Anwendbarkeit von Enterprise Security Assessments sowie Enterprise Architecture Tools für KMU

Kendime Ismailji [1] , Christof Mosler [2] , Silvia Knittl [3]

Abstract: Die zunehmende Cyber-Kriminalität bedarf eines präventiven Sicherheitsansatzes der Enterprise Security Architecture (ESA). Besonders kleine und mittelständische Unternehmen (KMU) tun sich oft schwer damit, Maßnahmen zur Widerstandsfähigkeit gegenüber Cyber-Angriffen umzusetzen. In diesem Artikel stellen wir unseren ESA-Ansatz für KMU vor. Dafür wurden Anforderungen hinsichtlich der Informationssicherheit an KMU identifiziert, priorisiert und mit einem bestehenden ESA-Rahmenwerk verglichen. Das Ergebnis bildet ein für KMU angepasstes Framework. Das bereits bestehende Framework wurde von 340 Fähigkeiten auf 100 Fähigkeiten gekürzt. Der Einsatz des neuen Frameworks hat bereits gezeigt, dass ESA für KMU anwendbar und vorteilhaft ist. ESA-Assessments benötigen ein geeignetes Werkzeug, welches deren Durchführung und Verwaltung unterstützt und die Ergebnisvisualisierung automatisiert. Dazu stellen wir die Anforderungsanalyse vor. Die Umsetzung der Anforderungen in einem ausgewählten Tool hat gezeigt, dass dadurch der ESA-Prozess optimiert wird. Der Werkzeugeinsatz reduziert den Pflegeaufwand und ermöglicht dadurch eine effizientere Arbeitsweise.

Keywords: Enterprise Security Architecture; ESA; KMU; EA-Tool; ISMS.

1 Präventive Sicherheit durch Enterprise Security Architecture (ESA)

Informationssicherheit hat heutzutage eine besondere Bedeutung, denn durch die zunehmende Digitalisierung verschaffen sich Cyberkriminelle neue Einfallstore. Um sich vor Cyberangriffen zu schützen, sind besondere Maßnahmen hinsichtlich der Sicherheit von Unternehmenswerten zu beachten. Enterprise Security Architecture (ESA) bietet einen präventiven Sicherheitsansatz, indem Cyber-Fähigkeiten (engl. Cyber Capabilities) zur Bewertung des Sicherheitsstatus eines Unternehmens festgelegt werden, welche die Organisationsstruktur, deren Prozesse und Technologien gesamtheitlich betrachten. Dadurch können Lücken in der Sicherheitsarchitektur identifiziert und Handlungsmaß-nahmen abgeleitet werden. Insbesondere für kleine und mittelständische Unternehmen (KMU) sind Rahmenbedingungen hinsichtlich Informationssicherheit und Datenschutz schwer einzu-

1 PwC, Cyber Privacy, Friedrichstr. 14, 70174 Stuttgart, kendime.ismailji@pwc.com
2 HFT Stuttgart, Wirtschaftsinformatik, Schellingstr. 24, 70174 Stuttgart, christof.mosler@hft-stuttgart.de
3 PwC, Cyber Privacy, Bernhard-Wicki-Str. 8, 80636 München, silvia.knittl@pwc.com, https://orcid.org/ 0000-0001-9507-8713

https://doi.org/10.30844/AKWI_2022_03

halten, denn bekannte Rahmenwerke, wie bspw. die ISO 27001 [ISO13] oder die Datenschutzgrundverordnung (DSGVO), sind in der Wahrnehmung häufig für große Unternehmen und Konzerne ausgelegt. Cyberkriminelle unterscheiden jedoch nicht zwischen den Unternehmensgrößen. Daher ist es umso wichtiger auch für KMU einen geeigneten Sicherheitsansatz festzulegen.

1.1 Ziele der Arbeit und Vorgehensweise

Das Ziel der Arbeit ist zum einen den Anpassungsbedarf eines bestehenden, im praktischen Einsatz befindlichen ESA-Frameworks für KMU zu bewerten. Zum anderen sollen durch einen geeigneten Tool-Einsatz die derzeitige Assessment-Dokumentation und ihre Verwaltung vereinfacht und Ergebnisse visualisiert werden. Der methodische Aufbau zum Erreichen dieser Ziele orientiert sich am Design Science-Ansatz (vgl. Hevner in [BHM20]). Dieser Ansatz umfasst gem. Hevner drei Zyklen: den der praktischen Relevanz (Relevance Cycle), der den aktuellen Stand der Technik einbezieht, den des Designs (Design Cycle), in dem aus der Verknüpfung von Theorie und Praxis ein Artefakt abgeleitet wird, und den der Evaluation (Rigor Cycle).

Entsprechend dieses Ansatzes beschreiben wir die Relevanz anhand eines aus unserer Beratungspraxis entwickelten ESA-Rahmenwerks. Zum besseren Verständnis stellen wir dieses in Abschnitt 1.2 vor. Die Herausforderungen bei der praktischen Anwendung bei KMU stellen wir in Abschnitt 1.3 dar. Verwandte Arbeiten, die sich mit ESA für KMU befassen und die einen Beitrag für unser Design liefern, stellen wir in Kapitel 2 vor. In Kapitel 3 entwickeln wir daraus ein Konzept für die Anpassung unseres ESA-Rahmenwerks für KMU. Dafür identifizieren wir die Cyber-Security-Anforderungen für KMU in Abschnitt 3.1. und konzipieren damit ein KMU-taugliches Assessment-Vorgehen in Abschnitt 3.2.

Ein weiteres Ziel ist, die bisherige Assessment-Dokumentation und -Verwaltung zu vereinfachen und die Ergebnisse zu visualisieren. Hier analysieren wir das vorgegebene Tool LeanIX, welches bereits im Kontext Enterprise Architecture genutzt wird und nun auf seine Anwendbarkeit für ESA geprüft werden soll. Damit soll der bisherige ESA-Prozess und -Assessment durchgeführt und ausgewertet werden. Zudem sollen sämtliche Ergebnisse im Tool abgebildet werden können. Darunter zählen z. B. Modellierungen, Diagramme, Roadmaps und Reifegradbewertungen. In Abschnitt 3.3 stellen wir die An-forderungsanalyse an das Tool und die Erstellung des Assessments für KMU vor. Dieses Konzept prüfen wir mit qualitativen Methoden auf Anwendbarkeit in Abschnitt 3.4. Wir diskutieren die Ergebnisse in Kapitel 4, fassen diese zusammen und geben einen Ausblick über mögliche folgende Entwicklungsschritte.

1.2 Grundlagen: Enterprise Security Architecture

Enterprise Security Architecture (ESA) [Mc20] ist ein Top-Down-Ansatz, der mit der Identifikation der Strategie und der Unternehmensziele startet. Der ESA-Ansatz ist methodisch abgeleitet vom Enterprise Architecture (EA) Management-Framework TOGAF [Th09]. Im Mittelpunkt stehen die zu untersuchenden Fähigkeiten und Kompetenzen (engl. Capabilities) des Unternehmens. Durch die Orientierung an den Methoden der EA wird ein ganzheitlicher Schutz gewährleistet, bei dem Mitarbeiter, Gebäude, Anlagen, IT-Systeme und Informationen einer Organisation berücksichtigt werden.

1.3 Herausforderungen bei der Umsetzung von ESA

Im Mittelpunkt aller Aktivitäten steht ein ESA-Framework, welches bei PwC entwickelt wurde. Mithilfe dieses aus der Praxis entstandenen Rahmenwerks wird die Unternehmenssicherheitsarchitektur aufgebaut und bewertet. Das Framework selbst kann bei Bedarf angepasst und weiterentwickelt werden und besteht aus 11 Domänen, von Strategie, Führung und Governance, bis hin zur Physischen Sicherheit, wie sie in Abbildung 1 dargestellt sind. Die Domänen sind wiederum in weitere Sub-Domänen untergliedert. Jede Sub-Domäne besteht wiederum aus verschiedenen Fähigkeiten, die die Sub-Domänen unterstützen. Insgesamt werden 340 Fähigkeiten beschrieben. Sie werden jeweils für die drei Ressourcen Menschen, d.h. Ablauf- und Aufbau-Organisation (People), Prozesse (Processes) und Technologien (Products) analysiert. Dabei definiert man vier Architektursichten (von Konzeption bis Technische Architektur), die jeweils andere Blickwinkel auf die Domänen bieten und in ihrem Zusammenspiel jedoch kohärent und konsistent sein sollten. Im Rahmen von ESA- Assessments wird das Rahmenwerk als Referenz verwendet. Die jeweilige Ist-Ausprägung in den aufgezeigten Dimensionen und Fähigkeiten wird bei den Unternehmen analysiert. Die Analyse-Ergebnisse werden in verschiedenen Berichtsformaten manuell aufbereitet und zusammengestellt.Herausforderungen bei der Umsetzung von ESA

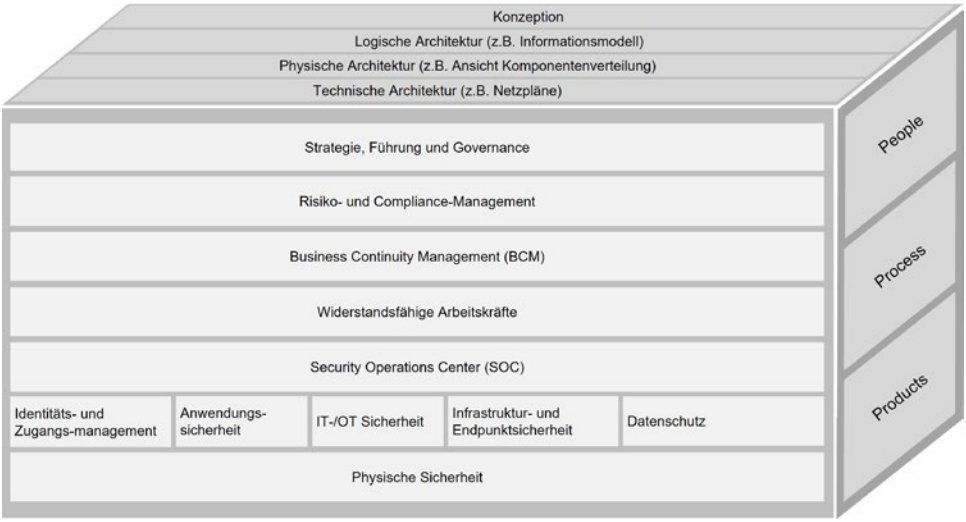

Abb. 1 Domänen und Dimensionen des ESA-Frameworks von PwC

Bisher wurden ESA-Assessments in großen Organisationen durchgeführt. Nun soll der Ansatz auch für KMU durchgeführt werden. Das dafür eingesetzte Framework ist umfangreich und detailliert, weshalb es insbesondere für Konzerne ausgelegt ist. Kleinere Unternehmen verfügen in der Regel nicht über die notwendigen Kapazitäten und das Know-how, um alle Aspekte dieser umfangreichen Assessments zu berücksichtigen. Hinzu kommt, dass inhaltlich viele der untersuchten Bereiche bei KMU vermeintlich gar keine Anwendung finden, da hier andere technische und juristische Anforderungen existieren. Daher ist es notwendig, das Assessment bzw. das ESA-Framework auf seine Anwendbarkeit für KMU zu bewerten und anzupassen.

Die ESA-Assessments unter Verwendung des ESA-Frameworks werden derzeit mittels Excel durchgeführt und dokumentiert. Das ESA-Framework besteht aus mehreren Domänen, die jeweils Sub-Domänen enthalten. Für jeden Kunden wird beim Scoping-Schritt ein individuelles Excel-Dokument erstellt, indem die Domänen des ESA-Frameworks entsprechend ausgewählt und das Framework individuell werden. Die Excel-Tabellen werden schnell unübersichtlich, Unwissende haben häufig Verständnisprobleme und verlieren den Überblick. Die Assessment-Auswertung wird ebenfalls in der Excel-Tabelle ergänzt und dokumentiert. Für den Kunden werden die ausgewerteten Beobachtungen und Empfehlungen mithilfe verschiedener anderer Tools (z.B. einer PowerPoint-Präsentation) visualisiert und berichtet. Ein Problem sind daher die Medienbrüche zwischen den einzelnen Phasen des Assessments. Werden Änderungen vorgenommen, so müssen diese manuell abgeändert und nachgezogen werden.

2 Verwandte Arbeiten

Die Vorteile von Ansätzen, die auf der Enterprise Architecture (EA) basieren, wurden in der Literatur bereits erläutert [Mc20]. Man erreicht damit eine ganzheitliche Sicht auf die Sicherheitsaspekte und involviert alle relevanten Unternehmensteile. Gleichzeitig werden auch strategische Ziele berücksichtigt. In dem erwähnten Artikel werden insgesamt 25 Security Frameworks untersucht, wobei sechs von ihnen auf EA basieren und jeweils komplette Organisationen betrachten: [Ho02], [Sc06], [RA08], [SLR09], [SCL09], [Je16].

Aus Sicht der Autoren der oben erwähnten Studie erfüllt jedoch keines dieser Ansätze die erforderlichen Anforderungen im Hinblick auf die Ganzheitlichkeit, wie sie EA zu liefern verspricht. Deshalb schlagen sie mit dem „Security Architecture Framework for Enterprises (SAFE)“ eine eigene Lösung vor, die genau wie unser Framework nach dem Design Science Research-Ansatz entwickelt wurde. Die Autoren beschreiben ihr Framework allerdings als sehr komplex und die bei der Entwicklung interviewten Teilnehmer stammen meistens aus großen Unternehmen. Der Einsatz dieses Frameworks im KMU-Kontext war nicht das Ziel der Forschung und wurde nicht ausreichend untersucht. Auch wurde bisher noch keine Fallstudie durchgeführt.

Andere Ansätze, die zwar nicht im Bereich der ESA anzusiedeln sind, praktisch jedoch ähnlich vorgehen (mit der Betrachtung von Schwerpunktbereichen und Fähigkeiten) basieren auf Reifegradmodellen. Einige davon fokussieren auf KMU und sind für uns deshalb besonders interessant: In 2014 wurde in [SR14] das „Information Security Focus Area Maturity Model (ISFAM)“ vorgestellt, dessen Assessments auf lediglich 161 Ja/Nein-Fragen basieren. Dieses Modell bietet dennoch eine ganzheitliche Sicht, bestehend aus 13 Schwerpunktbereichen (engl. Focus Areas), 51 Fähigkeiten (engl. Capabilities) und zwölf Reifegraden. Ähnlich wie in unserem ESA-Ansatz wurden diese verschiedenen Kategorien aus bekannten Security Frameworks abgeleitet (v.a. ISO 27000, CISSP [IS22] und aus dem IBM Security Framework [Bu13]). Zusätzlich wurden anhand der Abhängigkeiten von Fähigkeiten die passenden Reifegrade definiert.

In späteren Veröffentlichungen wurde das ISFAM-Modell aufgegriffen und erweitert. [Fr16] stellt mit dem Ansatz „Characterizing Organizations’ Information Security for SMEs (CHOISS)“ eine Möglichkeit vor, das ISFAM-Modell unternehmensspezifisch anzupassen. Bei den Assessments soll jeweils ein Schwerpunkt auf die elf organisatorischen Merkmale (engl. Organizational Characteristics, kurz OCs) des jeweiligen Unternehmens gesetzt werden. Dadurch wird die Analyse deutlich zielorientierter. In [Yi20] wurde diese Idee weiterentwickelt, indem vorab definierte OCs für Cluster von ähnlichen Organisationen bei der Reifegradbetrachtung eingesetzt werden. In der vorgestellten Studie wurde beispielsweise eine Gruppe von lokalen Unternehmen der Transport-, Logistik- und Verpackungsbranche untersucht.

Die Idee, dass man vor der Assessment-Durchführung die Analyse auf das jeweilige Unternehmen anpassen muss, liegt auch unserem ESA-Ansatz zugrunde. Denn als ersten Schritt

bei der Anwendung des Modells wird immer das Scoping durchgeführt (siehe Abschnitt 1.3), bei dem man die Assessment-Domains für die Kunden individuell anpasst.

Es gibt außerdem weitere Ansätze, die helfen sollen, IT-Security in KMU zu etablieren: Eine Übersicht der vielen relevanten Standards liefert z. B. die Studie der European Union Agency for Network and Information Security (ENISA) [Ma15]. Basierend auf dieser Übersicht wird auch eine Maßnahmenliste speziell für KMU abgeleitet. Weitere solche Listen von Empfehlungen für KMU finden sich in zahlreichen Leitlinien und Handbüchern, wie z.B. [Gl20] und [Sa18]. Die Autoren dieser Publikationen weisen jedoch explizit auf die Vorteile und die Notwendigkeit von systematischen und ganzheitlichen Ansätzen hin. In [THM07] findet sich ein solcher einfacher Ansatz, mit dem Unternehmen ausgehend von ihren Sicherheitszielen in einem vierstufigen Prozess entsprechende Aktionen identifizieren, implementieren und überwachen können. Und in [ET21] findet sich eine weitere Studie zu Security-Frameworks für KMU, in der 17 einheitliche Kontrollkategorien für vier Typen von KMU-Organisationen identifiziert werden. Davon ausgehend wird ein Prozess zur Definition von Maßnahmen definiert.

Allen diesen Vorschlägen fehlt jedoch die ganzheitliche Sicht wie sie bei ESA oder den oben erwähnten ISFAM-Ansätzen zu finden ist. Insbesondere bleiben größtenteils die strategischen Unternehmensziele sowie die Organisationsarchitektur unberücksichtigt.

3 Konzeption ESA-Assessment für KMU mit Werkzeugunterstützung

Im folgenden Kapitel beschreiben wir unser Vorgehen zur Lösung der in Abschnitt 1.3 dargelegten Problemstellung.

3.1 ESA-Konzept für KMU

Es gibt verschiedene Normen für Sicherheitskontrollen, wie z.B. die ISO/IEC 27001. Die Umsetzung der Maßnahmen aus dieser Norm stellt für KMU jedoch oft eine Herausforderung dar. Daher gibt es auch speziell für KMU entwickelte Rahmenwerke. Dazu zählen z.B. CISIS12 [IT22] und VdS 10000 [Vd22]. Um das ESA-Framework für KMU anzupassen und ein entsprechendes Assessment durchführen zu können, war es notwendig, relevante Anforderungen hinsichtlich der Informationssicherheit zu identifizieren. Dafür wurden die bereits genannten Sicherheitsstandards ISO 27001, CISIS12 und VdS 10000 näher betrachtet, um herauszufinden, welche Anforderungen auf KMU zutreffen. Aus diesem Vergleich wurden die in den Rahmenbedingungen enthaltenen, identifizierten Anforderungen in neu zusammen gesetzten Domänen aggregiert. Um anschließend den Abdeckungsgrad der unterschiedlichen Rahmenbedingungen mit dem aktuellen ESA-Framework im

nächsten Schritt zu identifizieren und die entsprechende Anpassung vornehmen zu können, wurden die Anforderungen entsprechend der drei Ebenen des ESA-Frameworks als strategisch, taktisch/betrieblich und technisch klassifiziert. Aus dem Vergleich haben sich insgesamt 28 Anforderungen ergeben, die gleich zu gewichten und als Muss-Anforderungen zu betrachten waren. Ein Auszug der zusammengestellten Anforderungen ist in der Tabelle 1 zu sehen. Die Tabelle zeigt außerdem die Gegenüberstellung der Sicherheitsstandards und die Abschnitte, in denen die jeweiligen Anforderungen zu finden sind.

ID	ESA-Sub-Domäne	ISO 27001	CISIS12	VdS 10000
R11	Kontinuierliche Verbesserung	Kapitel 10	N/A	N/A
R12	Business Continuity Management	A.17	N/A	Kapitel 17
R13	Steuerung von Dienstleistern/ Lieferanten	A.15	N/A	Kapitel 4
R14	Umgang mit personenbezogenen Daten	A.18	N/A	N/A
R15	Identifikation von kritischen Anwendun-gen	A.8	Schritt 6	Kapitel 9 Kapitel 10
R16	Softwaresicherheit - Erkennung vonSchadsoftware	A.12	N/A	Kapitel 10
R17	Umgang mit Informationssicherheits-vorfällen	A.16	Schritt 5	Kapitel 18
R18	Schwachstellenmanagement	A.12	N/A	Kapitel 10

Tab. 1 Übersicht: Mapping der Anforderungen der ISMS-Rahmenwerke (Auszug)

Aus dem Vergleich der Frameworks geht hervor, dass die Anforderungen der einzelnen Frameworks sich in den anderen widerspiegeln. Da CISIS12 mehr einen Prozess zum Aufbau eines ISMS darstellt, ist die Gegenüberstellung mit den einzelnen Rahmenbedingungen nicht vollständig. Anforderungen bezüglich des Datenschutzes (zum Schutz personenbezogener Daten) werden ausschließlich in der ISO 27001 beschrieben. Diese wurden dennoch den Muss-Anforderungen zugeordnet.

Die Anpassung des ESA-Frameworks erfolgte auf Grundlage der Gegenüberstellung der Rahmenbedingungen und der daraus aufgestellten Anforderungen. Für die Anpassung wurden die identifizierten Anforderungen aus der ISO 27001, CISIS12 und VdS 10000 mit dem vorhandenen ESA-Framework verglichen. Zur Schaffung eines Überblicks des Abdeckungsgrades der Anforderungen aus der ISO 27001, CISIS12 und der VdS 10000 diente ein Mapping der einzelnen Frameworks auf das ESA-Framework. Das ESA-Framework ist in einer detaillierten Excel-Datei dokumentiert. Strukturiert ist das Framework in Form einer Tabelle, in der die einzelnen Domänen, Subdomänen und Capabilities die einzelnen Spalten bilden. Die enthaltenen Domänen sind in der Abbildung 1 aufgeführt. Diese Domänen werden wiederum unterteilt in Sub-Domänen, die von mehreren Fähigkeiten unterstützt werden. Das Mapping erfolgte somit in der Excel-Tabelle des ESA-Framework. Für jedes gegenübergestellte Framework wurde in der Excel-Tabelle eine neue Spalte eingefügt, in der die passenden Controls den ESA-Fähigkeiten gegenübergestellt

und so gemappt wurden. Dabei wurden die einzelnen Controls der Frameworks (sowohl für die ISO 27001 als auch für die VdS 10000) näher betrachtet und so die Inhalte mit den ESA-Fähigkeiten verglichen. Damit erfolgte die Prüfung der Konformität der einzelnen Frameworks mit dem ESA-Framework. Das Mapping bildete die Grundlage zur Anpassung des ESA-Frameworks für KMU. Anhand des Mappings und der ausgearbeiteten Anforderungen wurden die Fähigkeiten des ESA-Frameworks mit den Schlüsselwörtern Muss, Soll und Kann wie folgt priorisiert. Muss: Diese Anforderungen sind Mindestanforderungen und somit als verpflichtend anzusehen und müssen zwingend erfüllt werden. Die Anforderungen sind in mindestens zwei der verglichenen Rahmenbedingungen enthalten. Soll: Die Umsetzung dieser Anforderungen wird empfohlen, ist jedoch nicht zwingend notwendig. Sie dienen der Erweiterung der Mindestanforderungen und sind in mindestens einem der verglichenen Rahmen-bedingungen enthalten. Kann: Optional umzusetzende Maßnahmen werden mit dem Schlüsselwort „kann“ gekennzeichnet. Diese Anforderungen sind wünschenswert, jedoch von untergeordneter Bedeutung und in der Detailtiefe zu spezifisch für KMU. Diese Anforderungen sind in maximal einem der verglichenen Rahmenbedingungen aufgeführt.

Die Priorisierung erfolgte entlang der einzelnen Fähigkeiten. Die in Tabelle 1 aufgeführten Anforderungen wurden dabei als Muss-Anforderungen aufgenommen. Zur Priorisierung der Sub-Domänen wurden die Summen der Muss-Fähigkeiten gebildet. Aus der Summe der Muss-Fähigkeiten und der Sub-Domänen ergibt sich in Tabelle 2 die aufgezeigte Priorisierung der Domänen.

Damit wurde das ESA-Framework von 340 auf 100 Fähigkeiten gekürzt. Anhand der Priorisierung und des Mappings entfallen die Domänen Security Orchestration und IT/OT-Security für das KMU-Framework. Der Fokus sollte auf die zuvor priorisierten Muss-Domänen gelegt werden. Diese Domänen beinhalten grundlegende Fähigkeiten, wie den Aufbau einer Organisation, die Definition einer Sicherheitsstrategie, die Festlegung von Zielen und den Aufbau eines Informationssicherheits-Teams. Zudem sollte auch Wert auf Awareness-Maßnahmen und die Sensibilisierung von Mitarbeitenden gelegt werden. Auch die Sub-Domänen Asset Management, Business Continuity Management (BCM), Schwachstellenmanagement, Sicherheitsvorfälle und Physische Sicherheit sind wesentliche Bestandteile des ESA-Frameworks, die auch in den verglichenen Frameworks verankert sind. Sie gelten somit als Mindestanforderungen und haben auch für KMU hohe Relevanz in der Gewährleistung der Unternehmenssicherheit.

Nr.	Domäne	Priorität	Sub-Domäne (muss)	Capabilities (muss)
1.1	Security Strategy & Leadership	muss	3	6
1.2	Risk & Compliance Management	muss	4	21
1.3	Security Resilient Architecture	muss	1	7
1.4	Resilient Workforce	muss	2	5
2.1	Cyber Defence	muss	3	17

2.2	Security Orchestration	kann	0	0
3.1	Identity & Access Management	muss	4	13
3.2	Infrastructure & Endpoint Security	muss	3	8
3.3	Application Security	soll	1	2
3.4	Data Protection & Privacy	muss	3	12
3.5	IT-OT Security	kann	0	0
3.6	Physical Security	muss	2	9
		Summe:	26	100

Tab. 2 Priorisierung der Anforderungen

Aus dem Mapping der Standards mit dem ESA-Framework geht hervor, dass alle Bereiche der ISO 27001 und der VdS 10000 weitestgehend umfassend vom ESA-Framework abgedeckt werden. Da CISIS12 eher einen Prozess als Anforderungen beschreibt, sind nicht alle Schritte zuordenbar. Die DSGVO beschreibt umfassend, wie mit personenbezogenen Daten umzugehen ist, wodurch auch nur ein kleiner Teil der Verordnung im Framework vorkommt.

3.2 Bewertung des ESA-Konzeptes für KMU

Zur Bewertung der ausgearbeiteten Anforderungen hinsichtlich der IT-Sicherheit in KMU und des angepassten ESA-Frameworks wurden zwei unterschiedliche praktische Anwendungsfälle betrachtet. Im ersten Fall wurde ein ESA-Assessment auf Grundlage des angepassten ESA-Frameworks mit einem mittelständischen Unternehmen durchgeführt. Zur Identifizierung des Ist-Zustands und somit der aktuellen Reifegrade der Unternehmensfähigkeiten im Bereich Informationssicherheit wurden dabei zwei Interviews mit dem Kunden durchgeführt. Im ersten Interview lag der Fokus auf der Analyse und der Bewertung der internen Prozesse. Dabei wurden Domänen wie Informationssicherheitsorganisation, Dienstleistersteuerung, Umsetzung von Awareness-Maßnahmen, Datensicherheit, Physische Sicherheit, Gebäude- und Endgerätesicherheit und Outsourcing betrachtet. Das zweite Interview wurde mit einem der IT-Dienstleister des Unternehmens durchgeführt und fokussierte sich somit auf die IT-Prozesse, darunter Domänen wie Fernzugriff, Wartung und Monitoring. Auf Basis der Beobachtungen in den beiden durchgeführten Interviews wurde eine Reifegradbewertung erstellt und visualisiert (vgl. Abbildung 2). Diese bildete die Grundlage für die Definition entsprechender Handlungsempfehlungen je Bereich, in denen das Unternehmen Optimierungsbedarf aufwies. Diese dienen generell dazu, die Reifegrade zu erhöhen und die Zielsicherheitsarchitektur aufzubauen.

Abb. 2 Übersicht der ermittelten Reifegrade im Anwendungsbeispiel

Im zweiten Anwendungsfall wurde ein Interview mit einem kleinen Unternehmen über die aktuelle Lage der IT-Sicherheit des Unternehmens durchgeführt, um so den Bedarf an Informationssicherheitsmaßnahmen zu identifizieren. Bei den Interviews wurde schnell klar, dass das mittelständische Unternehmen einen Basisschutz bereits eingerichtet hatte. Zu den Domänen Asset- und Krisen-Management (BCM), Security Training & Education, Identity & Account Management, Incident Management und Physical Security hatte das Unternehmen bereits Maßnahmen umgesetzt. Auch interne Awareness-Maßnahmen werden regelmäßig durchgeführt. Maßnahmen in der Domäne Schwachstellen-Management waren jedoch nicht umfassend umgesetzt. Regelmäßiges Monitoring, das Testen bzw. Durchführen von Übungen zu den umgesetzten Maßnahmen werden insbesondere im Krisen- und Schwachstellenmanagement vernachlässigt. Die stichprobenartige Kontrolle von Dokumenten und Leistungen findet nicht statt.

Im Vergleich zum ersten Anwendungsfall handelt es sich beim zweiten Fall um ein wesentlich kleineres Unternehmen mit weniger Ressourcen. Das kleine Unternehmen hat sich mit dem Thema IT-Sicherheit nicht umfassend beschäftigt und somit Maßnahmen bezüglich IT-Sicherheit und Datenschutz nicht bedacht und vernachlässigt. Das Thema IT-Sicherheit hat bisher keine große Rolle gespielt und wurde als nicht notwendig empfunden. Ein Basisschutz war daher nicht vorhanden. Den Mitarbeitenden war jedoch bewusst, dass Maßnahmen zur Gewährleistung der Unternehmenswerte, insbesondere durch die steigenden Cyber-Angriffe, notwendig sind.

Bei der Betrachtung der zwei Anwendungsfälle hat sich ergeben, dass die Unternehmen generell viel auf Vertrauen setzen, das die Basis für die interne Kommunikation und Zusammenarbeit bildet. Die Mitarbeitenden verbindet eine langjährige Zusammenarbeit, wodurch ein gegenseitiges Vertrauen aufgebaut wurde. Da die Unternehmen mit unter- schiedlichen Dienstleistern zusammenarbeiten, war die Domäne Third Party Management in den

Interviews besonders wichtig. Die Unternehmen legen Wert darauf, dass ihre Dienstleister gewisse Sicherheitsmaßnahmen umsetzen und vertrauen ihnen in dieser Hinsicht durch die jahrelange Zusammenarbeit. Dadurch lässt sich schlussfolgern, dass das Sicherheitsniveau der Dienstleister vorausgesetzt wird. Es wird davon ausgegangen, dass diese professionell mit den Unternehmensdaten umgehen. Entsprechende Verträge und Geheimhaltungsvereinbarungen wurden dennoch mit den Dienstleistern abgeschlossen.

Da in KMU oft ein familiäres Zusammenarbeiten vorzufinden ist, werden Kontrollen bzw. interne Audits und das Monitoring vernachlässigt. Sowohl zwischen den Mitarbeitenden untereinander als auch zu den langjährigen Dienstleistern wird auf Vertrauen gesetzt, und Monitoring, Stichproben, Tests und regelmäßige interne Audits als nicht notwendig empfunden.

3.3 Evaluation eines Werkzeugeinsatzes für ESA

Der ESA-Prozess stellt eine praxiserprobte Vorgehensweise zur Bewertung der Sicherheitsarchitektur eines Unternehmens dar. Durch die Analyse des Prozesses und die Erfahrungen aus der Praxis wurde deutlich, dass eine werkzeugunterstützende Prozessoptimierung mithilfe des Einsatzes eines Enterprise Architecture-Tools hilfreich wäre. Eine geeignete Werkzeugunterstützung würde Vorteile bieten, vor allem die Verbesserung der Daten- und Dokumentenverwaltung, Reduzierung des Pflegeaufwands sowie Effizienzsteigerung. Zur Optimierung des ESA-Prozesses soll daher ein Werkzeug zur Abbildung der Referenzarchitekturen eingesetzt werden. Dafür wurde eine Anforderungsanalyse durchgeführt. Die Basis zur Ermittlung der Anforderungen an das Tool bildete der ESA-Prozess. Die einzelnen Prozessschritte von ESA sollten im Tool abgebildet werden und damit das aktuelle Problem der vielen Medienbrüche beheben. Zudem haben sich beim praktischen Einsatz und durch den internen Austausch weitere Anforderungen ergeben. Insgesamt wurden 34 Anforderungen aufgestellt. Die Anforderungen wurden hinsichtlich ihrer Umsetzung analog dem Schablonenprinzip aus [Kl16] anhand der Schlüsselwörter Muss, Soll und Wird priorisiert. Muss-Anforderungen: Diese Anforderungen sind verpflichtend umzusetzen und sind zwingend zu erfüllen. Sie beschreiben die Mindestanforderungen an das Tool. Soll-Anforderungen: Die Soll-Anforderungen sind nicht zwingend notwendig, stellen jedoch einen Wunsch dar. Die Umsetzung wäre daher vorteilhaft und würde den Basisumfang erweitern. Wird-Anforderungen: Diese Anforderungen sind optional und haben eine untergeordnete Bedeutung. Die Realisierung dieser Anforderungen war nicht Bestandteil dieser Studie. Vielmehr dienen die Anforderungen zur zukünftigen Weiterentwicklung des Prozesses und somit auch des Tools.

Die Anforderungen wurden zudem in funktionale und nicht-funktionale Anforderungen (NF) unterteilt. Die funktionalen Anforderungen wurden untergliedert in allgemeine Anforderungen (A), Anforderungen hinsichtlich der Visualisierung der Ergebnisse (V) und zur Assessment-Durchführung (AS). Zu den allgemeinen Anforderungen zählen z. B. die Excel-Import- und Export-Funktion, die Taskverwaltung oder die Verknüpfung mit ande-

ren Tools. Das Tool sollte unterschiedliche Visualisierungsmöglichkeiten bieten, um die Ergebnisse entsprechend darstellen zu können. Die Assessment-Durchführung umfasst Anforderungen wie das Domain Scoping, Erstellen und Einpflegen von Kontrollfragen, die Durchführung von Interviews und das Dokumentieren von Handlungsempfehlungen. Ein Auszug der aufgestellten Anforderungen ist in Tabelle 3 dargestellt.

ID	Anforderung	Priorität	Erfüllungsgrad
..	..	..	..
A06	Export- und Importfunktion von Excel-Tabellen	Muss	vollständig
V11	Visualisierung der verschiedenen Ebenen	Muss	ausreichend
V14	Transformations-Roadmap	Muss	teilweise
V15	Dashboard (Benchmarking)	Soll, Wird	ausreichend
AS16	Domain Scoping	Muss	teilweise
NF25	Pflegeaufwand	Muss	ausreichend
NF30	Bedienbarkeit	Muss	vollständig

Tab. 3 Anforderungen an den Tooleinsatz (Auszug)

3.4 Umsetzung des ESA-Werkzeugkonzepts

Es gibt verschiedene Tools, die zur Abbildung von Referenzarchitekturen genutzt werden können. Unter anderem sind Microsoft-Produkte wie Excel, PowerPoint und Visio zur Darstellung und Dokumentation von Daten im Einsatz. Es hat sich jedoch herausgestellt, dass die Nutzung dieser Tools einen hohen Pflegeaufwand aufweist und Medienbrüche unvermeidbar sind, um alle notwendigen ESA-Prozessschritte zu durchlaufen und abzubilden. Daher sollten die in Tabelle 3 ausgearbeiteten Anforderungen in einem einzigen Tool abgebildet werden. Dafür wurde das Tool LeanIX [Le22] ausgewählt, da es bereits für EA bei PwC eingesetzt wird. Die Evaluation der Einsatzfähigkeit anderer Tools war in diesem ersten Schritt nicht Teil der Studie. LeanIX ist ein cloudbasiertes Enterprise Architecture Tool zum Planen, Analysieren und Überwachen des IT-Portfolios. Eins der Hauptprodukte von LeanIX ist das Enterprise Architecture Management. Damit lassen sich Architekturen abbilden und eine Übersicht der Applikationen, IT-Komponenten und Business Capabilities schaffen.

Um den Tool-Einsatz für ESA-Assessments zu bewerten, wurden die Prozessschritte im Tool abgebildet und Möglichkeiten gesucht, wie die einzelnen Schritte bzw. die Anforderungen damit abgedeckt werden könnten. Durch den Einsatz von LeanIX soll die Verwaltung und die Durchführung der Assessments vereinfacht werden, indem Medienbrüche verhindert und die ESA-Prozessschritte abgebildet werden. Insbesondere die Berichterstattung und damit das Generieren von Reports und anderen Darstellungen soll damit automatisiert erfolgen. Die ausgearbeiteten Anforderungen wurden in LeanIX abgebildet und

deren Umsetzung anhand der Kriterien: vollständig erfüllt, ausreichend erfüllt, teilweise erfüllt, nicht ausreichend erfüllt und nicht erfüllt bewertet.

Um das Tool in der Praxis zu testen, wurde das KMU-Assessment in LeanIX abgebildet und die Umsetzung der Anforderungen an der Durchführung eines Assessments analysiert. Dafür wurden die LeanIX-Standardfunktionen betrachtet. Ein entsprechender Workspace wurde für die Studie zur Verfügung gestellt. Das angepasste Framework bzw. die relevanten Fähigkeiten wurden mithilfe des Excel-Imports in LeanIX eingefügt und in Beziehung gesetzt. Für die Kontrollfragen, die aus den Fähigkeiten bei der Assessment-Durchführung abgeleitet werden, wurde die Survey-Funktion verwendet.

Es ist festzuhalten, dass die Funktionalitäten, die LeanIX anbietet, für die Darstellung der Ergebnisse und somit zum Generieren von Reports gut geeignet sind. Für die Durchführung der Assessments bietet sich die Survey-Funktion gut an. Die eingetragenen Antworten können jederzeit abgeändert und ergänzt werden. Wenn mehrere Interviews mit unterschiedlichen Stakeholdern geführt werden, können mehrere Survey Runs die Antworten voneinander trennen. Von den 34 aufgestellten Anforderungen wurden nur vier Muss-Anforderungen nur teilweise erfüllt und jeweils eine Soll-Anforderung nicht ausreichend und nicht erfüllt.

Die teilweise erfüllten Anforderungen könnten bei der Weiterentwicklung von LeanIX berücksichtigt werden. Es werden mit Unterstützung des Herstellers aktuell Möglichkeiten gesucht, diese Anforderungen bestmöglich abzubilden. Die Umsetzung der Anforderungen bezüglich der Transformation Roadmap kann so belassen werden. In der Roadmap wird die häufig verwendete 3-Phasen-Planung nicht abgebildet. Die Darstellung der Transformation Items in den vier bestehenden Kategorien reicht jedoch aus. Für das Domain Scoping bedarf es einer Datenbank, die aktuell nicht integriert ist. Dafür kann jedoch eine alternative Möglichkeit bei der Erweiterung des Tools gefunden werden. Der Aufwand für das Scoping in der Excel-Tabelle würde sich auch im Tool widerspiegeln. Das Problem bildet hierbei die zusätzliche Verwaltung der Excel-Dateien in einem vorgesehenen Ablageort. Die aktuelle Umsetzung ist insbesondere für Assessments mit KMU jedoch ausreichend. Die Erfüllung der Anforderung bezüglich der Übersichtlichkeit der Daten ist in LeanIX durch die verschiedenen Fact Sheets im Inventory zunächst etwas gewöhnungsbedürftig und bedarf einer kurzen Einarbeitung. Die Filterfunktion erleichtert jedoch das Verwalten der Fact Sheets und wird somit akzeptiert. Die nicht oder nicht ausreichend erfüllten Anforderungen gehören zu den Soll-Anforderungen. Somit hat die Umsetzung dieser Anforderung keine hohe Priorität. Zukünftig sollte ggf. auch für diese Anforderungen eine angemessene Lösung gefunden werden. Auch die Umsetzung bzw. Integration einer Datenbank sollte angedacht werden.

Schlussfolgernd ist festzuhalten, dass LeanIX für ESA und für die Assessments sowohl bei KMU als auch domänenspezifisch einsatzfähig ist. Das Tool beinhaltet essenzielle Funktionalitäten, die den ESA-Prozess optimieren. Ein geringer Restpflegeaufwand bleibt durch die eingeschränkte Durchführung des Domain Scopings und durch das Importieren des ESA-Frameworks bestehen.

4 Evaluation, Zusammenfassung und Ausblick

In diesem Artikel wurde die Anwendbarkeit von ESA für KMU betrachtet. Ausgehend von bekannten Informationssicherheits-Standards, wie etwa der Norm ISO/IEC 27001, der VdS-Richtlinie 10000 und CISIS12, wurde ein angepasstes ESA-Framework für die Durchführung von Assessments für KMU erstellt. Dazu wurden diese Standards miteinander verglichen und Anforderungen für KMU zusammengestellt sowie mit dem vorhandenen ESA-Framework von PwC gemappt. Damit wurde das ESA Framework von 340 Fähigkeiten auf 100 Fähigkeiten für KMU angepasst.

Auch wenn das neue Framework erst in zwei Kundenprojekten zum Einsatz kam, belegen die gewonnenen Erkenntnisse die grundsätzliche Einsetzbarkeit des angepassten ESA-Frameworks und somit die generelle Anwendbarkeit von ESA für KMU. Das angepasste Framework wird bei PwC auch zukünftig die Basis für Assessments mit KMU bilden und nach neuen Erkenntnissen weiter evaluiert und optimiert werden.

Schlussfolgernd ist festzuhalten, dass das angepasste Framework ein guter Leitfaden für die Assessments mit KMU darstellt. Im Rahmen weiterer Projekte muss der Fokus generell auf den priorisierten Sub-Domänen liegen. Die Domänen wie BCM, Schwachstellen- und Vorfalls-Management sollten näher betrachtet werden, insbesondere das Durchführen von Testdurchläufen und Simulationen. Dafür sind die entsprechenden Fähigkeiten der zugehörigen Sub-Domänen priorisiert worden. Das Framework beinhaltet die notwendigen Domänen, die auch in der Norm ISO/IEC 27001, in der VdS-Richtlinie 10000 und auch in CISIS12 aufgezählt werden, und deckt somit die notwendigen Domänen ab, ohne KMU mit der Ausführlichkeit und Detailtiefe des bisherigen ESA-Frameworks zu überfordern. Nach den bisherigen Erfahrungen sind die nun angepasste Tiefe der Sub-Domänen sowie die Anzahl der Fähigkeiten ausreichend, um KMU im Bereich Informationssicherheit zu bewerten.

Der bisherige ESA-Prozess erforderte mehrere verschiedene Tools und war aufwändig aufgrund von Medienbrüchen. Daher wurden Anforderungen für die Prozessoptimierung und den Werkzeugeinsatz für ESA-Assessments aufgestellt und in einem Tool exemplarisch umgesetzt und evaluiert. Für die Evaluation wurden die Anforderungen im Tool LeanIX abgebildet und mittels Praxisbeispielen bewertet. Die Umsetzung der Anforderungen im Tool LeanIX hat gezeigt, dass das Tool für ESA gut geeignet ist. Insbesondere für das Durchführen von Assessments mit KMU sind die aktuell vorhandenen Funktionalitäten ausreichend. Es hat sich herausgestellt, dass das Tool die Assessment-Durchführung unterstützen kann, die Dokumentation und Verwaltung sowohl vereinfacht als auch visualisiert und damit Medienbrüche reduziert.

In diesem Zusammenhang hat sich zudem herausgestellt, dass das vorhandene ESA- Framework (für große Unternehmen) Optimierungspotenzial aufweist. Die Anforderungen der Norm ISO/IEC 27001 und der VdS-Richtlinie 10000 werden in Zukunft mit aufgenommen, um eine Überleitung auf die einzelnen Standards vollständig zu ermöglichen. Zudem kann in zukünftigen Studien die Konformität der beiden ESA-Frameworks mit

weiteren Standards geprüft werden. Hierfür könnten z.B. das BSI IT-Grundschutz- und das NIST-Framework herangezogen werden.

Generell wurde bei der Anwendung erkannt, dass es außerdem empfehlenswert wäre, vorab ein Self-Assessment für Kunden zu erstellen und zugänglich zu machen. Dadurch könnten Kunden eine Selbsteinschätzung durchführen. So könnten Vorabgespräche vereinfacht werden und man erhielte die notwendigen Informationen, um basierend darauf ein kundenspezifisches Assessment zu erstellen und durchzuführen. Bezüglich des Tool-Einsatzes könnte die Umsetzung der identifizierten Soll- und Kann-Anforderungen in Betracht gezogen und das Tool ausgehend von den Anforderungen erweitert werden. Künftige Studien könnten sich daher damit befassen, wie die nicht oder nur teilweise erfüllten Anforderungen umgesetzt werden könnten.

Literaturverzeichnis

[BHM20] Brocke, Jan vom; Hevner, Alan; Maedche, Alexander: Introduction to Design Science Research. In: Design Science Research. Cases. Springer International Publishing, S. 1–13, 09 2020.

[Bu13] Buecker, Axel et. al: Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security. IBM Redbooks, 2013.

[ET21] ETSI: CYBER; Cybersecurity for SMEs; Part 1: Cybersecurity Standardization Essentials. Bericht ETSI TR 103 787-1, ETSI, 2021.

[Fr16] Frederik Mijnhardt et. al: Organizational Characteristics Influencing SME Information Security Maturity. Journal of Computer Information Systems, 56(2):106–115, 2016.

[Gl20] Global Cyber Alliance: GCA Cybersecurity Toolkit for Small Business Handbook. https://gcatoolkit.org/wp-content/uploads/2021/06/GCA-Toolkit-Handbook.pdf, 2020.

[Ho02] Ho, Latifa: Security Management Framework: A New Approach based on John Zachman's Framework for Enterprise Architecture. Bericht, GIAC Certifications, 2002.

[IS22] ISC2: CISSP website. https://www.isc2.org/Certifications/CISSP#, Stand: 3.5.2022.

[ISO13] ISO: INFORMATION SECURITY MANAGEMENT. Standard, International Organization for Standardization, Geneva, CH, 2013.

[IT22] IT-Sicherheitscluster e.V.: CISIS12. https://cisis12.de/en/, Stand 23.2.2022.

[Je16] Jeganathan, Seetharaman: Enterprise Security Architecure. ISSA Journal, 14(12):14–21, 2016.

[Kl16] Kluge, Roland: Schablonen für alle Fälle. https://www.sophist.de/fileadmin/user_ upload/Bilder_zu_Seiten/Publikationen/Wissen_for_free/MASTeR_Broschuere_3- Auflage_interaktiv.pdf, 2016. Stand: 1.3.2022.

[Le22] LeanIX: Enterprise Architecture Management (EAM). https://www.leanix.net/en/ products/enterprise-architecture-management, 2022. Stand 1.4.2022.

[Ma15] Manso, Clara Galan; Rekleitis, Evangelos; Papazafeiropoulos, Fotis; Maritsas, Vasilios: Information security and privacy standards for SMEs, 2015.

[Mc20] McClintock, Michelle et. al: Enterprise Security Architecture: Mythology or Methodology? In: Proceedings of the 22nd Inter- national Conference on Enterprise Information Systems - Volume 2: ICEIS, INSTICC, SciTePress, S. 679–689, 2020.

[RA08] Rachamadugu, Vijaykumar; Anderson, John A.: Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure. 2008 IEEE International Conference on Services Computing, 2:351–358, 2008.

[Sa18] Sage, Ola: Very Small Business Should Use the NIST Cybersecurity Framework. Bericht, CyberRx, 2018.

[Sc06] Scholtz, Tom: Structure and Content of an Enterprise Information Security Architecture. Bericht, Gartner, Inc., 2006.

[SCL09] Sherwood, John; Clark, Andrew; Lynas, David: Enterprise security architecture. Bericht, SABSA White Paper, 2009.

[SLR09] Shen, Yi; Lin, Frank; Rohm, C. E. Tapie: A Framework for Enterprise Security Architecture and Its Application in Information Security Incident Management. Communications of the IIMA, 9:2, 2009.

[SR14] Spruit, Marco René; Röling, M.W.M.: Isfam: the Information Security Focus Area Maturity Model. In: ECIS. 2014.

[Th09] The Open Group: TOGAF 9 - The Open Group Architecture Framework Version 9, 2009.

[THM07] Tawileh, Anas; Hilton, Jeremy; McIntosh, Stephen: Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. In: ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference. Vieweg, Wiesbaden, S. 331–339, 2007.

[Vd22] VdS Schadenverhütung GmbH: VdS 10000 - Informations-Sicherheit für KMU. https://vds.de/kompetenzen/cyber-security/vds-richtlinien/anforderungsrichtlinien-/-leitfaeden/vds-10000-informations-sicherheit-fuer-kmu, 2022. Stand: 23.2.2022.

[Yi20] Yigit Ozkan, B. et. al: Modelling adaptive information security for SMEs in a cluster. Journal of Intellectual Capital, 21(2):235–256, 2020.