Verein Hanseatischer Transportversicherer e.V.

IT-Grundschutz-Profil für Reedereien

Mindest-Absicherung für den Landbetrieb

Bremen, 18.12.2018

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	16.10.2018	BSI	Anlegen des Working Draft 1.0
1.0	30.11.2018	BSI, VHT, afEfa Verwaltungsgesellschaft mbH	Zusammenfassung der Ergebnisse aus den Workshops
1.0	18.12.2018	VHT	Finalisierung

Inhaltsverzeichnis

1 Vorwort

Im November 2017 veranstaltete der Verein Hanseatischer Transportversicherer e.V. (VHT) das jährliche Schadenverhütungsseminar für seine Mitglieder und Kunden. Diesmal war das Thema „Cyber-Risiken in der Schifffahrt“. Ganz aktuell, da fünf Monate zuvor der Erpressertrojaner „NotPetya“ auch die maritime Branche getroffen hatte.

Die Resonanz der Teilnehmer war so gut, dass wir uns entschieden, an dem Thema weiter anzuknüpfen. Bei den Recherchen wurde schnell klar, dass es zwar eine Fülle von Anbietern zum Cyberschutz gibt, jedoch keine maßgeschneiderte Absicherung speziell für Reeder und Schiffe - allenfalls Insellösungen.

Wir stießen bei der Suche unweigerlich auf das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn, schilderten ihnen unsere Ideen sowie Vorhaben und konnten bereits nach vier Monaten mit der Zusammenarbeit in Form eines Kick-off-Workshops beginnen.

Während der ersten Veranstaltung wurde dann die Entscheidung getroffen, sich zunächst mit der Absicherung des Landbetriebes zu beschäftigen. Die Erarbeitung der Absicherung des Schiffsbetriebes wird in einer weiteren Workshop-Reihe ab Januar 2019 angeboten.

In nur drei Treffen haben wir zusammen das „IT-Grundschutz-Profil für Reedereien. Mindest-Absicherung für den Landbetrieb“ (kurz: Grundschutz-Profil für Reedereien – Landbetrieb) erstellt.

Mit dem Grundschutz-Profil für Reedereien – Landbetrieb halten Sie ein nützliches Werkzeug in Ihren Händen, das nicht nur ihre Cyber-Sicherheit verbessert, sondern auch in großen Teilen die Anforderungen aus dem Datenschutz (BDSG sowie DSGVO) und der ISO-Zertifizierung 9001 mit abdeckt.

Bedenken Sie, dass nach Verlautbarung der IMO bis zum 1. Januar 2021 ein solches Konzept zur Cybersicherheit vorliegen muss!

Wir als VHT möchten Sie zusammen mit dem BSI dabei weiter unterstützen und laden Sie, als Reederei zur nächsten kostenlosen Workshop-Reihe „Grundschutz-Profil für Reederei – Schiff“ ein.

Danksagung

An dieser Stelle möchte ich mich bei allen Beteiligten bedanken. Besonders bei Frau Frauke Greven und Herrn Birger Klein vom BSI, die sich sehr schnell in die Besonderheiten der Schifffahrt eingefunden haben und uns mit viel Spaß und Freunde zum Ziel geführt haben.

Auch möchte ich mich bei Herrn Kersten Gevers von der Firma afEfa Verwaltungsgesellschaft mbH bedanken, der nach den Seminaren die entsprechenden Etappen zusammengefasst und aufgearbeitet hat.

Last but not least möchte ich meinen Dank an meine Kollegin Frau Birte Stützle aussprechen, die sich um die Organisation und Catering kümmerte und für die Teilnehmer eine angenehme Arbeitsatmosphäre geschaffen hat.

Herzlichen Dank Ihnen allen!

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 Landbetrieb“ umfasst ausgehend von zwei 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 „Umsetzungs-Fahrplan“ für IT-Fachleute,

2. Empfehlungen für die gezielte Nutzung der umfassenden Anforderungs- und Umsetzungshinweise aus dem IT-Grundschutz des BSI.

3 Formale Aspekte

Titel :	IT-Grundschutz-Profil für Reedereien – Mindest-Absicherung für den Landbetrieb
Autorenschaft:	Siehe Punkt 5 „Liste der Autorinnen und Autoren“
Herausgeberschaft:	Verein Hanseatischer Transportversicherer e.V. (VHT)
Registrierungsnummer:	Wird nach erfolgreichem Durchlaufen des Registrierungsverfahrens vom BSI vergeben
Versionsstand:	Veröffentlicht am 18.12.2018, Version 1.0, finalisiert im Dezember 2018
Revisionszyklus:	Die Aktualität des Dokuments soll alle drei Jahre überprüft werden.
Vertraulichkeit:	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 Mitwirkenden an diesem Dokument haben keinen Einfluss auf dessen weitere Nutzung durch die einzelnen Anwender und können daher naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen.

5 Urheberrecht

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.

Name	**Organisation**
Silke Angermann	ERGO Versicherung AG
Eckhard Bartkowski	SLOMAN NEPTUN Schiffahrts-Aktiengesellschaft
Jürgen Berentzen	WESSELS Reederei GmbH & Co. KG
Wilko Cramer	Aktiengesellschaft Reederei Norden-Frisia
Kpt. Peter Dopp	Navo Mare GmbH & Co. KG
Dipl. Ing. Kersten Gevers	afEfa Verwaltungsgesellschaft mbH
Torsten Gevers	Reederei Gerdes Gruppe
Andreas Held	RIGEL Schiffahrts GmbH & Co. KG
Louis Ravens	Lampe & Schwartze KG
Uwe Reder	Verein Hanseatischer Transportversicherer e.V.
Jan Ruhnau	Bremer Bereederungsgesellschaft mbH & Co. KG
Mathias Waack	DAL Deutsche Afrika-Linien GmbH & Co. KG; John T. Essberger GmbH & Co. KG
Udo Wienstroer	EMDER SCHLEPP-BETRIEB GMBH

7 Management Summary

7.1 Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an Reedereien, die die Informationssicherheit im Landbetrieb 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 definiert einen Mindest-Schutzbedarf im Reedereibetrieb an Land in den Geschäftsprozessen ‚Accounting‘ und ‚Technisches Management‘. Das 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 an Land zu definieren, müssen alle übrigen Geschäftsprozesse einer Reederei entsprechend der Vorgehensweise dieses IT-Grundschutz-Profils aufgenommen werden.

7.3 Aufgaben der Leitungsebene

Die Autorinnen und Autoren empfehlen der Leitungsebene einer Reederei die Anwendung dieses Profils als Grundlage für das Informationssicherheitskonzept des Landbetriebs einer Reederei. Allerdings bezieht sich dieses IT-Grundschutz-Profil ausschließlich auf die Geschäftsprozesse ‚Accounting' und ‚Technisches Management' und nicht auf die Gesamtorganisation eines Reedereibetriebs. Hierfür müssten alle übrigen relevanten Geschäftsprozesse entsprechend erfasst und dokumentiert werden. Damit ist es dann möglich, den Mindest-Schutzbedarf des Landbetriebs 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 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 Landbetrieb sicherstellen wollen.

8.2 Schutzbedarf

Das vorliegende IT-Grundschutz-Profil definiert ein Schutzniveau, das in Teilen über der Standard-Absicherung der IT-Grundschutz-Vorgehensweise liegt.

Im Rahmen des Geschäfts-Prozesses ‚Accounting' werden in der Regel große Mengen an personenbezogenen Daten verarbeitet, auf deren Vertraulichkeit hoher Wert gelegt wird. Darüber hinaus besteht meist ein erhöhter Schutzbedarf hinsichtlich der Verfügbarkeit der angebotenen Services. Daher ist für diese Bereiche ein Schutzbedarf von „hoch" bezüglich Vertraulichkeit und Integrität anzunehmen.

Im Rahmen des Geschäfts-Prozesses ‚Technisches Management' werden in der Regel sehr große Mengen an technischen, essentiell notwendigen Daten übermittelt, erfasst und verarbeitet. Hier besteht ein sehr hoher Schutzbedarf hinsichtlich der Implementierung des Bausteines „PMS-Software". Der Geschäftsprozess „PMS vorbeugende Wartung" kann – je nach Stand der im Unternehmen angewandten Informationstechnik - ohne Verfügbarkeit der Anwendung und/oder der Daten zu einer gravierende Beeinträchtigung der Aufgabenerfüllung führen sowie durch den Verlust der Integrität Existenzbedrohende Schäden verursachen.

Diese Schutzbedarfsfeststellungen sind bei der Anwendung des IT-Grundschutz-Profils zu berücksichtigen.

8.3 IT-Grundschutz-Vorgehensweise

Die in diesem IT-Grundschutz-Profil aufgeführten Anforderungen sind Empfehlungen für Reedereien zur Umsetzung der Informationssicherheit im Landbetrieb. 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-Profils für Reedereien wird für die IT-Infrastruktur und die angesprochenen Geschäftsprozesse mindestens das Standard-Schutzniveau und teilweise das Schutzniveau ‚hoch' bzw. ‚sehr hoch' erreicht.

8.5 ISO 27001-Kompatibilität

Mit der Umsetzung der IT-Grundschutz-Vorgehensweise ‚Standardabsicherung' wird diese kompatibel zu ISO 27001.

8.6 Rahmenbedingungen

Die in diesem 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).

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-Profils durchgeführt werden.

9 Abgrenzung des Informationsverbunds

9.1 Bestandteile des Informationsverbundes

Zum Informationsverbund des Landbetriebs 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 ‚Accouting' und ‚Technisches Management' 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 Landbetrieb notwendig sind, nicht berücksichtigt. Die Autorinnen und Autoren sind davon überzeugt, dass die beiden ausgewählten Geschäftsprozesse ‚Accouting' und ‚Technisches Management' 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. Im Rahmen der Strukturanalyse wurden neben den beiden o. g. Geschäftsprozessen im Wesentlichen die folgenden betrieblichen Anwendungsgebiete erfasst: Befrachtung, Operations, Human Recources, QHSE(Abkürzung für 'Quality, Health, Safety and Environment' (englisch) oder 'Qualität, Gesund-heit, Sicherheit, Umwelt' (deutsch)), Versicherungsmanagement, Schnittstellen-Kommunikation, Einkauf und Marketing.

Weiterhin ist die Informationssicherheit an Bord eines von der Reederei verwalteten Schiffes ausdrücklich nicht berücksichtigt worden. Die Autorinnen und Autoren sind der Meinung, dass die Informationssicherheit an Bord eines Schiffes Gegenstand eines separaten IT-Grundschutz-Profils sein sollte. Bei der Erstellung eines solchen Profils muss beachtet werden, dass die Prozesse, Anwendungen, IT-Systeme und Räumlichkeiten an Bord eines Seeschiffs weitestgehend durch internationale Bestimmungen (z.B. Baumustervorschriften, Ausrüstungsvorschriften) abgedeckt sind.

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;
- Räumliche Gegebenheiten / Infrastruktur (Liegenschaften, Gebäude, Räume).

10.1 Untersuchungsgegenstand

10.1.1 Geschäftsprozesse

Der **Geschäftsprozess ‚Accounting'** umfasst die Unterprozesse

- Accounting Land (Reederei);
- Accounting See (Schiffsgesellschaft);
- Accounting Crew / Landpersonal (Schiffsleitung / Personaldienstleister);
- Organisation Zahlungsprozesse;
- Zahlungsverkehr;
- Reporting;
- Buchhaltung / Steuern / Wirtschaftsprüfung.

Der **Geschäftsprozess 'Technisches Management'** umfasst die Unterprozesse

- Planung /Durchführung Klasse-Erneuerung und Werftaufenthalt;
- Schiffsinspektionen / -besuche;
- Mängelbehebung;
- Wartung / Planned Maintenance;
- Organisation Reparaturen und Service.

10.1.2 Anwendungen

- APP.1.1 Office-Produkte
- APP.1.2 Web-Browser
- APP.3.3 Fileserver
- APP.5.2 Microsoft Exchange und Outlook

10.1.3 IT-Systeme

- SYS.1.1 Allgemeiner Server
- SYS.1.5 Virtualisierung
- SYS.1.8 Speicherlösungen
- SYS.2.1 Allgemeiner Client
- SYS.3.1 Laptops
- SYS.3.2.1 Allgemeine Smartphones und Tablets
- SYS.3.2.2 Mobile Device Management (MDM)
- SYS.3.4 Mobile Datenträger
- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

10.1.4 Netze und Kommunikationsverbindungen

- NET.1.1 Netzarchitektur und -design
- NET.1.2 Netzmanagement
- NET.2.1 WLAN-Betrieb
- NET.3.1 Router und Switches
- NET.3.2 Firewall
- NET.3.3 VPN

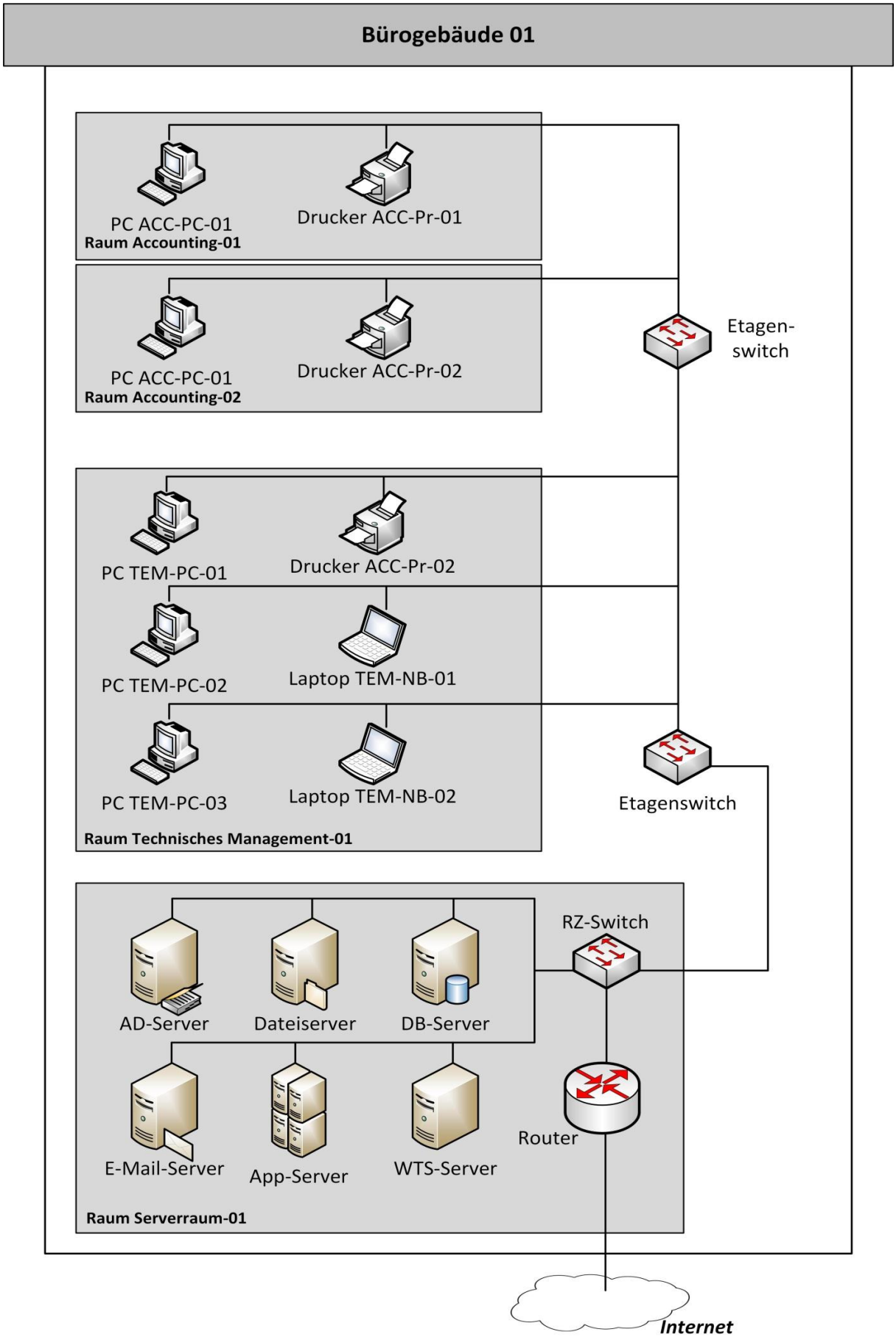
10.1.5 Räumliche Gegebenheiten / Infrastruktur

- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.3 Elektrotechnische Verkabelung
- INF.4 IT-Verkabelung
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz

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



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-Profils 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“

Die „Landkarte“ zeigt eine Übersicht zu allen wesentlichen Erkenntnissen aus der Strukturanalyse sowie der Modellierung (Auswahl passender IT-Grundschutz-Bausteine) – ausgehend von jeweils einem "wichtigen" Geschäftsprozess die Referenzarchitektur (Anwendungen, IT-Systeme sowie Räumlichkeiten), den jeweiligen Schutzbedarf und die Zuordnung der IT-Grundschutz-Bausteine inkl. Empfehlungen zur Umsetzungsreihenfolge. Wo keine Zuordnung bestehender Bausteine erfolgen kann, wird deutlich, dass eine eigene Risiko-Analyse und ggf. unternehmens- und/oder branchen-spezifische Lösungen notwendig sind.

Die Grafiken bieten quasi „Alles auf einen Blick“ und eröffnen so einen Einstieg in den individuellen IT-Sicherheitsprozess. Sie kann 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:

- Geschäftsprozess ‚Accounting‘ (14.1)
- Geschäftsprozess ‚Technisches Management‘ (14.2).

Hinweise zur Nutzung:
Die „Landkarte“ ist spaltenweise und nicht zeilenweise zu lesen. In Spalte 1 werden die relevanten Geschäftsprozesse für Reedereien 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 **Symbole „!“ bzw. „!!“** machen kenntlich, dass dieses Objekt 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:

- ➔ kein Ausrufezeichen = normal - Der Geschäftsprozess bzw. die Fachaufgabe kann mit tolerierbarem Mehraufwand mit anderen Mitteln (z. B. manuell) durchgeführt werden.
- ➔ ein Ausrufezeichen (!) = hoch - Der Geschäftsprozess bzw. die Fachaufgabe kann nur mit deutlichem Mehraufwand mit anderen Mitteln durchgeführt werden.
- ➔ zwei Ausrufezeichen (!!) = sehr hoch - Der Geschäftsprozess bzw. die Fachaufgabe kann ohne die Anwendung überhaupt nicht durchgeführt werden.

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.

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 Sicherheitsniveau notwendig sind. Im Einzelnen bedeuten die Markierungen:

***** 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.

****** Aktuell liegt im IT-Grundschutz-Kompendium dazu kein Baustein vor. Anforderungen und Umsetzungshinweise sind individuell zu entwickeln.

Anwendungen, IT-Systeme und Räume ohne eine Markierung mit einem Stern bedeutet, dass die in der Landkarte aufgeführten Bausteine aus dem IT-Grundschutz-Kompendium sind für die Erreichung des angestrebten Sicherheitsniveaus ausreichend.

11.2 Übersicht I: Allgemeine Bausteine (für das Unternehmen insgesamt von Relevanz)

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
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, wenn IT von Reederei eigenständig administriert wird)
OPS.1.1.3 Patch- und Änderungsmanagement (R1)
OPS.1.1.4 Schutz vor Schadprogrammen (R1)
OPS.1.1.5 Protokollierung (R1)
OPS.2.2 Cloud-Nutzung
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)

11.3 Übersicht II: Geschäftsrelevante Bausteine

11.3.1 OPS: Betrieb

OPS.1.2.4 Telearbeit (R3)
[OPS.3.1 Outsourcing für Dienstleister (bei Ship-Management im Auftrag) (R3)]

11.3.2 APP: Anwendungen

APP.1.1 Office-Produkte (R2)
APP.1.2 Web-Browser (R2)
APP.1.4 Mobile Anwendungen (Apps)
APP.3.1 Web-Anwendungen (R2)

APP.3.3 Fileserver (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
SYS.1.5 Virtualisierung (R2)
SYS.1.8 Speicherlösungen (R2)
SYS.2.1 Allgemeiner Client (R2)
SYS.2.2.2 Clients unter Windows 8.1
SYS.2.2.3 Clients unter Windows 10
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)
SYS.3.2.4 Android
SYS.3.3 Mobiltelefon
SYS.3.3 Mobiltelefon
SYS.3.4 Mobile Datenträger (R2)
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte (R2)
SYS.4.4 Allgemeines IoT-Gerät

11.3.4 NET: Netze und Kommunikation

NET.1.1 Netzarchitektur und -design (R2)
NET.1.2 Netzmanagement (R2)
NET.2.1 WLAN-Betrieb (R2)
NET.3.1 Router und Switches (R2)
NET.3.2 Firewall (R2)
NET.3.3 VPN (R2)
NET.4.1 TK-Anlagen
NET.4.2 VOIP
NET.4.3 Fax

11.3.5 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.8 Häuslicher Arbeitsplatz (R2)
INF.9 Mobiler Arbeitsplatz (R2)

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-Profils 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 BSI-Standards 200-2 ab, ggf. müssen außerdem Anforderungen aus dem Bereich des hohen Schutzbedarfs umgesetzt werden.
Bei den zugrundeliegenden Geschäftsprozessen ist grundsätzlich von einem Sicherheitsniveau der Stufe "normal" auszugehen, eine individuelle Schutzbedarfsfeststellung wird dringend 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	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Tabelle 1: Schutzbedarfskategorie „normal“

Schutzbedarfskategorie "hoch"	
1. Verstoß gegen Gesetze/Vorschriften/ Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Tabelle 2: Schutzbedarfskategorie „hoch“

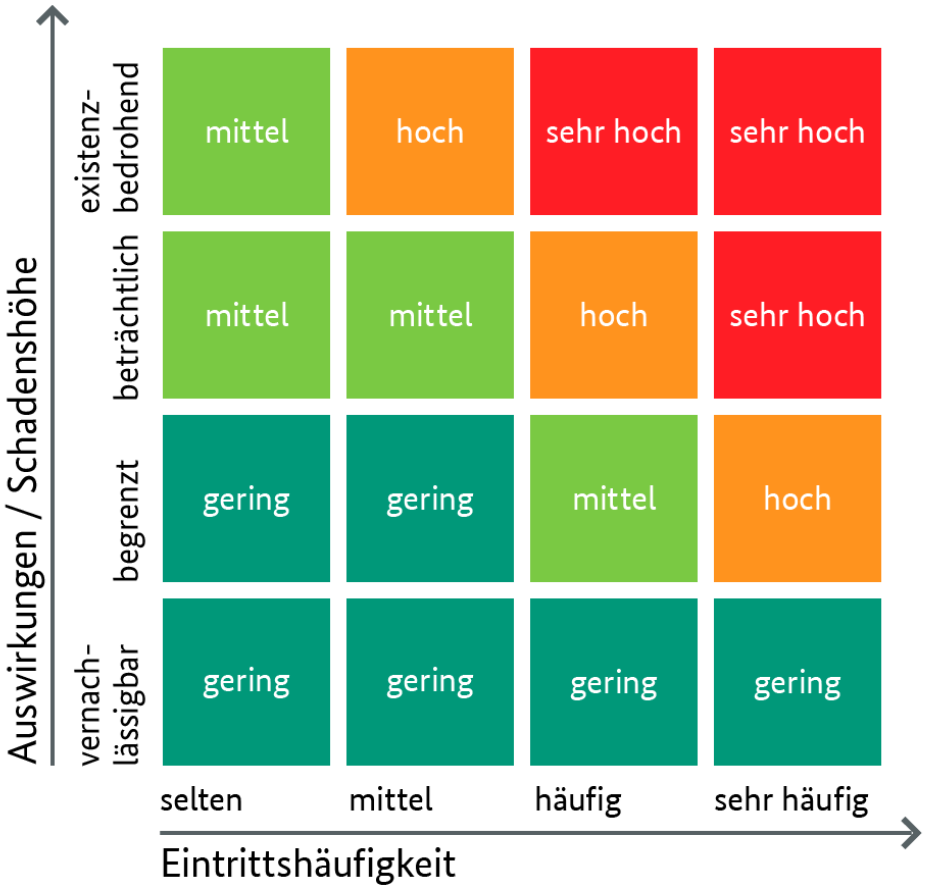
Schutzbedarfskategorie "sehr hoch"	
• Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
• Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
• Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
• Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
• Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
• Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

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, dass Sie an die Gegebenheiten und Erfordernisse Ihrer Institution anpassen können.



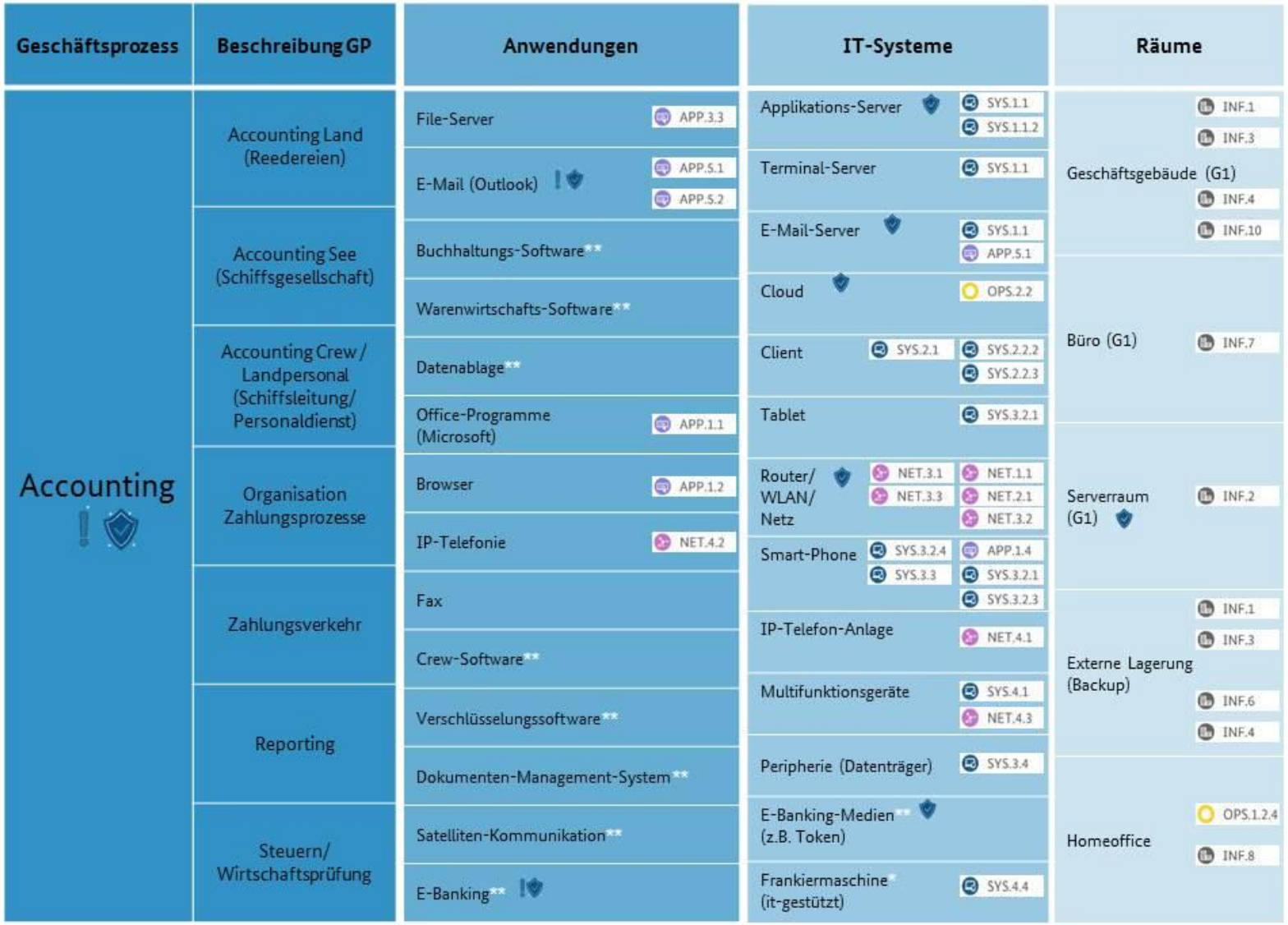
- **Risiken behandeln**
  In der Regel wird die Gefährdungsbewertung aufzeigen, dass nicht alle Gefährdungen durch das vorhandene Sicherheitskonzept ausreichend abgedeckt sind. In diesem Fall müssen Sie überlegen, wie angemessen mit den verbleibenden Gefährdungen umgegangen werden kann, und eine begründete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

- Geschäftsprozess ‚Accounting' (14.1)
- Geschäftsprozess ‚Technisches Management' (14.2).

14.1 Anhang 1: Grafik Geschäftsprozess ‚Accounting'



14.2 Anhang 2: Grafik Geschäftsprozess ‚Technisches Management'