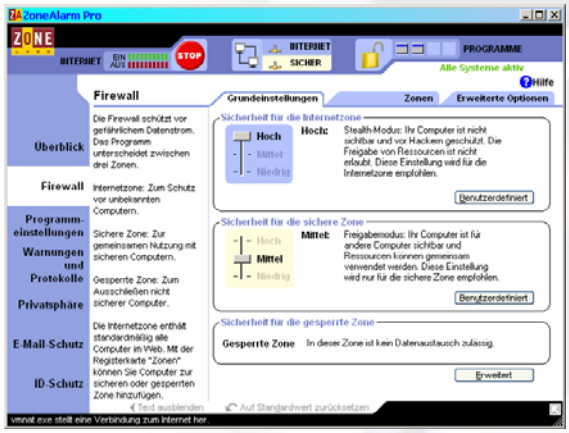

## Einordnung: Was ist ein Firewall?

- Ein Firewall ist ein IT-System

Beispiel: CISCO PIX

# Was ist ein Firewall?

- Ein Firewall ist eine Anwendungs-Software

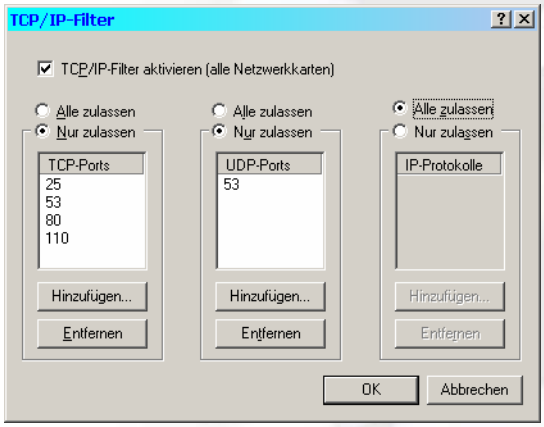



Beispiel: ZoneAlarm



# Was ist ein Firewall?

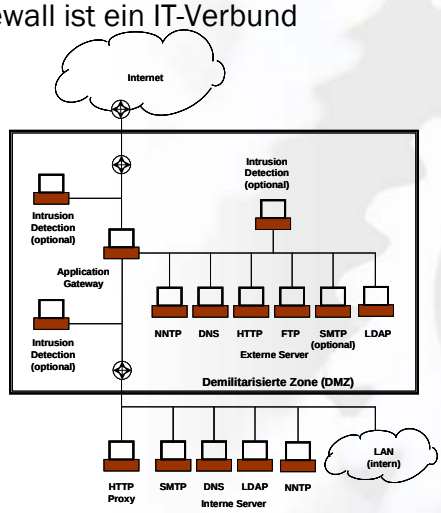
- Ein Firewall ist eine Funktion des Betriebssystems




Beispiel: IP-Filter in Windows 2000/XP

# Was ist ein Firewall?

- Ein Firewall ist ein IT-Verbund




Beispiel:
komplexes
Firewall-System
mit Servern
in einer DMZ




# Verschiebung von Bausteinen

- 6.3 Peer-to-Peer-Dienste wird zu B 5.1
  - von Schicht 3 – Sicherheit der IT-Systeme
  - nach Schicht 5 – Sicherheit in Anwendungen
- 7.3 Firewall wird zu B 3.301
  - von Schicht 4 – Sicherheit im Netz
  - nach Schicht 3 – Sicherheit der IT-Systeme
- 9.3 Telearbeit wird zu B 5.8
  - von Schicht 3 – Sicherheit der IT-Systeme
  - nach Schicht 5 – Sicherheit in Anwendungen

Einordnung in eigene Gruppe von IT-Systemen

## Aufbau von Teil B – Bausteine

- B 1 – Schicht 1: Übergeordnete Aspekte der IT-Sicherheit
  - B 1.1 Organisation (war 3.1)
  - B 1.2 Personal (war 3.2)
  - B 1.3 Notfallvorsorgekonzept (war 3.3)
  - B 1.4 Datensicherungskonzept (war 3.4)
  - B 1.6 Computer-Virenschutzkonzept (war 3.6)
  - B 1.7 Kryptokonzept (war 3.7)
  - B 1.8 Behandlung von Sicherheitsvorfällen (war 3.8)
  - B 1.9 Hard- und Software-Management (war 3.9)
  - B 1.10 Standardsoftware (war 9.1)
  - B 1.11 Outsourcing (war 3.10)
  - B 1.12 Archivierung (war 9.5)




## Aufbau von Teil B – Bausteine

- B 2 – Schicht 2: Sicherheit der Infrastruktur
  - B 2.1 Gebäude (war 4.1)
  - B 2.2 Verkabelung (war 4.2)
  - B 2.3 Büroraum (war 4.3.1)
  - B 2.4 Serverraum (war 4.3.2)
  - B 2.5 Datenträgerarchiv (war 4.3.3)
  - B 2.6 Raum für technische Infrastruktur (war 4.3.4)
  - B 2.7 Schutzschrank (war 4.4)
  - B 2.8 Häuslicher Arbeitsplatz (war 4.5)
  - B 2.9 Rechenzentrum (war 4.6)

## Aufbau von Teil B – Bausteine

- B 3 – Schicht 3: Sicherheit der IT-Systeme
  - Server
    - B 3.101 Allgemeiner Server (war 6.1)
    - B 3.102 Server unter Unix (war 6.2)
    - B 3.103 Server unter Windows NT (war 6.4)
    - B 3.104 Server unter Novell Netware 3.x (war 6.5)
    - B 3.105 Server unter Novell Netware 4.x (war 6.6)
    - B 3.106 Server unter Windows 2000 (war 6.9)
  - Clients
    - B 3.201 Allgemeiner Client (war 5.99)
    - B 3.202 Allgemeines nicht vernetztes IT-System (war 5.99)
    - B 3.203 Laptop (war 5.3)
    - B 3.204 Client mit wechselnden Benutzern (war 5.4)
    - B 3.205 Client unter DOS (war 5.1)




## Aufbau von Teil B – Bausteine

- B 3 – Schicht 3: Sicherheit der IT-Systeme
  - Netzkomponenten
    - B 3.301 Firewall (war 7.3)
    - B 3.302 Router und Switches (neu)
  - Sonstiges
    - B 3.401 TK-Anlage (war 8.1)
    - B 3.402 Faxgerät (war 8.2)
    - B 3.403 Anrufbeantworter (war 8.3)
    - B 3.404 Mobiltelefon (war 8.6)
- B 4 – Schicht 4: Sicherheit im Netz
  - B 4.1 Heterogene Netze (war 6.7)
  - B 4.2 Netz- und Systemmanagement (war 6.8)
  - B 4.3 Modem (war 7.2)
  - B 4.4 Remote Access (war 7.6)
  - B 4.5 LAN-Anbindung eines IT-Systems über ISDN (war 8.4)

## Aufbau von Teil B – Bausteine

- B 5 – Schicht 5: Sicherheit in Anwendungen
  - B 5.1 Peer-to-Peer-Dienste (war 6.3)
  - B 5.2 Datenträgeraustausch (war 7.1)
  - B 5.3 E-Mail (war 7.4)
  - B 5.4 WWW-Server (war 7.5)
  - B 5.5 Lotus Notes (war 7.7)
  - B 5.6 Faxserver (war 8.5)
  - B 5.7 Datenbanken (war 9.2)
  - B 5.8 Telearbeit (war 9.3)
  - B 5.9 Novell eDirectory (9.4)
  - B 5.10 Internet Information Server (war 7.8)
  - B 5.11 Apache Webserver (war 7.9)
  - B 5.12 Exchange/Outlook (war 7.10)




## Das Problem der Redundanz

- Identische Grundschutzmaßnahmen sind in mehreren Bausteinen enthalten
  1. um unterschiedliche Anwendungsbereiche zu beschreiben
  2. um die Wichtigkeit der Maßnahme zu unterstreichen
  3. aus historischen Gründen (weil damals noch keine übergreifenden Bausteine wie 3.9 verfügbar waren)
- Fälle 2 und 3 führen zur Mehrfacherfassung identischer Sachverhalte
  - erhöhter Aufwand bei der Erfassung
  - ggf. Verärgerung der Kunden („Schon wieder …!“)
  - Gefahr von Inkonsistenzen („Welche Version ist denn jetzt die richtige?“)
- Defizit bei einer mehrfach vorkommenden Maßnahme führt zur Nicht-Erfüllung mehrerer Bausteine

# Lösungsansätze

- Manuelles Kopieren der schon erfassten Daten, wenn dieselbe Maßnahme in einem weiteren Baustein vorkommt
- Werkzeuggestütztes Kopieren bei mehrfach referenzierten Maßnahmen
- Vergleich aller erfassten Daten zur gleichen Maßnahme in unterschiedlichen Bausteinen
  - manuell
  - werkzeuggestützt durch Konsistenz-Reports
- Kontrolle ist bei jedem Projekt wieder von Neuem erforderlich




# Manuelles Kopieren

**IT-Grundschutzerhebung: Formular zu Baustein 5.5 PC unter Windows NT**

| | | | | | |
|---|---|---|---|---|---|
| Nummer des IT-Systems: | | erfasst am: | | befragte Personen: | |
| Bezeichnung: | | erfasst durch: | | - " - | |
| Standort: | | | | - " - | |
| | | | | - " - | |
| | | | | - " - | |

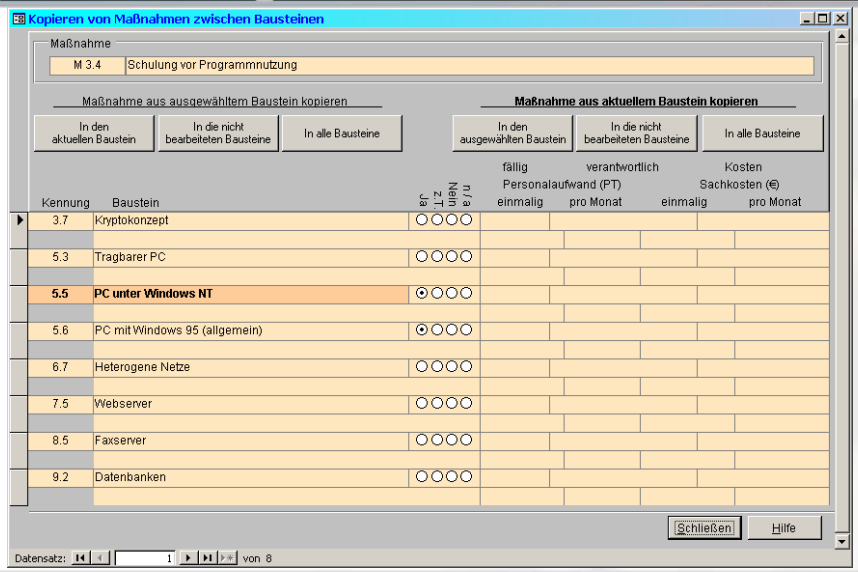
| Maßnahme (Priorität) [Siegel] | Baustein 5.5 PC unter Windows NT | entbehrlich | Ja | teilweise | Nein | Umsetzung bis | verantwortlich | Bemerkungen / Begründung für Nicht-Umsetzung | Kostenschätzung |
|---|---|---|---|---|---|---|---|---|---|
| M 1.29 (3) [A] | Geeignete Aufstellung eines IT-Systems (optional) | | | | | | | | |
| M 3.4 (1) [A] | Schulung vor Programmnutzung | | X | | | | | zentral geregelt | |
| M 3.5 (1) [A] | Schulung zu IT-Sicherheitsmaßnahmen | | | X | | | | im Aufbau | |

**IT-Grundschutzerhebung: Formular zu Baustein 7.7 Lotus Notes**

| | | | | | |
|---|---|---|---|---|---|
| Nummer des IT-Systems: | | erfasst am: | | befragte Personen: | |
| Bezeichnung: | | erfasst durch: | | - " - | |
| Standort: | | | | - " - | |
| | | | | - " - | |
| | | | | - " - | |

| Maßnahme (Priorität) [Siegel] | Baustein 7.7 Lotus Notes | entbehrlich | Ja | teilweise | Nein | Umsetzung bis | verantwortlich | Bemerkungen / Begründung für Nicht-Umsetzung | Kostenschätzung |
|---|---|---|---|---|---|---|---|---|---|
| M 1.29 (1) [A] | Geeignete Aufstellung eines IT-Systems | | | | | | | | |
| M 3.4 (1) [A] | Schulung vor Programmnutzung | | X | | | | | zentral geregelt | |
| M 3.5 (1) [A] | Schulung zu IT-Sicherheitsmaßnahmen | | | X | | | | im Aufbau | |

# Kopieren mit Werkzeug-Unterstützung






# Konsistenz-Überprüfung

## Konsistenz der Maßnahmenumsetzung

**Datenbestand:** Standort Bonn

**Bundesamt für Organisation und Verwaltung (BOV)**

| Nr. | Beschreibung | Ja | z.T. | Nein | n/a | fällig | verantwortlich | Personalaufwand (PT) einmalig | Bemerkungen | Sachkosten (€) einmalig | Kosten pro Monat |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **M 2.8** | **Vergabe von Zugriffsrechten** | | | | | | | | | | |
| 3.1 | Organisation | ◉ | ○ | ○ | ○ | | | | | | |
| **M 2.9** | **Nutzungsverbot nicht freigegebener Hard- und Software** | | | | | | | | | | |
| 5.3 | Tragbarer PC | ○ | ○ | ○ | ○ | | | | | | |
| 5.5 | PC unter Windows NT | ◉ | ○ | ○ | ○ | | | | | | |
| 5.6 | PC mit Windows 95 (allgemein) | ◉ | ○ | ○ | ○ | | | | | | |
| **M 2.10** | **Überprüfung des Hard- und Software-Bestandes** | | | | | | | | | | |
| 5.3 | Tragbarer PC | ○ | ○ | ○ | ○ | | | | | | |
| 5.5 | PC unter Windows NT | ◉ | ○ | ○ | ○ | | | | wird automatisch durchgeführt | | |
| 5.6 | PC mit Windows 95 (allgemein) | ○ | ○ | ◉ | ○ | 30.04.2001 | Hr. Meyer | | | | ca. DM 100,- / Monat |
| | | | 0,1 | | | | | | | | |
| **M 2.13** | **Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln** | | | | | | | | | | |
| 3.1 | Organisation | ◉ | ○ | ○ | ○ | | | | | | |
| 5.3 | Tragbarer PC | ○ | ○ | ○ | ○ | | | | | | |
| 5.5 | PC unter Windows NT | ○ | ◉ | ○ | ○ | 01.04.2002 | Hr. Schmitz | 100,00 | für Disketten noch nicht durchgängig geregelt | | DM 200,- / Monat |
| 5.6 | PC mit Windows 95 (allgemein) | ○ | ◉ | ○ | ○ | 01.04.2002 | Hr. Schmitz | 100,00 | für Disketten noch nicht durchgängig geregelt | | DM 200,- / Monat |

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

## Bewertung der Alternativen

- Manuelles Übertragen:
  - hoher Aufwand
  - Inkonsistenzen durch Unachtsamkeit
- Werkzeuggestütztes Kopieren:
  - Gefahr der Übernahme nicht zutreffender Informationen („Einmal zu viel geklickt, … und man bereut das für den Rest seines Lebens …“)
- Kontrolle durch Konsistenz-Reports
  - deckt Inkonsistenzen auf – aber …
  - … verhindert sie nicht
- Aufwand für die Behandlung der Inkonsistenzen muss bei allen Alternativen immer wieder getrieben werden




## Die Lösung des Problems

- Eine wirkliche Lösung muss das Problem an der Wurzel anpacken

⇒ Entfernen der Redundanzen im GSHB selbst

- Schritte zu einer Verbesserung:
  - Erkennen, wo die Redundanzen liegen
    - mehrfach referenzierte Maßnahmen
    - Maßnahmen, die sich inhaltlich überdecken
  - Umstrukturierung der Maßnahmenzuordnung
    - unter Verwendung übergeordneter Bausteine
    - unter Berücksichtigung der Zuordnung von Gefährdungen

⇒ Projekt „Restrukturierung und Weiterentwicklung des IT-Grundschutzhandbuches 2004“

# Entfernung formaler Redundanzen

- Eigenschaften formaler Redundanzen
  - Vorkommen derselben Maßnahme in mehreren Bausteinen
    - kann unterschiedliche Ausprägungen einer Maßnahme bedeuten (→ M 1.15 *Geschlossene Fenster und Türen* – unterschiedlich für Gebäude, Serverraum, Büro)
    - kann denselben Sachverhalt in verschiedenem Kontext angeben (→ M 3.4 *Schulung vor Programmnutzung* – wird i.a. zentral für alle Systeme / Anwendungen etc. geregelt)
  - Unterscheidung zwischen beiden Fällen erforderlich
    - M 1.15 muss i.a. mehrfach referenziert bleiben
    - M 3.4 kann i.a. ein einziges Mal abgehandelt werden
- Erkennung formaler Redundanzen
  - werkzeuggestützt durch Datenbankabfragen
  - ergab insgesamt 899 redundante Maßnahmen/Bausteine-Beziehungen




# Bericht zu formalen Redundanzen

**Redundante Maßnahmen und zugeordnete Bausteine**

| Nr. | Beschreibung | |
|---|---|---|
| **M 6.13** | **Erstellung eines Datensicherungsplans** | |
| B 1.3 | Notfallvorsorge-Konzept | Übergreifende Aspekte |
| B 5.8 | Telearbeit | IT-Anwendungen |
| **M 6.16** | **Abschließen von Versicherungen** | |
| B 1.3 | Notfallvorsorge-Konzept | Übergreifende Aspekte |
| B 2.9 | Rechenzentrum | Infrastruktur |
| **M 6.17** | **Alarmierungsplan und Brandschutzübungen** | |
| B 2.1 | Gebäude | Infrastruktur |
| B 2.9 | Rechenzentrum | Infrastruktur |
| **M 6.20** | **Geeignete Aufbewahrung der Backup-Datenträger** | |
| B 3.101 | Servergestütztes Netz | IT-Systeme |
| B 3.202 | Allgemeines nicht vernetztes IT-System (allgemein) | IT-Systeme |
| B 3.203 | Tragbarer PC | IT-Systeme |
| B 3.204 | PCs mit wechselnden Benutzern | IT-Systeme |
| B 3.205 | DOS-PC (ein Benutzer) | IT-Systeme |
| B 3.206 | Unix-System | IT-Systeme |
| B 3.207 | PC unter Windows NT | IT-Systeme |

## Entscheidungsfindung zur Entfernung von Redundanzen

- Maßnahmen in Pflicht-Bausteinen können aus allen anderen Bausteinen entfernt werden
  - Beispiel: M 3.4 *Schulung* ... nur noch in B 1.2 *Personal*
- Maßnahmen für Räume können entfallen, wenn sie für das Gebäude gelten und keine Sonderregelungen gelten
  - Beispiel: M 1.4 *Blitzschutz*... nur noch in B 2.1 *Gebäude*
- Allgemeine Maßnahmen können aus spezifischen Bausteinen in Pflichtbausteine verschoben werden
  - Beispiel: M 2.9 *Nutzungsverbot* ... nur noch in B 1.9 *Hw/Sw-Mgmt*
- Maßnahmen allgemeiner Art müssen in speziellen Bausteinen erhalten bleiben, wenn sie dort eine besondere Ausprägung haben oder von besonderer Wichtigkeit sind
  - Beispiel: M 2.17 *Zutrittsregelung* ... bleibt in B 2.4 *Serverraum*




## Ergebnis der Redundanzverringerung

- Reduktion der mehrfachen Zuordnungen von Maßnahmen zu Bausteinen
  - **899** mehrfache Zuordnungen werden auf **419** reduziert (-54 %)
  - Bericht schrumpft von **35** auf **19** Seiten (-46 %)
  - Zahl der Zuordnungen insgesamt sinkt von **1466** auf **1035** (-29 %)
- Zugeordnete Gefährdungen verschieben sich
  - Akkumulation bei den querschnittlichen Bausteinen
  - Korrektur durch Entfernen von Gefährdungen aus Bausteinen, für die sie nicht relevant sind
  - Überprüfung, ob diesen Gefährdungen dann noch Maßnahmen zugeordnet sind
  - Zahl der Zuordnungen insgesamt sinkt von **7647** auf **4779** (-38 %)

## Regeln für die Zuordnung der Gefährdungen zu Maßnahmen

- Maßnahme entfernt → alle Beziehungen in diesem Baustein zu den zugeordneten Gefährdungen entfernen
- Maßnahme verschoben → Zuordnungen der Gefährdungen übernehmen
- Maßnahme aus mehreren in einen einzigen Baustein übernommen
  - zunächst zugeordneten Gefährdungen übernehmen
  - überflüssige Zuordnungen entfernen
    - Zuordnungen allgemeiner Art in der Regel entfernen
    - Zuordnungen entfernen, wenn spezifischere Maßnahmen / Gefährdungen zugeordnet sind




## Regeln für die Zuordnung der Gefährdungen zu Maßnahmen

- Maßnahme neu zusätzlich übernommen → Gefährdungen zuordnen, die in vergleichbaren Bausteinen zugeordnet sind
- Zuordnung nicht entfernen, wenn durch ihr Entfernen
  - dieser Maßnahme keine weitere Gefährdung mehr in dem betreffenden Baustein zugeordnet ist
  - diese Gefährdung durch keine weitere Maßnahme in dem betreffenden Baustein mehr abgedeckt ist
- Verhindern, dass
  - Maßnahmen entstehen, die keiner Gefährdung zugeordnet sind
  - Gefährdungen existieren, die nicht wenigstens durch eine Maßnahme abgedeckt sind

## Sicherung der Konsistenz

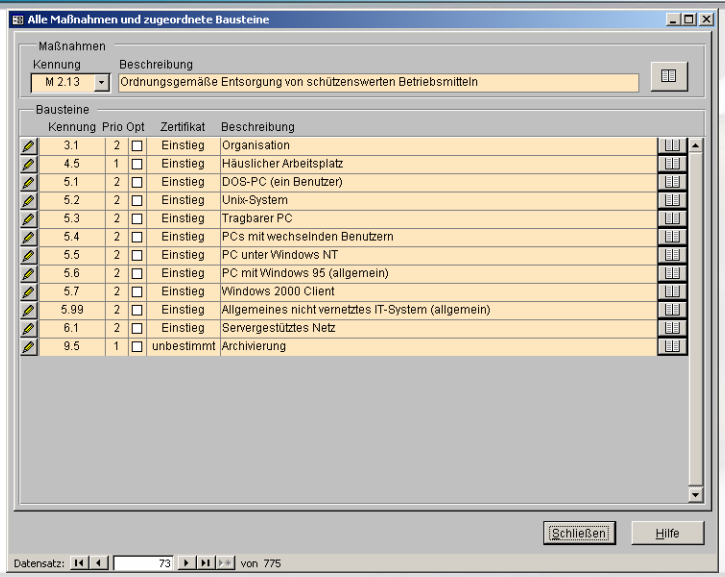
- Prüfung auf „verwaiste“ Maßnahmen / Gefährdungen
- Prüfung auf Angemessenheit
  - der Maßnahmen
  - der Gefährdungen
  - in den betreffenden Bausteinen
- Prüfung auf Notwendigkeit zusätzlicher, redundanter Einträge
  - wegen der Bedeutung von Maßnahmen / Gefährdungen
  - wegen besonderer, spezifischer Umstände
- Vergleich mit dem ursprünglichen Handbuch:
  Sind alle Änderungen korrekt / plausibel?




## Blick in den Werkzeugkasten

- Durchgängige Nutzung der IT-Sicherheitsdatenbank SAVe®
- Konsistenzbedingungen im Datenbank-Schema
- Interaktive Abfragen der Datenbank
- Berichte zu den definierten Zuordnungen
- ad-hoc Abfragen zur Überprüfung spezieller Fehlermöglichkeiten (z.B. verwaiste Objekte)
- Differenzprüfung zur früheren Version
  - Übertragung der Korrespondenztabellen
    - nach Excel
    - ins CSV-Format
    - auf einen VMS-Server
  - Analyse mit der DIFFERENCES-Utility

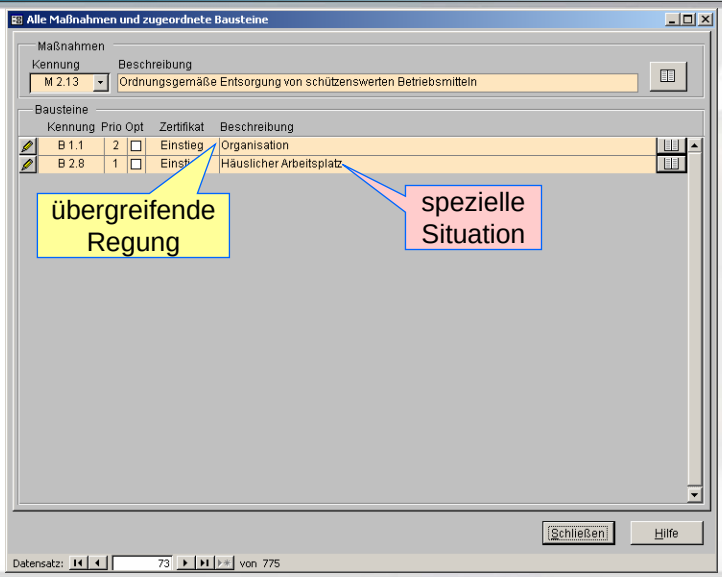
# Typische mehrfach referenzierte Maßnahme



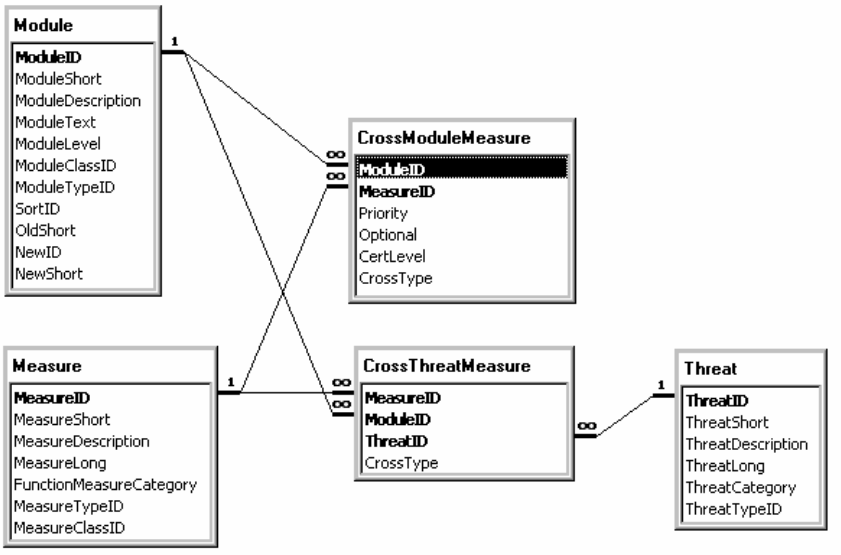




# Maßnahme in der bereinigten Struktur



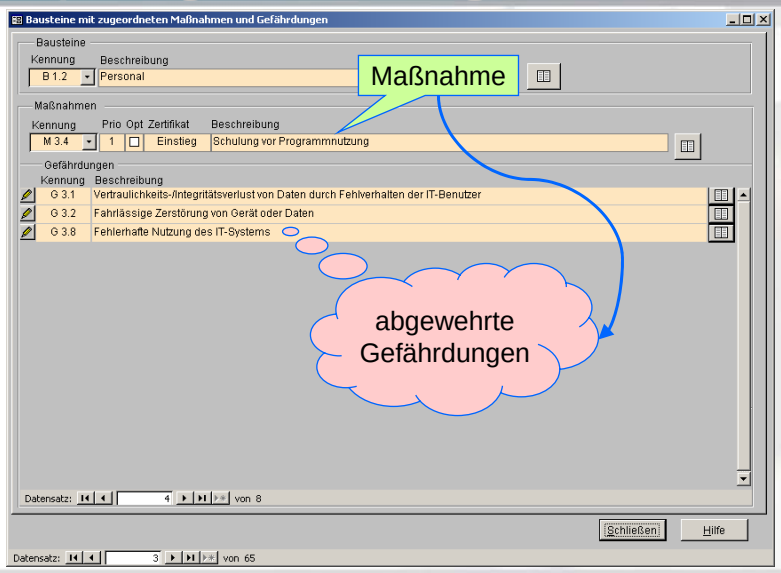
# Die relevanten Tabellen



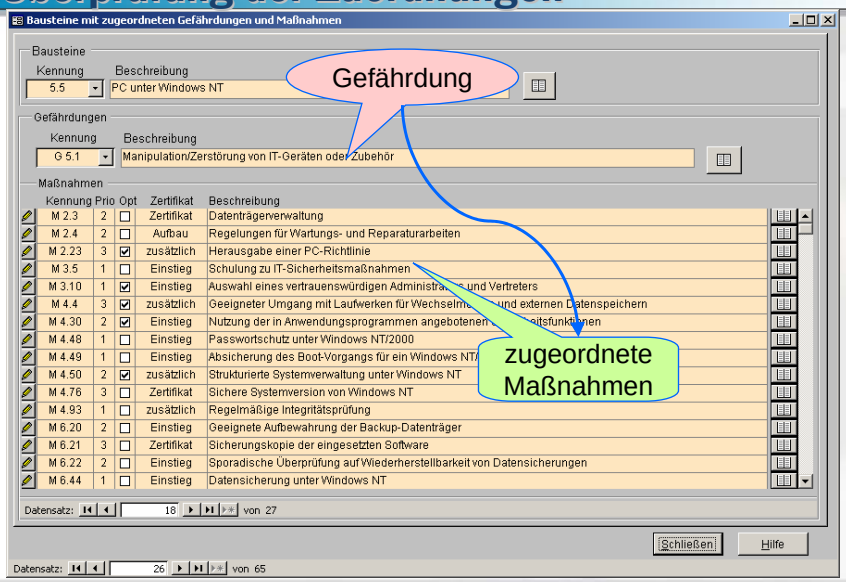




# Überprüfung der Zuordnungen

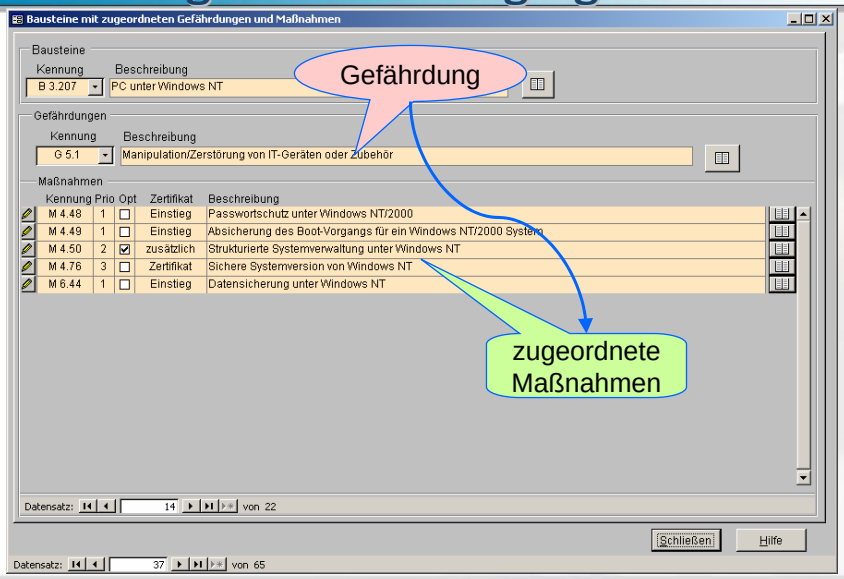


# Überprüfung der Zuordnungen



# Zuordnungen nach Bereinigung



# Zuordnungsbericht

## Maßnahmen, Bausteine und Gefährdungen

| Nr. | Beschreibung | |
|---|---|---|
| **M 1.1** | **Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften** | |
| **B 2.1** | **Gebäude** | **Infrastruktur** |
| G 1.3 | Blitz | |
| G 1.4 | Feuer | |
| G 4.1 | Ausfall der Stromversorgung | |
| G 4.2 | Ausfall interner Versorgungsnetze | |
| G 4.3 | Ausfall vorhandener Sicherungseinrichtungen | |
| **B 2.7** | **Schutzschrank** | **Infrastruktur** |
| G 1.4 | Feuer | |
| G 1.5 | Wasser | |
| G 1.7 | Unzulässige Temperatur und Luftfeuchte | |
| G 1.8 | Staub, Verschmutzung | |
| G 4.3 | Ausfall vorhandener Sicherungseinrichtungen | |
| G 5.1 | Manipulation/Zerstörung von IT-Geräten oder Zubehör | |
| G 5.4 | Diebstahl | |
| G 5.5 | Vandalismus | |
| **B 2.8** | **Häuslicher Arbeitsplatz** | **Infrastruktur** |
| G 1.4 | Feuer | |
| G 1.5 | Wasser | |
| **B 2.9** | **Rechenzentrum** | **Infrastruktur** |

Seite 1 von 197



# Darstellung nach Bausteinen

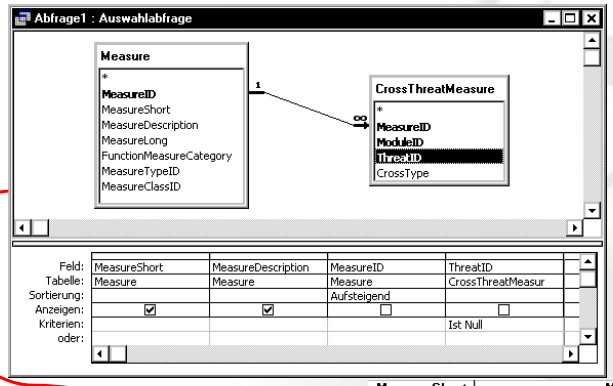
## Bausteine, Maßnahmen und Gefährdungen

Bundesamt für Organisation und Verwaltung (BOV)
Testdatenbestand neue Grundschutzstruktur

| Nr. | Prio | Opt. | Zertifikat | Beschreibung |
|---|---|---|---|---|
| **B 1.1** | | | | **Organisation** |
| **M 2.1** | 2 | ☐ | Einstieg | **Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz** |
| G 2.1 | | | | Fehlende oder unzureichende Regelungen |
| G 2.2 | | | | Unzureichende Kenntnis über Regelungen |
| G 2.6 | | | | Unbefugter Zutritt zu schutzbedürftigen Räumen |
| G 2.7 | | | | Unerlaubte Ausübung von Rechten |
| G 2.8 | | | | Unkontrollierter Einsatz von Betriebsmitteln |
| **M 2.2** | 2 | ☐ | Zertifikat | **Betriebsmittelverwaltung** |
| G 2.1 | | | | Fehlende oder unzureichende Regelungen |
| G 2.3 | | | | Fehlende, ungeeignete, inkompatible Betriebsmittel |
| G 2.5 | | | | Fehlende oder unzureichende Wartung |
| **M 2.4** | 2 | ☐ | Aufbau | **Regelungen für Wartungs- und Reparaturarbeiten** |
| G 2.1 | | | | Fehlende oder unzureichende Regelungen |
| G 2.3 | | | | Fehlende, ungeeignete, inkompatible Betriebsmittel |
| G 2.5 | | | | Fehlende oder unzureichende Wartung |
| G 2.8 | | | | Unkontrollierter Einsatz von Betriebsmitteln |

Seite 3 von 241

# Beispiel ad-hoc-Abfrage „Verwaiste Maßnahmen“




```
SELECT Measure.MeasureShort, Measure.MeasureDescription
  FROM Measure LEFT JOIN CrossThreatMeasure
  ON Measure.MeasureID = CrossThreatMeasure.MeasureID
  WHERE CrossThreatMeasure.ThreatID Is Null
  ORDER BY Measure.MeasureID;
```

| MeasureShort | MeasureDescription |
|---|---|
| M 2.271 | Festlegung einer Sicherheitsstrategie für den WWW-Zugang |
| M 4.176 | Auswahl einer Authentisierungsmethode für Webangebote |
| M 4.182 | Überwachen des IIS-Systems |
| M 4.193 | Sichere Installation eines Apache-Webservers |
| M 5.11 | Server-Konsole sperren |
| M 5.65 | Einsatz von S-HTTP |
| M 5.104 | Konfiguration des TCP/IP-Filters beim IIS-Einsatz |
| M 6.19 | Datensicherung am PC |




# Vergleich (Arbeitsversion)

```
------------------------------------------------------------------------------
File CHARLY$DKB200:[FGSEC.SICHERHEI  |  File CHARLY$DKB200:[FGSEC.SICHERHEI
------------------------------------------------------------------------------
                                     |  1001;4050;1004;1
                                     |  1001;4050;1005;1
                                     |  1001;4060;1002;1
                                     |  1001;4060;1003;1
                                     |  1001;4060;1004;1
                                     |  1001;4060;1006;1
                                     |  1001;4060;1007;1
                                     |  1001;4060;1008;1
                                     |  1001;4060;2002;1
                                     |  1001;4060;4001;1
                                     |  1001;4060;4002;1
                                     |  1001;4060;4003;1
------------------------------------------------------------------------------
                                     |  1002;4060;2001;1
                                     |  1002;4060;2002;1
                                     |  1002;4060;2004;1
                                     |  1002;4060;2006;1
                                     |  1002;4060;5017;1
------------------------------------------------------------------------------
                                     |  1004;4060;1003;1
                                     |  1004;4060;1004;1
                                     |  1004;4060;2004;1
------------------------------------------------------------------------------
                                     |  1005;4060;1003;1
                                     |  1005;4060;2004;1
------------------------------------------------------------------------------
                                     |  1006;4034;1004;1
                                     |  1006;4060;1004;1
                                     |  1006;4060;2001;1
                                     |  1006;4060;2002;1
                                     |  1006;4060;2004;1
------------------------------------------------------------------------------
2224;3060;2001;1                     |  2224;3090;2001;1
2224;3060;3001;1                     |  2224;3090;3001;1
2224;3060;3044;1                     |  2224;3090;3044;1
2224;3060;4022;1                     |  2224;3090;4022;1
2224;3060;5021;1                     |  2224;3090;5021;1
------------------------------------------------------------------------------
3004;3020;1002;1                     |  3003;4042;3021;1
3004;3020;1008;1                     |  3003;4042;4003;1
3004;3020;1010;1                     |
3004;3020;2001;1                     |
3004;3020;2002;1                     |
3004;3020;2019;1                     |
3004;3020;2036;1                     |
3004;3020;2037;1                     |
3004;3020;2039;1                     |
3004;3020;2049;1                     |
3004;3020;2055;1                     |
3004;3020;2056;1                     |
3004;3020;2063;1                     |
------------------------------------------------------------------------------
3004;3020;3003;1                     |
------------------------------------------------------------------------------
3004;3020;3009;1                     |  3004;3060;2001;1
3004;3020;3013;1                     |  3004;3060;3003;1
------------------------------------------------------------------------------

Number of difference sections found: 102
Number of difference records found: 2714

DIFFERENCES /IGNORE=()/WIDTH=76/MATCH=1/OUTPUT=-
    CHARLY$DKB200:[FGSEC.SICHERHEIT.GRUNDSCHUTZ.VGL0203]CTM.DIF;2/PARALLEL-
    /NONUMBER-
    CHARLY$DKB200:[FGSEC.SICHERHEIT.GRUNDSCHUTZ.VGL0203]CTM_POST.CSV;1-
    CHARLY$DKB200:[FGSEC.SICHERHEIT.GRUNDSCHUTZ.VGL0203]CTM_03.CSV;1
```

# Vergleich (Luxus-Version)

| hinzugefügt / ersetzt | entfernt / gelöscht |
|---|---|
| 3.1 M 2.16 Beaufsichtigung oder Begleitung von Fremdperson<br>3.1 M 2.18 Kontrollgänge | |
| 3.2 M 3.10 Auswahl eines vertrauenswürdigen Administrators<br>3.2 M 3.11 Schulung des Wartungs- und Administrationsperso | |
| 3.4 M 6.20 Geeignete Aufbewahrung der Backup-Datenträger<br>3.4 M 6.21 Sicherungskopie der eingesetzten Software<br>3.4 M 6.22 Sporadische Überprüfung auf Wiederherstellbarke<br>3.4 M 6.32 Regelmäßige Datensicherung | |
| | 3.6 M 2.9 Nutzungsverbot nicht freigegebener Hard- und So<br>3.6 M 2.10 Überprüfung des Hard- und Software-Bestandes<br>3.6 M 2.34 Dokumentation der Veränderungen an einem besteh<br>3.6 M 2.35 Informationsbeschaffung über Sicherheitslücken |
| 3.6 M 2.224 Vorbeugung gegen Trojanische Pferde | 3.6 M 3.4 Schulung vor Programmnutzung<br>3.6 M 3.5 Schulung zu IT-Sicherheitsmaßnahmen |
| | 3.6 M 6.24 Erstellen einer PC-Notfalldiskette<br>3.6 M 6.32 Regelmäßige Datensicherung<br>3.7 M 2.35 Informationsbeschaffung über Sicherheitslücken<br>3.7 M 2.39 Reaktion auf Verletzungen der Sicherheitspoliti |
| | 3.7 M 3.4 Schulung vor Programmnutzung<br>3.7 M 3.5 Schulung zu IT-Sicherheitsmaßnahmen |
| 3.9 M 2.26 Ernennung eines Administrators und eines Vertre | |
| 3.9 M 2.35 Informationsbeschaffung über Sicherheitslücken | |
| | 3.9 M 2.224 Vorbeugung gegen Trojanische Pferde |
| 3.9 M 4.1 Passwortschutz für IT-Systeme | 3.9 M 4.42 Implementierung von Sicherheitsfunktionalitäten |
| 3.9 M 4.93 Regelmäßige Integritätsprüfung | |
| 3.9 M 5.45 Sicherheit von WWW-Browsern | |




# Inhaltliche Redundanzen

- Überprüfung der Maßnahmenlisten
  - thematische Sortierung
  - inhaltlicher Vergleich verwandter Maßnahmen
- Spezifische Empfehlungen für jeden Einzelfall
  - Verschieben einzelner Maßnahmen in andere Bausteine
  - Umbenennen von Maßnahmen
  - Modernisierung von Maßnahmeninhalten
  - Verschieben von Inhalten zwischen Maßnahmen
  - Zusammenfassen verwandter Maßnahmen
  - Löschen von Maßnahmen
  - Umstrukturieren von Maßnahmen
- Insgesamt 28 Maßnahmen von den Änderungen betroffen

## Inhaltliche Redundanzen (Beispiele)

- M 2.224 *Vorbeugung gegen Trojanische Pferde*
  - verschieben in den Komplex der Maßnahmen
    - M 2.157 *Auswahl eines geeigneten Computer-Viren-Suchprogramms*
    - M 2.159 *Aktualisierung der eingesetzten Computer-Viren-Suchprogramme*
    - M 2.160 *Regelungen zum Computer-Virenschutz*
  - in Baustein B 1.6 *Computer-Virenschutzkonzept*
- M 4.1 *Passwortschutz für PC und Server*
  - ist so, wie sie heute formuliert ist, veraltet
  - daraus eigene neue Maßnahme zum Passwortschutz für Notebooks machen
    - Boot-Passwort
    - Plattenverschlüsselung ...




## Ersetzen der Prioritäten

- Maßnahmen besitzen (baustein-abhängig) Prioritäten
  - als Maß für die Wichtigkeit
  - als Vorgabe für die Reihenfolge der Umsetzung
- Maßnahmen sind z.T. als optional gekennzeichnet
- Maßnahmen sind zusätzlich für die Grundschutz-Zertifizierung kategorisiert
  - A – ab Einstiegsstufe erforderlich
  - B – ab Aufbaustufe erforderlich
  - C – für das Zertifikat gefordert
  - Z – zusätzlich – ergänzende, nicht geforderte Maßnahme
- Einstufungen der Maßnahmen sind nicht immer plausibel
- Inkonsistenzen zwischen Prioritäten und Kategorien
- Unklarheit: Welche Einordnung ist anzuwenden?

## Ersetzen der Prioritäten

- Formale Überprüfungen:
  - *unzulässig:* optionale Maßnahmen der Kategorien A, B, C
  - *unzulässig:* nicht optionale Maßnahmen der Kategorie Z
  - *fragwürdig:* hohe Priorität und Kategorie C
  - *fragwürdig:* niedrige Priorität und Kategorie A
- Inhaltliche Überprüfungen:
  - Ist die Priorität plausibel?
    → Falls nein, ist jetzt auch die Kategorie zweifelhaft!
  - Ist die Kategorie nachvollziehbar?
    - A – Maßnahme ist unabdingbar
    - B – Maßnahme ist notwendig für kontrollierte Arbeit
    - C – Maßnahme ist „zertifikatswürdig“
- Prioritäten und Optionalität sind nach Korrektur der unzulässigen / fragwürdigen Zuordnungen **überflüssig**




## Lebenszyklus der Maßnahmen in den Bausteinen

- Fragestellung: Welche Maßnahmen sollen in welcher Phase der Bearbeitung zu welchem Zweck ausgeführt werden?
- Gliederung der Maßnahmen in Lebenszyklus-Gruppen gibt einen „Fahrplan“ für die Umsetzung der Bausteine:
  - Zuordnung zu definierten Abläufen
  - hilft bei der Zuordnung von Verantwortlichkeiten
  - ermöglicht Verzicht auf Maßnahmenprioritäten
- Neuere Bausteine enthalten schon den Lebenszyklus
- Einige Bausteine beschreiben den Lebenszyklus in übergeordneten Maßnahmen
- Ältere Bausteine sind „nachzurüsten“

## Phasen des Lebenszyklus

- Strategie
  - Einsatzszenarien / Einsatzzweck definieren
  - Abwägung Risikopotential
- Konzeption
  - Sicherheitskonzept erstellen
  - Richtlinien für Einsatz festlegen
- Beschaffung
  - Anforderungen an zu beschaffende Produkte formulieren
  - Auswahl der geeigneten Produkte treffen
- Umsetzung
  - Testbetrieb
  - Sicherheitsmaßnahmen für Installation und Konfiguration
  - Schulung und Sensibilisierung aller Betroffenen




## Phasen des Lebenszyklus

- Betrieb
  - Sicherheitsmaßnahmen für den laufenden Betrieb
    - bei IT-Systemen beispielsweise Monitoring (z.B. Protokollierung)
  - Pflege und Weiterentwicklung, Änderungsmanagement
  - Wartung
- Aussonderung
  - Entzug von Berechtigungen, Ent-Katalogisierung
  - Vermeidung von Seiteneffekten
- Notfallvorsorge
  - Datensicherung
  - Redundanz
  - Umgang mit Sicherheitsvorfällen
  - Erstellen eines Notfallplans

## Bausteine mit Lebenszyklustext

- B 1.3 Notfallvorsorge-Konzept
- B 1.6 Computer-Virenschutzkonzept
- B 1.7 Kryptokonzept
- B 1.9 Hard- und Software-Management
- B 1.11 Outsourcing
- B 1.12 Archivierung
- B 3.101 Allgemeiner Server
- B 3.106 Windows 2000 Server
- B 3.201 Allgemeiner Client
- B 3.202 Allgemeines nicht vernetztes IT-System
- B 3.203 Tragbarer PC
- B 3.210 Internet-PC
- B 3.301 Firewall
- B 4.1 Heterogene Netze
- B 4.2 Netz- und Systemmanagement
- B 4.4 Remote Access
- B 5.4 Webserver
- B 5.5 Lotus Notes
- B 5.7 Datenbanken
- B 5.8 Telearbeit
- B 5.9 Novell eDirectory
- B 5.10 Internet Information Server
- B 5.11 Apache Webserver
- B 5.12 Exchange 2000 / Outlook 2000




## Bausteine mit Lebenszyklus-Maßnahme

| | | |
|---|---|---|
| B 1.0 | IT-Sicherheitsmanagement | (M 2.191) |
| B 1.4 | Datensicherungskonzept | (M 6.33) |
| B 1.8 | Behandlung von Sicherheitsvorfällen | (M 6.58) |
| B 2.4 | Serverraum | (M 1.58) |
| B 2.9 | Rechenzentrum | (M 1.49) |
| B 3.103 | Windows NT Netz | (M 2.91) |
| B 3.209 | Windows 2000 Client | (M 2.228) |
| B 3.404 | Mobiltelefon | (M 2.188) |
| B 5.1 | Peer-to-Peer-Dienste | (M 2.67) |
| B 5.3 | E-Mail | (M 2.118) |
| B 5.6 | Faxserver | (M 2.178) |

## Zu ergänzende Bausteine

- B 1.1 Organisation
- B 1.2 Personal
- B 1.10 Standardsoftware
- B 2.1 Gebäude
- B 2.2 Verkabelung
- B 2.3 Büroraum
- B 2.5 Datenträgerarchiv
- B 2.6 Raum für technische Infrastruktur
- B 2.7 Schutzschränke
- B 2.8 Häuslicher Arbeitsplatz
- B 3.102 Unix-Server
- B 3.104 Novell Netware 3.x
- B 3.104 Novell Netware 3.x
- B 3.105 Novell Netware Version 4.x
- B 3.204 PCs mit wechselnden Benutzern
- B 3.205 DOS-PC (ein Benutzer)
- B 3.206 Unix-System
- B 3.207 PC unter Windows NT
- B 3.208 PC mit Windows 95
- B 3.401 TK-Anlage
- B 3.402 Faxgerät
- B 3.403 Anrufbeantworter
- B 4.3 Modem
- B 4.5 LAN-Anbindung eines IT-Systems über ISDN
- B 5.2 Datenträgeraustausch




## Überarbeitung generischer IT-System-Bausteine

- Notwendige Arbeiten an allen 3 Bausteinen
  - Ergänzung um Lebenszyklus
  - Überprüfung der Zuordnung von Maßnahmen und Gefährdungen
  - inhaltliche Überprüfung der Maßnahmen und Gefährungen
- 6.1 Servergestütztes Netz → B 3.101 Allgemeiner Server
  - Festlegung generischer Maßnahmen und Gefährdungen für Server
  - in der Praxis durch spezifische Bausteine zu ergänzen
- 5.99 Allgemeines nicht vernetztes IT-System
  - B 3.201 Allgemeiner Client
    - Festlegung generischer Maßnahmen und Gefährdungen für Clients
    - in der Praxis durch spezifische Bausteine zu ergänzen
  - B 3.202 Allgemeines nicht vernetztes IT-System
- 5.3 Tragbarer PC → B 2.303 Laptop

# Neustrukturierung des IT-Grundschutzes

Dr. Gerhard Weck, INFODAS GmbH, Köln

27. DECUS Symposium 2004 in Bonn
Vortrag 1B07