

Handout **IT-Grundschutzhandbuch**

FH Furtwangen
Netzwerksicherheit, Praktikum
15.01.2005

Benjamin Bratkus,
Andre Böhringer,
Thomas Steinhart,
Tobias Satzger

Umfang: 8 Seiten

1. Einleitung

„Das IT-Grundschutzhandbuch enthält Standardsicherheitsmaßnahmen, Umsetzungshinweise und Hilfsmittel für zahlreiche IT-Konfigurationen, die typischerweise im heutigen IT-Einsatz anzutreffen sind. Dieses Informationsangebot soll zur zügigen Lösung häufiger Sicherheitsprobleme dienen, die Anhebung des Sicherheitsniveaus von IT-Systemen unterstützen und die Erstellung von IT-Sicherheitskonzepten vereinfachen.“

Quelle: IT-Grundschutzhandbuch, Kap. 1.1

Das regelmäßig aktualisiert und erweitert werdende Buch beschreibt also einerseits die Gefahren und Maßnahmen bezgl. der einzelnen Teile eines IT-Verbunds; andererseits wird ein Schema beschrieben, mit dessen Hilfe entsprechende Sicherheitsniveaus umgesetzt werden können – von der Strukturanalyse bis zur Realisierung. So kann eine Firma auf einfache Weise den Status quo ihres gesamten IT-Umfeldes überprüfen und verbessern.

Eine wesentliche Rolle im Aufbau des Buches spielt die Einteilung der einzelnen, auf Sicherheit zu überprüfenden Bereiche in sog. Bausteine.

2. Inhalt des Handbuchs

1 Wegweiser durch das IT-Grundschutzhandbuch

1.1 IT-Grundschutz: Ziel, Idee und Konzeption

allgemeine Beschreibung, Vorteile, Erweiterbarkeit

1.2 Aufbau und Leseart des Handbuchs

– Nennung der inhaltlichen Aufteilung des Buches, kurze Beschreibung dazu und Referenzierung auf die jeweiligen Kapitel

– Erläuterung des Prinzips der Bausteine

*Einstieg und
Vorgehensweise
(Kapitel 1 und 2)*

1.3 Anwendungsweisen des IT-Grundschutzhandbuchs

kurze Beschreibung der nötigen Schritte zur Umsetzung eines Sicherheitsstandards und Verweise auf die detaillierte Erläuterung in den nachfolgenden Kapiteln

1.4 Kurzdarstellung vorhandener Bausteine

im Vorab werden hier alle Bausteine knapp vorgestellt

1.5 Hilfsmittel

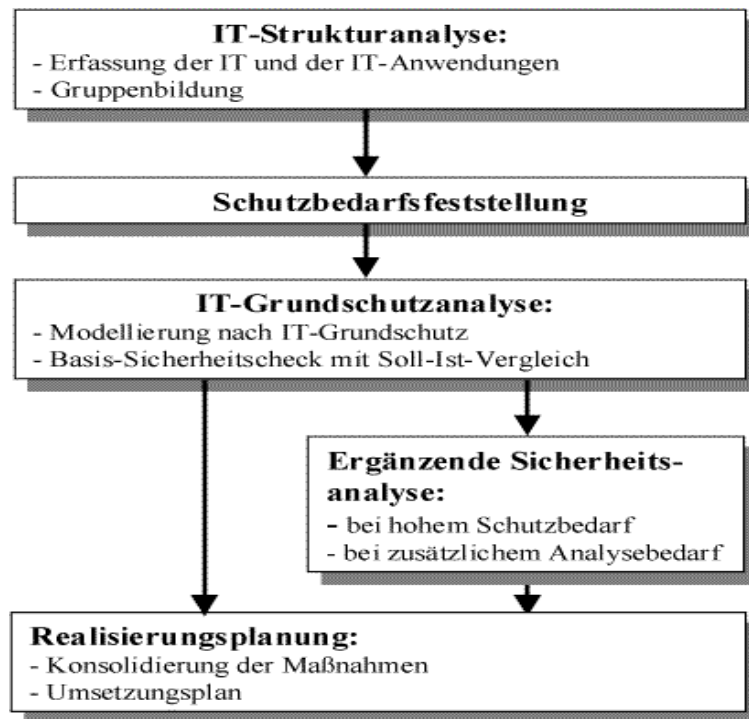
z.B. Software, weiterführende Dokumente

1.6 Informationsfluss

Kontakt, Registrierung, ...

Kapitel 1 umfasst also den Einstieg in dieses Buch. Dieses Kapitel ist jenen ans Herz zu legen, welche Antworten auf strukturelle Verständnisprobleme suchen. Außerdem kann in den Abschnitten 1.2 und 1.3 dem Bedürfniss nachgegangen werden zunächst einen Überblick über die restlichen Kapitel zu bekommen.

Kapitel 2 erläutert die in folgender Abbildung dargestellte Erstellung eines IT-Sicherheitskonzeptes.



Quelle: IT-Grundschutzhandbuch, Kap. 2

Geht es dem Leser tatsächlich um diese Umsetzung in die Praxis – was schließlich dem Hauptzweck des Buches entspricht – so ist dieses Kapitel unverzichtbar. Es werden für die einzelnen Stufen jeweils schematische Vorgehensweisen genau beschrieben die als komplettes Handwerkszeug für die Erstellung dienen.

2 Anwendung des IT-Grundschutzhandbuches

2.1 IT-Strukturanalyse

- Netzplanerhebung
- Komplexitätsreduktion durch Gruppenbildung
- Erhebung der IT-Systeme
- Erfassung der IT-Anwendungen und der zugehörigen Informationen

*Einstieg und
Vorgehensweise
(Kapitel 1 und 2)*

Auszug aus Beispielsliste von IT-Systemen:

Nr.	Beschreibung	Plattform	Anzahl	Aufstellungs- ort	Status	Anwender /Admin.
S1	Server für Personenverwaltung	Windows NT-Server	1	Bonn, r 1.01	In Betrieb	Personalre- ferat

Quelle: IT-Grundschutzhandbuch, Kap. 2.1

2.2 Schutzbedarfsfeststellung

Schutzbedarfsfeststellung der IT-Anwendungen und daraus Ableitung des Schutzbedarfes für höhere Ebenen, z. B. für Räume.

Auszug aus Beispieldarstellung der Ergebnisse:

Nr.	Beschreibung	Grundwert	Schutzbedarf	Begründung
S1	Server für Personenverwaltung	Vertraulichkeit	hoch	Maximumprinzip
		Integrität	mittel	Maximumprinzip
		Verfügbarkeit	mittel	Maximumprinzip

Quelle: IT-Grundschutzhandbuch, Kap. 2.2

2.3 Modellierung nach IT-Grundschutz

Den betrachtete IT-Verbund mit Hilfe der später im Buch beschriebenen Bausteine nachbilden.

Auszug aus Beispielmodellierung:

Nr.	Titel des Bausteins	Zielobjekt/ Zielgruppe	Ansprechpartner	Hinweise
3.1	Organisation	Standort Bonn		Der Baustein Organisation muss für die Standorte Bonn und Berlin separat bearbeitet werden, da in Berlin eigene organisatorische Regelungen gelten.
3.1	Organisation	Standort Berlin		
3.2	Personal	gesamtes Unternehmen		Die Personalverwaltung des Unternehmens erfolgt zentral in Bonn.
4.3.3	Datenträgerarchiv	R U.02 (Bonn)		In diesem Raum werden die Backup-Datenträger aufbewahrt
5.3	Tragbarer PC	C5		Die Laptops in Bonn bzw. Berlin werden jeweils in eine Gruppe zusammengefasst.
5.3	Tragbarer PC	C6		
7.5	WWW-Server	S5		S5 dient als Server für das Intranet
9.2	Datenbanken	S5		Auf dem Server S5 kommt eine Datenbank zum Einsatz

Quelle: IT-Grundschutzhandbuch, Kap. 2.3

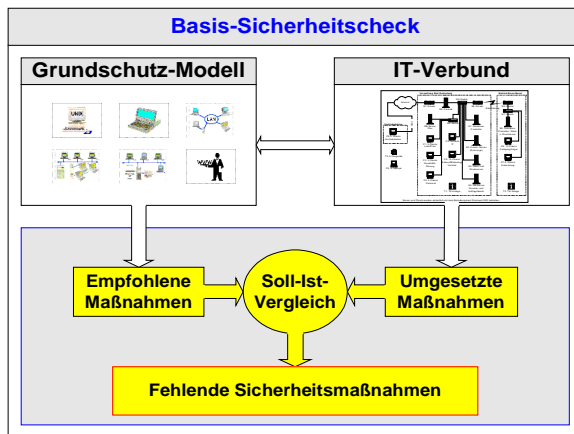
So werden also beispielsweise die Bausteine „Organisation“ und „Personal“ dem gesamten Unternehmen bzw. den Standorten zugeteilt. Die Laptops werden sinnvollerweise auf den, im Buch vorhandenen Baustein „Tragbarer PC“ abgebildet. Der als „S5“ bezeichnete Server wird anhand von 2 Bausteinen nachgebildet: „WWW-Server“ und „Datenbanken“. (vgl. oben abgebildete Tabelle)

Einstieg und Vorgehensweise (Kapitel 1 und 2)

Da in Kapitel 2.3 die Bausteine erstmals in dem Handbuch konkret Verwendung finden, sollte in diesem Zusammenhang deren Rolle klar werden. Hier ist der Punkt innerhalb des Prozesses der Erstellung eines IT-Sicherheitskonzepts bei dem der umfangreiche Teil der Gefährdungen und v.a. der Maßnahmen – durch den Brückenschlag zu den Bausteinen hin – schließlich erschlossen werden kann.

2.4 Basis-Sicherheitscheck

– Soll-Ist-Vergleich zwischen realisierten und empfohlenen Maßnahmen, die sich aus den Resultaten der Vorgehensweise aus den aufeinander aufbauenden Kapiteln aus 2. bisher ergeben haben.



Quelle: Foliensatz IT-Grundschatz-Forum 14.05.2003

*Einstieg und
Vorgehensweise
(Kapitel 1 und 2)*

– Dokumentation

2.5 Ergänzende Sicherheitsanalyse

Bei hohem Schutzbedarf evtl. klären ob „IT-Sicherheitsmaßnahmen durch höherwertige ergänzt oder ersetzt werden müssen“.

Quelle: IT-Grundschatzhandbuch, Kap. 2.5

2.6 Realisierung von IT-Sicherheitsmaßnahmen

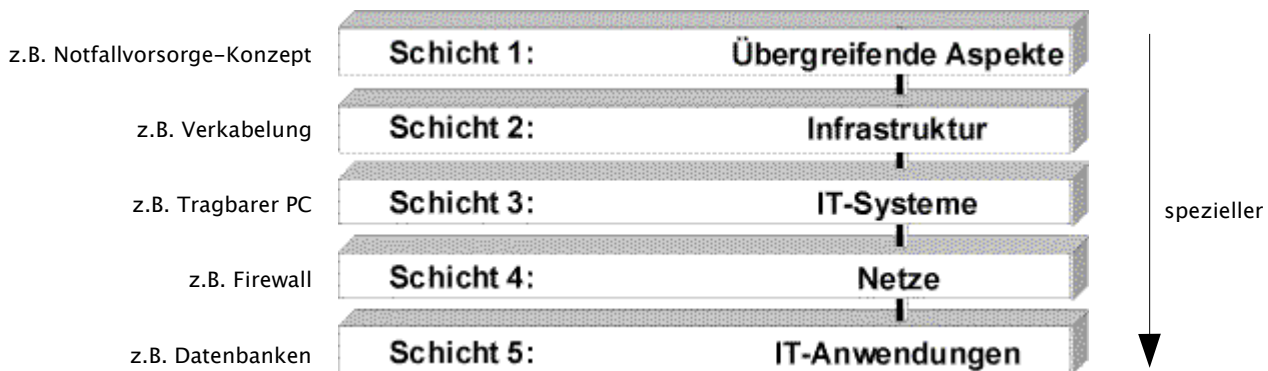
„In diesem Kapitel werden verschiedene Aspekte vorgestellt, die bei der Realisierung von IT-Sicherheitsmaßnahmen beachtet werden müssen. Dabei wird beschrieben, wie die Umsetzung als fehlend erkannter IT-Sicherheitsmaßnahmen geplant, durchgeführt, begleitet und überwacht werden kann.“

Quelle: IT-Grundschatzhandbuch, Kap. 2.6

2.7 IT-Grundschatzzertifikat

Bei entsprechenden Sicherheitsstandarts im Sinne des IT-Grundschatzhandbuchs und einer Überprüfung kann ein IT-Grundschatz-Zertifikat erhalten werden.

„Für die Abbildung eines im Allgemeinen komplexen IT-Verbunds auf die Bausteine des Handbuchs bietet es sich an, die IT-Sicherheitsaspekte gruppiert nach bestimmten Themen zu betrachten.“



Quelle: IT-Grundschutzhandbuch, Kap. 2.3

Diese Schichten entsprechen in etwa der Einteilung der Bausteine in die Kapitel 3–9. Eine genaue Zuordnung ist unter <http://www.bsi.bund.de/gshb/deutsch/etc/schichtenmodell.html> einzusehen. Die Inhalte der Kapitel 3–9, sowie G und M sind nicht zusammenhängend zu lesen. Sie können je nach Bedarf einzeln betrachtet werden. Die beschriebenen Bausteine sind gleich aufgebaut. So besteht der Baustein 5.2 Unix-System genauso wie alle anderen aus folgenden Bereichen:

- Beschreibung
- Gefährdungslage
- Maßnahmenempfehlungen

Der Baustein UNIX-System enthält natürlich nicht nur eine Gefährdung und eine Maßnahme sondern eine Vielzahl davon. Die Beschreibung der Gefährdungen und Maßnahmen ist in den nachfolgenden Kapiteln G und M aufgeführt. In den Bausteinen selbst sind Referenzierungen auf die einzelnen Punkte enthalten.

Um eine Maßnahmenempfehlungen umzusetzen ist es nicht zwingend erforderlich die jeweilige Gefährdungslage zu lesen. Dies dient nur dem Verständnis und der Sensibilisierung.

3 Übergeordnete Komponenten

3.0 IT-Sicherheitsmanagement

...

3.10 Outsourcing

...

9 Sonstige IT-Komponenten

9.1 Standardsoftware

...

9.5 Archivierung

*Bausteine
(Kapitel 3-9)*

G 1 Höhere Gewalt

G 1.1 Personalausfall

...

G 1.14 Datenverlust

...

G 5 Vorsätzliche Handlungen

G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör

...

G 5.111 Missbrauch aktiver Inhalte in E-Mails

*Gefährdungs-
kataloge
(Kapitel G)*

M 1 Infrastruktur

M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften

...

M 1.60 Geeignete Lagerung von Archivmedien

...

M 6 Notfallvorsorge

M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen

...

M 6.90 Datensicherung und Archivierung von E-Mails

*Maßnahmen-
kataloge
(Kapitel M)*

- Hilfsmittel

- Bezugsdokumente

- Vordrucke

- ...

Anhang

3. Übersicht

