Müller, Neumair, Reiser, Dreo Rodosek (Hrsg.): 10. DFN-Forum Kommunikationstechnologien,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 11

Leichtgewichtiges Security Incident und Event Management im Hochschulumfeld

Jule Anna Ziegler[1], Bastian Kemmler[1], Michael Brenner[1] und Thomas Schaaf[2]

Abstract: Für viele IT-Organisationen im Hochschulumfeld aber auch in kleineren und mittleren Unternehmen (KMUs) gewinnt die Etablierung eines prozessorientierten Informationssicherheitsmanagementsystems (ISMS) zunehmend an Bedeutung. Für die Gestaltung eines solchen Systems existieren verschiedene Rahmenwerke wie ISO/IEC 27000 oder IT-Grundschutz. Deren komplette Umsetzung strapaziert aber häufig die Ressourcen kleinerer IT-Organisationen übermäßig. Für den ISMS-Teilprozess Security Incident und Event Management (SIEM) wird als Lösungsvorschlag ein leichtgewichtiges Modell vorgestellt, das die Anforderungen aus etablierten Rahmenwerken berücksichtigt und relevante Prozessbausteine abbildet. Der leichtgewichtige SIEM-Prozess unterstützt somit eine ressourcenschonende Einführung eines ISMS. Basierend auf einer Anforderungsanalyse entsteht zunächst ein allgemeiner SIEM-Prozess, der als Grundlage für den leichtgewichtigen SIEM-Prozess dient. Dieser verzichtet durch Entfernen redundanter Prozessbausteine und sinnvolles Zusammenfassen auf jede vermeidbare Komplexität und halbiert die Anzahl der allgemeinen Prozessbausteine. Eine Experten-Evaluation validiert die grundsätzliche Anwendbarkeit des leichtgewichtigen SIEM-Prozesses.

Keywords: Security Incident und Event Management, SIEM, Information Security Management, IT Service Management

1 Einleitung

Informationssicherheit wird in der heutigen digitalen Gesellschaft immer wichtiger. Dies zeigt sich unter anderem durch die Berichterstattung in den Medien über Security Incidents, aber auch in dem zunehmenden Umfang gesetzlicher Verpflichtungen. Beispielsweise verlangt das im Juli 2015 beschlossene IT-Sicherheitsgesetz von Betreibern sogenannter kritischer Infrastrukturen, dass sie *angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen*[Bu15].

Entsprechend steigt auch für IT-Organisationen im Hochschulumfeld und in kleineren und mittleren Unternehmen (KMU) der Druck, ein sogenanntes Informationssicherheitsmanagementsystem (ISMS) zu etablieren – sei es nun eigenständig oder als Teil eines bereits bestehenden prozessorientierten Service-Managementsystems (SMS). Für die Gestaltung eines wirksamen Managementsystems für Informationssicherheit existieren verschiedene Rahmenwerke wie ISO/IEC 27000 oder IT-Grundschutz. Jedoch ist der Aufwand für

[1] Leibniz-Rechenzentrum, Boltzmannstr. 1, 85748 Garching b. München, {vorname}.{nachname}@lrz.de
[2] Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 München, schaaf@nm.ifi.lmu.de

Einführung und Betrieb eines ISMS erheblich und strapaziert oft die Ressourcen kleinerer IT-Organisationen. Dazu kommen noch weitere erschwerende Faktoren. Viele Mitarbeiter nehmen die Einführung eines Managementsystems zunächst vor allem als Verlust von Entscheidungsfreiheit und Flexibilität wahr. Die Reaktionen sind entsprechend erst mal negativ [ET02], was die Umsetzung solch eines *organisatorischen Change*, z.B. nach dem Vorgehen von Kotter [KR06], aufwändig macht. Umso tiefgreifender dabei die Veränderung und umso schlechter sie vermittelt werden kann (oder wird), umso größer sind die zu erwartenden Widerstände.

Auch für einen Security Incident und Event Management (SIEM) Prozess, als wesentlicher Baustein des ISMS, ist somit eine einfache Anwendbarkeit und Verständlichkeit für alle Mitarbeiter ein entscheidender Erfolgsfaktor für eine erfolgreiche und nachhaltige Einführung. Es leiten hieraus sich die folgenden Fragestellungen ab:

- Wie sieht ein zu den wichtigsten bestehenden Rahmenwerken konformer SIEM-Prozess aus?
- Wie kann die Komplexität und die Anzahl der Prozessbausteine reduziert werden, um einen leichtgewichtigen SIEM-Prozess zu erhalten?
- Welche Prozessbausteine des SIEM sind obligatorisch und welche sind optional?
- Welche Prozessbausteine des SIEM lassen sich zusammenfassen?

Leichtgewichtige Modelle, d.h. einfach anwendbare und leicht verständliche Modelle zum Management der Informationssicherheit existieren kaum und beantworten die oben gestellten Fragestellungen nur in geringem Umfang.

Vorarbeiten zu dieser Veröffentlichung finden sich in der Masterarbeit „Ein Fachkonzept für leichtgewichtiges Informationssicherheits-Management“[Zi16].

In Abschnitt 2 werden etablierte Rahmenwerke beschrieben, aus deren Anforderungen in Abschnitt 3 zunächst ein allgemeiner SIEM-Prozess entsteht. Im darauffolgenden Abschnitt 4 wird darauf aufsetzend ein leichtgewichtiger SIEM-Prozess abgeleitet. Abschnitt 5 beschreibt die Durchführung einer Experten-Evaluation, deren Ergebnisse die Anwendbarkeit des leichtgewichtigen SIEM-Prozesses untermauern. Das Paper endet mit einer Zusammenfassung und einem Ausblick.

2 Betrachtete Rahmenwerke

Die **ISO/IEC 27000** [IS13b] ist eine Standardfamilie zum Informationssicherheits-Management, die die Möglichkeit zur Zertifizierung bietet. Innerhalb dieser Standardfamilie beschreibt ISO/IEC 27001 [IS13b] die Anforderungen an ein ISMS sowie, im Anhang A auch Maßnahmen, die für die Etablierung eines SIEM relevant sind. SIEM ist auch Gegenstand im **Information Security Management Toolkit** [UC 1] der Universities and Colleges Information Systems Association (UCISA), welches auf der ISO/IEC 27001 [IS13b] und 27002 [IS13a] aufsetzt. Ein weiteres Rahmenwerk zum Informationssicherheitsmanagement ist der durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschriebene **IT-Grundschutz** [Bu16]. Dieser ist ebenfalls kompatibel mit

der ISO/IEC 27000 und besteht aus einem vierteiligen Standard sowie modular aufgebauten IT-Grundschutz-Katalogen mit bereits identifizierten Bausteinen, Maßnahmen sowie Gefährdungen.

Die **IT Infrastructure Library (ITIL)** [Ax11] ist demgegenüber eine Büchersammlung mit "Good Practices" zu einem SMS und gilt momentan als der De-facto Standard im IT-Service Management (ITSM) [Br11]. Der Fokus von ITIL liegt auf 25 Prozessen, die einem Service Lifecycle zugeordnet sind, darunter auch das Informationssicherheitsmanagement. Eine Standardfamilie für ein leichtgewichtiges SMS ist durch **FitSM** [Fi16] beschrieben, die aus sieben Teilen besteht. Insbesondere der Teil FitSM-2 [Fi22a] legt Ziele und Aktivitäten, u. a. zum Informationssicherheits-Management, fest.

Die mehrteilige Dokumentenfamilie **COBIT 5** [IS12b] rückt die Governance und das Management der Unternehmens-IT in den Vordergrund. Die Anforderungen zum SIEM sind im Handbuch COBIT 5: Enabling Processes [IS12a] innerhalb der Domäne der Management-Prozesse beschrieben.

Wesentlich für alle Rahmenwerke ist das Prinzip des Deming-Zyklus [De86] (Plan-Do-Check-Act, kurz PDCA) zur kontinuierlichen Verbesserung eines Managementsystems.

3 Harmonisierung der SIEM Prozessbausteine

Zur Sicherstellung der Kompatibilität mit etablierten Rahmenwerken dienen die Anforderungen der sechs vorgestellten Rahmenwerke als Grundlage für die Entwicklung eines leichtgewichtigen SIEM-Prozesses. Hierzu werden die Prozessbausteine zunächst in die grundlegenden Typen Aktivitäten und Outputs gruppiert. [3]

Diese Vorgehensweise ermöglicht in einem späteren Schritt eine Vergleichbarkeit der Prozessbausteine und kann auf beliebige Prozesse oder Themengebiete angewendet werden.

Nach Konsolidierung und Harmonisierung bedeutungsgleicher Begriffe ergeben sich, ausgehend von den Anforderungen der sechs vorgestellten Rahmenwerke, wie in Tabelle 1 ersichtlich, die folgenden Aktivitäten und Outputs:

3.1 Aktivitäten

A1 Entwickeln eines Incident Response Plans, Definieren von Eskalations- und Kommunikationswegen
A2 Überwachen und Aufzeichnen von Security Events
A3 Bewerten und Klassifizieren von Security Events
A4 Analysieren und Antworten auf Security Incidents und Events
A5 Definieren und Überwachen von Folgemaßnahmen
A6 Beseitigen der Ursachen, Untersuchen und Lindern der Konsequenzen
A7 Aufzeichnen aller Aktionen und Berichterstattung

[3] Inputs sind bereits in den Aktivitäten enthalten

A8 Durchführen eines Reviews nach einem Security Incident
A9 Durchführen von Tests zur Simulation von Security Incidents und deren Dokumentation

3.2 Outputs

O1 Dokumentierter Incident Response Plan zum Umgang mit Security Incidents
O2 Definierte Eskalations- und Kommunikationswege
O3 Bewertungs- und Entscheidungskriterien
O4 Berichte und Aufzeichnungen über Security Incidents und Events sowie Folgemaßnahmen
O5 Richtlinie für das Management von Security Incidents (oder vergleichbare beschreibende Dokumentation)

Tabelle 1: Gegenüberstellung der Rahmenwerke

	ISO/IEC 27001	**UCISA Toolkit**	**IT-Grundschutz**	**ITIL**	**FitSM**	**COBIT 5**
Aktivitäten						
A1		✓	✓			✓
A2	✓	✓	✓	✓	✓	(✓)
A3	✓	✓	(✓)		✓	✓
A4	✓	✓	✓	✓	✓	✓
A5			✓	✓	✓	
A6	(✓)	✓	✓	✓		✓
A7	(✓)	✓	(✓)	✓	(✓)	✓
A8	✓	✓	(✓)	(✓)	(✓)	(✓)
A9			✓			
Outputs						
O1		✓				✓
O2		✓	✓			✓
O3	(✓)	(✓)			(✓)	
O4	✓	✓	✓	✓	✓	✓
O5	✓	✓	✓	✓	✓	✓

Rahmenwerk enthält Aktivität bzw. Output ...
✓: ... explizit
(✓:) ... implizit

Aus den beschriebenen Aktivitäten lässt sich nun ebenfalls ein allgemeiner SIEM-Prozess ableiten (vgl. Abbildung 1).

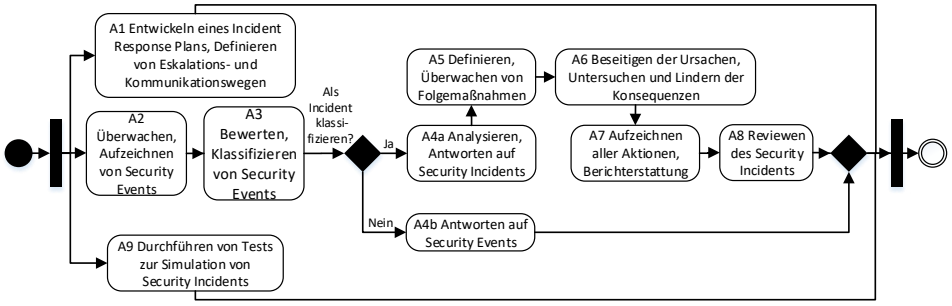


Abbildung 1: allgemeiner SIEM-Prozess

4 Der leichtgewichtige SIEM-Prozess

Zur Gestaltung eines einfach anwendbaren und leicht verständlichen Modells werden die in Abschnitt 3 vorgestellten Prozessbausteine (vgl. Tabelle 2) überprüft. Wo dies möglich ist ohne die Wirksamkeit des SIEM-Prozesses entscheidend zu gefährden, werden Bausteine zusammengefasst oder, in Einzelfällen, auch nicht essentielle Bausteine komplett gestrichen.

So lassen sich die Artefakte O1, O2 und O3 in einem leichtgewichtigen Modell in der Richtlinie (O5) (und der damit einhergehenden Prozessbeschreibung) für alle Security Incidents und Events auf einem gemeinsamen Niveau festschreiben. Denkbar sind hier ebenfalls verschiedene Verfahren für unterschiedliche Typen von Incidents bzw. Events, sodass je nach Klassifizierung in Aktivität A3 unterschieden werden kann. Jedoch sollte bei dieser Variante die Anzahl und Variabilität der Verfahren auf ein Minimum beschränkt werden. Somit werden beispielsweise Response Pläne, Eskalations- und Kommunikationswege, Bewertungs- und Entscheidungskriterien nur noch nach Typ des Incidents bzw. Events definiert. Benötigte Abweichungen werden an den Information Security Risk Manager eskaliert.

Mit ähnlicher Argumentation lässt sich die Aktivität A1 ebenfalls in die Richtlinie aufnehmen.

Weiter vereinfachend wirkt eine Zusammenfassung der Aktivitäten A5 und A6, da die Definition der Folgemaßnahmen und die damit einhergehende Durchführung und Beseitigung der Störung in kleineren und mittleren Organisation meist in einem Arbeitsschritt erledigt wird.

Verzichten kann man hingegen auf die Aktionen A7 und A8. Relevante Aufzeichnungen werden aufgrund der hohen Verbreitung von SMS-Tools meist ohnehin automatisch erstellt. Ein entsprechendes Erfolgs-/Nicht-Erfolgs-Review wird üblicherweise im Rahmen der Aktivitäten A5 und A6 implizit durchgeführt. Auch die Aktion A9 ist vernachlässigbar, da die Simulation von Security Incidents bei KMUs meist nicht organisationsintern sondern von entsprechend spezialisierten Unternehmen extern durchgeführt wird. Als Koordi-

Tabelle 2: Vergleich der Rahmenwerke mit dem leichtgewichtigen Modell

	ISO/IEC 27001	UCISA Toolkit	IT-Grundschutz	ITIL	FitSM	COBIT 5	leichtgewichtiges Modell
Aktivitäten							
A1		✓	✓			✓	R
A2	✓	✓	✓	✓	✓	(✓)	✓
A3	✓	✓	(✓)		✓	✓	✓
A4	✓	✓	✓	✓	✓	✓	✓
A5			✓	✓	✓		✓
A6	(✓)	✓	✓	✓		✓	
A7	(✓)	✓	(✓)	✓	(✓)	✓	(✓)
A8	✓	✓	(✓)	(✓)	(✓)	(✓)	(✓)
A9			✓				
Outputs							
O1		✓				✓	R
O2		✓	✓			✓	R
O3	(✓)	(✓)			(✓)		R
O4	✓	✓	✓	✓	✓	✓	✓
O5	✓	✓	✓	✓	✓	✓	✓

Rahmenwerk enthält Aktivität bzw. Output ...
✓: ... explizit | (✓:) ... implizit
R: als Verfahren in Richtlinie enthalten

nator dient hier ebenfalls der Information Security Risk Manager. Somit kann A9 ebenfalls als Eskalationszustand betrachtet werden.

Es ergibt sich somit der leichtgewichtige SIEM-Prozess aus Abbildung 2.

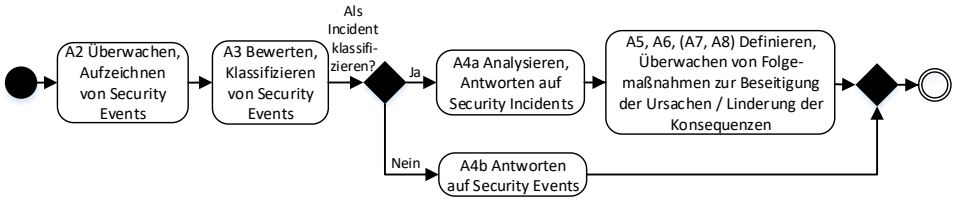


Abbildung 2: leichtgewichtiger SIEM-Prozess

Eine entsprechende RACI-Matrix (siehe Tabelle 3) bildet das zugehörige Mapping der Verantwortlichkeiten zwischen den jeweiligen Aktivitäten und den Rollen ab. Die Rollen

dazu entstammen aus dem FitSM-3 Rollenmodell [Fi22b]. Hierbei stellt der Prozessmanager ISM sicher, dass Security Incidents und Events effektiv erkannt, dokumentiert, klassifiziert und bearbeitet werden. Zusätzlich ist pro Asset bzw. Control ein Asset Owner bzw. Information Security Control Owner notwendig, dem die Verantwortung des jeweiligen Objektes (Asset/Control) obliegt.

Die im linken Teil der Tabelle dargestellten Outputs sind allen Aktivitäten zugeordnet und sind in diesem Rahmen zu erstellen.

Tabelle 3: Prozessbausteine des Security Incident und Event Managements

Security Incident und Event Management Prozess				
		Rollen		
Artefakte & Outputs	*Aktivitäten & Abläufe*	Prozessmanager ISM	Asset Owner	Information Security Control Owner
• O4, (O1, O2, O3, A1) Aufzeichnungen und Berichte über Security Events und Incidents sowie Folgemaßnahmen • O5 Richtlinie für das Management von Security Incidents	A2 Überwachen und Aufzeichnen von Security Events	A	I	R
	A3 Bewerten und Klassifizieren von Security Events	A	C	R
	A4a Analysieren und Antworten auf Security Incidents	A	C	R
	A4b Antworten auf Security Events	A / R		
	A5, A6, (A7,A8) Definieren und Überwachen von Folgemaßnahmen zur Beseitigung der Ursachen / Linderung der Konsequenzen	A	C	R

R = Responsible (Durchführungsverantwortlich)
A = Accountable (Verantwortlich im Sinne von Kostenverantwortung und Rechenschaftspflicht)
C = Consulted (wird um Rat gefragt)
I = Informed (wird informiert)

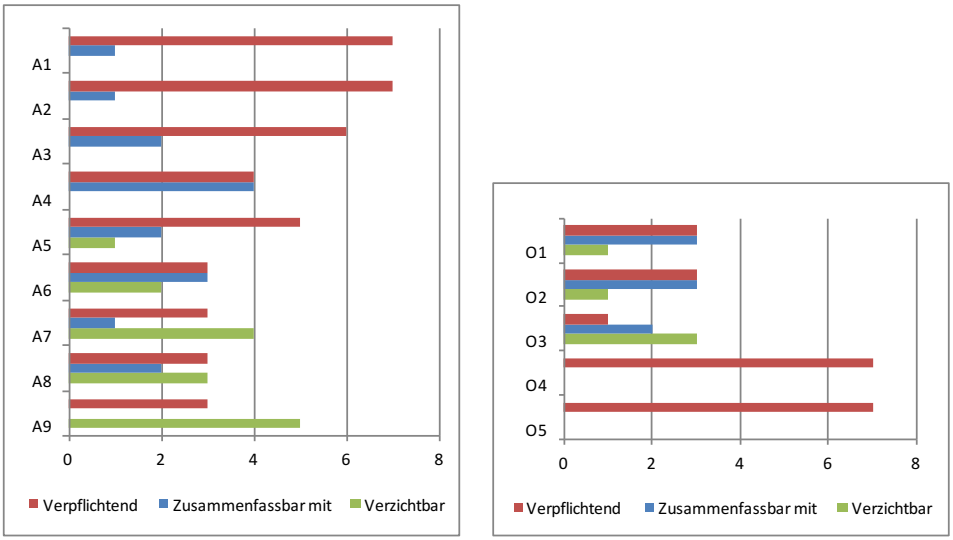
5 Experten-Evaluation

Zur Validierung des Modells beurteilten acht Experten aus Hochschulumfeld und Industrie (z. B. Berater/Trainer, Auditoren, Datenschutzbeauftragte) die Kritikalität und Rele-

vanz der einzelnen Prozessaktivitäten und -outputs. Durchgeführt wurde die Experten-Evaluation in Form eines Online-Fragebogens. Die unvoreingenommene Fragestellung (ohne Einsicht in das vorgestellte leichtgewichtige Modell) diente dazu, ein fundiertes Feedback über die Relevanz der Prozessbausteine zu erhalten.

Dabei bewerteten die Experten die Aktivitäten (A1 bis A9) und Outputs (O1 bis O4) aus Abschnitt 3 und klassifizierten diese entsprechend den Kategorien „Verpflichtend“, „Zusammenfassbar mit“oder „Verzichtbar“.

Abbildung 3 zeigt die Ergebnisse der Evaluation. Die X-Achse repräsentiert die Anzahl der Experten, die Y-Achse die entsprechenden Prozessbausteine.



(a) Aktivitäten

(b) Outputs [4]

Abbildung 3: Ergebnisse der Experten-Evaluation [5]

Abbildung 3a verdeutlicht, dass die Aktivitäten A1 bis A3 eine essentielle Rolle in einem leichtgewichtigen SIEM-Prozess spielen, wohingegen die Aktivitäten A7 bis A9 überwiegend als verzichtbar gelten. Die Tendenz zur Zusammenfassbarkeit sahen die Experten jeweils in den Aktivitäten A4 bis A6. Einer der befragten Experten begründete dies ebenfalls damit, dass die Aktivitäten A7 und A8 bereits implizit in A5 und A6 enthalten seien (vgl. Abschnitt 4).

Hinsichtlich der Outputs repräsentieren die Ergebnisse in Abbildung 3b eindeutig die Notwendigkeit des Outputs O4 in einem leichtgewichtigen SIEM-Prozess. Entsprechend unserer Einschätzung stuften die Experten die Outputs O1 bis O3 als zusammenfassbar ein.

[4] Bei Output O5 wurden die Experten zur Relevanz (sehr relevant, teilweise relevant, weniger relevant, gar nicht relevant) befragt. Fünf Experten halten O5 für sehr relevant. Zwei Experten halten O5 für teilweise relevant.

[5] Die Antwortoption „keine Angabe“ist in der Abbildung nicht aufgeführt.

In der Gesamtbetrachtung aller Prozessbausteine bestätigen die Experten den leichtgewichtigen SIEM-Prozess.

6 Zusammenfassung und Ausblick

Die Etablierung und der Betrieb eines ISMS für IT-Organisationen im Hochschulumfeld aber auch in kleineren und mittleren Unternehmen bedeutet für die betroffenen Unternehmen oft eine zeitaufwendige Einführung und hoher Ressourcenbedarf beim Betrieb. Bei der Betrachtung der Komplexität des dafür erforderlichen SIEM-Prozesses wird der Aufwand besonders deutlich. Eine Harmonisierung der SIEM-Prozessbausteine der in Abschnitt 2 vorgestellten Rahmenwerke und die folgende Extraktion eines allgemeinen SIEM-Prozesses (vgl. Abschnitt 3) verdeutlicht den entstehenden Aufwand.

Viele Prozessbausteine dieses zu Vorgaben mehrerer Rahmenwerke konformen Prozesses sind zusammenfassbar oder gar redundant (vgl. Abschnitt 4). Mittels sinnvollem Zusammenfassen und Entfernen lässt sich die Anzahl der Prozessbausteine des Prozesses reduzieren, ohne dass Funktion oder Wirksamkeit des Prozesses wesentlich eingeschränkt werden. Insbesondere die Verankerung von wenigen, spezifischen, kurzgefassten Verfahren in der SIEM-Richtlinie reduziert die allgemeine Prozesskomplexität.

Der Vorteil des leichtgewichtigen SIEM-Prozesses ist neben der kompakten Darstellung zusätzlich eine Vereinfachung der Anwendbarkeit im Hochschulumfeld und für kleine bis mittelgroße Organisationen. Mithilfe der Tabelle 3 sind die erforderlichen Prozessbausteine übersichtlich aufgelistet. Anhand des Mappings der Verantwortlichkeiten zwischen Rollen und Aktivitäten ist die Aufgabenverteilung leicht verständlich. Ein UML-Aktivitätsdiagramm unterstützt das Verständnis des Zusammenhangs und der Einordnung der Prozessbausteine. Der entstandene leichtgewichtige SIEM-Prozess ist dabei weiterhin kompatibel mit den etablierten Rahmenwerken, auf denen er ursprünglich basiert.

Ausblickend ist zur weiteren Bewertung des Modells im nächsten Schritt die praktische Umsetzung des leichtgewichtigen SIEM-Prozesses geplant.

Ebenso können analog zu dem hier beschriebenen Vorgehen weitere hilfreiche Artefakte, wie beispielhafte, leichtgewichtige Verfahrensbeschreibungen, zur Unterstützung der Umsetzung eines leichtgewichtigen Service Management Ansatzes (vgl. FitSM [Fi16]) entwickelt werden.

Danksagung

Die Autoren danken den Mitgliedern des MNM-Teams für hilfreiche Diskussionen und wertvolle Kommentare zu vorhergehenden Versionen des Papers. Das MNM-Team, unter der Leitung von Prof. Dr. Dieter Kranzlmüller und Prof. Dr. (em.) Heinz-Gerd Hegering, ist eine Forschungsgruppe mit Wissenschaftlern an den Münchner Universitäten, der Universität der Bundeswehr München und dem Leibniz-Rechenzentrum der Bayrischen Aka-

demie der Wissenschaften. Der Internetauftritt findet sich unter http://www.mnm-team.org.

Literaturverzeichnis

[Ax11] Axelos, Hrsg. ITIL service design. TSO The Stationery Office, London, 2nd ed.. Auflage, 2011.

[Br11] Brenner, Michael; Gentschen Felde, Nils; Hommel, Wolfgang; Metzger, Stefan; Reiser, Helmut; Schaaf, Thomas: Praxisbuch ISO-IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung ; [mit 80 Prüfungsfragen zur Vorbereitung auf die Foundation-Zertifizierung]. Hanser, München, 2011.

[Bu15] Bundestag: , Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), 17.07.2015.

[Bu16] Bundesamt für Sicherheit in der Informationstechnik: , IT-Grundschutz Webseite. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html, Version: 2016. Abruf: 24.Mrz.2016.

[De86] Deming, William Edwards: Out of the Crisis. Massachusetts Institute of Technology Center for Advances Engineering Study, Cambridge, Massachusetts, 1986.

[ET02] Elrod, P. David; Tippett, Donald D.: The “death valley” of change. Journal of Organizational Change Management, 15(3):273–291, 2002.

[Fi16] FitSM: , FitSM - Standards for lightweight IT service management. http://fitsm.itemo.org/, Version: 2016. Abruf: 1.Apr.2016.

[Fi22a] FitSM: , FitSM-2 Objectives and activities. http://fitsm.itemo.org/sites/default/files/FitSM-2_Objectives_and_activities.pdf, Version: 2.2. Abruf: 15.Mrz.2016.

[Fi22b] FitSM: , FitSM-3 Role model. http://fitsm.itemo.org/sites/default/files/FitSM-3_Role_model.pdf, Version: 2.2. Abruf: 15.Mrz.2016.

[IS12a] ISACA: COBIT 5 - Enabling Processes. ISACA, Illinois, 2012.

[IS12b] ISACA: COBIT 5 - Rahmenwerk für Governance und Management der Unternehmens-IT. ISACA, Illinois, 2012.

[IS13a] ISO/IEC: Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013). 2013.

[IS13b] ISO/IEC: Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013). 2013.

[KR06] Kotter, John P.; Rathgeber, Holger: Das Pinguin-Prinzip: Wie Veränderung zum Erfolg führt. Droemer, München, 2006.

[UC 1] UCISA: , UCISA Information Security Management Toolkit. https://www.ucisa.ac.uk/~/media/Files/members/activities/ismt/Complete%20with%20covers, Edition 1.0 Volume 1. Abruf: 20.Feb.2016.

[Zi16] Ziegler, Jule Anna: Ein Fachkonzept für leichtgewichtiges Informationssicherheits-Management. Masterarbeit, Ludwig-Maximilians-Universität München, 2016.