Mindestanforderungen an das Incident Management in KMUs

Stefan Großmann

Hochschule Furtwangen
stefan.grossmann@hs-furtwangen.de

SSRM GbR
stefan.grossmann@ssrm-konzepte.de

Zusammenfassung

Aufgrund der Vielzahl größerer vorhandener Standards und Regelwerke, die im Bereich der Informationssicherheit ein Incident Management fordern, ist es für klein- und mittelständische Unternehmen schwierig, ein Incident Management umzusetzen ohne die Standards und Regelwerke vollständig anwenden zu müssen. Dieser Beitrag soll KMUs, die ein Incident Management umsetzen wollen, eine Hilfestellung durch Mindestanforderungen geben. Dazu werden diese KMUs zusätzlich in ihre IT-Affinität unterteilt. Der folgende Vergleich der Maßnahmen aus den Standards und Regelwerken und eine anschließende Definition von umzusetzenden Mindestanforderungen, für die so unterteilten KMUs, bilden den Kern des Beitrages. Diese Mindestanforderungen werden zudem in einem Prozessschaubild dargestellt, das sich an einem Beispielprozess zum ISIM orientiert. Dabei liegt die Spanne von umzusetzenden Mindestanforderungen zwischen 4 bis 22 Maßnahmen.

1 Einleitung

Die zunehmende Digitalisierung und die damit zusammenhängende Abhängigkeit von IT-Systemen sorgt dafür, dass Sicherheitsvorfälle[1] (engl. Incidents) für Unternehmen immer kritischer werden [WoSa14]. Dieses gilt uneingeschränkt für alle Organisationen und somit auch für kleine und mittelständische Unternehmen (KMUs), denn auch in dieser Gruppe von Unternehmen sind Geschäftsprozesse häufig von der IT abhängig.

Wenn Informationstechnologie (IT) aufgrund eines Information Security Incidents ausfällt, können Geschäftsprozesse innerhalb der KMUs betroffen sein und zum Stillstand gebracht werden. Insbesondere wenn Kernprozesse eines Unternehmens von einem Incident betroffen sind, besteht die Wahrscheinlichkeit einer nachhaltigen Schädigung des Unternehmens.

Um zu verhindern, dass Information Security Incidents zu einem Geschäftsausfall führen, sollte jedes Unternehmen über die Einrichtung eines Incident Managements zumindest nachdenken, denn ein korrekt implementiertes Incident Management verringert die Wahrscheinlichkeit einer nachhaltigen Schädigung erheblich.

[1] Innerhalb des Projektes wurde der Begriff „Sicherheitsvorfall“ als „Informationssicherheits-Vorfall“ definiert (engl.: information security incident)

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 140-149.

Bei der Einführung eines systematischen Incident Management Prozesses können Unternehmen auf eine Vielzahl von Regelwerken und Normen zurückgreifen [ISO11, DIN14, DIN15, DIN11, BeZi15, ISAC12b, BSI14]. Jedoch sind viele dieser Regelwerke eher umfangreich und auf die Bedürfnisse größerer Unternehmen ausgelegt. Die hohen Kosten zur Umsetzung etablierter Informationssicherheitsstandards und auch das dazu notwendige Know-How wirken auf KMUs meistens abschreckend [BMWi12]. Daher können diese es sich in den meisten Fällen nicht leisten, Zeit und Geld in die Abarbeitung dieser Regelungen zu investieren und besitzen nur selten eigene Ansprechpartner, die diese Aufgabe übernehmen können.

Um KMUs einen Weg zur Einrichtung eines Information Security Incident Managements aufzeigen zu können, wurde im Rahmen des vorgestellten Projektes ein Vergleich etablierter Standards und Regelwerke durchgeführt. Bei diesem Vergleich wurden Gemeinsamkeiten und Unterschiede zwischen den Standards und Regelwerken entwickelt und ein Maßnahmenkatalog mit Mindestanforderungen herausgearbeitet.

Ziel des Vergleichs war die Erstellung eines vereinheitlichten ISIM[2], das auf die Unternehmensbedürfnisse (insbes. Unternehmensgröße und IT-Affinität von KMUs) angepasst werden kann.

Der folgende Text ist wie folgt gegliedert: Im zweiten Abschnitt werden die Einteilung von KMUs gemäß der Unternehmensgröße und der IT-Affinität und im dritten Abschnitt die verwendeten Standards und Regelwerke vorgestellt. Im vierten Abschnitt werden die Ziele und Maßnahmen und im fünften Abschnitt das Information Security Incident Management als Prozess dargestellt. Der sechste Abschnitt zeigt einen Maßnahmenkatalog und der letzte Abschnitt fasst die Resultate kurz zusammen und gibt einen Ausblick.

2 Einteilung von KMUs

Mit einer einfachen Einteilung der KMUs nach Beschäftigtenanzahl oder Umsatz, wie sie von der EU-Kommission oder dem Institut für Mittelstandsforschung Bonn vorgenommen wird, ist eine Definition von Mindestanforderungen für das Incident Management schwer realisierbar. Diese Einteilung trifft keine Aussage zu der Menge an verwendeter IT in den jeweiligen Unternehmen. Mit dieser Einteilung kann eine Schreinerei mit einem Trading-Unternehmen verglichen werden, solange diese eine ähnliche Anzahl an Mitarbeitern und einen ähnlichen Umsatz haben. Das Trading-Unternehmen wäre allerdings bei einem Ausfall ihrer IT durch einen Incident ungleich stärker betroffen als die Schreinerei. Daher musste zu der einfachen Unterteilung der KMUs in ihre Größen eine weitere Unterteilung vorgenommen werden.

Die Einteilung der KMUs wurde einerseits nach der Vorgabe der EU Kommission [Euro03] sowie einer selbst definierten Einheit der „IT-Affinität“ vorgenommen. Die IT-Affinität beschreibt den Anteil der kritischen Geschäftsprozesse, die von der IT abhängig sind. Mit dieser zusätzlichen Einteilung wird eine Zuordnung einzelner Incident Management Teilprozesse zu den jeweiligen Bereichen der KMUs ermöglicht. Tabelle 1 zeigt die Einteilung der Unternehmensgrößen nach Vorgabe der EU Kommission.

[2] Information Security Incident Management

Tab. 1: Unternehmensgrößen nach EU Kommission [Euro03]

Unternehmensgröße	Beschäftigte	Jahresumsatz	Jahresbilanz
kleinst	< 10	2 Mio	2 Mio
klein	< 50	10 Mio	10 Mio
KMU	< 250	50 Mio	43 Mio

Tabelle 2 zeigt die Prozentzahlen und zugehörigen Stufen der selbst definierten Einheit der „IT-Affinität“.

Tab. 2: Darstellung der kritischen Geschäftsprozesse abhängig von der IT

Stufe	Prozentzahl der kritischen Geschäftsprozesse abhängig von der IT
niedrig	20%
mittel	50%
hoch	90%

3 Standards und Rahmenwerke zum ISIM

Im Rahmen der Ableitung der Mindeststandards wurden verschiedene Regelwerke und Standards auf Maßnahmen zum Information Security Incident Management hin untersucht und deren Inhalte miteinander abgeglichen. Diese Regelwerke bzw. Standards bestanden aus der ISO/IEC 27035:2011 (Information Technology – Security techniques – Information Security Incident Management), der DIN ISO/IEC 27002:2014-02 (ab Abschnitt 5), der DIN ISO/IEC 27001:2015-03 (Anhang A), der Information Technology Infrastructure Library ITIL, COBIT 5 (COBIT 5 Enabling Processes DSS02 und der Präzisierung dieser in COBIT 5 for Information Security DSS02), dem Baustein B1.8 „Behandlung von Sicherheitsvorfällen“ aus dem IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (14. Ergänzungslieferung) sowie dem Open Information Security Management Maturity Model O-ISM3. Weitere Standards bzw. Regelwerke wie der „Computer Security Incident Handling Guide“ des National Institute of Standards and Technology (NIST) des U.S. Department of Commerce [USD12] oder der „Good Practice Guide for Incident Management“ der European Network and Information Security Agency (ENISA) [ENI10] wurden analysiert, aber in der Ableitung der Mindestanforderungen nicht näher betrachtet, da diese ein Computer Emergency Response Teams (CERT) voraussetzen bzw. fordern. Die Einrichtung eines CERTs ist jedoch für KMUs ein kaum zu realisierender Aufwand. Die VdS-Richtlinie 3473 „Cyber-Security für kleine und mittlere Unternehmen (KMU)“ [VDS15] enthält im Kapitel 18 einen kurzen Abschnitt zum Thema Sicherheitsvorfälle. Die dort dargestellten Empfehlungen stellen keine weiteren Anforderungen an KMUs, als die im Kapitel 4 aufgezeigten. Das Vorgehensmodell „Informationssicherheitsmanagementsystem in 12 Schritten“ (ISIS12) wurde nicht betrachtet.

4 Ziele und Maßnahmen

Um effektive Maßnahmen aus den verschiedenen Standards und Regelwerken ableiten zu können, wurden verschiedene Ziele des Incident Management Prozesses aus eben diesen herausgefiltert und in Haupt- und Nebenziele eingeteilt. Diese Auflistung zeigt Tabelle 3.

Tab. 3: Auflistung der Ziele des Information Security Incident Managements

	Ziele	Regel-werk
Hauptziele	Den normalen Service so schnell wie möglich wiederherstellen und Auswirkungen auf das Business so gering wie möglich halten	ITIL
	Verhindern bzw. Eindämmen der Auswirkungen des Information Security-Incidents, um die direkten und indirekten Kosten durch den IS-Incident zu vermindern	ISO/IEC 27035
Nebenziele	IT-bezogene Services sollen nutzbar sein	COBIT 5
	Sicherstellung einer konsistenten und wirksamen Strategie für das Management von Informationssicherheitsvorfällen, einschließlich der Kommunikation über Sicherheitsereignisse und -schwachstellen.	DIN ISO/IEC 27002
	Vorfälle werden gemäß vereinbarter Service Levels behoben	COBIT 5
	Informationssicherheit im laufenden Betrieb aufrechterhalten	Baustein B 1.8
	Behandlung von IS-Incidents im Vorfeld konzipieren und einüben	Baustein B 1.8
	Reaktionszeiten auf IS-Incidents minimieren	Baustein B 1.8
	IS-Events wurden erkannt, kategorisiert, eingestuft und abgearbeitet	ISO/IEC 27035
	Identifizierte IS-Incidents wurden bewertet und behandelt	ISO/IEC 27035
	Auswirkungen von IS-Incidents auf die Organisation oder den Geschäftsbetrieb wurden mit angemessenen Strategien, als Teil einer Incident Reaktion, minimiert. Evtl. auch im Zusammenspiel mit Kriseninterventionsplänen	ISO/IEC 27035
	Aus IS-Incidents wurden Lehren gezogen. Erhöhung der Chance, das zukünftige Auftreten von IS-Incidents zu verhindern und Verbesserung der Umsetzung und Nutzung von Beschränkungen innerhalb der Informationssicherheit. Verbesserung des ISIM (Lessons Learnt)	ISO/IEC 27035

Zusätzlich zu den Zielen wurden aus den Standards und Regelwerken Maßnahmen extrahiert. Dabei zeigte sich, dass das O-ISM3 keine expliziten Maßnahmen zum Incident Management enthält. Ebenso wurden aus ITIL keine Maßnahmen entnommen, da sich ITIL an der ISO/IEC 27001 orientiert. Die aus den Standards und Regelwerken extrahierten Maßnahmen wurden miteinander verglichen. Dieser Vergleich wurde herangezogen, um ähnliche oder gleiche Maßnahmen aus den Dokumenten herauszufiltern und auf die Umsetzbarkeit für KMUs zu prüfen.

Resultat dieser Prüfung ist ein Maßnahmenkatalog, der für einen Incident Management Prozess in KMUs herangezogen werden kann, da deren Umsetzbarkeit für KMUs möglich ist. Dabei wurde auf die Bedeutung der Maßnahme innerhalb des ISIM-Prozesses sowie auf die Kostenintensität bei der Umsetzung dieser geachtet. Tabelle 4 zeigt einen Teil der definierten Maßnahmen und deren Auftreten in den Standards und Regelwerken. Dabei steht der Haken (✓) für „tritt im Regelwerk auf“ und das Kreuz (×) für „tritt nicht im Regelwerk auf“. Um diese Maßnahmenauflistung übersichtlich zu halten, wurde darauf verzichtet, bei einigen Standards jeden

einzelnen Unterpunkt aufzuführen. Dafür wurden die übergeordneten Maßnahmenbeschreibungen genutzt. So geschehen bei dem Prozess DSS02 von COBIT 5 und zum Teil bei der ISO/IEC 27035. Die komplette Auflistung der Maßnahmen befindet sich in Abschnitt 6 als Katalog von Mindestanforderungen im Format eines Prozessschaubildes.

Tab. 4: Beispielhafte Auflistung der Maßnahmen und deren Auftreten in Regelwerken

Nr.	Maßnahme	Regelwerk			
		DIN ISO/IEC 27001/02	COBIT 5	Baustein B 1.8	ISO/IEC 27035
1	Verantwortlichkeiten und Verfahren	✓	×	✓	×
2	Definition eines Sicherheitsvorfalls	×	×	✓	×
3	Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen	✓	✓	✓	×
…					
8	Information Security Incident Response Team etablieren	×	×	✓	✓
…					
11	Informationssicherheitsereignisse werden detektiert und gemeldet	×	×	✓	✓
12	Meldung von Informationssicherheitsereignissen	✓	×	✓	×
13	Meldung von Schachstellen in der Informationssicherheit	✓	×	×	×
…					
22	Nachverfolgungsstatus und Berichtsanfertigung	×	✓	×	×
23	Dokumentation von Sicherheitsvorfällen	✓	✓	✓	✓

5 ISIM als Prozess in KMUs

Aus dem Vergleich der ausgewählten Standards und Regelwerke lässt sich unmittelbar ableiten, dass ein ISIM in einem Unternehmen grundsätzlich als eigenständiger Prozess etabliert werden sollte. Beispielsweise wird in COBIT 5 for Information Security der Prozess DSS02 und in der ISO/IEC 27035:2011 im Abschnitt 4.5 das ISIM als Prozess vorgeschlagen.

Der in Abbildung 1 schematisch dargestellte Prozess des ISIM wurde in Anlehnung an eine Veröffentlichung des Bundesministeriums des Innern entwickelt [BMI06]. Dieser Prozess zeigt auf, dass ohne eine Vorbereitungsphase kein Prozess zum ISIM entstehen kann. Des Weiteren ist die Erkennung eines Incidents elementarer Bestandteil des Prozesses. Ohne diesen Teil könnte niemand auf Incidents reagieren. Weiterhin muss ein erkannter Incident priorisiert wer-

den, um eventuelle Eskalationsmaßnahmen unternehmen zu können (Bsp.: Informationsweitergabe an Geschäftsleitung). Nach diesen Schritten folgt die Abarbeitung des Incidents nach den zu erstellenden Vorgaben. Im Anschluss sollten forensische Analysen durchgeführt werden, bevor der Prozess des ISIM abgeschlossen werden kann und der Sicherheitsvorfall behoben wurde.

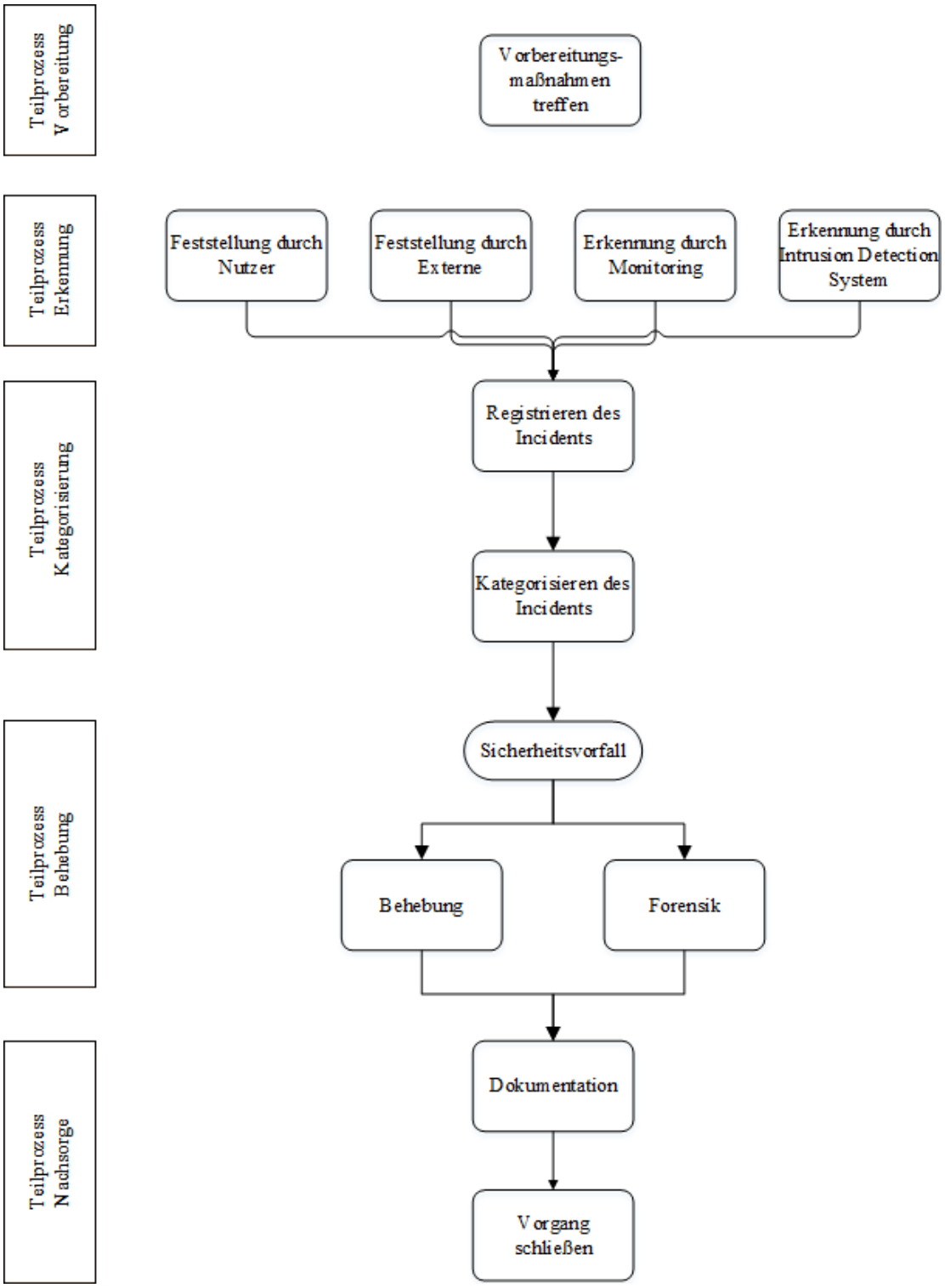

Abb. 1: Beispielhafter Allgemeiner ISIM-Prozess

6 Maßnahmenkatalog

Die Definition der Mindestanforderung im Incident Management Prozess integriert nun die KMU-Einteilung (Kleinst, Klein, KMU), die IT-Affinität (Niedrig, Mittel, Hoch) und die definierten Maßnahmen zu einem Mindestanforderungsschaubild gegliedert in die KMU-Größen. Weiterhin wurden die Mindestanforderungen so strukturiert, dass sie dem Incident Management Prozess entsprechen. Abbildungen 2 und 3 zeigen diese Mindestanforderungen in den jeweiligen Teilprozessen der Vorbereitung, Erkennung, Kategorisierung, Behebung und Nachsorge.

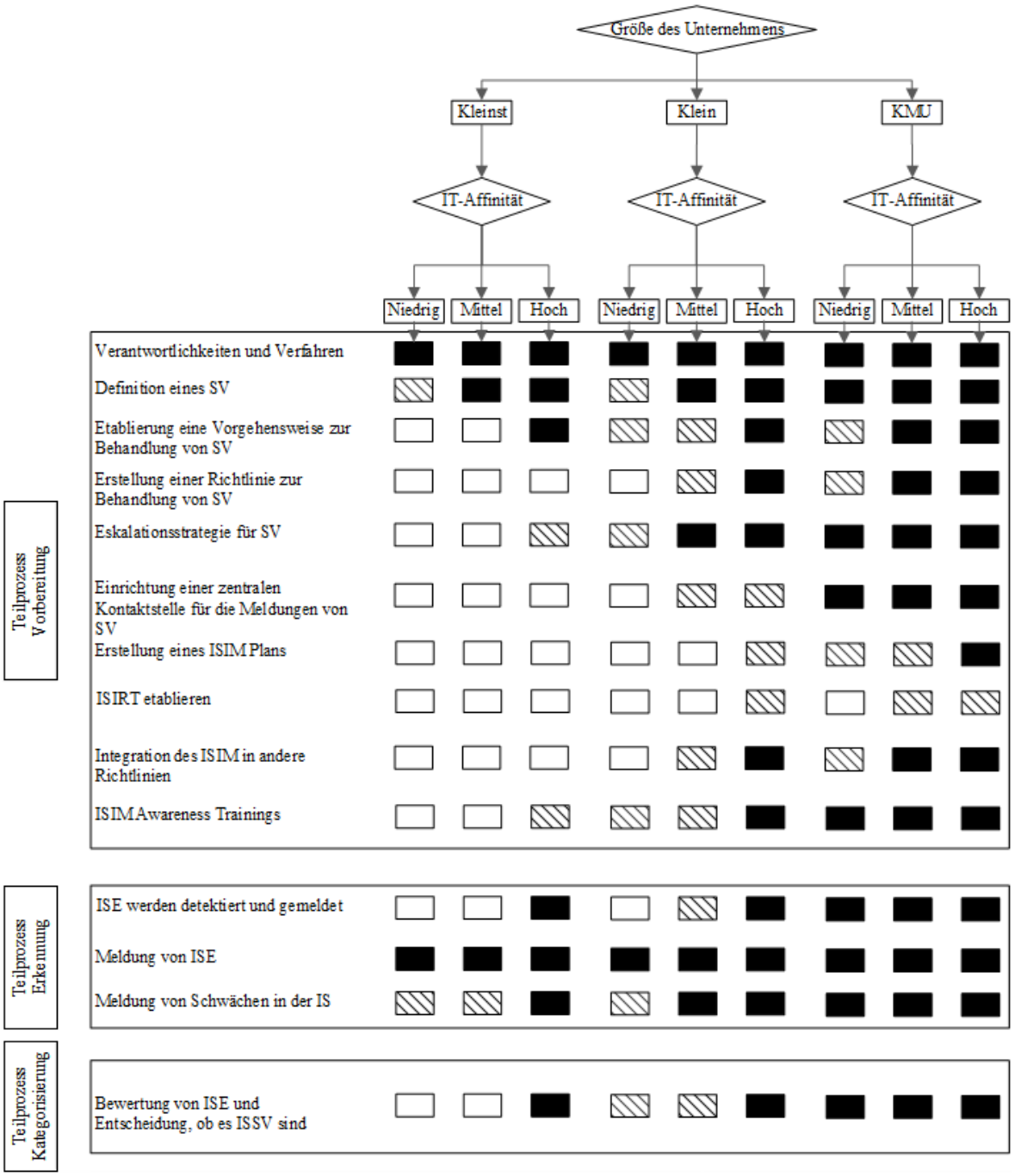

Abb. 2: Mindestanforderungen Teil 1 (Eine Legende findet sich unter Teil 2)

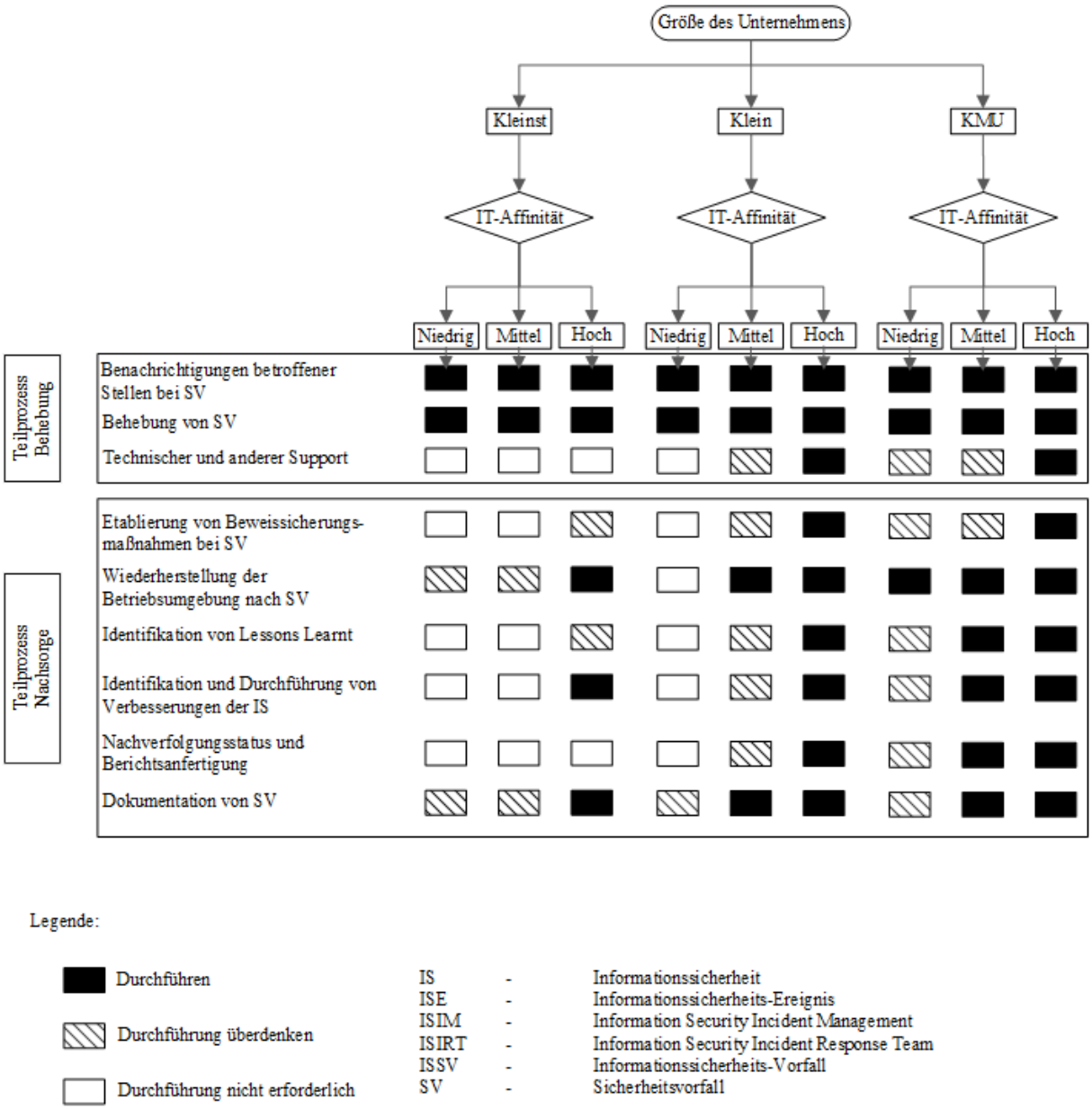

Abb. 3: Mindestanforderungen Teil 2

Unternehmen die sich in diesen Bereichen sehen sind dazu angehalten, die für sie zutreffenden Mindestanforderungen umzusetzen. Die Umsetzung von Maßnahmen aus den höheren Bereichen kann zusätzlich beschlossen werden. Weniger als diese Maßnahmen sollten nicht durchgeführt werden, da dadurch die Geschäftsfähigkeit des Unternehmens durch Informationssicherheitsvorfälle stark eingeschränkt werden kann.

Weiterhin sind die in diesem Abschnitt getroffenen Entscheidungen zu Umsetzungsmöglichkeiten der Mindestanforderungen nur Richtwerte. Abhängig von der Bedrohungslage in einem Unternehmen können Maßnahmen zusätzlich ergriffen oder auch vernachlässigt werden. Hierfür bietet sich eine separate Risikoanalyse für das Unternehmen an, um Risiken zu identifizieren und Schutzziele ableiten zu können.

7 Zusammenfassung und Ausblick

Wie vorangegangen dargestellt, sind bei Unternehmen mit höherem IT-Anteil Sicherheitsvorfälle risikobehafteter als bei Unternehmen mit weniger IT. Somit können Information Security Incidents die Geschäftsprozesse eines KMUs derart schädigen, sodass die Unternehmensexistenz stark gefährdet ist. Um die Wahrscheinlichkeit einer nachhaltigen Schädigung zu verringern bzw. zu verhindern, sollte ein korrekt implementiertes ISIM eingeführt werden. Dazu existieren eine Vielzahl von Regelwerken und Normen die jedoch eher auf die Belange großer Unternehmen ausgelegt sind. Daher kann ein ISIM in KMUs u.a. mit den hier vorgestellten Mindestanforderungen umgesetzt werden.

Computer Emergency Response Teams (CERTs) als Managed Security Service wurden in diesem Projekt nicht betrachtet. Gegenstand dessen war die Definition von Mindestanforderungen an KMUs im Bereich des ISIM, die diese selbst umsetzen sollten.

Weitere Optimierungsmöglichkeiten in Hinblick auf die Maßnahmenkataloge sollten durch die Integration weiterer Rahmenwerke im Bereich des Information Security Incident Managements anvisiert werden. Dieses könnte im Rahmen eines fortführenden Projektes realisiert werden. Weiterhin ist die technische Entwicklung zu berücksichtigen, um neue Methoden und Maßnahmen implementieren zu können. Bei Implementierung dieser Maßnahmen in ein Unternehmen, sollte der benannte Verantwortliche, im Rahmen von regelmäßigen Prüfungen der eingesetzten Maßnahmen, überprüfen, ob neue Rahmen- bzw. Regelwerke vorhanden sind und diese evtl. integrieren. Die regelmäßigen Prüfungen sollten mind. einmal im Jahr erfolgen und dienen zum Erhalt des ISIM.

Danksagung

An dieser Stelle möchte ich mich bei Frau Alicja Rothe bedanken, die mich während der Bearbeitung des Themas jederzeit unterstützt hat. Ein weiterer Dank gebührt dem Erst-Betreuer der zugehörigen Thesis, Herrn Prof. Dr. Dirk Koschützki, für seine immerwährende Hilfestellung bei fachbezogenen Angelegenheiten.

Literatur

[BeZi15] M. Beims, M. Ziegenbein: IT-Service Management in der Praxis mit ITIL – Der Einsatz von ITIL Edition 2011, ISO/IEC 20000:2011, COBIT 5 und PRINCE2. München: Carl Hanser Verlag 2015.

[BMI06] ITIL und Informationssicherheit. Berlin: Bundesministerium des Innern 2006.

[BMWi12] IT-Sicherheitsniveau in kleinen und mittleren Unternehmen – Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Berlin: Bundesministerium für Wirtschaft und Technologie 2012.

[BSI14] IT-Grundschutz-Kataloge – 14. Ergänzungslieferung. Bonn: Bundesamt für Sicherheit in der Informationstechnik 2014.

[DIN11] DIN ISO/IEC 27000. Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie. Berlin: Deutsches Institut für Normung e.V. 2011.

[DIN14] DIN ISO/IEC 27002. Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management [Entwurf]. Berlin: Deutsches Institut für Normung e.V. 2014.

[DIN15] DIN ISO/IEC 27001. Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen. Berlin: Deutsches Institut für Normung e.V. 2015.

[ENI10] European Network and Information Security Agency. Good Practice Guide for Incident Management. Zuletzt abgerufen am 28.05.2016 unter https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[Euro03] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. In: Amtsblatt der Europäischen Union. Artikel 2

[ISAC12a] COBIT 5 Enabling Processes. Rolling Meadows, Illinois: ISACA 2012.

[ISAC12b] COBIT 5 for Information Security. Rolling Meadows, Illinois: ISACA 2012.

[ISO11] ISO/IEC 27035. Information technology – Security techniques – Information security incident management. Genf: International Organization for Standardization.

[TOGr11] Open Information Security Management Maturity Model – O-ISM3. Berkshire: The Open Group 2011.

[USD12] U.S. Department of Commerce. Computer Security Incident Handling Guide – National Institute of Standards and Technology. Zuletzt abgerufen am 28.05.2016 unter http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[VDS15] VdS 3473. Cyber-Security für kleine und mittlere Unternehmen. VdS-Richtlinien für die Informationssicherheit. Köln: VdS Schadenverhütung GmbH

[WoSa14] K. Wolf, S. Sahling: Incident Management – Komplexe Störungen in der IT erfolgreich beheben. München: Carl Hanser Verlag 2014.