IT-Grundschutz

Teil I:

Einführung in das Konzept
IT-Grundschutz

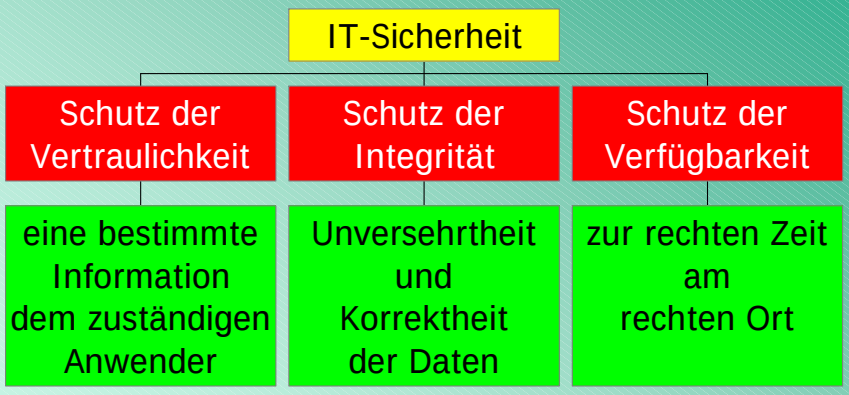
BSI-Errichtungsgesetz

(BGBL. I S. 2834 ff.) vom 17.12.1990

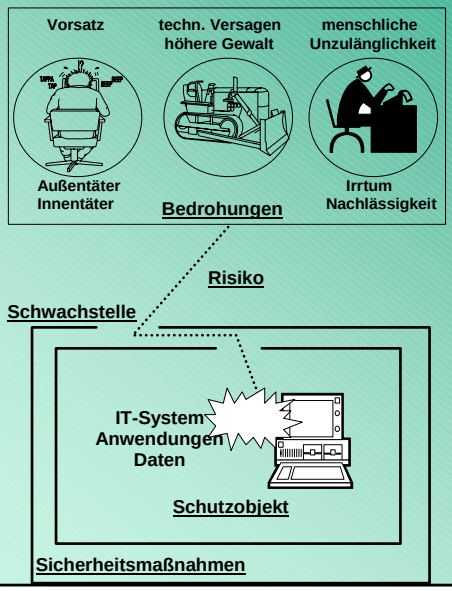
Das BSI hat folgende Aufgaben:

1. Untersuchung von Sicherheitsrisiken und Entwicklung von Geräten
2. Kriterienentwicklung/Werkzeuge
3. Prüfung und Bewertung/Zertifizierung
4. Zulassung (Verschlusssachen)
5. Unterstützung (BfD)
6. Unterstützung (Polizeien)
7. **Beratung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik**

Grundwerte der IT-Sicherheit



Bedrohungen für die IT-Sicherheit



Typische Sicherheitsfragen

Organisation

- Wie sieht ein sicheres Passwort aus?

Personal

- Was ist beim Ausscheiden von Mitarbeitern zu beachten?

Infrastruktur

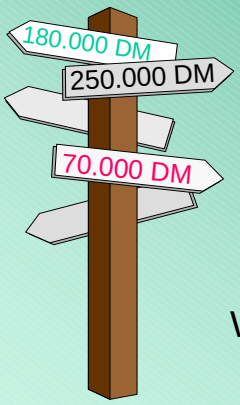
- Mit welchen Maßnahmen wird ein Serverraum abgesichert?

Technik

- Wie setzt man eine Firewall ein?

Methodik für IT-Sicherheit?

Viele Wege führen zur IT-Sicherheit...



Welcher Weg ist der effektivste?

IT-Grundschutz

Ideen

- Gesamtsystem enthält typische Komponenten (z.B. Server und Clients, Betriebssysteme)
- Pauschalisierte Gefährdungen und Eintrittswahrscheinlichkeiten
- Empfehlung geeigneter Bündel von Standard-Sicherheitsmaßnahmen
- konkrete Umsetzungshinweise für Maßnahmen

IT-Grundschutz

Vorteile

- arbeitsökonomische Anwendungsweise durch Soll-Ist-Vergleich
- kompakte IT-Sicherheitskonzepte durch Verweis auf Referenzquelle
- praxiserprobte Maßnahmen mit hoher Wirksamkeit
- Erweiterbarkeit und Aktualisierbarkeit

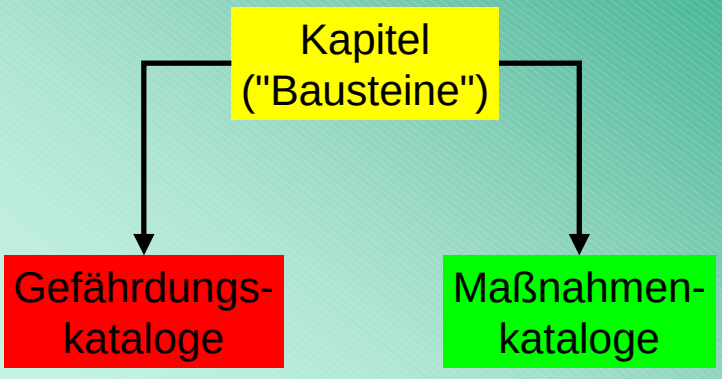
Ziel des IT-Grundschutzes

9

Durch organisatorische, personelle, infrastrukturelle und technische Standard-Sicherheitsmaßnahmen ein Standard-Sicherheitsniveau für IT-Systeme aufbauen, das auch für sensiblere Bereiche ausbaufähig ist.

Struktur des IT-Grundschutzhandbuchs

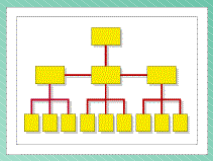
10



Bausteine in Kapitel 3:

Übergeordnete Komponenten

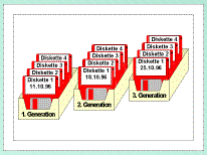
IT-Sicherheits-management



Organisation

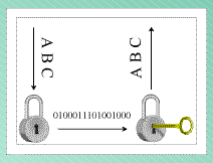
Personal

Notfallvorsorge-Konzept



Datensicherungs-Konzept

Computer-Virenschutzkonzept

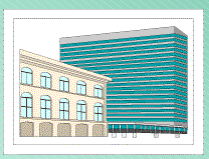


Kryptokonzept

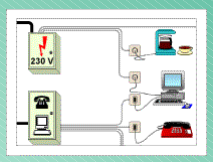
Behandlung von Sicherheitsvorfällen

Bausteine in Kapitel 4:

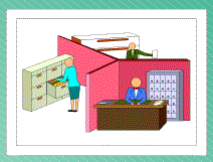
Infrastruktur



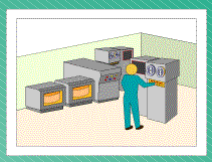
Gebäude



Verkabelung

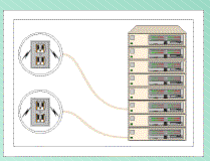


Büroraum



Serverraum

Datenträger-archiv



Raum für techn. Infrastruktur

Schutzschränke

Häuslicher Arbeitsplatz

13

Bausteine in Kapitel 5:

Nicht vernetzte IT-Systeme und Clients

DOS-PC

PCs mit wechselnden Benutzern

Tragbarer PC

Unix-System

PC unter Windows NT

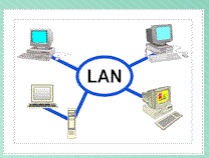
PC mit Windows 95

Allgemeines nicht vernetztes IT-System

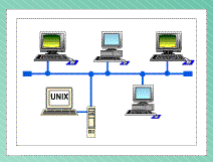
14

Bausteine in Kapitel 6:

Server und Netze

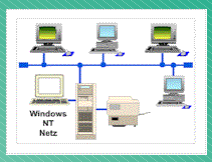


Servergestütztes Netz



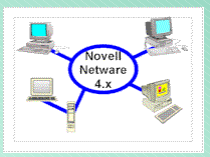
Unix-Server

Peer-to-Peer-Netz

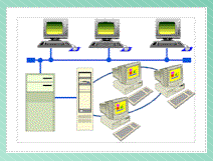


Windows NT Netz

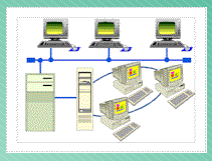
Novell Netware 3.x



Novell Netware 4.x



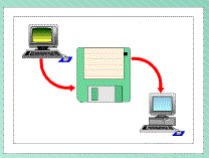
Heterogene Netze



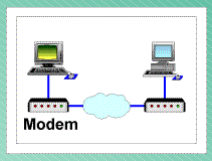
Netz- und System-management

Bausteine in Kapitel 7:

Datenübertragungseinrichtungen



Datenträgeraustausch



Modem

Firewall

E-Mail

WWW-Server

Remote Access

Bausteine in Kapitel 8:

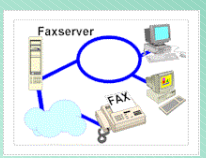
Telekommunikation

TK-Anlage

Faxgerät

Anrufbeantworter

Anbindung über ISDN

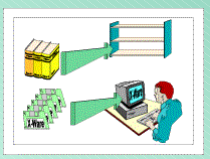


Faxserver

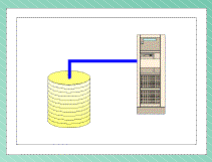
Mobiltelefon

Bausteine in Kapitel 9:

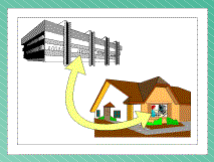
Sonstige IT-Komponenten



Standardsoftware



Datenbanken



Telearbeit

Beispiel einer Standard-Sicherheitsmaßnahme

Maßnahmenkatalog Organisation | M 2.4 | Bemerkungen

M 2.4 Regelungen für Wartungs- und Reparaturarbeiten

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator, IT-Benutzer

Als vorbeugende Maßnahme, um IT vor Störungen zu bewahren, ist die ordnungsgemäße Durchführung von Wartungsarbeiten von besonderer Bedeutung. Die **rechtzeitige Einleitung** von Wartungsarbeiten und die Überprüfung ihrer Durchführung sollte von einer zentralen Stelle aus wahrgenommen werden (z. B. Beschaffungsstelle). Dabei sollten die Wartungsarbeiten von vertrauenswürdigen Personen oder Firmen durchgeführt werden.

Wartungs- und Reparaturarbeiten im Hause

Für Wartungs- und Reparaturarbeiten, insbesondere wenn sie durch Externe durchgeführt werden, sind Regelungen über deren **Beaufsichtigung** zu treffen: während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, daß sie beurteilen kann, ob während der Arbeit nicht-autorisierte Handlungen vollzogen werden. Weiterhin ist zu überprüfen, ob der Wartungsauftrag ausgeführt wurde.

19

Empfehlungen zum IT-Grundschutz

Der Bundesbeauftragte für den Datenschutz
15. Tätigkeitsbericht 1993-1994

"Dabei gehe ich davon aus, das für jedes IT-System, in dem personenbezogene Daten verarbeitet werden oder das hierfür geeignet ist, die für dieses System vom Grundschutzhandbuch empfohlenen Maßnahmen realisiert werden müssen.“

Schreiben vom 28.03.1996 an die
Landesbeauftragten für den Datenschutz

"Soweit bisher Erfahrungen vorliegen, wird vor allem die Praxisnähe dieses Konzeptes [IT-Grundschutzhandbuch] positiv gewürdigt und von einer spürbaren Erhöhung der Datensicherheit berichtet."

20

Empfehlungen zum IT-Grundschutz

Der Bundesrechnungshof
in einem Schreiben an die Landesrechnungshöfe

"In der Bundesverwaltung wird dieses Handbuch häufig mit Erfolg eingesetzt, und es hat dazu beigetragen, den Aufwand für die Erstellung der Sicherheitskonzepte zu senken, und ihre Qualität zu steigern. Zudem läßt sich ein nachprüfbarer Sicherheitsstandard erreichen.“

KES

"Grundschutz heißt: Nicht in jedem Fall sind umfangreiche Analysen und aufwendige Risikoberechnungen nötig. Manchmal reicht es, einfach das Vernünftige zu tun. Ein Konzept, das zum Bestseller wurde."

Freiwillig registrierte Anwender

(Auszug)

	derzeit
über 4.000	registrierte Anwender,
	davon
über 500	im Ausland
	und im Jahr 1999
ca. 12.000	verteilte Handbücher
	und CD-ROMs

- BASF
- DATEV eG
- Deutsche Bank AG
- Deutsche Telekom AG
- Hamburg-Mannheimer
- IBM Deutschland
- Merck KGaA
- Robert Bosch GmbH,
- Siemens AG
- Volkswagen AG
- u.v.m

IT-Grundschutz

Teil II:

Anwendung des

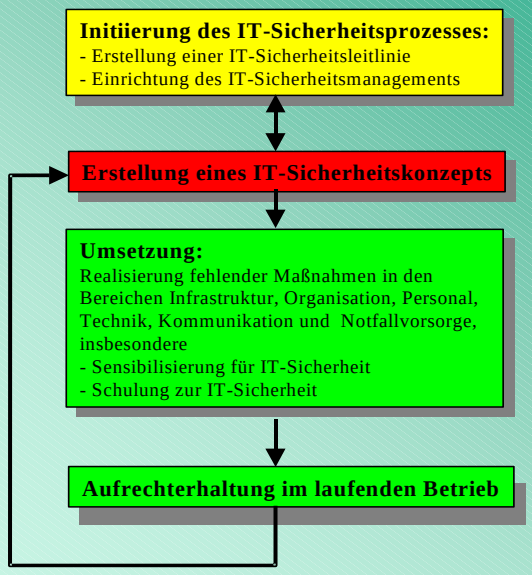
IT-Grundschutzhandbuchs

Verantwortung des Managements

Grundregeln

- Die Initiative für IT-Sicherheit geht vom Management aus.
- Die Verantwortung für IT-Sicherheit liegt beim Management.
- Nur wenn sich das Management um IT-Sicherheit bemüht, wird die Aufgabe "IT-Sicherheit" wahrgenommen.

Übersicht über den IT-Sicherheitsprozess



25

Erstellen einer IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie sollte mindestens enthalten:

- Stellenwert der IT Sicherheit und Bedeutung der IT für die Aufgabenerfüllung,
- Sicherheitsziele und die Sicherheitsstrategie für die eingesetzte IT,
- Zusicherung, dass die IT Sicherheitsleitlinie von der Leitungsebene durchgesetzt wird,
- Beschreibung der etablierten Organisationsstruktur für die Umsetzung des IT-Sicherheitsprozesses

26

Einrichtung des IT-Sicherheitsmanagements

Der IT-Sicherheitsbeauftragte

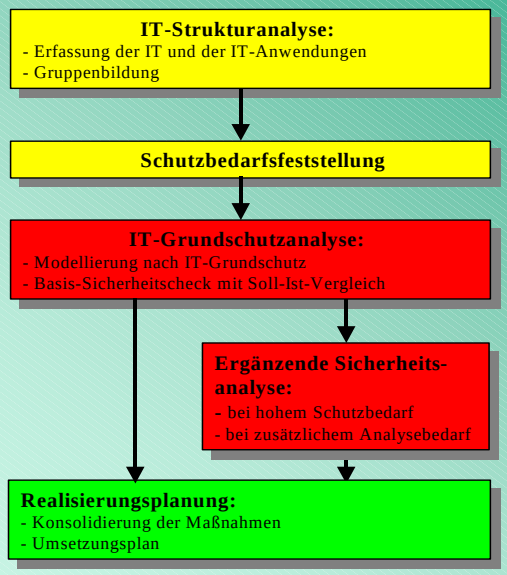
- ist verantwortlich für die Wahrnehmung aller Belange der IT-Sicherheit innerhalb der Organisation,
- koordiniert die Erstellung des IT-Sicherheitskonzepts, des Notfallvorsorgekonzepts, etc.
- erstellt den Realisierungsplan für IT-Sicherheitsmaß-nahmen und prüft die Realisierung,
- stellt den Informationsfluss zur Leitungsebene und zu den IT-Verantwortlichen sicher,
- etc.

Einrichtung des IT-Sicherheitsmanagements

Das IT-Sicherheitsmanagement-Team

- unterstützt den IT-Sicherheitsbeauftragten bei der Wahrnehmung seiner Aufgaben,
- bestimmt IT-Sicherheitsziele und -strategien,
- entwickelt die IT-Sicherheitsleitlinie und prüft deren Umsetzung,
- wirkt mit bei der Erstellung des IT-Sicherheitskonzepts,
- prüft die Wirksamkeit der IT-Sicherheitsmaßnahmen,
- erstellt Schulungs- und Sensibilisierungsprogramme,
- etc.

Erstellen eines IT-Sicherheitskonzepts



29

IT-Strukturanalyse

Netzplanerhebung

Auswertung eines Netzplans

- IT-Systeme, z. B. Clients, Server, Netzkomponenten
- Netzverbindungen zwischen diesen Systemen
- Verbindungen nach außen, z. B. Einwahl oder Internet

Aktualisierung des Netzplans

- Netzplan ist meist nicht auf aktuellem Stand
- IT-Verantwortliche und Administratoren konsultieren
- ggf. Netz- und Systemmanagement heranziehen

30

IT-Strukturanalyse

Komplexitätsreduktion

Gleichartige Komponenten sollten zu einer Gruppe zusammengefasst werden.

Voraussetzungen:

- gleicher Typ
- gleiche oder nahezu gleiche Konfiguration
- gleiche oder nahezu gleiche Netzanbindung
- gleiche Rahmenbedingungen (Administration und Infrastruktur)
- gleiche Anwendungen

IT-Strukturanalyse

Erhebung der IT-Systeme

Beispiel (Auszug)

Nr.	Beschreibung	Plattform	Anz.	Ort	Status	Anwender/ Admin.
S1	Server für Personal-verwaltung	Windows NT Server	1	Bonn, R 1.01	in Betrieb	Personal-referat
S2	Primärer Domänen-Controller	Windows NT Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows 95	2	Berlin, R 2.01	in Betrieb	alle IT-Anwender in Berlin
N1	Router zum Internet-Zugang	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
T1	TK-Anlage für Bonn	ISDN-TK-Anlage	1	Bonn, B.02	in Betrieb	alle Mitarb. in Bonn

IT-Strukturanalyse

Erfassung der IT-Anwendungen

Beispiel (Auszug)

Beschreibung der IT-Anwendungen			IT-Systeme						
Anw.-Nr.	IT-Anwendung/ Informationen	Pers.-bez. Daten	S1	S2	S3	S4	S5	S6	S7
A1	Personaldaten-verarbeitung	X	X						
A4	Benutzer-Authentisierung	X		X				X	
A5	Systemmanagement			X					
A7	zentrale Dokumentenverwaltung					X			

Schutzbedarfsfeststellung

Das IT-Grundschutzhandbuch unterscheidet drei Schutzbedarfskategorien anhand der maximalen Schäden und Folgeschäden bei Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit:

- niedrig bis mittel

begrenzte und überschaubare Schäden

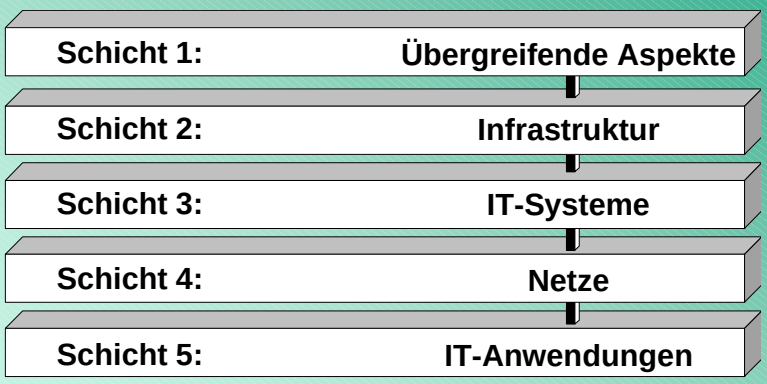
- hoch

beträchtliche Schäden möglich

- sehr hoch

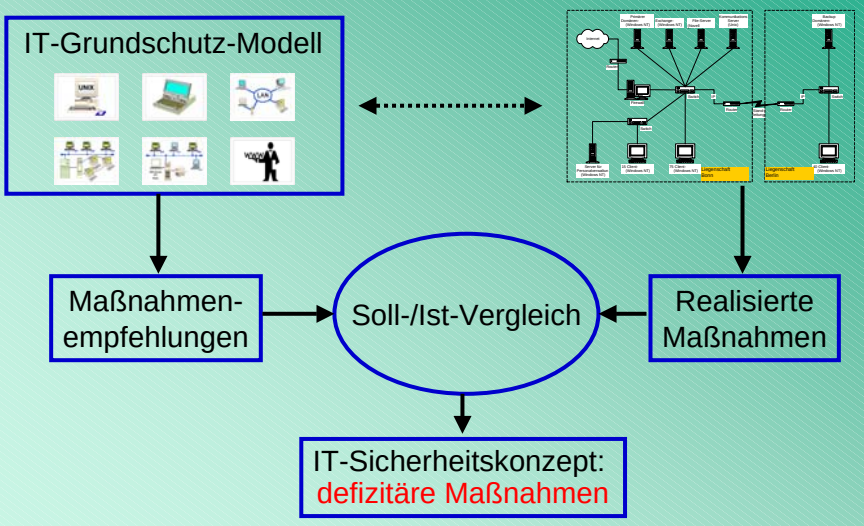
existentiell bedrohliche, katastrophale Schäden möglich

Modellierung nach IT-Grundschutz



Basis-Sicherheitscheck

Soll-/Ist-Vergleich



Basis-Sicherheitscheck

Ergebnisdarstellung

IT-Grundschutzerhebung: Formular zu Baustein 8.5 Faxgerät

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

Maßnahme (Priorität)	Baustein Faxgerät	entbehrlich	Ja	teilweise	Nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
M 2.30 (2)	Regelung für die Einrichtung von Benutzern / Benutzergruppen								
M 2.64 (1)	Kontrolle der Protokolldateien								
M 2.178 (1)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung								
M 2.179 (1)	Regelungen für den Faxserver-Einsatz								
M 2.180 (1)	Einrichten einer Fax-Poststelle								
M 2.181 (1)	Auswahl eines geeigneten Faxservers								
M 3.4 (1)	Schulung vor Programmnutzung								
M 3.5 (1)	Schulung zu IT-Sicherheitsmaßnahmen								

Ergänzende Sicherheitsanalyse

Ist durchzuführen, wenn

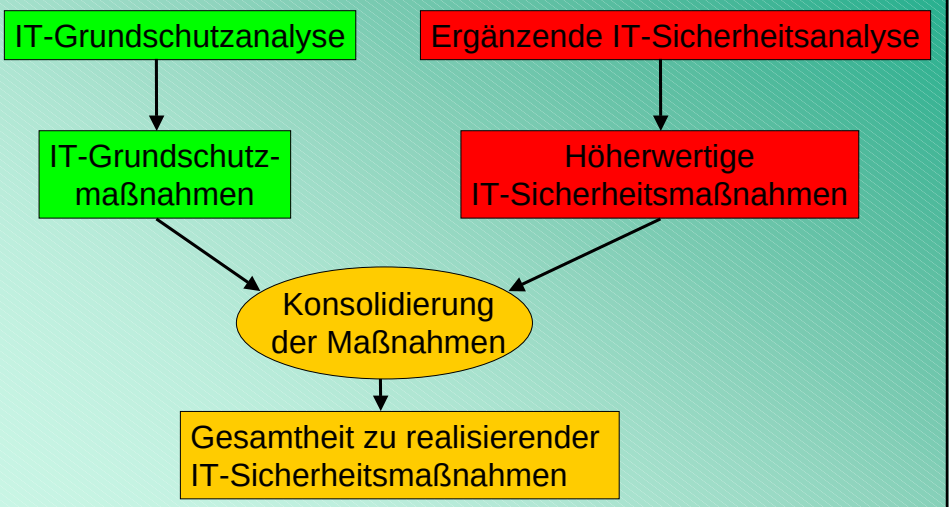
- Schutzbedarfskategorie "hoch" oder "sehr hoch" in mindestens einem der drei Grundwerte vorliegt,
- zusätzlicher Analysebedarf besteht (z. B. bei besonderem Einsatzumfeld) oder
- wenn für bestimmte Komponenten oder Aspekte kein geeigneter Baustein im IT-Grundschutzhandbuch existiert.

Ergänzende Sicherheitsanalyse

Mögliche Vorgehensweisen sind

- Risikoanalyse
  - relevante Bedrohungen ermitteln
  - Eintrittswahrscheinlichkeiten schätzen
- Penetrationstest
  - Verhalten eines Angreifers simulieren
  - Blackbox- und Whitebox-Ansatz unterscheiden
- Differenz-Sicherheitsanalyse
  - höherwertige Maßnahmen identifizieren
  - Schutzklassenmodelle

Konsolidierung der Maßnahmen



Realisierung von IT-Sicherheitsmaßnahmen

Schritt 1: Sichtung der Untersuchungsergebnisse

Welche Maßnahmen sind nicht oder nur teilweise umgesetzt?

Schritt 2: Konsolidierung der Maßnahmen

Welche IT-Grundschutzmaßnahmen werden durch höher- oder gleichwertige Maßnahmen ersetzt?

Schritt 3: Kosten- und Aufwandsschätzung

Welche einmaligen/wiederkehrenden Investitions- bzw. Personalkosten entstehen?

Realisierung von IT-Sicherheitsmaßnahmen

Schritt 4: Festlegung der Umsetzungsreihenfolge

Welche fehlenden Maßnahmen sollten zuerst umgesetzt werden?

Schritt 5: Festlegung der Verantwortlichkeit

Wer setzt welche Maßnahme bis wann um?
Stehen die erforderlichen Ressourcen zur Verfügung?

Schritt 6: Realisierungsbegleitende Maßnahmen

Werden die Mitarbeiter geschult und sensibilisiert, so dass die IT-Sicherheitsmaßnahmen akzeptiert werden?

Realisierung von IT-Sicherheitsmaßnahmen

Beispiel für einen Realisierungsplan (Auszug)

Zielobjekt	Bau-stein	Maßnahme	Umset-zung bis	Verant-wortlich	Budget-rahmen	Bemer-kung
Gesamte Institution	3.1	M 2.11 Regelung des Passwort-gebrauchs	31.12.00	Umsetzung: Herr Müller Kontrolle: Frau Meier	einmalig 2 AT	
Gruppe Clients C1	5.5	Z 2 chipkarten-gestützte Authen-tisierung und lokale Verschlüs-selung der Fest-platten	31.12.00	Umsetzung: Herr Schulz Kontrolle: Frau Meier	einmalig 1400,- Euro + 2 AT wieder-kehrend 2 AT/Jahr	
usw.						