

# **IT-Grundschutz-Profil für Reedereien**

## **Mindest-Absicherung für den Schiffsbetrieb**

## Änderungshistorie

Version	Datum	Name	Beschreibung
0.1		BSI	Anlegen des Working Draft 1.0
0.2		BSI, VHT, afEfa Verwaltungsgesellschaft mbH	Zusammenfassung der Ergebnisse aus den Workshops
1.0	16.01.2020	VHT	Finalisierung

# Inhaltsverzeichnis

1	Vorwort .....	4
2	Einleitung .....	6
3	Formale Aspekte.....	7
4	Haftungsausschluss.....	7
5	Urheberrecht .....	7
6	Liste der Autorinnen und Autoren.....	8
7	Management Summary.....	9
7.1	Zielgruppe .....	9
7.2	Zielsetzung .....	9
7.3	Aufgaben der Leitungsebene .....	9
8	Festlegung des Geltungsbereichs (Scope).....	10
8.1	Zielgruppe .....	10
8.2	Schutzbedarf.....	10
8.3	IT-Grundschutz-Vorgehensweise .....	10
8.4	Abdeckung Vorgehensweise .....	10
8.5	ISO 27001-Kompatibilität .....	10
8.6	Rahmenbedingungen.....	10
8.7	Verpflichtung zur Erfüllung.....	10
9	Abgrenzung des Informationsverbunds .....	11
9.1	Bestandteile des Informationsverbundes.....	11
9.2	Nicht berücksichtigte Objekte .....	11
9.3	Verbindung zu anderen IT-Grundschutz-Profilen .....	11
10	Referenzarchitektur.....	11
10.1	Untersuchungsgegenstand .....	12
10.1.1	Geschäftsprozesse .....	12
10.1.2	Anwendungen .....	12
10.1.3	IT-Systeme .....	13
10.1.4	Netze und Kommunikationsverbindungen .....	14
10.1.5	Räumliche Gegebenheiten / Infrastruktur.....	14
10.2	Umgang mit Abweichungen .....	14
10.3	Netzplan .....	15
11	Zu erfüllende Anforderungen und umzusetzende Maßnahmen .....	15
11.1	Alles auf einen Blick - Arbeitshilfe: „Landkarte“ .....	15
11.2	Übersicht I: Übergeordnete Bausteine .....	17
11.2.1	ISMS.1 Sicherheitsmanagement (R1).....	17
11.2.2	ORP: Organisation und Personal .....	17

11.2.3	CON: Konzeption und Vorgehensweisen .....	17
11.2.4	OPS: Betrieb .....	17
11.2.5	DER: Detektion von Sicherheitsvorfällen und Reaktion bei Vorfällen .....	18
11.2.6	SYS: IT-Systeme .....	18
11.2.7	IND: Industrielle IT.....	18
11.2.8	INF: Infrastruktur.....	18
11.3	Übersicht II: Bausteine aus der Landkarte .....	18
Die in diesem Kapitel aufgelisteten Bausteine finden sich auch in den Landkarten und sind dort einzelnen Zielobjekten zugeordnet.....		
11.3.1	OPS: Betrieb .....	18
11.3.2	APP: Anwendungen.....	18
11.3.3	SYS: IT-Systeme .....	18
11.3.4	NET: Netze und Kommunikation.....	19
11.3.5	IND: Industrielle IT.....	19
11.3.6	INF: Infrastruktur.....	19
12	Restrisikobetrachtung / Risikobehandlung.....	20
13	Anwendungshinweise .....	21
14	Anhang .....	24
14.1	Anhang 1: Landkarte Geschäftsprozess ‚Technischer Betrieb‘ .....	25
14.2	Anhang 2: Landkarte Geschäftsprozess ‚Nautischer Betrieb‘ .....	26
14.3	Anhang 3: Landkarte Geschäftsprozess ‚Ladungsbetrieb‘ .....	27
14.4	Anhang 4: Landkarte Geschäftsprozess ‚Kommunikation‘ .....	28

# 1 Vorwort

„Cybersicherheit fängt nicht an der Pierkante an oder hört da auf“. Mit diesem Eingangssatz begrüßte ich die Teilnehmenden unserer Workshops zum IT-Grundschutz. Damit lag der Fokus gleich zu Beginn auf den Möglichkeiten zur Minimierung von Cyber-Risiken.

Die Workshop-Reihe „Schiffsbetrieb“ starteten wir unverzüglich nach der Fertigstellung des „Landbetriebs“ im Januar 2019. Als Neuerung luden wir - neben den Reedereien und den Schiffmanagement-Firmen auch OEM's<sup>1</sup>) ein, die für die technische Ausstattung und deren (Cyber)Sicherheit auf Schiffe zuständig sind sowie weitere maritimen Dienstleister. Der Gedanke war eine größtmögliche Schnittmenge aus „Mensch“, „Technologie“ und „Prozess“ zu erhalten. Wobei das IT-Grundschutz-Profil „Schiffsbetrieb“ ein Prozess darstellt.

Es sind die Besatzungsmitglieder, die sich das Schiff als Arbeitsplatz und Lebensraum für mehrere Wochen oder Monate mit anderen Seeleuten aus anderen Ländern und Kulturkreisen teilen. Jeder von ihnen hat eine andere Sicht auf Cybersicherheit. Es ist ein Prozess, für die Abwehr von Cyber-Gefahren an Bord zu sorgen, sodass dieser in den täglichen Bordbetrieb übernommen und gelebt wird. Es wird keine einmalige und schon gar nicht leichte Aufgabe sein. Das Grundschutzprofil soll hier eine erste Hilfestellung – ein Rahmenwerk – sein. Jede Reederei kann individuell, passend zu den jeweiligen Bedürfnissen und Budgets auf dieses Grundschutzprofil aufbauen.

Wir freuen uns, dass neben den Reedereien auch maritime Dienstleister sowie verschiedenste Forschungsinstitute an der Entwicklung des Grundschutzprofils „Schiffsbetrieb“ mitwirkten und ihre wertvolle Expertise mit einbrachten.

In besondere Erinnerung bleibt mir die Ausarbeitung der Geschäftsprozesse „Nautik“, „Maschine“, „Ladung“ und „Kommunikation“ welches wir Mitte Juni 2019 in den Räumen des Bundeswirtschaftsministeriums in Bonn unter großer Begeisterung und Beteiligung der Teilnehmenden entwickelten.

Prozesse müssen identifiziert, beschrieben, installiert, gelebt und kontinuierlich weiterentwickelt werden. Dieser Satz lässt sich leicht aufschreiben. Allerdings wurde die Beispielprozesse in den Workshops und Expertenkreise mehrmals hinterfragt, geändert und vereinfacht. Für die Implementierung eines ISMS (Information Security Management System) übernahmen die Workshops unter der Leitung des BSI die Vorarbeit eine Beispiel-Reederei abzubilden. Die weitere Ausarbeitung und Feinarbeit liegen nun in Ihren Händen.

Meiner Meinung nach funktioniert Cybersicherheit nur wenn Mensch – Prozess – Technologie sich im ausgewogen Gleichgewicht befinden. Ein rein blindes Vertrauen nur auf die Technologie ist nicht ratsam.

Mit dem IT-Grundschutz-Profil „Schiffsbetrieb“ wurde eine Möglichkeit geschaffen, die betrieblichen Prozesse zu identifizieren und entsprechende Vorsichtsmaßnahmen zu treffen. Sie als Interessierte und Verantwortliche erhalten ein umsetzbares und kostenloses Tool mit dem Sie sofort arbeiten können. Es wächst mit Ihrer Organisation und Technologie und bietet Ihnen auch weiterhin eine ausgezeichnete Basis, um sich an Bord vor Cyber-Gefahren zu schützen.

Auch in Zukunft werden wir uns als VHT weiter um die CYBER-Belange kümmern.

Uwe Reder, VHT

---

<sup>1</sup> Original Equipment Manufacturer

## **Danksagung**

Mein ganz besonderer Dank gilt den Teilnehmenden, die seit der ersten Stunde an den IT-Grundschutz-Profil Workshops bzw. an den Expertenkreisen teilgenommen haben und sich in Form von Diskussionen und Mitarbeit eingebracht haben und / oder bei Übernahme und deren Bearbeitung von Grundschutzbausteinen mitgewirkt haben.

Auch bedanke ich mich beim Institut für den Schutz maritimer Infrastrukturen, DLR die uns die Räumlichkeiten bei der letzten Veranstaltung im November zur Verfügung gestellt haben.

Uwe Reder, VHT

## 2 Einleitung

Reedereien sind verpflichtet, ihre IT-Systeme und Geschäftsprozesse durch technische und organisatorische Maßnahmen ausreichend abzusichern. Diese Verpflichtungen ergeben sich z. B. aus datenschutzrechtlichen Anforderungen (u. a. EU-Datenschutz-Grundverordnung und Bundesdatenschutzgesetz 2018) und zukünftig aus Anforderungen der International Maritime Organization (IMO). Darüber hinaus sind die erheblichen Investitionen der Reedereien in ihre IT-Ausstattungen über angemessene Sicherheitsvorkehrungen zu schützen. Im Hinblick auf die Grundsätze der Wirtschaftlichkeit umfasst das hier beschriebene Profil die Mindestanforderungen, um hohe materielle und immaterielle Schäden (z. B. Rufschäden bzw. Vertrauensverlust) abzuwenden, die einer Reederei durch den Bruch der Vertraulichkeit, Datenmanipulation oder Nichtverfügbarkeit der IT-Infrastruktur entstehen können.

Im Rahmen seines Engagements in der Allianz für Cyber-Sicherheit, einer Initiative des Bundesamts für Sicherheit in der Informationstechnik (BSI), hat der VHT in Kooperation mit dem BSI einen Prozess initiiert, der es Reedereien erleichtert, ihr Sicherheitskonzept nach IT-Grundschutz auf ihre individuellen Rahmenbedingungen anzupassen. Der IT-Grundschutz des BSI ist eine seit Jahren bewährte Methodik, 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 pauschaliert, so dass es schließlich allen interessierten Reedereien möglich ist, mit Hilfe der Schablone die Informationssicherheit in der eigenen Institution zu erhöhen. Das spart viel Arbeit und Zeit.

Das vorliegende Dokument „IT-Grundschutz-Profil für Reedereien - Mindest-Absicherung für den Schiffsbetrieb“ umfasst ausgehend von vier als relevant betrachteten Geschäftsprozessen 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

1. eine „Landkarte“ als Entscheidungsgrundlage für die Unternehmensleitung und „Umsetzungsfahrplan“ für IT-Fachleute,
2. Empfehlungen für die gezielte Nutzung der umfassenden Anforderungs- und Umsetzungshinweise aus dem IT-Grundschutz des BSI.

### 3 Formale Aspekte

<b>Titel :</b>	IT-Grundschutz-Profil für Reedereien – Mindest-Absicherung für den Schiffsbetrieb
<b>Autorenschaft:</b>	Siehe Punkt 6 „Liste der Autorinnen und Autoren“
<b>Herausgeberschaft:</b>	Verein Hanseatischer Transportversicherer e.V. (VHT)
<b>Versionsstand:</b>	Veröffentlicht am 24.01.2020, Version 1.0 Finalisiert im Januar 2020
<b>IT-Grundschutz-Kompendium</b>	Dieses IT-Grundschutz-Profil basiert auf dem IT-Grundschutz-Kompendium des BSI in der Edition 2019
<b>Revisionszyklus:</b>	Die Aktualität des Dokuments soll alle drei Jahre überprüft werden.
<b>Vertraulichkeit:</b>	Das Dokument in der hier vorliegenden Version ist offen zugänglich. Darüber hinaus wird es eine als vertraulich eingestufte Version geben, die nur Anwenderinnen und Anwendern zugänglich ist, die an der Erstellung der weiteren Version beteiligt waren bzw. sind. Es ist vorgesehen, dass die Einstufung nach TLP (Traffic Light Protocol) „amber“ erfolgt.

### 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 des Workshops „IT-Grundschutz-Profil für Reedereien“. Eine Weitergabe an Dritte ist ausdrücklich erwünscht.



## 6 Liste der Autorinnen und Autoren

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

<b>Name</b>	<b>Organisation</b>
Kersten Gevers	afEfa IT & Beratung GmbH
Leif Oelschläger	BOCS Bremen Overseas Chartering and Shipping GmbH
Jan Schirrmacher	bremenports GmbH & Co. KG
Jan Ruhnau	Bremer Bereederungsgesellschaft mbH & Co. KG
Klemens Kowalski	Bundesanstalt für Landwirtschaft und Ernährung
Martin Tölle	Bundesanstalt für Landwirtschaft und Ernährung
Heiko Zahn	Carl Büttner GmbH
Asmus Hammer	Consist Software Solutions GmbH
Henry Grow	Consist Software Solutions GmbH
Udo Wienstroer	Emder Schlepp-Betrieb GmbH
Silke Angermann	ERGO Versicherung AG
Christian Hemminghaus	Fraunhofer Institut FIKE
Dr. Felix Greve	Hamburg Südamerikanische Dampfschiffahrts-Gesellschaft A/S & Co KG
Frank Steffen	Hamburg Südamerikanische Dampfschiffahrts-Gesellschaft A/S & Co KG
Michael Ippich	Hartmann AG
Julius Vieregge	Howden Group
Christian Fölster	Inmarsat Global Limited
Carl Wrede	Institut für den Schutz maritimer Infrastrukturen, DLR e.V
Darian Sulies	Institut für den Schutz maritimer Infrastrukturen, DLR e.V
Malte Struck	Institut für den Schutz maritimer Infrastrukturen, DLR e.V
Dr. Nils Meyer-Larsen	ISL Institut für Seeverkehrswirtschaft und Logistik
Andreas Held	ITE Solutions GmbH
Thomas Nintemann	Kanzlei Thomas Nintemann
Louis Ravens	Lampe & Schwartz KG
Reinhard Kalkofen	Lampe & Schwartz KG
Steffen Thormann	Mund & Fester GmbH & Co. KG
Stefan Hentschel	NSB Niederelbe Schifffahrtsgesellschaft mbH & Co. KG
Andreas Fehrs	NSC Shipping GmbH & Cie. KG
Philip Timons	NSC Shipping GmbH & Co. KG
Martin Förster	NSSLGlobal GmbH
Anna Hanses	NSSLGlobal GmbH
Benjamin Weltz	PETER DÖHLE Schifffahrts-KG
Wilko C. Bruhn	Raytheon Anschütz GmbH
Philipp Maas	Rhenus Schiffsmanagement GmbH
Dirk Eggers	Sandomeer, Schulte & Partner
Ingo Wenske	SLOMAN NEPTUN Schifffahrts-Aktiengesellschaft
Arne Maskus	Thomas Schulte Ship Management
Christoph Niendorf	Veinland GmbH
Uwe Reder	Verein Hanseatischer Transportversicherer e.V.
Jan Lausch	Wärtsilä SAM Electronics GmbH
Mattias Hamann	Waterway IT Solutions GmbH
Florian zum Felde	Waterway IT Solutions GmbH & Co. KG
Jürgen Berentzen	WESSELS Reederei GmbH & Co. KG

## **7 Management Summary**

### **7.1 Zielgruppe**

Dieses IT-Grundschutz-Profil richtet sich an Reedereien, die die Informationssicherheit im Schiffsbetrieb 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 vier Geschäftsprozesse im Schiffsbetrieb einer Muster-Reederei in den Fokus und empfiehlt entsprechend der Herangehensweise der Standard-Absicherung nach IT-Grundschutz Sicherheitsanforderungen, die zu erfüllen sind. Diese vier Geschäftsprozesse sind:

- Technischer Betrieb
- Nautischer Betrieb
- Ladungsbetrieb
- Kommunikation

Das IT-Grundschutz-Profil hilft beim Einstieg in die Informationssicherheit und der Feststellung der gravierendsten Schwachstellen in diesen Prozessen und gibt darüber hinaus Unterstützung für eine weiterführende Schutzbedarfsfeststellung und Risikoanalyse.

Um einen Mindest-Schutzbedarf des gesamten Reedereibetriebs auf dem Schiff zu definieren, müssen alle übrigen Geschäftsprozesse einer Reederei entsprechend der Vorgehensweise dieses IT-Grundschutz-Profiles aufgenommen werden.

### **7.3 Aufgaben der Leitungsebene**

Die Autorinnen und Autoren empfehlen der Leitungsebene einer Reederei die Anwendung dieses IT-Grundschutz-Profiles als Grundlage für das Informationssicherheitskonzept des Schiffsbetriebs einer Reederei. Allerdings bezieht sich dieses IT-Grundschutz-Profil ausschließlich auf die Geschäftsprozesse ‚Technischer Betrieb‘, ‚Nautischer Betrieb‘, ‚Ladungsbetrieb‘ und ‚Kommunikation‘ und nicht auf die Gesamtorganisation eines Reedereibetriebs. Hierfür müssten alle übrigen relevanten Geschäftsprozesse entsprechend erfasst und dokumentiert werden. Damit ist es dann möglich, den Handlungsbedarf für den Schiffsbetrieb zu ermitteln und entsprechende Schutzmaßnahmen auszuwählen.

Die Autorinnen und Autoren empfehlen, dass Reedereien, 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 Reedereien, die die Informationssicherheit im Schiffsbetrieb sicherstellen wollen.

### **8.2 Schutzbedarf**

Das vorliegende IT-Grundschutz-Profil definiert ein Niveau, das der Standard-Absicherung der IT-Grundschutz Vorgehensweise entspricht und für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen.

Darüber hinaus sind einige Zielobjekte mit erhöhtem Schutzbedarf identifiziert worden, wie z.B. das Steuerungsnetzwerk oder die Brücke. Für diese Zielobjekte sind auf Grundlage der noch im Detail durchzuführenden Risikoanalyse ggf. weitere Sicherheitsmaßnahmen zu ermitteln und umzusetzen.

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

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen sind Empfehlungen für Reedereien zur Umsetzung der Informationssicherheit im Schiffsbetrieb. Sie decken mindestens die Anforderungen der „Standard-Absicherung“ des BSI-Standards 200-2 ab, teilweise müssen außerdem Anforderungen aus dem Bereich des hohen bzw. sehr hohen Schutzbedarfs umgesetzt werden.

### **8.4 Abdeckung Vorgehensweise**

Mit der Anwendung des IT-Grundschutz-Profiles für Reedereien wird mindestens das Standard-Schutzniveau erreicht, teilweise das Schutzniveau ‚hoch‘ bzw. ‚sehr hoch‘.

### **8.5 ISO 27001-Kompatibilität**

Mit der Umsetzung der IT-Grundschutz-Vorgehensweise ‚Standard-Absicherung‘ wird diese kompatibel zu ISO 27001.

### **8.6 Rahmenbedingungen**

Die in diesem IT-Grundschutz-Profil dargestellten Anforderungen hinsichtlich der Informationssicherheit berücksichtigen die Vorgaben der EU-Datenschutz-Grundverordnung (EU-DS-GVO), des Bundesdatenschutzgesetz (BDSG 2018) und zukünftige Anforderungen der International Maritime Organization (IMO).

Dieses IT-Grundschutz-Profil basiert auf dem IT-Grundschutz-Kompendium des BSI in der Edition 2019.

### **8.7 Verpflichtung zur Erfüllung**

Aus den in Punkt 8.6 genannten Vorgaben ergibt sich, dass Reedereien verpflichtet sind, die Informationssicherheit sicherzustellen. Die Sicherstellung der Informationssicherheit kann mit Hilfe des vorliegenden IT-Grundschutz-Profiles durchgeführt werden.

## 9 Abgrenzung des Informationsverbunds

### 9.1 Bestandteile des Informationsverbundes

Zum Informationsverbund des Schiffsbetriebs einer Reederei gehören alle Prozesse, Anwendungen, IT-Systeme und Räumlichkeiten, die für die Abwicklung des Gesamt-Prozesses einer Reederei notwendig sind. Das vorliegende IT-Grundschutz-Profil beschränkt sich auf die Geschäftsprozesse ‚Technischer Betrieb‘, ‚Nautischer Betrieb‘, ‚Ladungsbetrieb‘ sowie ‚Kommunikation‘ und die Betrachtung der damit verbundenen Anwendungen, IT-Systeme und Räumlichkeiten.

### 9.2 Nicht berücksichtigte Objekte

Es werden im vorliegenden IT-Grundschutz-Profil alle übrigen Prozesse, die für die Abwicklung des Gesamt-Prozesses einer Reederei im Schiffsbetrieb notwendig sind, nicht berücksichtigt. Die Autorinnen und Autoren sind davon überzeugt, dass die vier ausgewählten Geschäftsprozesse ‚Technischer Betrieb‘, ‚Nautischer Betrieb‘, ‚Ladungsbetrieb‘ und ‚Kommunikation‘ ausreichend repräsentativ für alle nicht berücksichtigten Geschäftsprozesse sind und dass eine Reederei das vorliegende IT-Grundschutz-Profil sehr gut als Grundlage für die Entwicklung und Fortführung eines individuellen Informationssicherheitsmanagementsystems verwenden kann.

Weiterhin ist die Informationssicherheit an Land (Landbetrieb) der Reederei ausdrücklich nicht berücksichtigt worden. Hierzu wird auf das bereits erstellte **IT-Grundschutz-Profil für Reedereien - Mindest-Absicherung für den Landbetrieb** verwiesen.

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

Für die Absicherung des Landbetriebs einer Reederei wird auf das **IT-Grundschutz-Profil für Reedereien - Mindest-Absicherung für den Landbetrieb** verwiesen.

## 10 Referenzarchitektur

Die Referenzarchitektur (auch ‚Untersuchungsgegenstand‘ genannt) legt fest, auf welche Objekte (Zielobjekte) die Anforderungen des IT-Grundschutzes im Sinne dieses IT-Grundschutz-Profiles 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;
- Räumliche Gegebenheiten / Infrastruktur (Schiffe, Räume).

## 10.1 Untersuchungsgegenstand

### 10.1.1 Geschäftsprozesse

Der **Geschäftsprozess ‚Technischer Betrieb‘** umfasst die Unterprozesse

- Remote-Management
- Fernwartung
- Instandhaltung
- Maintenance predictive
- Monitoring (Performance)
- Betrieb der Hauptmaschine
- Notstromversorgung
- Maschinensteuerung
- Safety + Security
- Umwelt-Systeme (Marpol)
- Ballasten (Gewichtsausgleich)
- Bunkering (Tanken)

Der **Geschäftsprozess ‚Nautischer Betrieb‘** umfasst die Unterprozesse

- Routenplanung
- Voyage Execution
  - Routen-Monitoring
  - Kollisions-Verhütung
  - Reporting
  - Dokumentation
  - Ballast-Wasser Management
- Notfallmanagement
- Administration

Der **Geschäftsprozess ‚Ladungsbetrieb‘** umfasst die Unterprozesse

- Stau-Planung (Stabilität)
- Beladung
- Entladung
- Ladungsfürsorge (Monitoring)
- Kommunikation (Informationsaustausch, Reporting)

Der **Geschäftsprozess ‚Kommunikation‘** umfasst die Unterprozesse

- Querbezüge Technik/Nautik/Ladung
- Private Kommunikation

### 10.1.2 Anwendungen

- Hersteller-Software
- Dienstleister-Software
- Standard-Software
- Office
- E-Mail
- Cloud
- M2M-Software

- ECDIS
- Auto Pilot
- Office Anwendungen
- Bridge Alert Management
- Radar-Software
- Seekarten Korrektursoftware
- GMDSS
- Wetter-Software
- Digitale Publikationen
- Digitales Log.-buch
- Planungssoftware (indiv.)
- Monitoring-Software (Sensorik)
- Fileserver/-dienst (inkl. Automatische Datenübertragung)
- Cloud (inkl. Webhosting)
- Reporting-software
- Fernwartung
- Webbrowser (Business, Privat)
- E-Mail / Groupware (insbesondere Schiff-Land; Crew; Passangers, etc.)
- DNS
- DHCP
- Userverwaltung (AD, Verzeichnisdienst)
- Schnittstellen (z.B. Telex, Telefax zu IT)
- Fileserver/-dienst (inkl. Automatische Datenübergabung)
- Datenbank
- Monitoring-Software (Sensorik)

### **10.1.3 IT-Systeme**

- Steuerungssysteme (z.B. Hauptmaschine, WTS)
- Clients (Windows; Terminal-Server)
- Server (Windows und Linux)
- Telefonie (VOIP, Satellit, SAT-C, Funk, etc.)
- Netzwerk (Router & Switches/LAN/WLAN/VPN/Firewall)
- Steuerungsnetz (OT) Sensorik
- Überwachungssysteme Sensorik (z.B. Brandmeldesystem)
- IOT
- Peripherie, Multifunktionsgeräte
- Mobile Geräte (Tablet, Foto-Kamera)
- GPS
- Voyage Daten Recorder (VDR)
- AIS
- Steuerungsnetz (OT) Sensorik
- ECDIS-PC (auch Multifunktions-Displays, Radar, Conning, etc.)
- Navigations-Systeme (z.B. INS)
- Navigationsnetzwerk Sensoren: Echolot, Kreiselkompass, Magnetkompass, Speedlog und z.B. NMEA-to-Ethernet Wandler
- Mobile Datenträger
- Telefonie (VOIP, Satellit, SAT-C, Funk, etc.)
- WAN (Sat.-Anlage, LTE)
- Peripherie, Multifunktionsgeräte
- Laptop

#### **10.1.4 Netze und Kommunikationsverbindungen**

- Firewall
- Router
- Switches
- LAN
- WLAN
- VPN
- Telefon (VOIP, Satellit, SAT-C, Funk)
- Telefax
- Telex
- Netzwerk

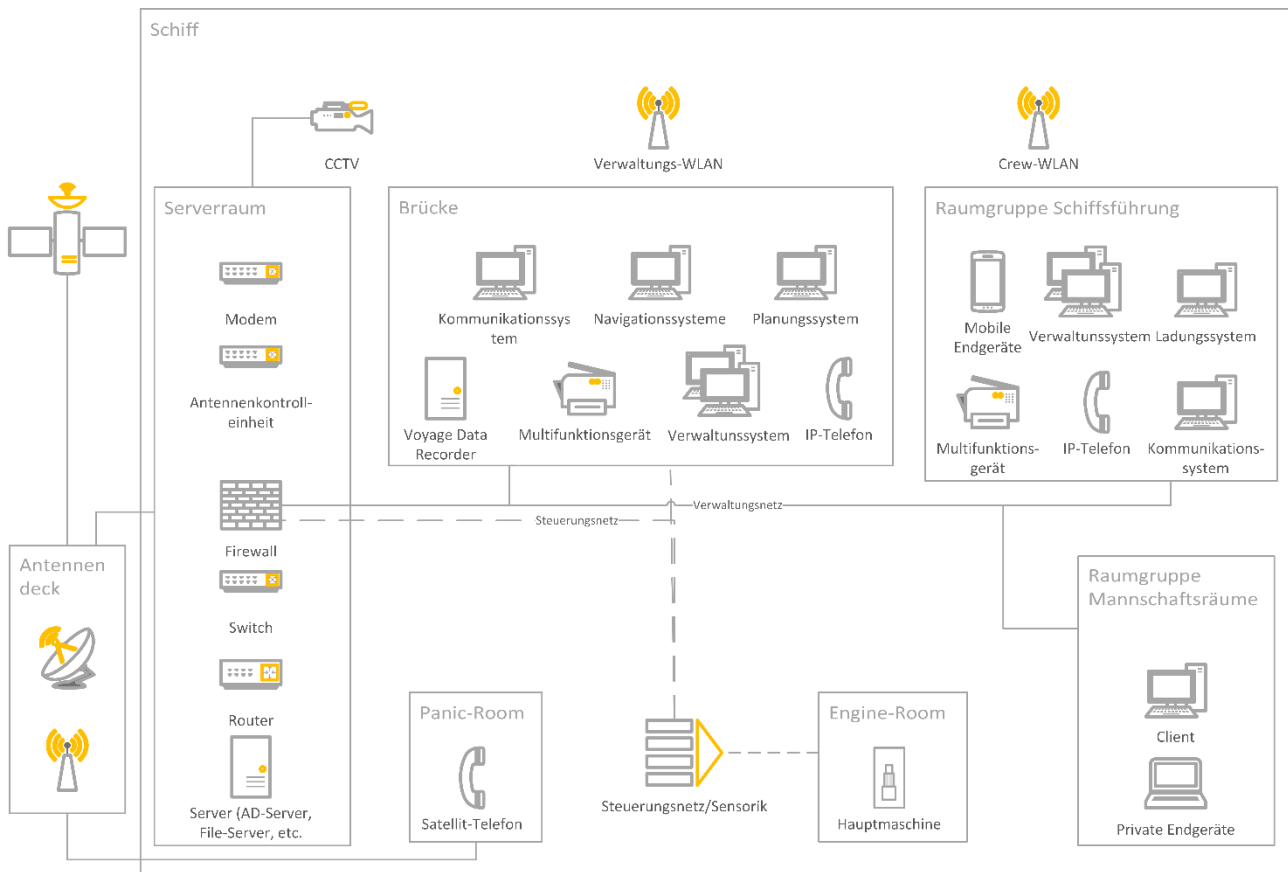
#### **10.1.5 Räumliche Gegebenheiten / Infrastruktur**

- Brücke
- Engine Room
- Schiffsführung (Captains, Cabin, Engine-Control-Room)
- Mannschaftsräume
- Serverraum
- Antennen-Deck
- Panic Room (Zitadelle)
- Schiff

### **10.2 Umgang mit Abweichungen**

Weicht der zu schützende Informationsverbund von der Referenzarchitektur ab, sind die zusätzlichen oder nicht vorhandenen Objekte zu dokumentieren. Diesen sind geeignete Bausteine des IT-Grundschutz-Kompendiums zuzuordnen. Die aus den Bausteinen abgeleiteten Anforderungen müssen in Abhängigkeit des angestrebten Schutzniveaus angepasst werden.

## 10.3 Netzplan



Raumgruppen sind zu verstehen als ähnlich ausgestatte und gleich zu behandelnde Räume.

## 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. 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 Informationen zur Gefährdungslage, die die 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 vier 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 Referenzar-



chitektur (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 branchenspezifische 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 beiden hier behandelten Geschäftsprozessen sind im Anhang zu finden:

- Technischer Betrieb (14.1)
- Nautischer Betrieb (14.2)
- Ladungsbetrieb (14.3)
- Kommunikation (14.4)

**Hinweise zur Nutzung:**

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.

Die Kennzeichnung mit einem oder zwei **Schutzschildern** verweist auf einen besonderen Schutzbedarf. 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" (hier dann keine Kennzeichnung)	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch" (hier dann ein Schutzschild)	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch" (hier dann zwei Schutzschilder)	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

## 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 und müssen ebenfalls umgesetzt werden.

### 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.6 Löschen und Vernichten (R1)

CON.7 Informationssicherheit auf Auslandsreisen (R3)

CON.8 Software-Entwicklung (R3)

CON.9 Informationsaustausch (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.1.2.2 Archivierung (R3)

OPS.1.2.4 Telearbeit (R3)

OPS.1.2.5 Fernwartung (R3)

OPS.2.1 Outsourcing für Kunden (R2)

OPS.2.2 Cloud-Nutzung (R2)

OPS.3.1 Outsourcing für Dienstleister (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.2.3 Bereinigung weitreichender Sicherheitsvorfälle (R2)
- DER.3.1 Audits und Revisionen (R3)
- DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision (R3)
- DER.4 Notfallmanagement (R3)

### **11.2.6 SYS: IT-Systeme**

- SYS.3.2.2 Mobile Device Management (MDM) (R2)

### **11.2.7 IND: Industrielle IT**

- IND.1 Betriebs- und Steuerungstechnik (R2)

### **11.2.8 INF: Infrastruktur**

- INF.9 Mobiler Arbeitsplatz (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 1.2.5 Fernwartung
- OPS.2.2 Cloud-Nutzung

### **11.3.2 APP: Anwendungen**

- APP.1.1 Office-Produkte
- APP.1.2 Web-Browser
- APP.1.4 Mobile Anwendungen (Apps)
- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory
- APP.2.3 OpenLDAP
- APP.3.1 Webanwendungen
- APP.3.2 Webserver
- APP.3.3 Fileserver
- APP.3.4 Samba
- APP.3.6 DNS-Server
- APP.4.3 Relationale Datenbanksysteme
- APP.5.1 Allgemeine Groupware
- APP.5.2 Microsoft Exchange und Outlook

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

- SYS.1.1 Allgemeiner Server
- SYS.1.2.2 Windows Server 2012
- SYS.1.3 Server unter Unix
- SYS.1.5 Virtualisierung
- SYS.1.7 IBM Z-System
- SYS.1.8 Speicherlösungen
- SYS.2.1 Allgemeiner Client
- SYS.2.2.2 Clients unter Windows 8.1
- SYS.2.2.3 Clients unter Windows 10
- SYS.2.3 Clients unter Unix
- SYS.2.4 Clients unter macOS
- SYS.3.1 Laptops

- SYS.3.2.1 Allgemeine Smartphones und Tablets
- SYS.3.2.2 Mobile Device Management (MDM)
- SYS.3.2.3 iOS (for Enterprise)
- SYS.3.2.4 Android
- SYS.3.3 Mobiltelefon
- SYS.3.4 Mobile Datenträger
- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
- SYS.4.4 Allgemeines IoT-Gerät

#### **11.3.4 NET: Netze und Kommunikation**

- NET.1.1 Netzarchitektur und -design
- NET.1.2 Netzmanagement
- NET.2.1 WLAN-Betrieb
- NET.2.2 WLAN-Nutzung
- NET.3.1 Router und Switches
- NET.3.2 Firewall
- NET.3.3 VPN
- NET.4.1 TK-Anlagen
- NET.4.2 VoIP
- NET.4.3 Faxgeräte und Faxserver

#### **11.3.5 IND: Industrielle IT**

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

#### **11.3.6 INF: Infrastruktur**

- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.3 Elektrotechnische Verkabelung
- INF.4 IT-Verkabelung
- INF.6 Datenträgerarchiv
- INF.7 Büroarbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

## 12 Restrisikobetrachtung / Risikobehandlung

Die Basis- und Standard-Anforderungen der IT-Grundschutz-Bausteine wurden so festgelegt, dass dazu passende Maßnahmen für normalen Schutzbedarf und für typische Informationsverbünde 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-Grundschutz-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-Grundschutz-Kompendium.
- Es gibt zwar einen geeigneten Baustein, die Einsatzumgebung des Zielobjekts ist allerdings für den IT-Grundschutz untypisch.

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

## 13 Anwendungshinweise

### I. Hinweise zur Schutzbedarfsfeststellung

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen decken mindestens die Anforderungen der „Standard-Absicherung“ des IT-Grundschutzes ab, ggf. müssen außerdem Anforderungen aus dem Bereich des hohen Schutzbedarfs umgesetzt werden, wenn erhöhter Schutzbedarf festgestellt wurde.

Eine individuelle Schutzbedarfsfeststellung wird nach der Methode des IT-Grundschutzes 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 ist eine Risikoanalyse durchzuführen und ggf. weitere angemessene Maßnahmen zu identifizieren und umzusetzen.

#### 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.

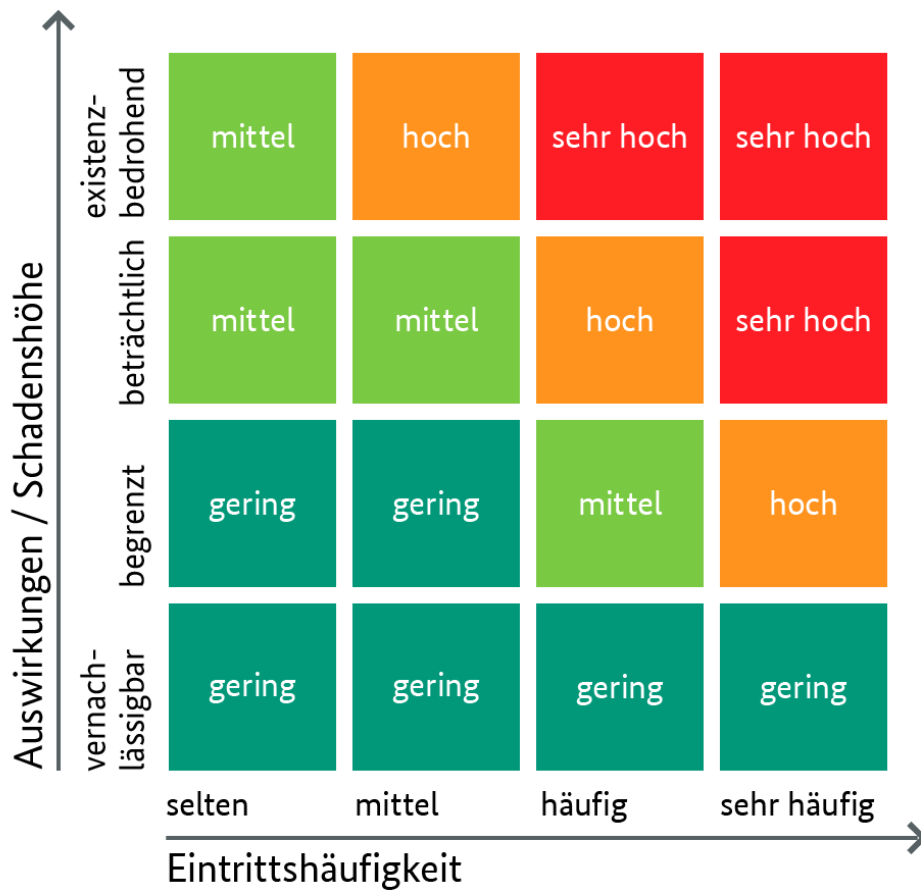
- **Häufigkeit und Auswirkungen einschätzen**

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 beiden hier behandelten Geschäftsprozessen:

- Technischer Betrieb (14.1)
- Nautischer Betrieb (14.2)
- Ladungsbetrieb (14.3)
- Kommunikation (14.4)






















## 14.1 Anhang 1: Landkarte Geschäftsprozess ‚Technischer Betrieb‘

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Technischer Betrieb	Remote-Management	Hersteller-Software  CON.4 (z.B. Water Treatment System, Separator, Maschine) *  CON.5	Steuerungssysteme *  IND.2.1 (z.B. Hauptmaschine, WTS)  IND.2.2  IND.2.3  IND.2.4	Brücke *  INF.2
	Fernwartung	Dienstleistungs-/ Ship Management Software,  CON.4	Clients (Windows)  SYS.2.1	Engine Room *  INF.10
	Instandhaltung	Planned Maintenance Software (PMS), Einkauf *  CON.5	 SYS.2.2.2  SYS.3.1	Schiffsführung * (Captains Cabin, Engine-Control-Room,...)
	Maintenance predictive	Standard-Software *  CON.4	Server *  SYS.1.1  SYS.1.2.2 (Win, Linux, Terminal)  SYS.1.3  SYS.1.5  SYS.1.7  SYS.1.8	
	Monitoring (Performance)	Office Anwendungen  APP.1.1  APP.1.2	Telefonie (VOIP, Satellit, SAT-C, Funk, etc.) *  NET.4.1  NET.4.2  NET.4.3	Mannschafts-Räume  INF.10
	Betrieb der Hauptmaschine	Cloud *  OPS.2.2	Netzwerk (Router&Switches/ LAN/WLAN/ VPN/Firewall)  NET.1.1  NET.1.2  NET.2.1  NET.2.2  NET.3.1  NET.3.2  NET.3.3	Serverraum  INF.2
	Notstromversorgung	M2M-Software **	Steuerungsnetz (OT)  IND.2.1	Antennen-Deck ***
	Maschinensteuerung		Sensorik  IND.2.4  IND.2.3  IND.2.2  IND.2.7	Panic Room ** (Zitadelle)
	Safety + Security		Überwachungssysteme  IND.2.1 Sensorik  IND.2.3 (z.B. Brandmeldesystem)  IND.2.7	Schiff *  INF.1  INF.3  INF.4  INF.9
	Umwelt-Systeme (Marpol)		IoT *  SYS.4.4	
	Ballasten (Gewichtsausgleich)		Peripherie, Multifunktionsgeräte  SYS.4.1	
	Bunkering (Tanken)		Mobile Geräte  SYS.3.2.1  SYS.3.2.2 (Tablet, Foto-Kamera)  SYS.3.2.3  SYS.3.2.4  SYS.3.3  SYS.3.4	























































## 14.2 Anhang 2: Landkarte Geschäftsprozess ‚Nautischer Betrieb‘

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Nautischer Betrieb	Routenplanung  Voyage Execution  Routen-Monitoring  Kollisions-Verhütung  Reporting  Dokumentation  Ballast-Wasser Management  Notfall-management  Administration	ECDIS *  	GPS (empfangende und verarbeitende IT-Systeme) **	Brücke * 
		Auto Pilot *   	Voyage Daten Recorder (VDR) **	Engine Room *
		Office Anwendungen  	AIS * 	
		Bridge Alert Management * 	Steuerungsnetz (OT)  	Schiffsführung  (Captains Cabin, Engine-Control-Room,...)
		Radar-Software **	Sensorik   	
		Seekarten Korrektursoftware * 	ECDIS-PC ** (auch Multifunktions-Displays, Radar, Conning, etc.)	
		GMDSS **	Navigations-Systeme  (z.B. INS) *	Serverraum 
		Wetter-Software **	Navigationsnetzwerk *   	Antennen-Deck **
		Digitale Publikation * 	Sensoren: Echolot, Kreiselkompass, Magnetkompass, Speedlog und z.B. NMEA-to-Ethernet Wandler	
		Digitales Log.-buch * 	Clients (Windows)    	Schiff *    
	Mobile Geräte      			
	Netzwerk (Router&Switches/ LAN/WLAN/ VPN/Firewall)       			

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

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume	
Ladungs- betrieb	Stau-Planung (Stabilität)  Beladung  Entladung  Ladungs- fürsorge (Monitoring)  Kommuni- kations (Informations- austausch, Reporting)	Planungssoftware (indiv.)**  CON.5	APP.1.4 APP.3.1	Mobile Datenträger (Ladungsdaten)  SYS.3.4	Brücke *  INF.2
		Monitoring-Software (Sensorik) *	APP.1.4 APP.3.1 CON.4 CON.5	Kommunikationssystem **  Clients (Windows (Laptop)  SYS.2.1  SYS.2.2.2  SYS.2.2.3  SYS.3.1	Schiffsführung*  INF.6 (Captains Cabin, Engine-Control-Room,...) *
		Fileserver/-dienst (inkl. Automatische Datenübertragung)	APP.3.3 APP.3.4	Server (Win, Linux, Terminal) *  SYS.1.1  SYS.1.2.2  SYS.1.3  SYS.1.5  SYS.1.7  SYS.1.8	
		Office Anwendungen	APP.1.1 APP.1.2	CCTV *  SYS.4.4	
		Cloud	OPS.2.2	Netzwerk (Router&Switches/ LAN/WLAN/ VPN/Firewall)  NET.1.1  NET.1.2  NET.2.1  NET.2.2  NET.3.1  NET.3.2  NET.3.3	Serverraum  INF.2
				Steuerungsnetz (OT) Sensorik  IND.2.1  IND.2.4  IND.2.3  IND.2.2  IND.2.7	Antennen-Deck **
				Mobile Geräte  SYS.3.2.1  SYS.3.2.2 (Tablet, Foto-Kamera)  SYS.3.2.3  SYS.3.2.4  SYS.3.3  SYS.3.4	Schiff *  INF.1  INF.3  INF.4  INF.9
				Peripherie, Multifunktionsgeräte  SYS.4.1	

## 14.4 Anhang 4: Landkarte Geschäftsprozess ‚Kommunikation‘

Geschäftsprozess	Beschreibung GP	Anwendungen (Plattform)	IT-Systeme	Räume
Kommunikation	Querbezüge Technik Nautik/ Ladung  Private Kommunikation	Reporting-Software **	Mobile Datenträger  SYS.3.4	Brücke *  INF.2
		Fernwartung  OPS.1.2.5	Clients (Windows)  SYS.2.1	Engine Room * 
		Webbrowser (Business, Privat)  APP.1.2	(Laptop)  SYS.2.2.2	Schiffsführung * (Captains Cabin, Engine-Control-Room,...)
		E-Mail / Groupware (insbesondere Schiff-Land; Crew, Passangers, ect.)  APP.5.1  APP.5.2	 SYS.2.2.3  SYS.3.1	
		DNS  APP.3.6	Server *  SYS.1.1  SYS.1.2.2	
			(Win, Linux, Terminal)  SYS.1.3  SYS.1.5	
			 SYS.1.7  SYS.1.8	
			Telefonie (VOIP, Satellit, SAT-C, Funk, etc.) *  NET.4.1  NET.4.2  NET.4.3	
		Userverwaltung (AD, Verzeichnisdienst)  APP.2.1  APP.2.2  APP.2.3	Netzwerk (Router&Switches/ LAN/WLAN/ VPN/Firewall)  NET.1.1  NET.1.2  NET.2.1  NET.2.2  NET.3.1  NET.3.2  NET.3.3	Mannschafts- Räume *  INF.10
		Schnittstellen ** (z.B. Telex, Telefax, zu IT)		Serverraum  INF.2
		Fileserver/-dienst (inkl. Automatische Datenübertragung)  APP.3.3  APP.3.4	WAN (Sat.-Anlage, LTE) **	Antennen-Deck **
		Datenbank  APP.4.3	Peripherie, Multifunktionsgeräte  SYS.4.1	Panic Room ** (Zitadelle)
		Monitoring-Software (Sensorik) *  APP.1.4  APP.3.1  CON.4  CON.5	Mobile Geräte  SYS.3.2.1  SYS.3.2.2 (Tablet, Foto-Kamera)  SYS.3.2.3  SYS.3.2.4  SYS.3.3  SYS.3.4	Schiff *  INF.1  INF.3  INF.4  INF.7  INF.9
		Cloud und Webanwendungen  APP.3.2  OPS.2.2		