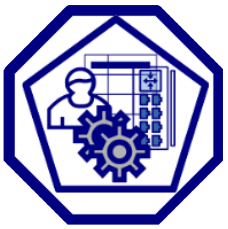
Information zum (Weblink)
Datenschutz - Service
oder Fragen per Mail an:
Mail2@volkerschroer.de



Broschüre "Informationssicherheit mit System - Der IT-Grundschutz des BSI")

Basiswissen BSI / IT-Grundschutz

Meine kurz und knappe Zusammenfassung aus der IT – Grundschutzschulung des BSI [1]

Der Online-Kurs zum IT-Grundschutz basiert auf dem IT-Grundschutz-Kompendium und den BSI - Standards 200-1,-2 und -3. ... Im Fokus ... stehen die Ziele des IT-Grundschutzes, aus welchen Komponenten er besteht und wie die IT-Grundschutz-Methodik generell anzuwenden ist. Ein Angebot an Anwender aus Wirtschaft und Verwaltung … (Auszüge)*

**) m. E. und Entscheider*

Sie wollen es kurz und direkt? Sprechen wir!

Das Inhaltsverzeichnis ist mit Text – Links unterlegt. Mit einem Klick können Sie das entsprechende Thema direkt aufrufen. Lesen Sie nur, die für Sie interessanten Themenkomplexe. Vielen Dank für Ihr Interesse.

Inhaltsverzeichnis

(Einfach Thema nach Wahl anklicken)

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann. Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

1. Einleitung:

Datenschutz und IT-Grundschutz haben drei markant - auffällig verbindende Elemente:

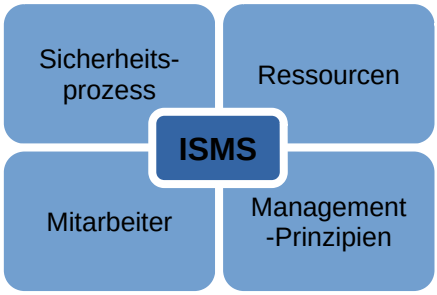
✓✓ **Vertrauchlichkeit (C)[2]** ✓✓ **Integrität (I)[2]** ✓✓ **Verfügbarkeit (A)[2]**

Die Verantwortlichen (meist Geschäftsleitung) sind für beide Themen in der Verantwortung und können „nur“ die Organisation auf Datenschutz- (DSB) und Informationssicherheitsbeauftragte (ISB) delegieren. Da hierfür Zeit, Personal, Budget u.s.w. erforderlich ist, kann ein „Management – Wissen“ hilfreich sein. Gleiches gilt natürlich gegenseitig für die Beauftragten. Der Online-Kurs des BSI bietet eine kurzweilige Information zum Thema IT – Grundschutz. Nach Durchlauf habe ich für den „eiligen Leser“ die aus meiner Sicht wichtigsten Themen zusammengetragen.

Die Informationssicherheit muss den Herausforderungen der Komplexität der Gefährdungslage, der Ganzheitlichkeit der Sicherheitskonzepte, dem Zusammenwirken, der Angemessenheit und Nachhaltigkeit der Sicherheitsmaßnahmen und der Erfüllung externer Anforderungen gerecht werden. Den Kern des BSI Angebots bilden die BSI – Standards und das IT – Grundschutz – Kompendium. Die Kernelemente sind:

1 *Quelle: BSI: „Online-Kurs: Informationssicherheit mit IT-Grundschutz“*
2 *Hinweis: (Confidentiality – Vertraulichkeit | Integrity – Integrität | Availability- Verfügbarkeit)*

2. Sicherheitsmanagement[3]



Damit alle Maßnahmen zielgerichtet gesteuert und erfasst werden ist ein ISMS (Informationssicherheitsmanagementsystem) erforderlich, zur Festlegung der Managementprinzipien (Ziele, Kommunikation, Regeln, Kosten-Nutzen), der Ressourcen und Mitarbeiter sowie die Beschreibung eines Sicherheitsprozesses.

i) Der Sicherheitsprozess

Dieser folgt dem klassischen Qualitätszyklus „Plan – Do – Check – Act“, beginnend mit der Initiierung durch Übernahme der Verantwortung durch die Leitungsebene, Konzeption & Planung, Budgetierung von Personal, Zeit, Finanzen und der Entscheidung über die Vorgehensweise. Für die operativen Aufgaben ist je nach Umfang, ein (ISB) Informationssicherheitsbeauftragter zu benennen (beraten, steuern, initiieren, koordinieren, prüfen, berichten, dokumentieren), der zwecks Wahrung der Unabhängigkeit direkt der Leitung zu unterstellen ist, keinem Konflikt unterliegt (z. B. IT – Leiter) und über die fachliche Qualifikation verfügt. Für die speziellen Anforderungen in der industriellen Produktion kann ergänzend ein (ICS-ISB) Industrial – Control – Systems – Informationssicherheitsbeauftragter benannt werden.

ii) Management – Prinzipen

Die Sicherheitsrichtlinie ist ein wichtiges Grundsatzdokument der Leitung zu verbindlichen Prinzipien und dem anzustrebendem Niveau der Informationssicherheit. Es sollte allen Mitarbeitern bekannt sein und kontinuierlich aktualisiert werden. Die Maßnahmen zur Einhaltung der Leitlinien werden in einem Sicherheitskonzept für einen definierten Geltungsbereich / Informationsverbund festgelegt, der aufgrund der organisatorischen Strukturen oder Anwendungen gut abgrenzbar ist und wesentliche Aufgaben und Geschäftsprozesse umfasst (Organisation, Infrastruktur, IT – Systeme, Anwendungen, Mitarbeiter). Ein grafischer Netzplan kann eine hilfreiche Unterstützung zu einer tabellarischen Aufstellung sein.

iii) Vorgehensweise

Die IT – Grundschutzmethodik sieht drei Varianten zur Vorgehensweise:

- **Basisabsicherung**: zum Einstieg zur Sicherung mit Basismaßnahmen
- **Kernabsicherung**: lenkt die Aufmerksamkeit auf die „Kronjuwelen“
- **Standardabsicherung**: entspricht der Empfehlung des BSI – IT - Grundschutzes

3. Strukturanalyse[4]

i) IT - Infrastrukturübersicht

Ziel ist es, die Objekte und deren Zusammenwirken zu identifizieren und angemessene Schutzmaßnahmen festzulegen. Dabei können Gruppen bei gleichgelagerten Anforderungen gebildet werden. (Typ, Netzanbindungen, Konfiguration, Schutzbedarf, Anwendungen). Ein Beispiel sind die Clients im Vertrieb, die allerdings nicht mit den mobilen Geräten wegen unterschiedlichem (Netz-) Zugang zu einer Gruppe gehören können.

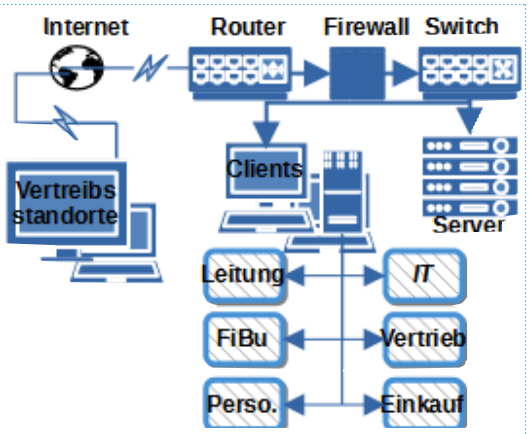


Abb. 1: einfache Infrastrukturübersicht

ii) Erhebung in 5 Schritten

(1) **Geschäftsprozesse** (Kennung, Name, Ziel, Abläufe, Verantwortlicher, benötigte Ressourcen)

(2) **Anwendungen** (Kennung, Name, Ziel, Verantwortlicher, Nutzer)

(3) **Netzplan** (IT – Systeme, interne & externe Verbindungen)

3 *Hinweis: BSI Standard 200-1 Managementsysteme*
4 *Hinweis: BSI Standard 200-2 IT-Grundschutz Methodik*

(4) **IT – Systeme** (Clients, Server Gruppen, Netzkomponenten, Netzdrucker, Produktionssysteme, Endgeräte Scanner, Drucker, Telekommunikation, Mobilgeräte, IoT's mit Bezeichnung, Gruppen, Kurzbeschreibung, Plattform, Standort, Status, Nutzer, Administrator)

(5) **Räumlichkeiten** (Gebäude und Räume mit aktiver IT)

iii) Schutzbedarfsfeststellung

Dient zur Feststellung eines Schadens bei Verletzung der Grundwerte: Vertraulichkeit - Integrität - Verfügbarkeit. Für die 5 Erhebungsschritte werden jeweils folgende Kategorien empfohlen:

- **Normal**: Schaden ist begrenzt und überschaubar
- **Hoch**: Schaden kann beträchtliches Ausmaß annehmen
- **Sehr hoch**: Schaden kann existentiell bedrohlich, katastrophales Ausmaß annehmen

47 elementare Schadensmöglichkeiten sind im IT – Grundschutzkompendium aufgelistet[5]

- ✔ **Vererbung** des Schutzbedarfs von sehr hoch zu hoch und/oder zu normal
- ✔ **Kumulation** des Schutzbedarfs, wenn die Einzelanwendung „normal" die Gesamtheit z. B. auf einem Server aber als „hoch" einzustufen ist.
- ✔ **Verteilung** des Schutzbedarfs, wenn bei Ausfall sofort eine Alternative zur Verfügung steht

4. Schichtenmodell und Modellierung [5]

Für die ermittelten, einzelnen Zielobjekte werden mit dem Bausteinsystem des IT – Grundschutz Kompendiums die relevanten Sicherheitsanforderungen bestimmt. Dabei gilt (Sprachgebrauch):

- ➔ „MUSS, DARF NUR" – Anforderungen müssen unbedingt erfüllt werden
- ➔ „DARF NICHT / KEIN" – in keinem Fall zu tun
- ➔ „SOLLTE" - davon kann bei stichhaltiger Begründung abgesehen werden
- ➔ „SOLLTE NICHT / KEIN" – kann bei stichhaltiger Begründung getan werden

Im Informationsverbund ergibt sich ein Prüfplan für den Bestand und ein Entwicklungskonzept für Neuplanungen. Die Bausteine / Schichten befinden sich unterteilt nach:

Prozess – Bausteine		**System – Bausteine**	
ISMS	Sicherheitsmanagement	IND	Industrielle IT
ORP	Organisation & Personal	APP	Anwendungen
CON	Konzepte & Vorgehensweise	SYS	IT – Systeme
OPS	Betrieb	NET	Netze & Kommunikation
DER	Detektion & Reaktion	INF	Infrastruktur

- ➢ **Tabellarisches Beispiel Branche Handwerk: Abrechnung [6]**

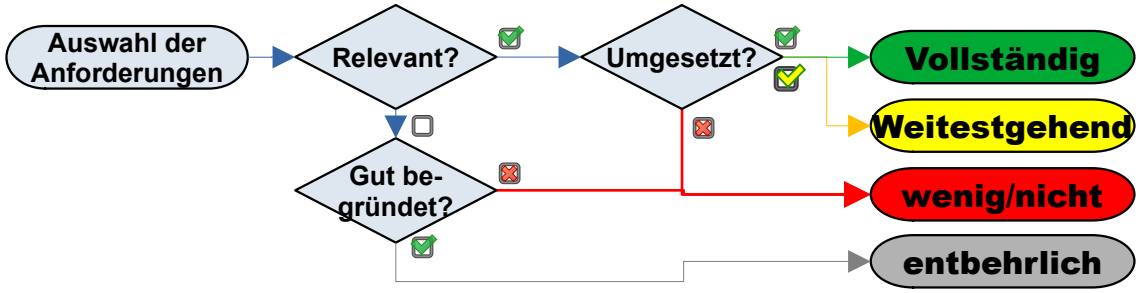
5 *Hinweis: BSI IT - Grundschutz Kompendium*
6 *Quelle: BSI – Branchenprofile, hier „Handwerk"*

Geschäftsprozess	Beschreibung Geschäftsprozess	ANWENDUNGEN (PLATTFORM)	IT – SYSTEME	RÄUME
Abrechnung	Fakturierung	Branchensoftware (Windows) (**)	PC **SYS 2.1** **SYS 2.2.2** **SYS 2.2.3**	Gebäude **INF: 1,2,3,4,7**
		Office-Programm (**)		Home Office INF 8; OPS 1.2.4
	Finanz-, Lohn & Gehaltsbuch-haltung	Finanzbuch-haltungsprogram m + Lohn & Gehalt (**)		Mobiles Arbeiten **INF 9**
		E-Mail (Outlook) **APP 5.2; 5.3**		Fuhrpark (**)

Unter „*APP 5.2 Microsoft Exchange und Outlook*“ befinden sich im IT – Grundschutz - Kompendium eine Beschreibung, die Spezifizierung der Gefährdungslage, die Anforderungen an die Absicherung: Basis, Standard und bei erhöhtem Schutzbedarf. „*SYS 2.1 Allgemein für Client*“ gilt in Kombination mit „*SYS 2.2.2*“ unter Windows 8.1 und „*SYS 2.2.3*“ unter Windows 10. „*OPS 1.2.4 Telearbeit*“ gilt in Kombination mit „*INF 8 Häuslicher Arbeitsplatz*“. Die Inhaltsangabe leitet zügig zum entsprechenden bzw. erforderlichen Baustein. **(**)** = Kein Baustein siehe unter Risikoanalyse.

5. IT – Grundschutz – Check

Mit der Strukturanalyse und der Modellierung gilt es zu prüfen, ob hinreichender Schutz besteht und was noch zu tun bleibt. Die Prüfung ist wie folgt zu dokumentieren:



und – natürlich – entsprechende Maßnahmen für „wenig/nicht“ sind einzuleiten.

6. Risikoanalyse (Zusatzbedarf)[7]

i) Voraussetzungen:

Mit den Bausteinen im Kompendium sind passende und ausreichende Maßnahmen für den normalen Schutzbedarf typischer Informationsverbünde und Anwendungsszenarien gegeben. Zusätzlicher Bedarf an einer Risikoanalyse besteht:

- bei hohem bis sehr hohem Schutzbedarf in mindestens einem der *drei Grundwerte* (**C**onfidentiality – Vertraulichkeit | **I**ntegrity – Integrität | **A**vailability - Verfügbarkeit),
- wenn kein hinreichend passender Baustein im Grundschutz – Kompendium verankert **(**)**,
- wenn die Einsatzumgebung untypisch für den Ansatz im Baustein ist.

Gefährdungsübersicht

Der BSI – Standard 200-3 Risikomanagement[7] führt auf den Seiten 13ff als Hilfsmittel insgesamt 47 elementaren Gefährdungen und deren Wirkung auf die Grundwerte auf. Beispiele:

Kennzeichen	Gefährdung	Grundwerte
G 0.2	Ungünstige klimatische Bedingungen	I, A

7 Quelle: BSI – Standard 200-3 Risikomanagement IT - Grundschutzmethodik

G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	C, A
G 0.32	Missbrauch von Berechtigungen	C, I, A
G 0.42	Social Engineering	C, I

Die Liste ist nicht abschließend und kann/sollte um Hinweise von Beteiligten (Administratoren, Betreuer, Nutzer), Hersteller, Dienstleister oder veröffentlichte Publikationen ergänzt werden. Wichtig ist der Bezug zur Sicherheit der Grundwerte: „C, I, A“.

ii) Risikoeinstufung und Bewertung

Schadensauswirkungen & Höhe (Y-Achse)

vernachlässigbar	Auswirkungen gering bis vernachlässigbar
begrenzt	Auswirkungen begrenzt bis überschaubar
beträchtlich	Auswirkungen beträchtlich, noch tragbar
Existenzbedrohend	bedrohliche bis katastrophale Auswirkungen

Eintrittshäufigkeit (X-Achse)

selten	höchstens alle 5 Jahre (Kenntnisstand)
mittel	Eintritt alle 5 Jahre bis pro Jahr möglich
häufig	Eintritt pro Jahr bis pro Monat möglich
sehr häufig	Eintritt mehrmals im Monat möglich

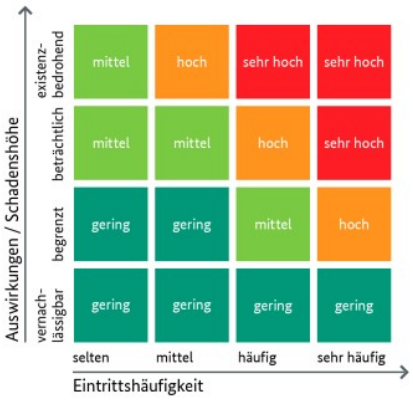


Abbildung. 3 Seite 27 (BSI-ST-200-3: Matrix zur Einstufung von Risiken

Bewertung

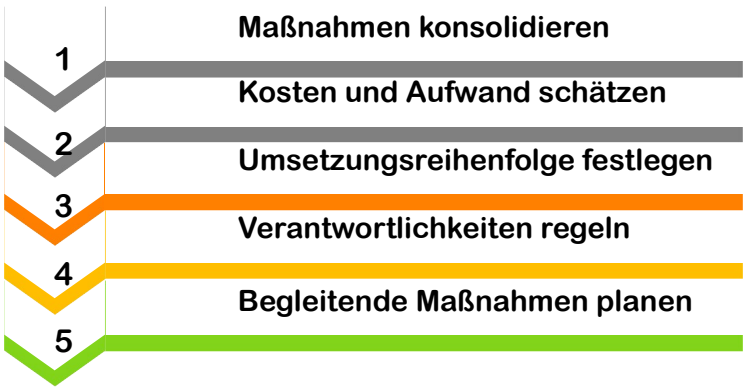
gering	Die umgesetzten bzw. vorgesehenen Maßnahmen im Sicherheitskonzept bieten einen ausreichenden Schutz
mittel	Die umgesetzten bzw. vorgesehenen Maßnahmen im Sicherheitskonzept reichen möglicherweise nicht aus
hoch	Die umgesetzten bzw. vorgesehenen Maßnahmen im Sicherheitskonzept bieten keinen ausreichenden Schutz und das Risiko kann so nicht akzeptiert werden.
sehr hoch	Die umgesetzten bzw. vorgesehenen Maßnahmen im Sicherheitskonzept bieten keinen ausreichenden Schutz und das Risiko kann NICHT AKZEPTIERT werden.

iii) Risikobehandlung & Sicherheitskonzept

Optionen zur Behandlung der erkannten Risiken (BSI – Standard 200-3 Seiten 33ff) sind (A) Risikovermeidung durch Änderung / Umstrukturierung der Geschäftsprozesse, (B) Risikoreduktion durch weitere Schutzmaßnahmen, (C) Risikotransfer durch Absicherung bzw. Versicherung und (D) Risikoakzeptanz und Dokumentation, weil Eintritt nur unter äußerst seltenen bis unwahrscheinlichen Umständen oder Konstellationen oder der Aufwand unangemessen hoch gegenüber der Schadenswirkung ist. Das Sicherheitskonzept ist entsprechend der getroffenen Entscheidung anzupassen, zu modifizieren.

7. Umsetzungsplanung

Zweifelsfrei ist nach Durchführung der einzelnen Punkte meist ein gutes Sicherheitsniveau erreicht. Jedoch ist die IT – Infrastruktur mit den Geschäftsprozessen kein statisches Objekt. Technik und Geschäftsprozesse zeichnen sich durch dynamische Entwicklungen aus. Mit dem regelmäßigen Grundschutz – Check werden



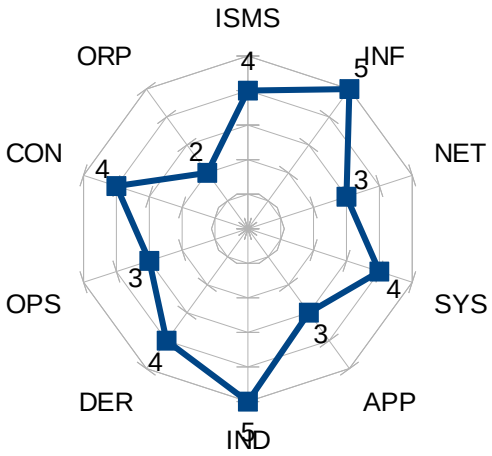
immer wieder zusätzliche Neuerungen oder Änderungen auftreten, die es zu konsolidieren gilt. Neben der Akzeptanzprüfung sollten (5) als begleitende Maßnahmen auch Schulungen und Sensibilisierungen der betroffenen Mitarbeiter nicht unberücksichtigt bleiben.

8. Aufrechterhaltung & Verbesserung

Je komplexer die Struktur desto eher benötigt man einen schlanken Überblick. Beliebt sind Kennzahlen (jeweils Anzahl und schwere sicherheitsrelevanter Ereignisse, Angriffe, Verletzungen im Zeitablauf u. ä.). Ein „sparsamer“ Umgang unter Berücksichtigung von Aufwand, Übersichtlichkeit und Aussagekraft ist dabei m. E. angebracht. Für Umsetzungsprojekte eignen sich andere Vorgehensweisen (z. B. der A3-Report). Aussagefähiger fand ich den Vorschlag eines Reifegradmodells für den IT – Grundschutz (ggf. aggregiert aus den Bereichen) in folgender, beispiehafter Form:

IT - Grundschutz
Umsetzungsstatus Bereich

ISMS Sicherheitsmanagement
ORP Organisation & Personal
CON Konzepte & Vorgehensweise
OPS Betrieb
DER Detektion & Reaktion
IND Industrielle IT
APP Anwendungen
SYS IT – Systeme
NET Netze & Kommunikation
INF Infrastruktur



Die Skala geht von 0 = Zentrum bis 5 Außen in folgender Definition:

0	Kein Prozess und keine Planung vorhanden
1	Planung vorhanden, aber noch geringe bis keine Umsetzung
2	Wesentliche Teile des Prozesses sind umgesetzt, aber keine systematische Dokumentation
3	Prozess ist vollständig umgesetzt und dokumentiert
4	Prozesse werden darüber hinaus regelmäßig auf Effektivität geprüft
5	Zusätzliche Maßnahmen zur kontinuierlichen Verbesserung sind vorhanden.

9. Schlussbemerkung:

Wie schon in der Einleitung bemerkt, sind IT – Grundschutz und der Datenschutz eng mit einander verzahnt. Auch die Methodik hat viele Gemeinsamkeiten. Bei Fragen zum DATENSCHUTZ freue ich mich über Ihre Kontaktaufnahme und hoffe dies ist eine informative Zusammenfassung für Sie.

Bei Bedarf, einfach einmal sprechen!