

# **IT-Grundschutz-Profil für Papierfabriken**

## Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	23.04.2019	BSI	Anlegen des Working Draft 1.0
1.0	05.06.2019	BSI, VDP	Zusammenfassung der Ergebnisse aus den Workshops
1.0	01.07.2019	VDP	Finalisierung

# Inhaltsverzeichnis

## Inhalt

1	Vorwort .....	5
2	Einleitung .....	6
3	Formale Aspekte.....	7
4	Haftungsausschluss.....	7
5	Urheberrecht .....	7
6	Liste der Autorinnen und Autoren .....	8
7	Management Summary .....	8
7.1	Zielgruppe .....	8
7.2	Zielsetzung .....	8
8	Festlegung des Geltungsbereichs (Scope).....	9
8.1	Zielgruppe .....	9
8.2	Schutzbedarf.....	9
8.3	IT-Grundschutz-Vorgehensweise .....	9
8.4	ISO 27001-Kompatibilität .....	9
9	Abgrenzung des Informationsverbunds .....	10
9.1	Bestandteile des Informationsverbundes.....	10
9.2	Nicht berücksichtigte Objekte .....	10
9.3	Verbindung zu anderen IT-Grundschutz-Profilen .....	10
10	Referenzarchitektur.....	10
10.1	Untersuchungsgegenstand .....	11
10.1.1	Geschäftsprozesse .....	11
10.1.2	Anwendungen .....	11
10.1.3	IT-Systeme .....	12
10.1.4	Netze und Kommunikationsverbindungen.....	12
10.1.5	Räumliche Gegebenheiten / Infrastruktur.....	12
10.2	Umgang mit Abweichungen .....	12
10.3	Netzplan .....	13
11	Zu erfüllende Anforderungen und umzusetzende Maßnahmen .....	13
11.1	Alles auf einen Blick - Arbeitshilfe: „Landkarte“ .....	13
11.2	Übersicht I: Übergeordnete Bausteine .....	14
11.2.1	ISMS.1 Sicherheitsmanagement (R1).....	15
11.2.2	ORP: Organisation und Personal .....	15
11.2.3	CON: Konzeption und Vorgehensweisen .....	15
11.2.4	OPS: Betrieb.....	15
11.2.5	DER: Detektion von Sicherheitsvorfällen und Reaktion bei Vorfällen .....	15

11.2.6	APP: Anwendungen .....	15
11.2.7	SYS: IT-Systeme .....	15
11.2.8	IND: Industrielle IT.....	15
11.3	Übersicht II: Bausteine aus der Landkarte .....	16
11.3.1	OPS: Betrieb.....	16
11.3.2	APP: Anwendungen .....	16
11.3.3	SYS: IT-Systeme .....	16
11.3.4	IND: Industrielle IT.....	16
11.3.5	NET: Netze und Kommunikation .....	16
11.3.6	INF: Infrastruktur .....	17
12	Risikobetrachtung / Risikobehandlung .....	17
13	Anwendungshinweise .....	18
14	Anhang .....	21
14.1	Anhang 1: Landkarte Geschäftsprozess ‚Order-to-Cash‘ .....	22
14.2	Anhang 2: Landkarte Geschäftsprozess ‚Produktion‘ .....	23
14.3	Anhang 3: Landkarte Geschäftsprozess ‚Logistik‘ .....	24
14.4	Anhang 4: Hinweise zur Nutzung .....	25

# 1 Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der VDP haben am VAP/VDP-Unternehmertag 2018 vereinbart, gemeinsam mit Vertretern der Papierindustrie ein branchenspezifisches IT-Grundschutz-Profil zu erarbeiten.

Es wurde ein Expertenkreis gebildet, der unter der Leitung des BSI in mehreren Workshops dieses IT-Grundschutz-Profil für Papierfabriken erstellt hat.

In Papierfabriken werden nahezu alle Prozesse durch Informationstechnologie (IT) unterstützt. Die Digitalisierung ist als wichtiger Faktor der komplexen Produktionsprozesse und in der industriellen Produktion unverzichtbar. Die Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten und in der Informationstechnologie, sind ein wichtiges Ziel zur Aufrechterhaltung von Geschäftsprozessen und Abwehr von Schäden.

Auf Grund relativ ähnlicher Geschäfts- und Produktionsprozesse soll das folgende IT-Grundschutz-Profil den Unternehmen mit den beschriebenen Methoden und Bausteinen die wirkungsvolle und handhabbare Umsetzung eines Sicherheitskonzepts und die Gewährleistung von Informationssicherheit nach der IT-Grundschutz Vorgehensweise ermöglichen.

Wir danken den Experten aus den VDP-Mitgliedsunternehmen und den Mitarbeiterinnen und Mitarbeitern des BSI, mit deren Einsatz dieses IT-Grundschutz-Profil erstellt werden konnte.

Verband Deutscher Papierfabriken e. V. (VDP)

## 2 Einleitung

### Relevanz der Informationssicherheit für die Papierindustrie

Der VDP engagiert sich in der Allianz für Cyber-Sicherheit, einer Initiative des Bundesamts für Sicherheit in der Informationstechnik (BSI). Im Rahmen einer Kooperation mit dem BSI hat der Verband den Prozess zur Erstellung eines IT-Grundschutz-Profil initiiert. Das IT-Grundschutz-Profil erleichtert es IT-Sicherheitsverantwortlichen in Papierfabriken, ihr Sicherheitskonzept basierend auf dem IT-Grundschutz auf die individuellen Rahmenbedingungen im Unternehmen anzupassen. Der IT-Grundschutz des BSI ist eine seit Jahren bewährte Methodik zum Aufbau eines Managementsystems für Informationssicherheit (ISMS), um das Niveau der Informationssicherheit in Institutionen jeder Größenordnung zu erhöhen.

Für einen erleichterten Einstieg in den IT-Sicherheitsprozess ist das vorliegende IT-Grundschutz-Profil erstellt worden. Ein IT-Grundschutz-Profil ist ein Muster-Sicherheitskonzept, das als Schablone für Institutionen mit vergleichbaren Rahmenbedingungen dient. Schritte, die nach IT-Grundschutz zu gehen sind, sind in diesem Muster pauschalisiert. So ist es schließlich allen Interessierten in der Branche möglich, mit Hilfe der Schablone die Informationssicherheit im jeweiligen Betrieb zu erhöhen. Das spart viel Arbeit und Zeit.

Das vorliegende Dokument „IT-Grundschutz-Profil für Papierfabriken“ umfasst ausgehend von drei als relevant betrachteten Geschäftsprozessen: Order-to-cash, Produktion, Logistik, u. a.

- eine Liste der relevanten Zielobjekte (Anwendungen, IT-Systeme sowie Räumlichkeiten), die es zu schützen gilt,
- eine Zuordnung der dazu passenden IT-Grundschutz-Bausteine mit Anforderungen und Umsetzungshinweisen sowie
- Empfehlungen zur Umsetzungsreihenfolge.

Zentrale Hilfestellungen für die Umsetzung im Betrieb bieten „Landkarten“ als Entscheidungsgrundlage für die Unternehmensleitung und ein „Umsetzungs-Fahrplan“ für IT-Fachleute.

### 3 Formale Aspekte

<b>Titel :</b>	IT-Grundschutz-Profil für Papierfabriken
<b>Autorenschaft:</b>	Siehe Punkt 6 „Liste der Autorinnen und Autoren“
<b>Herausgeberschaft:</b>	Verband Deutscher Papierfabriken e. V. (VDP) German Pulp and Paper Association
<b>Registrierungsnummer:</b>	Wird nach erfolgreichem Durchlaufen des Registrierungsverfahrens vom BSI vergeben
<b>Versionsstand:</b>	Veröffentlicht am 04.07.2019, Version 1.0, finalisiert im Juni 2019
<b>Revisionszyklus:</b>	Die Aktualität des Dokuments soll alle zwei Jahre überprüft werden.
<b>Vertraulichkeit:</b>	Das Dokument in der hier vorliegenden Version ist offen zugänglich.

### 4 Haftungsausschluss

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Autorinnen und Autoren haben keinen Einfluss auf die Nutzung dieses IT-Grundschutz-Profiles durch Anwenderinnen und Anwender und kennen auch nicht die individuellen Anforderungen an ihre Sicherheitskonzepte, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

### 5 Urheberrecht

Alle Inhalte dieses Werkes, insbesondere Texte und Grafiken, sind urheberrechtlich geschützt. Das Urheberrecht liegt, soweit nicht ausdrücklich gekennzeichnet, bei den Teilnehmerinnen und Teilnehmern der Workshop-Reihe „IT-Grundschutz-Profil für Papierfabriken“. Eine Weitergabe an Dritte ist ausdrücklich erwünscht.

## 6 Liste der Autorinnen und Autoren

An der Erarbeitung dieses Dokumentes waren die Teilnehmerinnen und Teilnehmer der Workshop-Reihe „IT-Grundschutz-Profil für Papierfabriken“ beteiligt. Die Workshops wurden vom VDP veranstaltet, die Moderation lag beim BSI. Die Beteiligten werden in der nachfolgenden Tabelle in alphabetischer Reihenfolge aufgeführt.

Name	Organisation
Bette, Carsten	Drewsen Spezialpapiere GmbH & Co. KG
Brabender, Katrin	Verband Deutscher Papierfabriken e. V.
Drolshage, Burkhard	WEPA Hygieneprodukte GmbH
Hoppe, Klaus	R.D.M. Arnsberg GmbH
Landsmann, Dirk	Mitsubishi HiTec Paper Europe GmbH
Middelberg, Ulrich	Steinbeis Papier GmbH
Morgenbrod, Bernd	KANZAN Spezialpapiere GmbH
Platzer, Gerald	SAPPI Papier Holding GmbH
Schmidt, Volker	Kabel Premium Pulp & Paper GmbH
Schüller, Marco	Moritz J. Weig GmbH & Co. KG
Steiner, Charlotte	Verband Deutscher Papierfabriken e. V.
Stern, Alexander	Schoellershammer GmbH & Co. KG
Wasserer, Michael	Fripa Papierfabrik Albert Friedrich KG
Wirtz, Günter	Schoellershammer GmbH & Co. KG
Zeppenfeld, Manfred	WEPA Hygieneprodukte GmbH

## 7 Management Summary

### 7.1 Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an Vertreterinnen und Vertreter von Papierfabriken, die die Informationssicherheit in ihrem Betrieb sicherstellen wollen.

Es ist insbesondere gedacht für die Verantwortlichen in der Geschäftsleitung, in der IT-Administration und im Qualitätsmanagement, bei denen die Zuständigkeit für Umsetzung und Aufrechterhaltung der Informationssicherheit liegt.

### 7.2 Zielsetzung

Dieses IT-Grundschutz-Profil nimmt drei Geschäftsprozesse einer Muster-Papierfabrik in den Fokus und empfiehlt Maßnahmen entsprechend der Herangehensweise der Basis-Absicherung nach IT-Grundschutz. Diese Absicherung kann auf die individuellen Rahmenbedingungen übertragen und somit das Niveau je nach Bedarf Schritt für Schritt modular erhöht werden. Diese drei Geschäftsprozesse sind:

- **Order-to-Cash (kaufmännische Auftragsabwicklung)**
- **Produktion**
- **Logistik.**

Durch die vorgeschlagenen Maßnahmen unterstützt das IT-Grundschutz-Profil beim Einstieg in die Informationssicherheit und der Feststellung der gravierendsten Schwachstellen in diesen Prozessen. Darüber hinaus kann das IT-Grundschutz-Profil Hilfe bei der Durchführung einer weiterführenden Schutzbedarfsfeststellung und Risikoanalyse leisten, wenn eine Schutzbedarfskategorie über „normal“ zugrunde gelegt werden soll. Informationen hierzu sind im Abschnitt 13 zu finden.

Um den Handlungsbedarf für den gesamten Betrieb zu ermitteln, müssten alle übrigen Geschäftsprozesse einer Papierfabrik entsprechend der Vorgehensweise dieses IT-Grundschutz-Profiles aufgenommen werden.

### **Aufgaben der Leitungsebene**

Die Autorinnen und Autoren empfehlen der Leitungsebene einer Papierfabrik die Anwendung dieses IT-Grundschutz-Profiles als Grundlage für das Informationssicherheitskonzept des Betriebs. Allerdings bezieht sich dieses IT-Grundschutz-Profil ausschließlich auf die oben genannten Geschäftsprozesse und nicht auf die Gesamtorganisation einer Papierfabrik. Hierfür müssten alle übrigen relevanten Geschäftsprozesse entsprechend erfasst und dokumentiert werden. Damit ist es dann möglich, den Handlungsbedarf für den Gesamtbetrieb zu ermitteln und entsprechende Schutzmaßnahmen auszuwählen.

Die Autorinnen und Autoren empfehlen, dass Papierfabriken, die z. B. Teile ihrer technischen Infrastruktur durch Dritte betreiben lassen, das vorliegende IT-Grundschutz-Profil als Grundlage für die Auswahl entsprechender Dienstleister verwenden. Die hier formulierten Anforderungen sollten in den Vertragsbedingungen enthalten sein.

## **8 Festlegung des Geltungsbereichs (Scope)**

### **8.1 Zielgruppe**

Dieses IT-Grundschutz-Profil richtet sich an Papierfabriken.

### **8.2 Schutzbedarf**

Die in dem IT-Grundschutz-Profil verwendete Vorgehensweise der Basis-Absicherung setzt keinen Fokus auf den Schutzbedarf (die Ausprägungen der Schutzbedarfskategorien), da es sich um eine grundlegende Absicherung in der Breite und nicht Tiefe handelt. Erst mit der darauf aufbauenden Vorgehensweise der Standard-Absicherung findet er Berücksichtigung. Teilprozesse können über den Schutzbedarf der Basis-Absicherung hinausgehen und bedürfen der gesonderten Prüfung.

### **8.3 IT-Grundschutz-Vorgehensweise**

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen sind Empfehlungen für Papierfabriken und verwenden die Basis-Absicherung nach dem BSI-Standard 200-2. Gemäß IT-Grundschutz ist es empfehlenswert perspektivisch mindestens die Standard-Absicherung gemäß IT-Grundschutz anzustreben und umzusetzen. Für den Teilprozess „Energieversorgung“ im Geschäftsprozess Produktion soll exemplarisch gezeigt werden, wie sich die Standard-Absicherung gestalten lässt.

### **8.4 ISO 27001-Kompatibilität**

Diesem IT-Grundschutz-Profil liegt prinzipiell die Basis-Absicherung gemäß IT-Grundschutz zugrunde. Wird davon abweichend durchgängig mindestens die IT-Grundschutz-Vorgehensweise „Standard-Absicherung“ umgesetzt, ist diese zu der ISO 27001 kompatibel.

## 9 Abgrenzung des Informationsverbunds

### 9.1 Bestandteile des Informationsverbundes

Zum Informationsverbund gehören alle Prozesse und Verfahren in einer Papierfabrik, die für die Abwicklung des Kerngeschäfts notwendig sind. Gegenstand des vorliegenden IT-Grundschutz-Profils sind die Prozesse und Verfahren aus den folgenden Anwendungsgebieten:

- **Order-to-Cash (kaufmännische Auftragsabwicklung)**
- **Produktion**
- **Logistik**

### 9.2 Nicht berücksichtigte Objekte

Im IT-Grundschutz-Profil für Papierfabriken werden andere Prozesse, die für die Abwicklung des Gesamt-Prozesses einer Papierfabrik notwendig sind, nicht berücksichtigt. Die Autorinnen und Autoren sind davon überzeugt, dass die drei ausgewählten Geschäftsprozesse einerseits von herausragender Bedeutung für die Informationssicherheit, andererseits ausreichend repräsentativ für alle nicht berücksichtigten Geschäftsprozesse sind. Eine Papierfabrik kann das vorliegende IT-Grundschutz-Profil sehr gut als Grundlage für die Entwicklung und Fortführung eines individuellen Informationssicherheitsmanagementsystems verwenden.

### 9.3 Verbindung zu anderen IT-Grundschutz-Profilen

Zu diesem Zeitpunkt gibt es keine Verweise auf andere IT-Grundschutz-Profile.

## 10 Referenzarchitektur

Die Referenzarchitektur (auch ‚Untersuchungsgegenstand‘ genannt) legt fest, auf welche Objekte die Anforderungen des IT-Grundschutzes im Sinne dieses IT-Grundschutz-Profils angewendet werden müssen.

Dazu gehören

- Geschäftsprozesse,
- Anwendungen (Software-Programme),
- vorhandene IT-Systeme (u.a. Clients, Server, Netzkopplungselemente, Mobile Devices) sowie eingesetzte Netze, Kommunikationseinrichtungen, externe Schnittstellen,
- und räumliche Gegebenheiten / Infrastruktur (Liegenschaften, Gebäude, Räume).

## 10.1 Untersuchungsgegenstand

### 10.1.1 Geschäftsprozesse

Der **Geschäftsprozess, Order-to-Cash (kaufmännische Auftragsabwicklung)**<sup>4</sup> umfasst die Unterprozesse:

- Sales/Auftragsabwicklung
- Finance/Controlling
- Planung

Der **Geschäftsprozess 'Produktion'** umfasst die Unterprozesse:

- Rohstoffversorgung
- Energieversorgung (hier werden exemplarisch Standard-Anforderungen angesetzt)
- Entsorgung
- Instandhaltung/ Wartung
- MES-/Prozessleitsystem
- Qualitätsleitsystem

Der **Geschäftsprozess 'Logistik'** umfasst die Unterprozesse:

- Lager/automatisiert
- Versand
- Transport

### 10.1.2 Anwendungen

- MS Exchange
- ERP
- EDI
- Datenbank
- E-Commerce
- CRM
- Office & E-Mail Client
- Banking Software
- DMS
- Office 365 (Cloud)
- Reporting (BI)
- Mobile Device Management (MDM)
- Browser
- Zoll-Applikation
- Produktionsplanungssoftware (PPS)
- MES
- QLS
- PLS
- Environmental Systeme
- Energiemanagementsystem
- Personaleinsatzplanung – Cloud
- Lagerverwaltungssystem (LVS)
- Yard-Management (z.B. auch LKW-Self-Service, Waage)

### **10.1.3 IT-Systeme**

- Virtualisierter Server
- Windows-Server
- Server
- Linux-Server
- Windows 10 Client
- Terminal-Server
- Tablets
- Smartphone
- Notebooks
- Fax
- Drucker-Multifunktionsgerät
- Kiosk-Systeme
- IP-Kameras
- Sensoren
- SPS
- EWS
- HMI
- Maschine

### **10.1.4 Netze und Kommunikationsverbindungen**

- Telefonanlage
- Router
- Switches
- LAN
- WLAN
- VPN
- Firewall
- Schnittstellen

### **10.1.5 Räumliche Gegebenheiten / Infrastruktur**

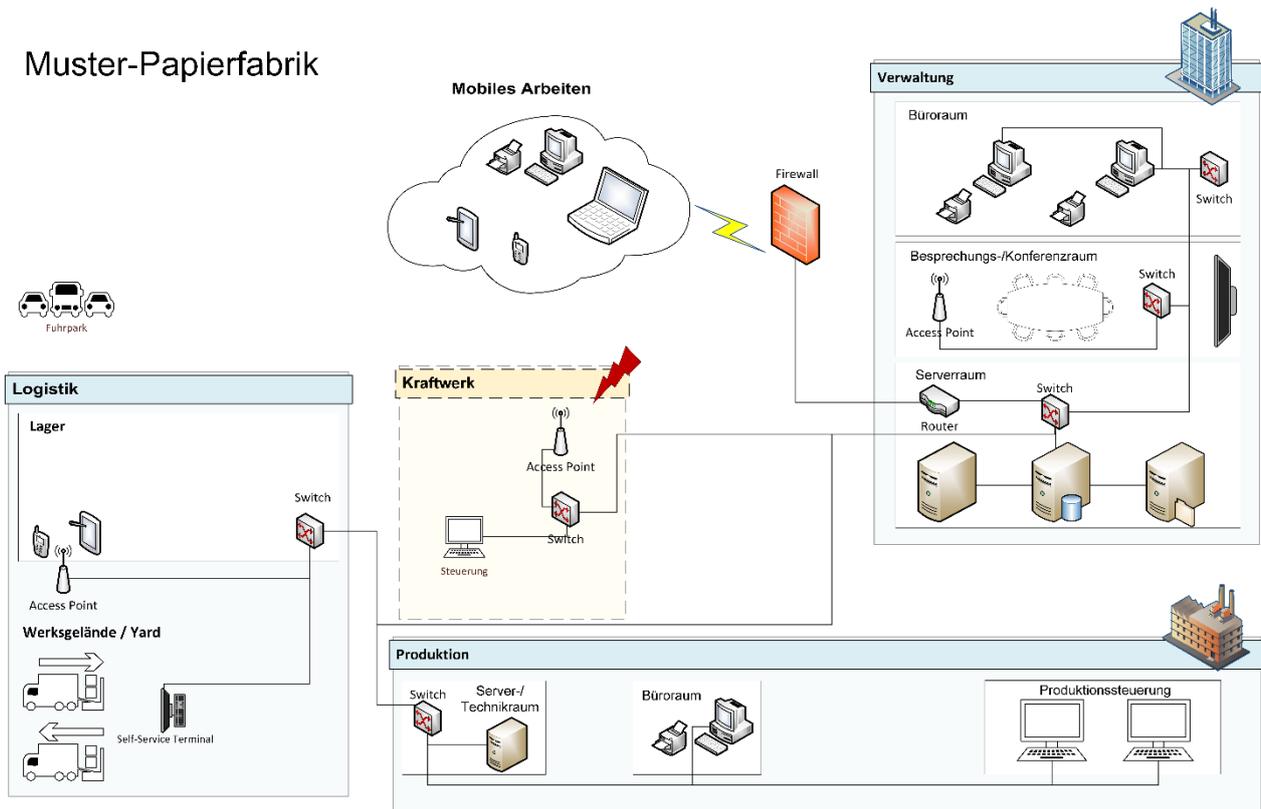
- Gebäude
- Büroraum
- Serverraum
- Technikraum
- Rechenzentrum (Outsourcing)
- Netzverteiler-Schrank/Raum
- Werksgelände (inkl. Yard)
- Home-Office
- Mobiles Arbeiten

## **10.2 Umgang mit Abweichungen**

Weicht der zu schützende Informationsverbund im jeweiligen Betrieb von der in diesem IT-Grundschutz-Profil dargestellten Referenzarchitektur ab, sind die zusätzlichen oder nicht vorhandenen Zielobjekte zu dokumentieren. Wie nach der IT-Grundschutz-Methodik üblich, sind diesen Objekten dann geeignete Bausteine des IT-Grundschutz-Kompendiums, sofern vorhanden, zuzuordnen.

## 10.3 Netzplan

### Muster-Papierfabrik



## 11 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Anhand der Referenzarchitektur lassen sich passende IT-Grundschutz-Bausteine auswählen. Sie enthalten Erläuterungen zu Gefährdungslage und Sicherheitsanforderungen sowie weiterführende Informationen.

Die in diesem IT-Grundschutz-Profil aufgeführten Bausteine aus dem IT-Grundschutz-Kompendium sind für die Erreichung des angestrebten Sicherheitsniveaus im Regelfall ausreichend. Alle Basis-Anforderungen der Bausteine aus Kapitel 11.2 und 11.3 müssen auf geeignete Weise erfüllt werden. Vom IT-Grundschutz-Profil abweichende Einsatzumgebungen oder Komponenten erfordern u. U. die Anwendung weiterer Bausteine. Daher ist im Rahmen der Anwendung des IT-Grundschutz-Profiles eine Überprüfung notwendig.

### Tipp für die Geschäftsleitung:

Jeder IT-Grundschutz-Baustein enthält beispielhaft Informationen zur Gefährdungslage, die mögliche Risiken bei mangelnder Umsetzung der empfohlenen Sicherheitsanforderungen beschreiben.

Zu vielen Bausteinen gibt es zusätzlich Umsetzungshinweise mit detaillierten Beschreibungen passender Sicherheitsmaßnahmen, die als Grundlage für Sicherheitskonzeptionen verwendet werden können.

### 11.1 Alles auf einen Blick - Arbeitshilfe: „Landkarte“

Für jeden der drei hier betrachteten Geschäftsprozesse wurde eine „Landkarte“ erstellt. Die Landkarte zeigt alle wesentlichen Erkenntnisse aus der Strukturanalyse und der Modellierung (Auswahl passender IT-Grundschutz-Bausteine). Für jeweils einen Geschäftsprozess werden die Referenzarchitektur (Anwendungen, IT-Systeme sowie Räumlichkeiten) und die Zuordnung der IT-Grundschutz-Bausteine inkl. Empfehlungen zur Umsetzungsreihenfolge dargestellt. Wo keine Zuordnung

bestehender Bausteine erfolgen kann, wird deutlich, dass eine eigene Risikoanalyse und ggf. unternehmens- und/oder branchen-spezifische Lösungen notwendig sind.

In Form von Grafiken bieten die Landkarten quasi alles auf einen Blick und eröffnen so einen Einstieg in den individuellen IT-Sicherheitsprozess. Sie können sowohl als Entscheidungsgrundlage für die Unternehmensleitung als auch als „Umsetzungs-Fahrplan“ für IT-Fachleute dienen.

Die Landkarten zu den hier behandelten Geschäftsprozessen, ebenso wie die Hinweise zur Nutzung diese und Erklärungen der verwendeten Symbole, sind im Anhang zu finden:

- **Order-to-Cash (kaufmännische Auftragsabwicklung)**
- **Produktion**
- **Logistik**

Die Herangehensweise nach Basis-Absicherung, die diesem IT-Grundschutz-Profil zugrunde liegt, sieht vor, dass bei der Anwendung als Mindestmaß die Basis-Anforderungen der jeweiligen Bausteine umgesetzt werden müssen. Beim Teilprozesses „Energieversorgung“ sind zusätzlich die Standard-Anforderungen umzusetzen.

## **11.2 Übersicht I: Übergeordnete Bausteine**

Die in diesem Kapitel aufgelisteten Bausteine sind nicht in den Landkarten zu finden, da sie sich eher auf den gesamten Informationsverbund beziehen und nicht auf einzelne Zielobjekte. Beispiele hierfür sind die Bausteine ISMS.1 und CON.3, die nicht auf ein einzelnes Zielobjekt wie ein IT-System, sondern übergreifend auf den gesamten Informationsverbund angewandt werden. Diese Bausteine sind für ein ganzheitliches Konzept eines Informationssicherheitssystems notwendig. Der Aufwand in der konkreten Ausgestaltung hängt stark vom individuellen Fall ab.

### **Tipp zur Umsetzungsreihenfolge:**

Die folgenden Bausteine sind mit Hinweisen zur Bearbeitungsreihenfolge versehen:

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.
- R2: Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.
- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, es wird aber empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

### **11.2.1 ISMS.1 Sicherheitsmanagement (R1)**

### **11.2.2 ORP: Organisation und Personal**

ORP.1 Organisation (R1)

ORP.2 Personal (R1)

ORP.3 Sensibilisierung und Schulung (R1)

ORP.4 Identitäts- und Berechtigungsmanagement (R1)

ORP.5 Compliance Management (Anforderungsmanagement) (R3)

### **11.2.3 CON: Konzeption und Vorgehensweisen**

CON.1 Kryptokonzept (R3)

CON.2 Datenschutz (R2)

CON.3 Datensicherungskonzept (R1)

CON.4 Auswahl und Einsatz von Standardsoftware (R2)

CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen (R3)

CON.6 Löschen und Vernichten (R1)

CON.7 Informationssicherheit auf Auslandsreisen (R3)

### **11.2.4 OPS: Betrieb**

OPS.1.1.2 Ordnungsgemäße IT-Administration (R1)

OPS.1.1.3 Patch- und Änderungsmanagement (R1)

OPS.1.1.4 Schutz vor Schadprogrammen (R1)

OPS.1.1.5 Protokollierung (R1)

OPS.1.1.6 Software-Tests und –Freigaben (R1)

OPS.1.2.3 Informations- und Datenträgeraustausch (R3)

OPS.2.4 Fernwartung (R3)

### **11.2.5 DER: Detektion von Sicherheitsvorfällen und Reaktion bei Vorfällen**

DER.1 Detektion von sicherheitsrelevanten Ereignissen (R2)

DER.2.1 Behandlung von Sicherheitsvorfällen (R2)

DER.2.2 Vorsorge für die IT-Forensik (R3)

DER.3.1 Audits und Revisionen (R3)

DER.4 Notfallmanagement (R3)

### **11.2.6 APP: Anwendungen**

APP.1.4 Mobile Anwendungen (Apps) (R2)

### **11.2.7 SYS: IT-Systeme**

SYS.3.4 Mobile Datenträger (R2)

### **11.2.8 IND: Industrielle IT**

IND.1 Betriebs- und Steuerungstechnik (R2)

## **11.3 Übersicht II: Bausteine aus der Landkarte**

Die in diesem Kapitel aufgelisteten Bausteine finden sich auch in den Landkarten und sind dort einzelnen Zielobjekten zugeordnet.

### **11.3.1 OPS: Betrieb**

OPS.1.2.2 Archivierung (R3)  
OPS.1.2.4 Telearbeit (R3)  
OPS.2.1 Outsourcing für Kunden (R2)  
OPS.2.2 Cloud-Nutzung (R2)

### **11.3.2 APP: Anwendungen**

APP.1.1 Office-Produkte (R2)  
APP.1.2 Web-Browser (R2)  
APP.4.2 SAP-ERP-System (R2)  
APP.4.3 Relationale Datenbanksysteme (R2)  
APP.5.1 Allgemeine Groupware (R2)  
APP.5.2 Microsoft Exchange und Outlook (R2)

### **11.3.3 SYS: IT-Systeme**

SYS.1.1 Allgemeiner Server (R2)  
SYS.1.2.2 Windows Server 2012 (R2)  
SYS.1.3 Server unter Unix (R2)  
SYS.1.5 Virtualisierung (R2)  
SYS.2.1 Allgemeiner Client (R2)  
SYS.2.2.3 Clients unter Windows 10 (R2)  
SYS.3.1 Laptops (R2)  
SYS.3.2.1 Allgemeine Smartphones und Tablets (R2)  
SYS.3.2.2 Mobile Device Management (MDM) (R2)  
SYS.3.2.3 iOS (for Enterprise) (R2)  
SYS.3.2.4 Android (R2)  
SYS.3.3 Mobiltelefon (R2)  
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte (R2)  
SYS.4.4 Allgemeines IoT-Gerät (R2)

### **11.3.4 IND: Industrielle IT**

IND.2.1 Allgemeine ICS-Komponente (R2)  
IND.2.2 Speicherprogrammierbare Steuerung (SPS) (R2)  
IND.2.3 Sensoren und Aktoren (R2)  
IND.2.4 Maschine (R2)  
IND.2.7 Safety Instrumented Systems (R2)

### **11.3.5 NET: Netze und Kommunikation**

NET.1.1 Netzarchitektur und -design (R2)  
NET.1.2 Netzmanagement (R2)  
NET.2.1 WLAN-Betrieb (R2)  
NET.2.2 WLAN-Nutzung (R2)  
NET.3.1 Router und Switches (R2)  
NET.3.2 Firewall (R2)  
NET.3.3 VPN (R2)

NET.4.1 TK-Anlagen (R2)  
NET.4.2 VOIP (R2)  
NET.4.3 Faxgeräte und Faxserver (R2)

### **11.3.6 INF: Infrastruktur**

INF.1 Allgemeines Gebäude (R2)  
INF.2 Rechenzentrum sowie Serverraum (R2)  
INF.3 Elektrotechnische Verkabelung (R2)  
INF.4 IT-Verkabelung (R2)  
INF.7 Büroarbeitsplatz (R2)  
INF.9 Mobiler Arbeitsplatz (R2)  
INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum (R2)

## **12 Risikobetrachtung / Risikobehandlung**

Die Basis- und Standard-Anforderungen der IT-Grundschatz-Bausteine wurden so festgelegt, dass dazu passende Maßnahmen für normalen Schutzbedarf und für typische Informationsverbände und Anwendungsszenarien einen angemessenen und ausreichenden Schutz bieten. Hierfür wurde vorab geprüft, welchen Gefährdungen die in den Bausteinen behandelten Sachverhalte üblicherweise ausgesetzt sind und wie den daraus resultierenden Risiken zweckmäßig begegnet werden kann. Anwenderinnen und Anwender des IT-Grundschatz-Profiles benötigen daher in der Regel für den weitaus größten Teil des gewählten Informationsverbundes keine aufwändigen Untersuchungen mehr zur Festlegung erforderlicher Sicherheitsmaßnahmen.

Ein zusätzlicher Analysebedarf besteht lediglich in folgenden drei Fällen:

- Ein Zielobjekt hat einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.
- Es gibt für ein Zielobjekt keinen hinreichend passenden Baustein im IT-Grundschatz-Kompendium.
- Es gibt zwar einen geeigneten Baustein, die Einsatzumgebung des Zielobjekts ist allerdings für den IT-Grundschatz untypisch.

Hinweise zur Durchführung einer Risikoanalyse sind in Abschnitt 13 zu finden.

# 13 Anwendungshinweise

## I. Hinweise zur Schutzbedarfsfeststellung

Bei den hier betrachteten Geschäftsprozessen geht dieses IT-Grundschutz-Profil grundsätzlich von einem Schutzbedarf der Kategorie "normal" aus. Weiterhin soll hiermit insbesondere der Einstieg in den Informationssicherheitsprozess erleichtert werden. Aus diesem Grund werden zunächst, aber auch als absolutes Minimum, die Anforderungen der „Basis-Absicherung“ zur Umsetzung vorgeschlagen.

Eine individuelle Schutzbedarfsfeststellung wird nach der Grundschutzmethode dringend empfohlen. Sofern durch die Schutzbedarfsfeststellung ein „erhöhter Schutzbedarf“ (Kategorie „hoch“ oder „sehr hoch“) für einzelne Zielobjekte definiert wird, reichen die Maßnahmen der Basis- und Standard-Absicherung nicht mehr aus. Ab diesem Zeitpunkt wird die Prüfung der in den Bausteinen aufgeführten Maßnahmen für den erhöhten Schutzbedarf empfohlen.

### Informationen zu den Schutzbedarfskategorien

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich der IT-Grundschutz auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien unterteilt wird:

Schutzbedarfskategorien	
"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Schutzbedarfskategorie "normal"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	<ul style="list-style-type: none"> <li>• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen</li> <li>• Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen</li> </ul>
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> <li>• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.</li> </ul>
3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> <li>• Eine Beeinträchtigung erscheint nicht möglich.</li> </ul>
4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> <li>• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden.</li> <li>• Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.</li> </ul>
5. Negative Innen- oder Außenwirkung	<ul style="list-style-type: none"> <li>• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.</li> </ul>
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> <li>• Der finanzielle Schaden bleibt für die Institution tolerabel.</li> </ul>

**Tabelle 1:** Schutzbedarfskategorie „normal“

Schutzbedarfskategorie "hoch"	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	<ul style="list-style-type: none"> <li>• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen</li> <li>• Vertragsverletzungen mit hohen Konventionalstrafen</li> </ul>
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> <li>• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.</li> </ul>
3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> <li>• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.</li> </ul>
4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> <li>• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt.</li> <li>• Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.</li> </ul>
5. Negative Innen- oder Außenwirkung	<ul style="list-style-type: none"> <li>• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.</li> </ul>
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> <li>• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.</li> </ul>

**Tabelle 2:** Schutzbedarfskategorie „hoch“

Schutzbedarfskategorie "sehr hoch"	
<ul style="list-style-type: none"> <li>• Verstoß gegen Gesetze/ Vorschriften/Verträge</li> </ul>	<ul style="list-style-type: none"> <li>• Fundamentaler Verstoß gegen Vorschriften und Gesetze</li> <li>• Vertragsverletzungen, deren Haftungsschäden ruinös sind</li> </ul>
<ul style="list-style-type: none"> <li>• Beeinträchtigung des informationellen Selbstbestimmungsrechts</li> </ul>	<ul style="list-style-type: none"> <li>• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.</li> </ul>
<ul style="list-style-type: none"> <li>• Beeinträchtigung der persönlichen Unversehrtheit</li> </ul>	<ul style="list-style-type: none"> <li>• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich.</li> <li>• Gefahr für Leib und Leben</li> </ul>
<ul style="list-style-type: none"> <li>• Beeinträchtigung der Aufgabenerfüllung</li> </ul>	<ul style="list-style-type: none"> <li>• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.</li> <li>• Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.</li> </ul>
<ul style="list-style-type: none"> <li>• Negative Innen- oder Außenwirkung</li> </ul>	<ul style="list-style-type: none"> <li>• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.</li> </ul>
<ul style="list-style-type: none"> <li>• Finanzielle Auswirkungen</li> </ul>	<ul style="list-style-type: none"> <li>• Der finanzielle Schaden ist für die Institution existenzbedrohend.</li> </ul>

**Tabelle 3:** Schutzbedarfskategorie „sehr hoch“

## II. Hinweise zur Durchführung einer Risikoanalyse

Das grundlegende Verfahren zur Untersuchung von Sicherheitsgefährdungen und deren Auswirkungen ist eine Risikoanalyse. Der BSI-Standard 200-3: *Risikomanagement* bietet hierfür eine effiziente Methodik. Für das konkrete Vorgehen und eine detaillierte Beschreibung wird an dieser Stelle daher auf den BSI-Standard 200-3 verwiesen. Im Folgenden eine kurze Auflistung der durchzuführenden Schritte einer Risikoanalyse:

- **Zielobjekte zusammenstellen**

Voraussetzung für die Durchführung von Risikoanalysen im Rahmen der Standard-Absicherung ist, dass bei der Strukturanalyse die Zielobjekte des Informationsverbundes zusammengestellt sind, deren Schutzbedarf festgestellt ist und ihnen bei der Modellierung soweit möglich passende IT-Grundschutz-Bausteine zugeordnet wurden. Eine Risikoanalyse ist für solche Zielobjekte durchzuführen, die einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder für die es keinen passenden IT-Grundschutz-Baustein gibt oder die in Einsatzszenarien betrieben werden, die für den IT-Grundschutz untypisch sind.

- **Gefährdungsübersicht anlegen**

Der erste Schritt einer Risikoanalyse ist es, die Risiken zu identifizieren, denen ein Objekt oder ein Sachverhalt ausgesetzt ist. Hierfür ist zunächst zu beschreiben, welchen Gefährdungen das Objekt oder der Sachverhalt unterliegt. Hierzu hat das BSI eine Liste von elementaren Gefährdungen erstellt.

- **Gefährdungsübersicht ergänzen**

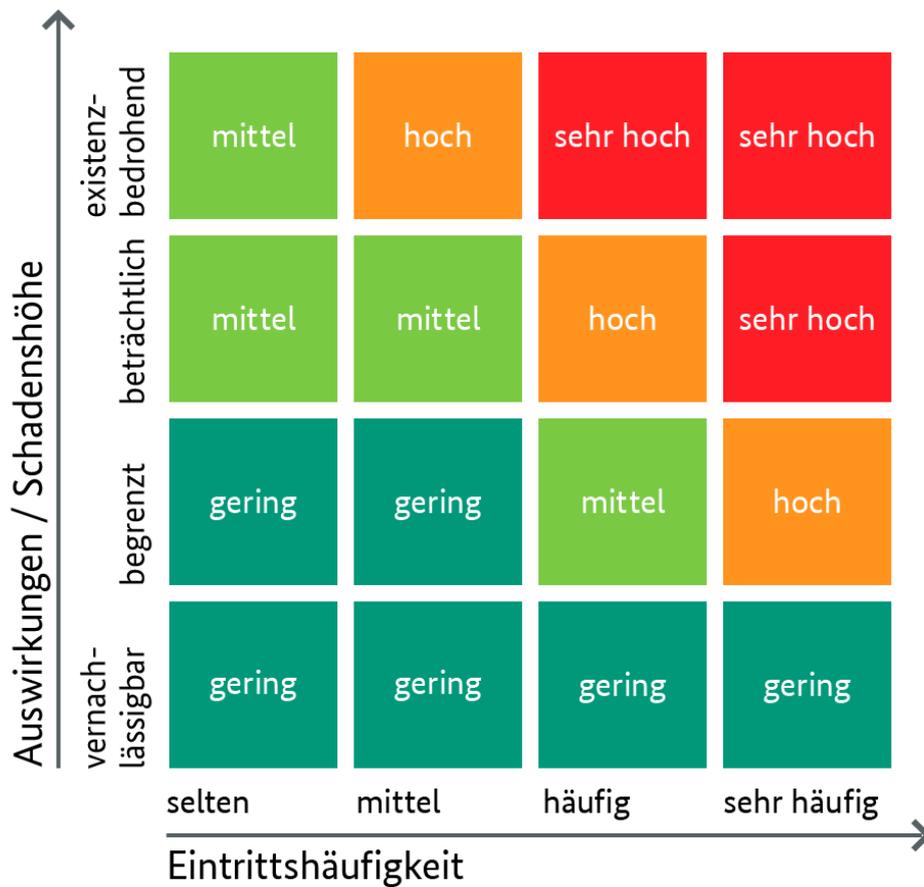
Auch wenn die Zusammenstellung elementarer Gefährdungen vielfältige Bedrohungen berücksichtigt, denen Informationen und Informationstechnik ausgesetzt sind, so kann dennoch nicht ausgeschlossen werden, dass weitere Gefährdungen zu betrachten sind. Dies gilt insbesondere dann, wenn es für ein Zielobjekt keinen geeigneten Baustein gibt oder es in untypischen Einsatzszenarien betrieben wird. Im Anschluss an den ersten Teilschritt prüfen Sie daher, ob neben den relevanten elementaren Gefährdungen weitere Gefährdungen zu untersuchen sind.

- **Häufigkeit und Auswirkungen einschätzen**

Die Höhe eines Risikos ergibt sich aus der Häufigkeit einer Gefährdung und der drohenden Schadenshöhe. Ein Risiko ist umso größer, je häufiger eine Gefährdung ist, umgekehrt sinkt es, je geringer der mögliche Schaden ist. Grundsätzlich können beide Größen sowohl quantitativ, also mit genauen Zahlenwerten, als auch qualitativ, also mit Hilfe von Kategorien zur Beschreibung der Größenordnung, bestimmt werden.

- **Risiken bewerten**

Nachdem Sie die Eintrittshäufigkeiten und Schadensauswirkungen einer Gefährdung eingeschätzt haben, können Sie das aus beiden Faktoren resultierende Risiko bewerten. Es ist auch hierfür zweckmäßig, eine nicht zu große Anzahl an Kategorien zu verwenden – drei bis fünf sind üblich, oft werden auch nur zwei Kategorien verwendet. Der BSI-Standard 200-3 enthält ein Beispiel mit vier Stufen, das Sie an die Gegebenheiten und Erfordernisse Ihrer Institution anpassen können.



- **Risiken behandeln**

In der Regel wird die Gefährdungsbewertung aufzeigen, dass nicht alle Gefährdungen durch das vorhandene Sicherheitskonzept ausreichend abgedeckt sind. In diesem Fall müssen Sie überlegen, wie angemessen mit den verbleibenden Gefährdungen umgegangen werden kann, und eine begründete Entscheidung hierzu treffen.

- **Sicherheitskonzeption konsolidieren**

Als Abschluss der Risikoanalyse sind die zusätzlichen Maßnahmen, deren Umsetzung beschlossen wurde, in das vorhandene Sicherheitskonzept zu integrieren (= Konsolidierung des Sicherheitskonzepts) und darauf aufbauend der Sicherheitsprozess fortzusetzen.

## 14 Anhang

Die Landkarten zu den hier behandelten Geschäftsprozessen:

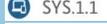
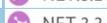
- Order-to-Cash (kaufmännische Auftragsabwicklung) (14.1)
- Produktion (14.2)
- Logistik (14.3).

Anwendungshinweise zu den Landkarten und die Erklärung der verwendeten Symbolik sind im Anhang 14.4 zu finden.

## 14.1 Anhang 1: Landkarte Geschäftsprozess ,Order-to-Cash ‘

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Order-to-Cash	Sales  Finance  Controlling  Planung (Sales-Fokus)	ERP [SAP ERP]  APP.4.2	Telefonanlage !  NET.4.1  NET.4.2	Gebäude (in dem alle Räume sind)  INF.1  INF.3  INF.4  INF.10
		MSEExchange  APP.5.1  APP.5.2	Virtualisierter Server (z.B. ESX, VMWARE) !  SYS.1.1  SYS.1.5	Büro  INF.7
		EDI ** !	Windows Server (z.B. Exchange) !  SYS.1.1  SYS.1.2.2	Serverraum !  INF.2
		Datenbank  APP.4.3	Linux Server (z.B. SAP) *  SYS.1.1  SYS.1.3	Rechenzentrum (Outsourcing)  INF.2  OPS.2.1
		e-Commerce**	Windows 10 Client  SYS.2.1  SYS.2.2.3	Technikraum und Schaltschrank * !
		CRM **	Terminal-Server *  SYS.1.1  SYS.1.2.2	Mobiles Arbeiten  INF.9
		Schnittstellen ** (z.B. Banken, PPS)	Netze (Router, Switches, LAN, WLAN, Firewall) !  NET.1.1  NET.1.2  NET.2.1  NET.2.2  NET.3.1  NET.3.2  NET.3.3	
		Office & E-Mail Client  APP.1.1	Smartphone  SYS.3.2.3  SYS.3.2.1  SYS.3.2.4  SYS.3.3	
		Banking Software **	Tablets  SYS.3.2.3  SYS.3.2.1  SYS.3.2.4  SYS.3.3	
		DMS**	Notebooks  SYS.3.1	
		Office 365 (Cloud) *  OPS.2.2	Multifunktionsgeräte, Drucker, Faxen  SYS.4.1  NET.4.3	
		Reporting (BI) **		
		Mobile Device Management (MDM)  SYS.3.2.2		
		Telefonanlage !  NET.4.2  NET.4.1		
		Browser  APP.1.2		

## 14.2 Anhang 2: Landkarte Geschäftsprozess ‚Produktion‘

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Produktion	<p>Rohstoff- versorgung !</p> <p><u>Energie- versorgung</u> !</p> <p>Entsorgung !</p> <p>Instand- haltung/ Wartung</p> <p>MES/ Prozess- leit system !</p> <p>Qualitäts- leit system</p>	ERP [SAP ERP] 	Windows Server !  SYS.1.1  SYS.1.2.2	Gebäude  INF.1 (in dem alle  INF.3 Räume sind)  INF.4  INF.10
		Personaleinsatzplanung* (Cloud) 	Windows 10 Client !  SYS.2.1  SYS.2.2.3	Technikraum und Schaltschrank ** !
		Schnittstellen ** (z.B. zwischen MES und ERP)	Netze (Router, Switches, LAN, WLAN, Firewall) !  NET.1.1  NET.1.2  NET.2.1  NET.2.2  NET.3.1  NET.3.2  NET.3.3	Büro  INF.7
		Produktionsplanungssoftware (PPS) **	SPS !  IND.2.1  IND.2.2	Serverraum !  INF.2
		MES** !	EWS* !  IND.2.1	Mobiles Arbeiten  INF.9
		QLS**	HMI* !  IND.2.1	Home-Office  INF.8  OPS.1.2.4
		PLS** !	Smartphone/ Tablets etc.  SYS.3.2.3  SYS.3.2.1  SYS.3.2.4  SYS.3.3	
		Environmental System ** !	Maschine* !  IND.2.1  IND.2.4	
		Energiemanagementsystem **	Sensoren* !  IND.2.1  IND.2.3	
		Office-Programme 	SS  IND.2.7 (Safety Instrumented Systems)	

### 14.3 Anhang 3: Landkarte Geschäftsprozess ‚Logistik‘

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Logistik	Lager/ ! automatisiert	ERP [SAP ERP]	Telefonanlage ! 	Gebäude (in dem alle Räume sind)   
		Zoll-Applikation (für Export) **	Virtualisierter Server (z.B. ESX, VMWARE) ! 	
		MSExchange 	Windows Server (z.B. Exchange) ! 	
	Disposition	EDI **	Linux Server (z.B. SAP) * 	Büro
		Datenbank	Windows 10 Client 	Serverraum !
		Schnittstellen (z.B. Spedition-Marktplatz) **	Terminal-Server (z.B. Citrix) ! 	Rechenzentrum (Outsourcing) 
	Zoll- anmeldung	Office-Programme & E-Mail Client	Netze (Router, Switches, LAN, WLAN, Firewall)    	Technikraum und Schaltschrank ** !
		DMS(Archivierung) *		
		Office 365 (Cloud) *		
	(Atlas)	Reporting (BI) **	Smartphone  	Mobiles Arbeiten
		Mobile Device Management (z.B. Staplerterminals) !	Tablets  	
		Lagerverwaltungssystem (LVS) ** !	Notebooks	
	Versand !	Telefonanlage ! 	Multifunktionsgeräte, Drucker, Fax 	Werksgelände **
		Browser	Kiosk-Systeme ** !	
		Yard-Management ** ! (z.B. auch LKW-Self-Service, Waage)	IP-Kameras *	

## 14.4 Anhang 4: Hinweise zur Nutzung

Die „Landkarte“ ist spaltenweise und nicht zeilenweise zu lesen. In Spalte 1 werden die relevanten Geschäftsprozesse benannt. In Spalte 2 werden die Geschäftsprozesse anhand von typischen Aufgaben in diesem Bereich näher beschrieben. Daraus ergeben sich Anwendungen, die für die Erfüllung der Aufgaben benötigt werden (Spalte 3). Diese Anwendungen laufen auf entsprechenden IT-Systemen (Spalte 4), die sich in bestimmten Räumlichkeiten des Betriebes befinden (Spalte 5).

Die **Kennzeichnung mit einem oder zwei Ausrufezeichen** verweist auf eine herausgehobene Priorisierung eines Objekts, welches für die Durchführung der Aufgaben im jeweiligen Geschäftsprozess von besonderer Bedeutung ist. Das könnte zum Beispiel für die Unternehmensleitung ein Hinweis darauf sein, die Anstrengungen zur Sicherung dieses Zielobjekts zu priorisieren:

- keine Kennzeichnung = normale Priorität  
Der Geschäftsprozess bzw. die Fachaufgabe kann mit tolerierbarem Mehraufwand mit anderen Mitteln (z. B. manuell) durchgeführt werden.
- ein Ausrufezeichen = hohe Priorität  
Der Geschäftsprozess bzw. die Fachaufgabe kann nur mit deutlichem Mehraufwand mit anderen Mitteln durchgeführt werden.
- zwei Ausrufezeichen = sehr hohe Priorität  
Der Geschäftsprozess bzw. die Fachaufgabe kann ohne die Anwendung überhaupt nicht durchgeführt werden.

Die **weißen Schilder** bezeichnen die passenden IT-Grundschutz-Bausteine, die auf das jeweilige Zielobjekt anzuwenden sind. Es kommt vor, dass ein Baustein in mehreren Geschäftsprozessen eine Rolle spielt. Bei der Umsetzung der entsprechenden Sicherheitsanforderungen können sich so Synergien ergeben, indem die Maßnahmen, die für einen priorisierten Geschäftsprozess umgesetzt werden, bereits auf andere ausstrahlen und dort wirken.

Die **Markierung mit weißen Sternchen (\*)** an den Anwendungen, IT-Systemen und Räumen zeigt, dass hier weitere Schritte zur Erreichung des angestrebten Sicherheitsniveaus notwendig sind. Im Einzelnen bedeuten die Markierungen:

- kein Kennzeichnung  
Die aufgeführten Bausteine aus dem IT-Grundschutz-Kompendium sind für die Erreichung des angestrebten Sicherheitsniveaus ausreichend.
- ein Stern (\*)  
Die hier aufgeführten Bausteine aus dem IT-Grundschutz-Kompendium sind für die Erreichung des angestrebten Sicherheitsniveaus allein nicht ausreichend. Weitere Anforderungen und Umsetzungshinweise sind individuell zu entwickeln.
- zwei Sterne (\*\*)  
Aktuell liegt im IT-Grundschutz-Kompendium dazu kein Baustein vor. Anforderungen und Umsetzungshinweise sind individuell zu entwickeln. Dies erfordert in der Regel auch eine Risikoanalyse, um die zu treffenden Maßnahmen auf das festgestellte Geschäftsrisiko auszurichten. Informationen hierzu befinden sich im Abschnitt 13.

### Standard-Absicherung für die Energieversorgung:

In der Landkarte zum Geschäftsprozess „Produktion“ (14.2) wurde der Teilprozess „Energieversorgung“ aufgenommen. Die diesem Prozess zugeordneten Zielobjekte sind **unterstrichen** dargestellt. Bei der Bearbeitung dieser Zielobjekte und der anwendbaren Bausteine wird zusätzlich zu den Basis-Anforderungen, die Umsetzung der Standard-Anforderungen empfohlen.