

INFODAS GmbH IT-Sicherheitsdatenbank

The logo for SAVE, featuring the word "SAVE" in a bold, black, sans-serif font. The letter "e" is red. A black swoosh underline starts under the "S" and curves around the "e". A registered trademark symbol (®) is located to the upper right of the "e".

SAVE®

— Migration der Grundschutz-Version —

INFODAS GmbH, Köln

Datenbank-Version V4.0

Revision 4.0.x — Stand 7. Juni 2006

Grundschutz-Handbuch Version 2005

Erläuterungen

Dieses Handbuch ergänzt die Auslieferung von SAVe®, Version V4.0, der IT-Sicherheitsdatenbank der INFODAS GmbH, Köln. Der alleinige Vertrieb – in gedruckter wie in elektronischer Form – liegt bei INFODAS.



Gesellschaft für Systementwicklung
und Informationsverarbeitung mbH
Rhonstr. 2
50765 Köln

Tel.: (0221) 7 09 12 – 0
Fax: (0221) 7 09 12 – 55
[mailto: save@infodas.de](mailto:save@infodas.de)
<http://www.save-infodas.de/>

© 2002-2006 INFODAS GmbH, Köln, alle Rechte vorbehalten.

Jegliche Weitergabe und Vervielfältigung dieser Unterlage sowie Verwertung und Mitteilung ihres Inhaltes sind nur mit ausdrücklicher Zustimmung der INFODAS GmbH gestattet.

Zuwiderhandlungen können strafrechtlich verfolgt werden und verpflichten zum Schadenersatz.

SAVe® ist ein eingetragenes Warenzeichen der INFODAS GmbH, Rhonstr. 2, Köln.

Microsoft Access®, Microsoft Windows®, Microsoft Office® u.a. sind eingetragene Warenzeichen der Microsoft Deutschland GmbH bzw. Microsoft Cooperation, Redmont, USA.

Das IT-Grundschutzhandbuch wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185-189, 53133 Bonn vertrieben. Die Weitergabe auf der SAVe®-CD-ROM erfolgt mit ausdrücklicher Zustimmung des BSI.

Inhalt

1	Überblick.....	1
1.1	Änderungen im Grundschatz	1
1.1.1	<i>IT-Grundschatzmethodik wird herausgestellt.....</i>	<i>1</i>
1.1.2	<i>Gliederung entspricht Schichtenmodell.....</i>	<i>1</i>
1.1.3	<i>Geänderte Bausteinzuordnungen.....</i>	<i>2</i>
1.1.4	<i>Lebenszyklusmodell in allen Bausteinen.....</i>	<i>2</i>
1.1.5	<i>Weniger Redundanz bei der Zuordnung von Maßnahmen.....</i>	<i>3</i>
1.2	Auswirkungen auf SAVE®	3
2	Vorarbeiten.....	5
3	Installation der Version V4.0	6
4	Konversion der Benutzerdaten	7
4.1	Automatische Konversion.....	7
4.2	Manuelle Nachbearbeitung	8
4.2.1	<i>Neue Bausteine bei Modellierung und Basis-Sicherheitscheck berücksichtigen.....</i>	<i>8</i>
4.2.2	<i>Bausteinbezeichnungen und -zuordnungen anpassen.....</i>	<i>9</i>
4.2.3	<i>Auf geänderte Zuordnung von Maßnahmen achten.....</i>	<i>9</i>
4.2.4	<i>Prüfen, ob Umsetzung der Maßnahmen den Anforderungen entspricht.....</i>	<i>13</i>

Abbildungen

Abb. 1	— Frage nach Deinstallation früherer Versionen.....	6
Abb. 2	— Auswahl des Installationsverzeichnis.....	6
Abb. 3	— Meldung der Konversion.....	7
Abb. 4	— Abschluss der Konversion.....	8
Abb. 5	— Aktivierung zusätzlicher Bausteine (Beispiel).....	9
Abb. 6	— Liste aufgehobener Maßnahmenzuordnungen	10
Abb. 7	— Daten zu Maßnahmen ohne Bausteinbezug	11
Abb. 8	— Aufruf der Kopierfunktion	11
Abb. 9	— Kopieren der Daten zur Maßnahmenumsetzung zwischen Bausteinen	12
Abb. 10	— Prüfung der Baustein-Zuordnung von Maßnahmen.....	13

1 Überblick

1.1 Änderungen im Grundschatz ¹

Das IT-GSHB wird kontinuierlich an die Entwicklung der Informationstechnik angepasst. Es wird um neue Bausteine ergänzt, bestehende Bausteine werden aktualisiert. Dies gilt auch für die Version 2005, die sich darüber hinaus durch einige strukturelle Änderungen auszeichnet. Diese tragen sowohl dazu bei, künftige Weiterentwicklungen des Handbuchs zu erleichtern, als auch dessen Anwendung zu vereinfachen und die Konformität zu internationalen Standards wie ISO 13335 und ISO 17799 zu verdeutlichen.

1.1.1 IT-Grundschatzmethodik wird herausgestellt

Das IT-GSHB ist aufgeteilt worden und zwar in

- einen Teil zur **IT-Grundschatzmethodik in Buchform**, in dem die Ziele und das methodische Vorgehen bei der Anwendung des Handbuchs beschrieben sind, sowie
- eine **Zusammenstellung von Katalogen** bestehend aus Bausteinen (B), Gefährdungen (G) und Maßnahmen (M), die wie gewohnt als Loseblatt-Sammlung herausgegeben wird.

Der erste Teil enthält die bisherigen Kapitel 1 und 2 des IT-GSHB in einer überarbeiteten Fassung sowie als drittes Kapitel den bisherigen Baustein 3.0 *IT-Sicherheitsmanagement*. Diese Hervorhebung verdeutlicht die übergreifende Bedeutung der Planungs- und Lenkungsarbeiten für das angemessene Funktionieren der einzelnen organisatorischen, infrastrukturellen, technischen und personellen Maßnahmen zur IT-Sicherheit.

1.1.2 Gliederung entspricht Schichtenmodell

Während die Maßnahmen- und Gefährdungskataloge im Prinzip unverändert sind, wurden die Bausteine grundlegend überarbeitet. So ist ihre Sortierung jetzt dem Schichtenmodell angepasst. Anstelle der bisherigen Kapitel 3 bis 9 treten daher die fünf neuen Kapitel:

- **B 1 Übergeordnete Aspekte der IT-Sicherheit**, mit den bisherigen Kapiteln 3.1 bis 3.10 sowie den Bausteinen *Standardsoftware* (früher Kapitel 9.1, jetzt B) und *Archivierung* (bislang Kapitel 9.5, jetzt B 1.12),
- B 2 Sicherheit der Infrastruktur **mit den Bausteinen des bisherigen Kapitels 4 zur Sicherheit von Gebäuden, Räumen und Verkabelung**,
- B 3 Sicherheit der IT-Systeme, **in dem die Sicherheitsaspekte von Servern, Clients, Netz- und Telekommunikationskomponenten behandelt werden und das die diesbezüglichen Bausteine aus den früheren Kapiteln 5 bis 8 enthält**,

¹ Der Text dieses Abschnitts wurde im wesentlichen dem Faltblatt „Die neue Struktur des IT-Grundschatzhandbuchs: Wie wirkt sie sich auf IT-Sicherheitskonzepte aus?“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entnommen.

- **B 4 Sicherheit im Netz**
mit derzeit fünf Bausteinen zur Sicherheit in Netzen (B 4.1 *Heterogene Netze*, B 4.2 *Netz- und Systemmanagement*, B 4.3 *Modem*, B 4.4 *Remote Access* und B 4.5 *LAN-Anbindung eines IT-Systems über ISDN*),
- **B 5 Sicherheit in Anwendungen**,
in dem anwendungsspezifische Sicherheitsaspekte beschrieben werden und das Bausteine aus den bisherigen Kapiteln 6 bis 9 enthält, beispielsweise *Peer-to-Peer-Dienste* (früher Kapitel 6.3, jetzt B 5.1), *Datenträgeraustausch* (Kapitel 7.1 wird zu B 5.2), *Faxserver* (früher Kapitel 8.5, jetzt B 5.6) oder *Datenbanken* (früher Kapitel 9.2, jetzt B 5.7).

1.1.3 Geänderte Bausteinzusordnungen

Einige Bausteine wurden im Schichtenmodell umsortiert. So sind jetzt grundsätzlich alle Bausteine für die Sicherheit von Netzkomponenten der Schicht 3 *IT-Systeme* zugeordnet. Ein anderes Beispiel: B 5.8 *Telearbeit*, war bislang in der Schicht 3 und ist nun Teil von Schicht 5 *Anwendungen*.

Die Bausteine der Schicht 3 werden darüber hinaus wie folgt gruppiert:

- B 3.1 *Server*,
- B 3.2 *Clients*,
- B 3.3 Netzkomponenten und
- B 3.4 Sonstige IT-Systeme.

Die **Bausteine zu Clients und Servern** werden **einheitlich** strukturiert. Wie bislang schon für die Server gibt es mit dem neuen Baustein B 3.201 *Allgemeiner Client* jetzt einen Baustein, der die generellen Sicherheitsmaßnahmen für Clients zusammenfasst und ergänzend zu den betriebssystemspezifischen Bausteinen anzuwenden ist.

1.1.4 Lebenszyklusmodell in allen Bausteinen

Alle Bausteine enthalten einen einführenden Teil, der die empfohlenen Maßnahmen in ein **Lebenszyklusmodell** mit den Phasen Strategie, Konzeption, Beschaffung, Umsetzung, Betrieb, Aussonderung und Notfallvorsorge einordnet. Dies erleichtert die Entscheidung darüber, welche Maßnahme in welcher Bearbeitungsphase zu welchem Zweck ausgeführt werden soll.

Die bislang vorhandenen Vermerke zu Umsetzungsprioritäten konnten daher entfallen. Anstelle dessen wird bei den Verweisen auf Maßnahmen mit einem Buchstaben vermerkt, für welche **Siegelstufe** deren Umsetzung erforderlich ist. Es wird unterschieden, ob eine Maßnahme

- für alle drei Ausprägungen der IT-Grundschutzqualifizierung umgesetzt sein muss (= „A“),
- für die Selbsterklärung Aufbaustufe und das IT-Grundschutzzertifikat (= „B“) oder
- nur für das IT-Grundschutzzertifikat (= „C“).

Maßnahmen, die zusätzlich zum IT-Grundschutz umgesetzt werden können, werden durch ein „Z“ markiert.

1.1.5 Weniger Redundanz bei der Zuordnung von Maßnahmen

Eine IT-Sicherheitsmaßnahme kann auf verschiedenen Schichten und für verschiedenartige IT-Komponenten bedeutsam sein. In der Praxis kam es deswegen in den früheren Versionen des IT-GSHB zu einer hohen Anzahl von redundanten Zuordnungen von Maßnahmen. Die Anzahl dieser Redundanzen wurde in der neuen Version stark verringert:

So wurden Maßnahmen, die in Pflichtbausteinen enthalten sind, aus allen anderen Bausteinen entfernt, beziehungsweise Maßnahmen, die bislang in mehreren konkreten Bausteinen vorhanden waren, in einen übergeordneten Baustein verschoben.

Beispiel: Die Maßnahme M 3.11 *Schulung des Wartungs- und Administrationspersonals*, die bisher in den Bausteinen 6.1 *Servergestütztes Netz*, 7.4 *E-Mail*, 9.2 *Datenbanken* und in weiteren 14 Bausteinen enthalten war, ist im Grundschatzhandbuch Version 2005 nur noch im Baustein B 1.2 *Personal* enthalten.

1.2 Auswirkungen auf SAVe®

Erstanwendern des IT-Grundschatzhandbuchs wird durch die Umstrukturierung der Einstieg erleichtert, weil das Handbuch klarer strukturiert ist und der Umfang der insgesamt zu betrachtenden und zu dokumentierenden Maßnahmen geringer geworden ist – und dies ohne Abstriche bei der IT-Sicherheit vornehmen zu müssen.

Für Anwender, die ihr IT-Sicherheitskonzept bereits mit dem IT-Grundschatzhandbuch angefertigt haben, fallen eine Reihe von Anpassungsaufgaben an, wenn sie ihr Konzept an die umstrukturierte Version 2005 ausrichten wollen. Diese umstrukturierte Version des Grundschatzes liegt der Version V4.0 von SAVe® zugrunde. Deshalb ändert sich das zugrundeliegende Sicherheitsmodell beim Wechsel von der Version V3.2-x zur Version V4.0 von SAVe® in erheblichem Umfang.

- Die Bausteine wurden umbenannt, neu gruppiert und nach dem Schichtenmodell des Grundschatzes angeordnet. Diese Änderung wird von SAVe® automatisch bei der Konversion der Benutzerdaten, also der Modell- und Erweiterungs-Datenbanken durchgeführt.
- Die Maßnahmen wurden zum Teil anderen Zertifizierungsstufen zugewiesen. Diese Änderung hat normalerweise keine direkten Auswirkungen auf schon erstellte IT-Sicherheitskonzepte.
- Die bisherigen Prioritäten und die Optionalitätsmarkierung der Maßnahmen wurden durch die Zuweisung einer Lebenszyklusphase ersetzt.
- Die Zuordnung zwischen Bausteinen, Maßnahmen und Gefährdungen wurde völlig überarbeitet, wobei vor allem ein Großteil der im früheren Grundschatzhandbuch vorhandenen Redundanzen entfernt wurde. Diese Änderungen können bei der Konversion von Modell-Datenbanken nur zum Teil automatisch durchgeführt werden, so dass an dieser Stelle einige manuelle Nachbearbeitungen erforderlich werden.

Die hier vorliegende Schrift gibt Hinweise, wie die im letzten Punkt genannten Nachbearbeitungen möglichst effizient und mit minimalem Datenverlust durchgeführt werden können. In der Regel ist ein gewisser Datenverlust nur mit manueller Bearbeitung vermeidbar, wenn zu Maßnahmen, die früher mehreren Bausteinen zugeordnet waren, unterschiedliche Informatio-

nen in diesen Bausteinen erfasst wurden, die jetzt alle nur noch einem einzigen Baustein zuzuordnen sind.

Beispiel: Wenn für die Maßnahme M 3.11 unterschiedliche Informationen in den Bausteinen 6.1, 7.4 und 9.2 erfasst wurden, muss ein Weg gefunden werden, bei der neuen, eindeutigen Zuordnung zum Baustein B 1.2 die bisherigen Daten zu konsolidieren. Es muss ein resultierender Umsetzungsstatus festgelegt werden, und die Kommentare aus den früheren Bausteinen müssen zu einem neuen Kommentar zusammengefasst werden, der ggf. spezifische Hinweise auf die ursprünglichen unterschiedlichen Anwendungsbereiche dieser Maßnahme enthält. Eine automatische Kombination der ursprünglichen Maßnahmeninstanzen ist weder möglich noch sinnvoll.

Diese Nachbearbeitungen betreffen lediglich die Umorganisation der Ergebnisse des Basis-Sicherheitschecks. Die Ergebnisse der IT-Strukturanalyse, Schutzbedarfsfeststellung und Modellierung brauchen nicht angepasst zu werden, und eventuell notwendige Korrekturen der Risikoanalyse ergeben sich höchstens als Folge der Umstrukturierung des Basis-Sicherheitschecks.

2 Vorarbeiten

Ziel der Vorarbeiten ist es, die mit der Version V3.2-x verwalteten Benutzerdaten so zu dokumentieren, dass die Zuordnung zweifelhafter Maßnahmenbeschreibungen des Basis-Sicherheitschecks mit möglichst geringem Aufwand durchgeführt werden kann.

Vor Installation der Version V4.0 sollten für jede vorhandene Modell-Datenbank die folgenden Berichte mit der Version V3.2-x von SAVe® erzeugt werden:

- Modellierung → Bausteine in den Teilmodellen
- Basis-Sicherheitscheck → Maßnahmenstatus
- Basis-Sicherheitscheck → Prüffragen zur Maßnahmenumsetzung (sofern erfasst)
- Basis-Sicherheitscheck → Konsistenz der Maßnahmenumsetzung

Diese Berichte werden nachher benötigt, um in Zweifelsfällen eine sinnvolle Zuordnung von Daten zur Maßnahmenumsetzung durchführen zu können, wenn die betreffende Maßnahme einem neuen Baustein zugeordnet wurde und möglicherweise die alte Zuordnung ganz aufgehoben wurde.

3 Installation der Version V4.0

Bei der Installation der Version V4.0 kann gewählt werden, ob die alte Version V3.2-x deinstalliert werden soll.

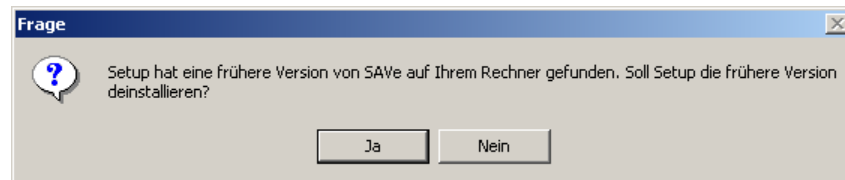


Abb. 1 — Frage nach Deinstallation früherer Versionen

Es empfiehlt sich, auf die Deinstallation der früheren Version vorerst zu verzichten, um eventuelle Unklarheiten, die bei der Datenübernahme in die neue Version auftreten können, mit Hilfe der älteren Version analysieren zu können. Es ist ohne weiteres möglich, beide Versionen von SAVE® nebeneinander zu betreiben, doch **muss** die neue Version in diesem Fall in ein anderes Verzeichnis installiert werden; eine Installation in dasselbe Verzeichnis zerstört die alte Version und führt zu einer nicht lauffähigen neuen Version.

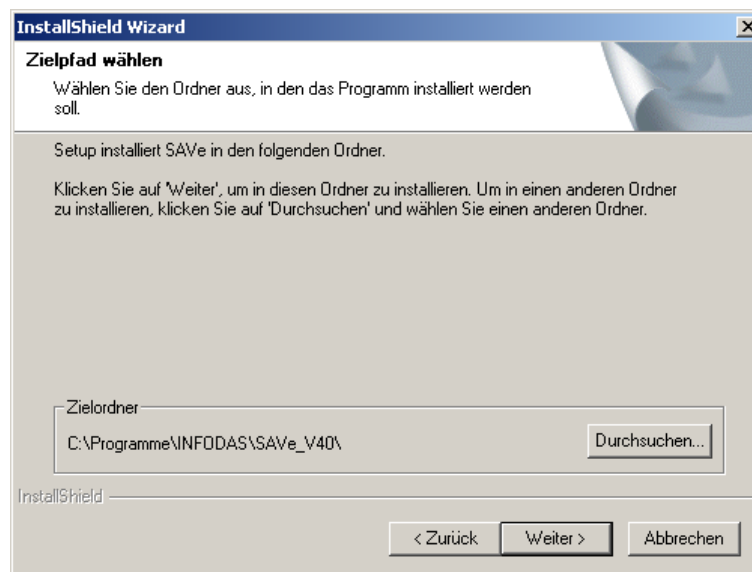


Abb. 2 — Auswahl des Installationsverzeichnisses

Die Installationsroutine schlägt deshalb ein eigenes Verzeichnis für die Neuinstallation vor; dieser Vorschlag kann /sollte übernommen werden.

Es empfiehlt sich, bei der Installation die Grundschutz-Dokumentation mit zu installieren, um später im Zweifelsfall direkt in den Originaldokumenten des BSI nachschauen zu können.

4 Konversion der Benutzerdaten

4.1 Automatische Konversion

Beim erstmaligen Öffnen von Modell- und Erweiterungsdatenbanken, die zuletzt mit der Version V3.2-x von SAVe® bearbeitet wurden, führt SAVe® V4.0 automatisch eine Konversion in das Format der Version V4.0 durch. (Datenbanken früherer Versionen von SAVe® müssen zuerst in die Version V3.2-x konvertiert werden, ehe sie in die Version V4.0 konvertiert werden können.) Sofern eine Modell-Datenbank modellspezifische Erweiterungen enthält, werden diese bei diesem Vorgang mit konvertiert.

Wichtig: Die Konversion läuft nur dann korrekt ab, wenn alle Erweiterungen, die unter der Version V3.2-x bei der Bearbeitung genutzt wurden, vor dem Öffnen der Modell-Datenbank geladen wurden. Daten nicht geladener Erweiterungen werden nicht konvertiert und sind daher nach der Konversion nicht mehr zugreifbar!

Nach dem erstmaligen Start von SAVe® V4.0 sollten deshalb mit dem Menübefehl *Extras* → *Spezielle Funktionen* → *Erweiterungen* → *Laden* zunächst alle Erweiterungen geladen werden, die bei der Arbeit mit der Version V3.2-x genutzt wurden. Die betrifft, neben eventuell selbst erstellten Erweiterungen, vor allem die folgenden beiden von INFODAS gelieferten Standard-Erweiterungen:

- Bei Nutzung der Datenschutz-Funktionen ist die Erweiterungs-Datenbank

`Extension_Datenschutz.mdb`

(im Unterverzeichnis *Erweiterungen* des Installationsverzeichnis) zu laden.

- Bei Nutzung der militärischen Version M3.2-x von SAVe® ist in der Version V4.0 die lad- und entladbare militärische Erweiterungs-Datenbank

`Extension_mil.mdb`

(im Unterverzeichnis *Erweiterungen* des Installationsverzeichnis) zu laden. In der Version V4.0 gibt es keine eigene militärische Version von SAVe® mehr, sondern SAVe® schaltet zwischen ziviler und militärischer Version um, wenn diese Erweiterung ge- und entladen wird.

Diese Erweiterungen können für alle weiteren Arbeiten geladen bleiben. Sie bleiben auch über das Programmende und den Neustart hinweg installiert.



Abb. 3 — Meldung der Konversion

Nach dem Laden der Erweiterungen können die einzelnen zu bearbeitenden Modell-Datenbanken geladen und konvertiert werden. Wenn eine Modell-Datenbank der Version V3.2-x mit dem Menübefehl *Datei* → *Öffnen* geladen wird, erscheint ein Fenster, das auf die Konversion hinweist.

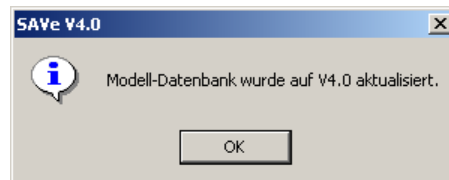


Abb. 4 — Abschluss der Konversion

Nach Durchführung der Konversion wird dies dem Benutzer gemeldet. Die Datenbank sollte sicherheitshalber geschlossen und auf Betriebssystemebene kopiert werden, ehe sie weiter bearbeitet wird, um im Notfall auf eine Version zurückgreifen zu können, die dem Stand unmittelbar nach der Konversion entspricht. Die ursprüngliche Modelldatenbank steht weiter zur Verfügung; sie hat einen Namen, der um die Kennung *_V32* ergänzt wurde, also in der Form *Modellname_V32.mdb*.

4.2 Manuelle Nachbearbeitung

Die Änderungen in der Zuordnung von Maßnahmen zu Bausteinen erfordern einige Anpassungen in den Daten, die in Basis-Sicherheitschecks nach der alten Struktur des Grundschatzhandbuchs erfasst wurden. Diese Änderungen werden durch die Möglichkeit zum Kopieren von Daten zur Maßnahmenumsetzung in SAVE® unterstützt, so dass sich der Aufwand der manuellen Nachbearbeitung bei typischen IT-Sicherheitskonzepten in Grenzen hält.²

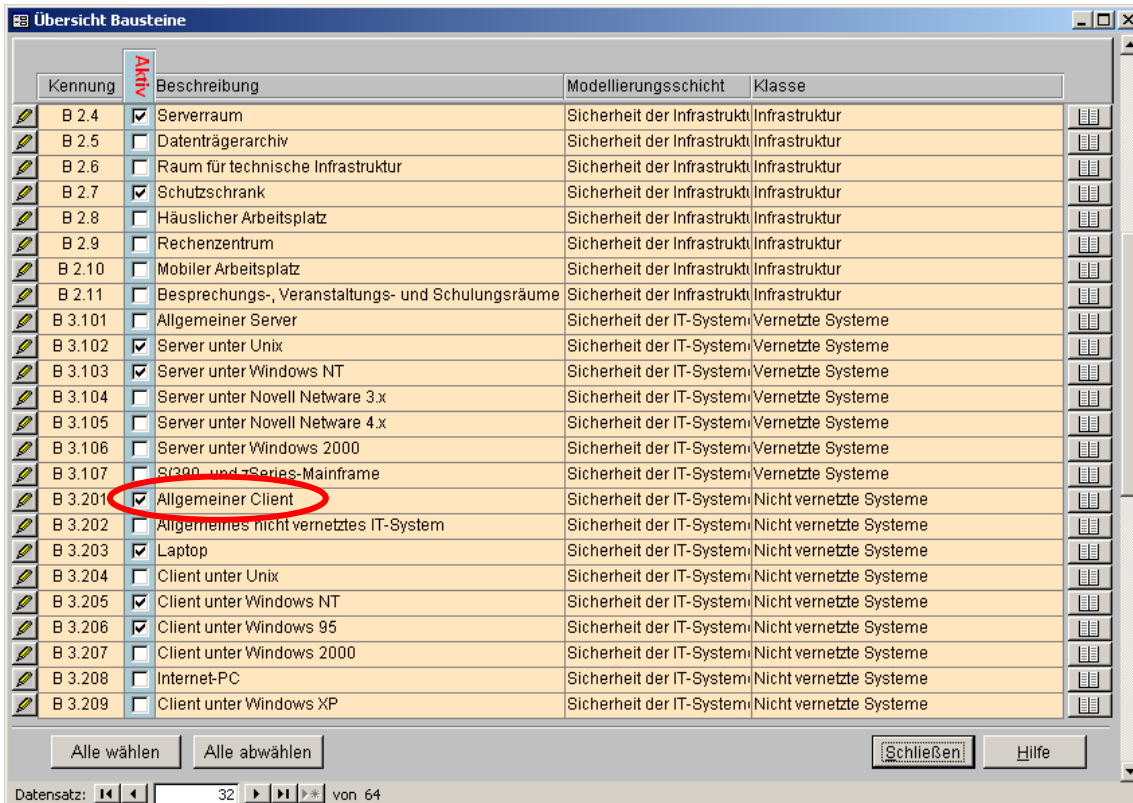
4.2.1 Neue Bausteine bei Modellierung und Basis-Sicherheitscheck berücksichtigen

Es ist zu prüfen, ob und inwieweit die neuen Bausteine berücksichtigt werden müssen. Gegebenenfalls ist das IT-Sicherheitskonzept entsprechend zu ergänzen.

Beispiel: Für Clients ist der neue Baustein B 3.201 *Allgemeiner Client* anzuwenden, da die zugehörigen Maßnahmen nicht mehr in den betriebssystemspezifischen Bausteinen für Clients enthalten sind.

In SAVE® können die zusätzlich erforderlichen Bausteine mit Hilfe des Menübefehls *Modellierung* → *Bausteine* → *Bausteine manuell auswählen* in den einzelnen Teilmodellen aktiviert werden. Die Maßnahmen dieser Bausteine stehen dann für eine Erfassung im Basis-Sicherheitscheck zur Verfügung.

² Die folgenden Abschnitte entsprechen den Empfehlungen des obengenannten Faltblattes des BSI.



Kennung	aktiv	Beschreibung	Modellierungsschicht	Klasse
B 2.4	<input checked="" type="checkbox"/>	Serverraum	Sicherheit der Infrastrukt	Infrastruktur
B 2.5	<input type="checkbox"/>	Datenträgerarchiv	Sicherheit der Infrastrukt	Infrastruktur
B 2.6	<input type="checkbox"/>	Raum für technische Infrastruktur	Sicherheit der Infrastrukt	Infrastruktur
B 2.7	<input checked="" type="checkbox"/>	Schutzschrank	Sicherheit der Infrastrukt	Infrastruktur
B 2.8	<input type="checkbox"/>	Häuslicher Arbeitsplatz	Sicherheit der Infrastrukt	Infrastruktur
B 2.9	<input type="checkbox"/>	Rechenzentrum	Sicherheit der Infrastrukt	Infrastruktur
B 2.10	<input type="checkbox"/>	Mobiler Arbeitsplatz	Sicherheit der Infrastrukt	Infrastruktur
B 2.11	<input type="checkbox"/>	Besprechungs-, Veranstaltungs- und Schulungsräume	Sicherheit der Infrastrukt	Infrastruktur
B 3.101	<input type="checkbox"/>	Allgemeiner Server	Sicherheit der IT-System	Vernetzte Systeme
B 3.102	<input checked="" type="checkbox"/>	Server unter Unix	Sicherheit der IT-System	Vernetzte Systeme
B 3.103	<input checked="" type="checkbox"/>	Server unter Windows NT	Sicherheit der IT-System	Vernetzte Systeme
B 3.104	<input type="checkbox"/>	Server unter Novell Netware 3.x	Sicherheit der IT-System	Vernetzte Systeme
B 3.105	<input type="checkbox"/>	Server unter Novell Netware 4.x	Sicherheit der IT-System	Vernetzte Systeme
B 3.106	<input type="checkbox"/>	Server unter Windows 2000	Sicherheit der IT-System	Vernetzte Systeme
B 3.107	<input type="checkbox"/>	S/390 und zSeries-Mainframe	Sicherheit der IT-System	Vernetzte Systeme
B 3.201	<input checked="" type="checkbox"/>	Allgemeiner Client	Sicherheit der IT-System	Nicht vernetzte Systeme
B 3.202	<input type="checkbox"/>	Allgemeines nicht vernetztes IT-System	Sicherheit der IT-System	Nicht vernetzte Systeme
B 3.203	<input checked="" type="checkbox"/>	Laptop	Sicherheit der IT-System	Nicht vernetzte Systeme
B 3.204	<input type="checkbox"/>	Client unter Unix	Sicherheit der IT-System	Nicht vernetzte Systeme
B 3.205	<input checked="" type="checkbox"/>	Client unter Windows NT	Sicherheit der IT-System	Nicht vernetzte Systeme
B 3.206	<input checked="" type="checkbox"/>	Client unter Windows 95	Sicherheit der IT-System	Nicht vernetzte Systeme
B 3.207	<input type="checkbox"/>	Client unter Windows 2000	Sicherheit der IT-System	Nicht vernetzte Systeme
B 3.208	<input type="checkbox"/>	Internet-PC	Sicherheit der IT-System	Nicht vernetzte Systeme
B 3.209	<input type="checkbox"/>	Client unter Windows XP	Sicherheit der IT-System	Nicht vernetzte Systeme

Abb. 5 — Aktivierung zusätzlicher Bausteine (Beispiel)

4.2.2 Bausteinbezeichnungen und -zuordnungen anpassen

Verweise auf Bausteine im IT-GSHB sind den neuen Bezeichnungen anzupassen, die Zuordnung von Bausteinen zu Schichten ist den geänderten Eingruppierungen anzugleichen.

Beispiel: Der bisherige Baustein 7.3 *Firewall* hat als B 3.301 *Sicherheitsgateway (Firewall)* eine neue Kapitelnummer sowie einen neuen Titel erhalten und er ist nicht mehr in Schicht 4 sondern in Schicht 3 eingruppiert.

Diese Anpassungen werden von SAVE® bei der Konvertierung der Modell-Datenbanken automatisch durchgeführt; es sind daher hierfür keine Aktivitäten des Nutzers erforderlich.

4.2.3 Auf geänderte Zuordnung von Maßnahmen achten

Bausteine können neue Maßnahmen enthalten oder Maßnahmen können in Bausteinen gestrichen worden sein. Dies kann Auswirkungen auf ein IT-Sicherheitskonzept haben. Wenn eine Maßnahme aus einem Baustein gestrichen wurde, weil sie in einem übergeordneten Pflichtbaustein enthalten ist oder in diesen verschoben wurde, ist die (gegebenenfalls neu anzufertigende) Dokumentation zu der Maßnahme im Pflichtbaustein daraufhin zu prüfen, ob sie alle Sicherheitsvorkehrungen umfasst, die für den untergeordneten Baustein formuliert worden sind.

Beispiel: M 1.8 *Raumbelegung unter Berücksichtigung von Brandlasten* ist jetzt nur noch im Baustein *Gebäude* enthalten, nicht mehr im Baustein *Serverraum*. Es muss daher geprüft wer-

den, ob der Teil des IT-Sicherheitskonzepts, der sich mit Serverräumen befasst, Aussagen zu M 1.8 enthält, die nicht bereits schon für das Gebäude formuliert sind, in dem sich die Serverräume befinden. Gegebenenfalls ist die Dokumentation zu M 1.8 für das Gebäude entsprechend zu ergänzen.

Immer dann, wenn in den untergeordneten Bausteinen weitgehend oder ausschließlich auf eine entsprechende Regelung im übergeordneten Pflichtbaustein verwiesen wurde, dürfte der Umstellungsaufwand hier eher gering sein.

Gelöschte Bausteinzusordnungen

Auf dieser Seite werden die Zuordnungen zwischen Maßnahmen und Bausteinen dargestellt, die in der Version 2004 des Grundschutzhandbuchs noch vorhanden waren, aus der Version 2005 jedoch entfernt wurden.

In der nachfolgenden Liste stellen die den Bausteinen zugeordneten Buchstaben in Klammern die zugewiesenen Qualifizierungsstufen dar. Folgende Qualifizierungsstufen sind vorgesehen:

Stufe	Erläuterung
A (Einstieg)	Diese Maßnahmen müssen für alle drei Ausprägungen der Qualifizierung nach IT-Grundschutz (Selbsterklärung Einstiegsstufe, Selbsterklärung Aufbaustufe und IT-Grundschutz-Zertifikat) umgesetzt sein. Diese Maßnahmen sind essentiell für die Sicherheit innerhalb des betrachteten Bausteins. Sie sind vorrangig umzusetzen.
B (Aufbau)	Diese Maßnahmen müssen für die Selbsterklärung Aufbaustufe und für das IT-Grundschutz-Zertifikat umgesetzt sein. Sie sind besonders wichtig für den Aufbau einer kontrollierbaren IT-Sicherheit. Eine zügige Realisierung ist anzustreben.
C (Zertifikat)	Diese Maßnahmen müssen für das IT-Grundschutz-Zertifikat umgesetzt sein. Sie sind wichtig für die Abrundung der IT-Sicherheit. Bei Engpässen können sie zeitlich nachrangig umgesetzt werden.
Z (zusätzlich)	Diese Maßnahmen müssen weder für eine Selbsterklärung noch für das IT-Grundschutz-Zertifikat verbindlich umgesetzt werden. Sie stellen Ergänzungen dar, die vor allem bei höheren Sicherheitsanforderungen erforderlich sein können.

M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften

- ◆ [B 2.8](#) (4.5) (A) Häuslicher Arbeitsplatz
- ◆ [B 2.9](#) (4.6) (A) Rechenzentrum

M 1.2 Regelungen für Zutritt zu Verteilern

- ◆ [B 2.9](#) (4.6) (A) Rechenzentrum
- ◆ [B 3.401](#) (8.1) (A) TK-Anlage

M 1.4 Blitzschutzeinrichtungen

- ◆ [B 2.9](#) (4.6) (A) Rechenzentrum

Abb. 6 — Liste aufgehobener Maßnahmenzuordnungen

Die hiervon betroffenen Maßnahmen können den Listen *Gelöschte Bausteinzusordnungen* und *Neu zugeordnete Bausteine* der HTML-Version des Grundschutzhandbuchs (unter dem Menüpunkt [Hilfsmittel → Checklisten und Formulare](#) über den Link *Referenzlisten zu den Änderungen in der Version 2005 des IT-Grundschutzhandbuchs*) entnommen werden.

Sofern Daten zu diesen Maßnahmen erfasst wurden, sind sie in SAVe® über den Menübefehl *Berichte → Basis-Sicherheitscheck → Maßnahmen ohne Bausteinbezug* für die Maßnahmen zu entnehmen, deren Bausteinzusordnung mit der neuen Grundschutzversion aufgelöst wurde.

315 Maßnahmen ohne Bausteinbezug			Datenbestand: G1 - Übergeordnete Aspekte			
Bundesamt für Organisation und Verwaltung (BOV)						
Nr.	Beschreibung	Ja z.T. Nein n/a	fällig	verantwortlich	Bemerkungen	Kosten
				Personalaufwand (PT) einmalig pro Monat	Sachkosten (€) einmalig pro Monat	
M 3.5	Schulung zu IT-Sicherheitsmaßnahmen				erforderlich	
M 3.10	Auswahl eines vertrauenswürdigen Administrators und Vertreters					
B 3.101	Allgemeiner Server	⊗ ○ ○ ○ ○				
B 5.3	E-Mail	⊗ ○ ○ ○ ○				
M 3.11	Schulung des Wartungs- und Administrationspersonals					
B 3.101	Allgemeiner Server	⊗ ○ ○ ○ ○			ausreichende Schulung der Administratoren und ihrer Vertreter ist durch permanente Weiterbildung sichergestellt	
B 5.3	E-Mail	○ ⊗ ○ ○ ○	30.06.2006	H. Assmann	Schulungskonzept z.Z. in Weiterentwicklung	
M 4.1	Passwortschutz für IT-Systeme					
B 3.101	Allgemeiner Server	⊗ ○ ○ ○ ○				
M 4.2	Bildschirm Sperre					
B 3.101	Allgemeiner Server	⊗ ○ ○ ○ ○				
M 4.3	Regelmäßiger Einsatz eines Anti-Viren-Programms					
B 3.101	Allgemeiner Server	⊗ ○ ○ ○ ○				
M 4.44	Prüfung eingehender Dateien auf Makro-Viren					
B 3.101	Allgemeiner Server	⊗ ○ ○ ○ ○				

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

Wk Consulting Edition INFODAS GmbH
Version V4.0-1 07.06.2006 SAVE® © 2000 - 2006 INFODAS GmbH Seite 315-4 von 6

Abb. 7 — Daten zu Maßnahmen ohne Bausteinbezug

Mit Hilfe des Menübefehls *Berichte* → *Basis-Sicherheitscheck* → *Unbearbeitete Maßnahmen* lassen sich die Maßnahmen identifizieren, denen nach dem neuen Zuordnungsschema Bausteine zugeordnet wurden, die im alten Grundschutzhandbuch nicht zugeordnet waren. Zumindest für diese Maßnahmen sollten die Daten, die dazu erfasst waren, aus den bisherigen Bausteinen übernommen werden.

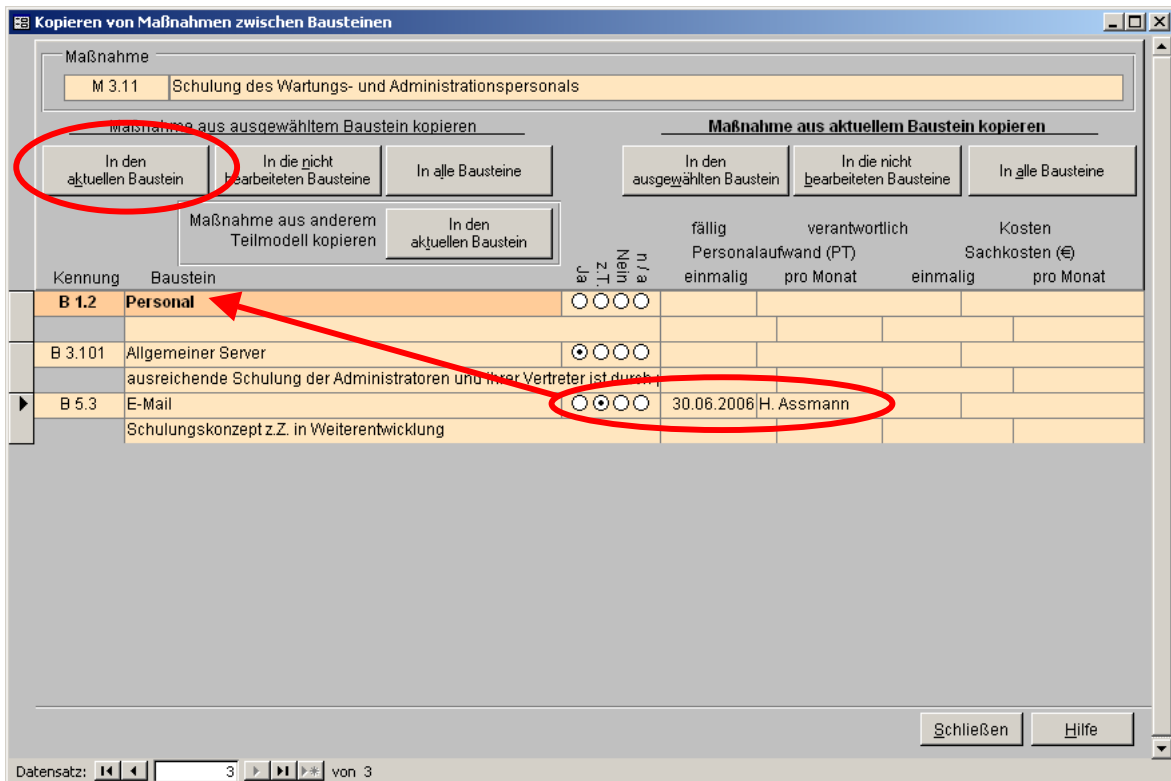
Dies kann dadurch geschehen, dass die betreffenden Maßnahmen im Basis-Sicherheitscheck (Menübefehl *Basis-Sicherheitscheck* → *Planen / Erfassen* → *Umsetzung der Maßnahmen erfassen*) selektiert und bearbeitet werden.



Abb. 8 — Aufruf der Kopierfunktion

Die Kopierfunktion des dabei aufgerufenen Formulars zeigt auch die alten, nicht mehr zugeordneten Instanzen der betreffenden Maßnahmen an und erlaubt somit, eine geeignete Instanz auszuwählen und deren Daten in den jetzt zugeordneten Baustein zu übernehmen. Die Daten der zugeordneten Kontrollfragen werden dabei mit in den neuen Baustein kopiert.

Beispiel: Für die Maßnahme M 3.11 kann es am zweckmäßigsten sein, die Daten zum ehemaligen Baustein 7.4, dem jetzigen Baustein B 5.3, in den neu zugeordneten Baustein B 1.2 zu übernehmen.



Kennung	Baustein	fällig	verantwortlich	Kosten
		Personalaufwand (PT)	Sachkosten (€)	
		einmalig	pro Monat	einmalig
B 1.2	Personal			
B 3.101	Allgemeiner Server			
B 5.3	E-Mail	30.06.2006	H. Assmann	

Abb. 9 — Kopieren der Daten zur Maßnahmenumsetzung zwischen Bausteinen

Sofern die Informationen mehrerer Instanzen derselben Maßnahme zusammengefasst werden sollen, muss dies manuell geschehen. Für umfangreichere Texte kann es dabei sinnvoll sein, SAVE® in den Versionen V4.0 und V3.2-x gleichzeitig nebeneinander laufen zu lassen und die Texte über die Zwischenablage zu transferieren.

Es ist auf jeden Fall empfehlenswert, auch alle anderen Maßnahmen daraufhin zu prüfen, ob sie eventuell noch in anderen Bausteinen referenziert werden. Dies geschieht am besten mit Hilfe des Berichts, der mit dem Menübefehl *Berichte* → *Basis-Sicherheitscheck* → *Maßnahmenstatus* erzeugt wird.

Die aktuelle Zuordnung der Maßnahmen zu Bausteinen lässt sich dabei über den Bericht *Maßnahmen und Bausteine* des Bereichs *Sicherheitsanalyse* oder interaktiv über den Menübefehl *Sicherheitsanalyse* → *Sicherheitsstruktur* → *Maßnahmen und zugeordnete Bausteine* bestimmen.

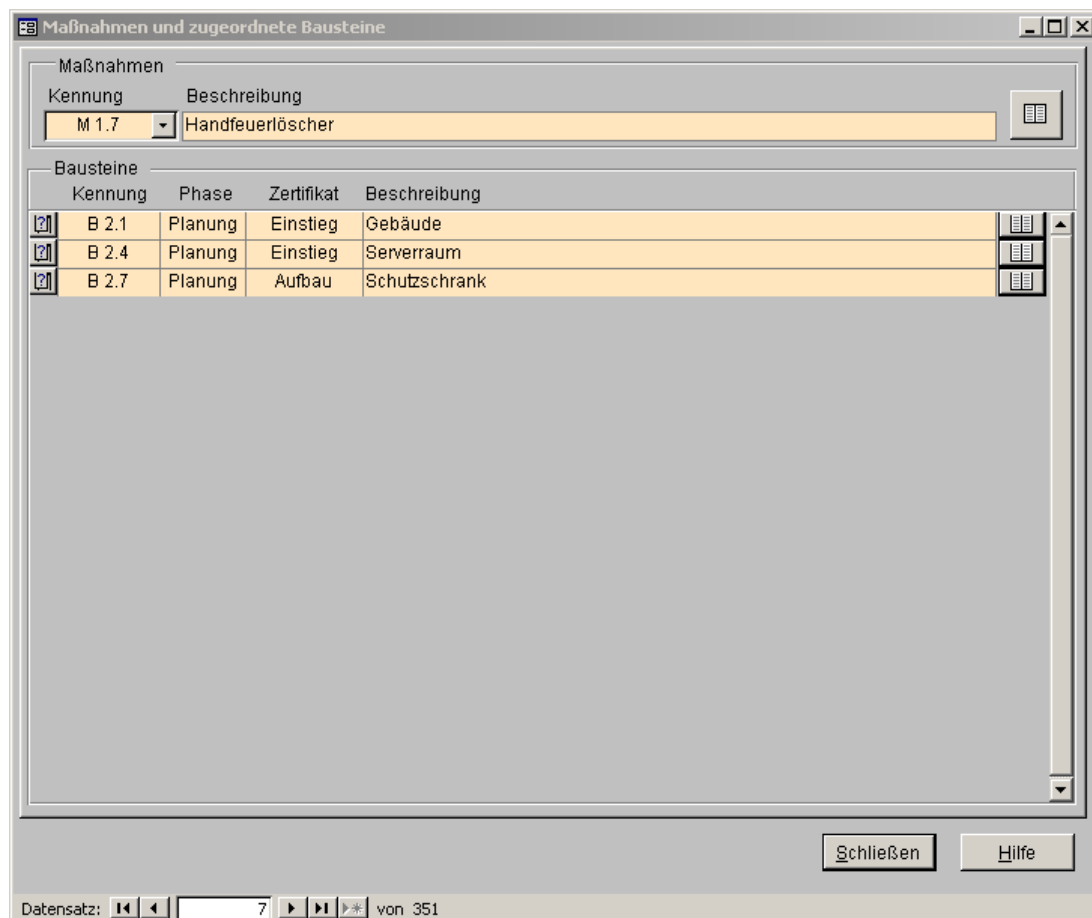


Abb. 10 — Prüfung der Baustein-Zuordnung von Maßnahmen

Bei dieser Arbeit stellen die im Rahmen der Vorarbeiten (siehe Abschnitt 2) erzeugten Berichte eine wesentliche Hilfe dar.

4.2.4 Prüfen, ob Umsetzung der Maßnahmen den Anforderungen entspricht

Dort, wo sich die Beschreibung einer Maßnahme geändert hat, ist zu prüfen, ob die Art und Weise der vorhandenen Umsetzung den neuen Anforderungen genügt. Die hiervon betroffenen Maßnahmen können der Liste *Inhaltliche Änderungen* → *Geänderte Maßnahmen* der HTML-Version des Grundschatzhandbuchs entnommen werden.

Eine ähnliche Überprüfung ist für die Maßnahmen sinnvoll, deren Zuordnung zur Zertifizierungsstufe sich geändert hat, zumindest wenn das Sicherheitskonzept als Basis für eine Grundschatz-Zertifizierung oder einer der Vorstufen einer solchen Zertifizierung verwendet wird. Es ist möglich, dass durch die Änderung der Zertifizierungsstufe Maßnahmen, die bisher nicht relevant waren, jetzt zu berücksichtigen sind oder dass bisher relevante Maßnahmen entfallen. Die davon betroffenen Maßnahmen können der Liste *Maßnahmen mit geänderter Zertifizierungsstufe* der HTML-Version des Grundschatzhandbuchs entnommen werden.

Die zu den betreffenden Maßnahmen erfassten Daten müssen manuell überprüft und ggf. angepasst werden; eine automatische Änderung ist an dieser Stelle nicht möglich.