



Projekt CONTAIN – Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten

Teilvorhaben:
Effiziente Reaktion auf IT-Sicherheitsvorfälle
durch Standardisierung und Best Practices

Schlussbericht

Version 1.0

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung



Bundesministerium
Finanzen

SIFO.de



Förderkennzeichen	13N16587
Vorhaben	Effiziente Reaktion auf IT-Sicherheitsvorfälle durch Standardisierung und Best Practices
Laufzeit d. Vorhabens	01.03.2023 – 30.08.2025
Berichtszeitraum	01.03.2023 – 30.08.2025
Datum	23.02.2026
<p><i>Das Gesamtprojekt CONTAIN wird auf Österreichischer Seite innerhalb des Sicherheitsforschungs-Förderprogramms KIRAS durch das Bundesministerium für Finanzen (BMF) gefördert (Projektnummer: FO999902707). Auf deutscher Seite wird das Projekt innerhalb des Programms Forschung für die zivile Sicherheit vom Bundesministerium für Bildung und Forschung (BMBF) gefördert (FNZ: 13N16581-13N1658).</i></p>	

Kontaktinformationen		
Name	Organisation	E-Mail
Sebastian Hauschke-Kuhn	Verband der Elektrotechnik, Elektronik und Informationstechnik VDE e.V. - DKE	sebastian.hauschke-kuhn@vde.com

Inhaltsverzeichnis

1.	Eingehende Darstellung (Teil II).....	4
1.1.	Einleitung	4
1.2.	Ausgangslage und Zielsetzung des Teilvorhabens	4
1.3.	Durchführung des Vorhabens	5
1.3.1.	AP 2 – Szenaranalyse (Teil-AP 2.1 und 2.2)	5
1.3.1.1.	Teil-AP 2.1: Identifikation und Beschreibung relevanter Szenarien	5
1.3.1.2.	Teil-AP 2.2: Analyse von Abläufen und Bedarf an Instrumenten zur Erhöhung des Reifegrads	6
1.3.2.	AP 3 – CONTAIN-Rahmenwerk (Teil-AP 3.4 und 3.5)	7
1.3.2.1.	Teil-AP 3.4: Referenzmodellierung und Querschnittsthemen.....	7
1.3.2.2.	Teil-AP 3.5: Glossar und Anwendungsleitfaden	8
1.3.3.	AP 4 – Effiziente Reaktionen durch Anforderungen an die Informationssicherheit (Teil-AP 4.8)	8
1.3.4.	AP 5 – Demonstration und Evaluation (Teil-AP 5.3)	10
1.3.5.	AP 6 – Dissemination (Teil-AP 6.1).....	10
1.4.	Vergleich mit der ursprünglichen Planung.....	11
1.4.1.	Arbeitspakete und inhaltliche Umsetzung	11
1.4.2.	Zeitliche Planung und Umsetzung eines Framework-Distributionsaspekts	12
1.4.3.	Abweichungen bei Dienstreisen und Präsenzterminen	12
1.4.4.	Auswirkungen auf Zielerreichung und Qualität.....	12
1.4.5.	Kostenneutrale Verlängerung der Projektlaufzeit.....	13
1.5.	Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten	14
1.5.1.	Einordnung des zahlenmäßigen Nachweises.....	14
1.6.	Ergebnisse, Nutzen und Anschlussfähigkeit	15
1.7.	Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens	16
1.8.	Erfolgte oder geplante Veröffentlichungen	17
1.9.	Wesentliche Ergebnisse	17
1.10.	Quellenverzeichnis	18

1. Eingehende Darstellung (Teil II)

1.1. Einleitung

Das Verbundprojekt CONTAIN („Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten“) adressiert die steigende Bedrohung durch Cybervorfälle, insbesondere Ransomware, und deren Auswirkungen auf Unternehmen und Lieferketten. Der VDE e. V. leistete im Projekt CONTAIN mit dem Teilvorhaben „Effiziente Reaktion auf IT-Sicherheitsvorfälle durch Standardisierung und Best Practices“ Beiträge mit dem Schwerpunkt auf Normung, Standardisierung, Wissensaufbereitung und Wissenstransfer.

Das Teilvorhaben des VDE e. V. wurde im BMBF-Programm „Forschung für die zivile Sicherheit (2018–2023)“ innerhalb der Fördermaßnahme „Zivile Sicherheit – Bedrohungen aus dem digitalen Raum“ durchgeführt.

Der vorliegende ausführliche Bericht beschreibt die im Teilvorhaben des VDE durchgeführten Arbeiten, die erzielten Ergebnisse sowie den Vergleich zwischen der ursprünglichen Planung gemäß Teilvorhabenbeschreibung und der tatsächlichen Umsetzung. Die Arbeiten des VDE erfolgten entlang der im Projekt definierten Arbeitspakete und wurden projektbegleitend in das Konsortium eingebracht.

1.2. Ausgangslage und Zielsetzung des Teilvorhabens

Ausgangspunkt des Teilvorhabens war die Feststellung, dass insbesondere kleine und mittlere Unternehmen (KMU) häufig nicht über ausreichende personelle, organisatorische und fachliche Ressourcen verfügen, um IT-Sicherheitsvorfälle strukturiert vorzubereiten und zu bewältigen. Normen und Standards wie die ISO/IEC-27000-Reihe oder die IEC-62443-Reihe definieren zwar Anforderungen an die Informationssicherheit, lassen jedoch häufig offen, wie diese Anforderungen in der Praxis umzusetzen sind.

Ziel des Teilvorhabens des VDE war es daher, durch Analyse relevanter Normen und Standards, durch Einbindung von Experten aus Normungs- und Standardisierungsgremien sowie durch die Auswertung praktischer Erfahrungen aus dem CERT@VDE-Netzwerk einen Beitrag zur Schließung dieser Lücke zu leisten. Die gewonnenen Erkenntnisse sollten in ein praxisorientiertes Rahmenwerk einfließen und Unternehmen bei der effektiven und effizienten Reaktion auf IT-Sicherheitsvorfälle unterstützen.

1.3. Durchführung des Vorhabens

1.3.1. AP 2 – Szenaranalyse (Teil-AP 2.1 und 2.2)

Im Rahmen des Arbeitspakets 2 beteiligte sich der VDE an der Szenaranalyse mit dem Ziel, realitätsnahe und praxisrelevante Grundlagen für die weiteren Arbeiten im Projekt CONTAIN zu schaffen. Der Schwerpunkt lag dabei auf der systematischen Analyse von Normen und Standards sowie auf der Erhebung des Stands der Praxis durch Interviews mit Partnern aus dem CERT@VDE-Netzwerk.

1.3.1.1. Teil-AP 2.1: Identifikation und Beschreibung relevanter Szenarien

Im Teil-AP 2.1 unterstützte der VDE die Identifikation und Beschreibung relevanter Szenarien für IT-Sicherheitsvorfälle, insbesondere im Kontext von Ransomware. Grundlage hierfür bildete eine umfassende Recherche und Analyse nationaler, europäischer und internationaler Normen und Standards aus den Bereichen Incident Response & Incident Management, Vulnerability Handling, Industrial Security sowie Digitale Beweisführung.

Die Analyse zielte darauf ab, Rollen, Prozesse, Schnittstellen und Bedrohungsvektoren zu identifizieren, die für die Beschreibung und Strukturierung der Szenarien erforderlich sind. Die Ergebnisse wurden in Form einer strukturierten Normenlandschaft zusammengeführt, die einen Überblick über einschlägige Standards, deren Anwendungsbereiche sowie deren Relevanz für die Bewältigung von IT-Sicherheitsvorfällen bietet.

Diese Normenlandschaft wurde dem Projektkonsortium vorgestellt und gemeinsam diskutiert. Dabei wurden insbesondere Überschneidungen, Ergänzungen und potenzielle Lücken zwischen verschiedenen Normenwerken identifiziert. Die gewonnenen Erkenntnisse dienen als fachliche Grundlage für die weitere Ausarbeitung und Priorisierung der im Projekt betrachteten Szenarien.

1.3.1.2. Teil-AP 2.2: Analyse von Abläufen und Bedarf an Instrumenten zur Erhöhung des Reifegrads

Im Teil-AP 2.2 lag der Fokus auf der Erhebung des Stands der Praxis bei kleinen und mittleren Unternehmen sowie auf der Identifikation von Bedarfen zur Erhöhung des Reifegrads im Umgang mit IT-Sicherheitsvorfällen. Zu diesem Zweck führte der VDE Interviews mit Partnern aus dem CERT@VDE-Netzwerk durch.

Die Interviews richteten sich an Ansprechpartner mit Verantwortung im Bereich IT-Sicherheit und Incident Response. Ziel war es, Einblicke in bestehende organisatorische Strukturen, Prozesse und Entscheidungswege zu gewinnen sowie Erfahrungen aus bereits aufgetretenen Vorfällen zu erfassen. Die Interviews wurden anhand eines strukturierten Leitfadens durchgeführt, dokumentiert und anonymisiert ausgewertet.

Der Mehrwert der beiden Interviews lag in der Kombination zweier komplementärer Perspektiven: einer unternehmensübergreifenden Sicht auf Cybersecurity-Anforderungen in industriellen Systemen sowie einer technologie- und produktnahen Sicht auf konkrete sicherheitsrelevante Umsetzungen.

Aus den Interviews ergaben sich dennoch wiederkehrende Muster hinsichtlich der organisatorischen Einbettung von Incident Response, der Bedeutung klar definierter Rollen und Eskalationsstufen sowie der Herausforderungen bei der unternehmensübergreifenden Kommunikation, insbesondere entlang von Lieferketten. Darüber hinaus zeigte sich, dass vorhandene Normen und Standards bei kleinen und mittleren Unternehmen zwar bekannt sind, deren konkrete Umsetzung in der Praxis jedoch häufig mit Unsicherheiten verbunden ist.

Die Ergebnisse der Interviews wurden mit den Erkenntnissen aus der Normenanalyse abgeglichen. Auf dieser Basis konnten Bedarfe an unterstützenden Instrumenten identifiziert werden, die Unternehmen bei der operationalen Umsetzung von Anforderungen an die Informationssicherheit unterstützen. Die gewonnenen Erkenntnisse flossen sowohl in die Weiterentwicklung der Szenarien als auch in die Ableitung von Anforderungen an die Informationssicherheit im Rahmen des Teil-AP 4.8 ein.

Insgesamt bildete das Arbeitspaket 2 damit eine zentrale Grundlage für die weiteren Arbeiten im Projekt CONTAIN, da es sowohl die theoretischen Anforderungen aus Normen und Standards als auch die praktischen Erfahrungen und Bedarfe aus der Unternehmenspraxis zusammenführte.

1.3.2. AP 3 – CONTAIN-Rahmenwerk (Teil-AP 3.4 und 3.5)

Im Arbeitspaket 3 war der VDE an der Konzeption, Strukturierung und inhaltlichen Ausgestaltung des CONTAIN-Rahmenwerks beteiligt. Ziel der Arbeiten des VDE im Rahmen dieses Arbeitspakets war es, die im Projekt gewonnenen Erkenntnisse aus Normenanalyse, Interviews und Anforderungsdefinitionen strukturiert zusammenzuführen und in das Rahmenwerk einzubringen.

Das CONTAIN-Rahmenwerk wurde als webbasiertes Wiki umgesetzt und ist als lebendes Dokument konzipiert. Diese Umsetzungsform ermöglicht eine kontinuierliche Weiterentwicklung, Ergänzung und Aktualisierung der Inhalte über die Projektlaufzeit hinaus. Der VDE brachte seine Expertise insbesondere bei der Strukturierung des Rahmenwerks, bei der Verwendung normkonformer Terminologie sowie bei der Einordnung der Inhalte in bestehende Normen und Standards ein.

Das Rahmenwerk ist modular aufgebaut und umfasst unter anderem eine Einleitung mit Nutzungsleitfaden, ein Vorgehensmodell, eine Framework-Übersicht, Rollenbeschreibungen, Übersichten zu relevanten Normen und Standards, Anforderungen an die Informationssicherheit, organisationsübergreifende Aspekte, sowie ein Glossar.

1.3.2.1. Teil-AP 3.4: Referenzmodellierung und Querschnittsthemen

Im Teil-AP 3.4 wirkte der VDE an der Referenzmodellierung von Querschnittsthemen mit, insbesondere im Hinblick auf Anforderungen an die Informationssicherheit. Die in anderen Arbeitspaketen entwickelten Inhalte wurden abstrahiert, generalisiert und als Leitlinien, Prozesse oder Referenzen im Rahmenwerk dokumentiert. Die Ergebnisse aus dem Teil-AP 4.8 wurden als zentrales Querschnittsthema in das Rahmenwerk integriert und mit weiteren Inhalten wie Rollenbeschreibungen, Normenreferenzen und Handlungshilfen verknüpft.

Durch die Arbeiten im Arbeitspaket 3 wurde eine zentrale Wissensbasis geschaffen, die als verbindendes Element zwischen Normung, Analyse, Training und praktischer Anwendung dient. Das CONTAIN-Rahmenwerk wurde im Projektverlauf erstellt, iterativ erweitert und für die Projektarbeiten genutzt.

1.3.2.2. Teil-AP 3.5: Glossar und Anwendungs- leitfaden

Im Teil-AP 3.5 arbeitete der VDE an der Erstellung eines projektweiten Glossars sowie an redaktionellen Regeln zur konsistenten Darstellung der Inhalte. Ziel war es, die Verständlichkeit und Einheitlichkeit des Rahmenwerks sicherzustellen und eine einheitliche Terminologie zu etablieren. Hierzu wurde eine Sammlung zentraler Begriffe erstellt, die Definitionen aus Normen und Standards mit praxisnahen Erläuterungen verbindet.

1.3.3. AP 4 – Effiziente Reaktionen durch Anforder- ungen an die Informationssicherheit (Teil-AP 4.8)

Das Arbeitspaket 4 stellte einen zentralen inhaltlichen Schwerpunkt des Teilvorhabens des VDE dar. Ziel des Teil-AP 4.8 war es, Anforderungen an die Informationssicherheit im Kontext der Bewältigung von IT-Sicherheitsvorfällen systematisch abzuleiten, zu strukturieren und für die weitere Projektarbeit aufzubereiten.

Im Mittelpunkt stand die Analyse von Anforderungen aus Normen und Standards. Der VDE untersuchte hierzu unter anderem normative Vorgaben zur Incident Response, zum Krisenmanagement, zur digitalen Beweisführung, zum Vulnerability Handling sowie zur Business Continuity. Relevante Anforderungen wurden identifiziert, zusammengeführt und im Hinblick auf ihre Anwendbarkeit bei der Bewältigung von IT-Sicherheitsvorfällen eingeordnet.

Ziel dieser Analyse war es, die Vielzahl vorhandener normativer Anforderungen nicht isoliert zu betrachten, sondern ihre praktische Umsetzbarkeit, ihre gegenseitigen Abhängigkeiten sowie ihre Relevanz für unterschiedliche Phasen eines IT-Sicherheitsvorfalls zu berücksichtigen. Dabei zeigte sich, dass normative Vorgaben häufig als Leitplanken formuliert sind und Interpretationsspielräume eröffnen. Normen und Standards beschreiben in der Regel allgemeine Anforderungen und beantworten die Frage, „was“ Anwender tun müssen. Die konkrete Ausgestaltung und Umsetzung dieser Anforderungen – also die Frage nach dem „Wie“ – bleibt hingegen organisations- und situationsabhängig. Insbesondere für kleine und mittlere Unternehmen besteht hier ein Bedarf an Konkretisierung, Priorisierung und strukturierter Hilfestellung.

Die eruierten Normen und Standards wurden im Rahmen des Teil-AP 4.8 auf Anforderungen an die Informationssicherheit untersucht und gemeinsam mit dem IT-Sicherheitscluster e. V. fachlich eingeordnet. Auf dieser Basis wurde ein Fragenkatalog entwickelt, der als strukturierte Orientierungshilfe zur Selbsteinschätzung konzipiert ist und sich insbesondere an kleine und mittlere Unternehmen richtet.

Der im Projekt erstellte Fragenkatalog CONTAINplus erweitert dabei den bestehenden Ansatz ISA+ des IT-Sicherheitsclusters um projektspezifische Inhalte und Anforderungen und macht diesen für den Kontext der Bewältigung von IT-Sicherheitsvorfällen nutzbar. CONTAINplus ist Bestandteil des webbasierten CONTAIN-Rahmenwerks und wurde im Projektverlauf im Wiki dokumentiert.

Der Fragenkatalog umfasst 50 Fragen, die organisatorische, technische und rechtliche Aspekte der Informationssicherheit adressieren. Innerhalb der Themenbereiche sind sogenannte K.-o.-Fragen definiert, deren Nichterfüllung auf grundlegende Defizite hinweist. Ziel ist es, eine strukturierte Einordnung des eigenen Umsetzungsstands zu ermöglichen.

Ein zentrales Gestaltungsprinzip von CONTAINplus ist die Verständlichkeit und Anwendbarkeit auch für Entscheidungsträger ohne tiefgehende technische Expertise. Das Vorgehensmodell ermöglicht es, erste Bedarfe und Schwachstellen eigenständig zu identifizieren. Ergänzend können externe, unabhängige Beratungsleistungen hinzugezogen werden, um die Ergebnisse weiter einzuordnen und konkrete Handlungsempfehlungen abzuleiten. Beratung und Auditierung sind dabei konzeptionell getrennt.

Die Struktur von CONTAINplus orientiert sich an grundlegenden Elementen eines Informationssicherheitsmanagementsystems (ISMS) und berücksichtigt insbesondere Aspekte der Vorbereitung, Bewältigung und Nachbereitung von IT-Sicherheitsvorfällen.

Die im Teil-AP 4.8 abgeleiteten Anforderungen wurden im Projektverlauf regelmäßig im Projektkonsortium eingebracht und diskutiert. Dies erfolgte unter anderem im Rahmen von Projekttreffen sowie begleitend zu projektinternen Austausch- und Demonstrationsformaten, etwa bei gemeinsamen Spiel- und Reflexionsphasen. Ziel war es, die Anforderungen im Projektkontext zu veranschaulichen, ihre Verständlichkeit zu prüfen und Rückmeldungen aus unterschiedlichen fachlichen Perspektiven aufzunehmen.

Darüber hinaus wurde im Teil-AP 4.8 der Konformitätsgrad der Bewältigung von IT-Sicherheitsvorfällen zu bestehenden Informationssicherheitsmanagementsystemen untersucht. Grundlage hierfür waren die Analyse bestehender Sicherheitsmanagementsysteme und Industriestandards sowie die Einbeziehung der im Projekt gewonnenen Erkenntnisse aus den Interviews und der Normenanalyse des Teil-AP 2.2. Ergänzend flossen der kontinuierliche fachliche Austausch und die Diskussionen in den einschlägigen Fachgremien aus dem Teil-AP 6.1 in die Arbeiten ein. Ziel war es, bestehende Anforderungen einzuordnen und mögliche Standardisierungslücken im Kontext der Bewältigung von IT-Sicherheitsvorfällen zu identifizieren.

Die Ergebnisse aus dem Teil-AP 4.8 wurden als Querschnittsthema in das CONTAIN-Rahmenwerk integriert und dort dokumentiert.

1.3.4. AP 5 – Demonstration und Evaluation (Teil-AP 5.3)

Im Rahmen des Arbeitspakets 5 unterstützte der VDE die Durchführung und Auswertung projektinterner Demonstrations- und Evaluationsaktivitäten. Dabei unterstützte der VDE insbesondere die Identifikation und Einbindung relevanter Stakeholder aus seinem Expertennetzwerk, darunter Experten aus Normungs- und Standardisierungsgremien der Deutschen Kommission Elektrotechnik (DKE) sowie Partner aus dem CERT@VDE-Netzwerk.

Die Federated Exercise diente der Demonstration und Erprobung der im Projekt entwickelten Konzepte und Werkzeuge. Die dabei gewonnenen Erkenntnisse flossen in die weitere Verfeinerung der Projektergebnisse ein, u. a. in die Weiterentwicklung von CONTAINplus.

1.3.5. AP 6 – Dissemination (Teil-AP 6.1)

Im Rahmen des Arbeitspakets 6 leistete der VDE Beiträge zum Dialog mit der Fachöffentlichkeit, zur Einbindung relevanter Akteure sowie zur Verbreitung der Projektergebnisse.

Das Projekt CONTAIN sowie die im Teilvorhaben des VDE erarbeiteten Ergebnisse wurden kontinuierlich in nationalen Normungs- und Standardisierungsgremien vorgestellt. Hierzu zählten unter anderem das DIN/DKE-Gemeinschaftsgremium Cybersecurity; DKE/AK 713.0.7 „Cyber Security & Data Protection (Gefahrenmelde- und Überwachungsanlagen)“ und DKE/UK 931.1 „IT-Sicherheit in der Automatisierungstechnik“ sowie weitere relevante DKE-Gremien. Die dort eingebrachten Rückmeldungen und Diskussionsbeiträge wurden in das Projektkonsortium zurückgespiegelt und bei der Weiterentwicklung der Projektergebnisse berücksichtigt.

Darüber hinaus wurden Zielsetzung, Motivation und Ansatz des Projekts CONTAIN im Rahmen einer Projektvorstellung in der Fachzeitschrift DIN-Mitteilungen des Deutschen Instituts für Normung (DIN e. V.) einer normungsnahen Fachöffentlichkeit vorgestellt. Der Beitrag diente der Information über den Projektansatz und die Einordnung in den Kontext von Normen und Standards im Bereich der Cybersecurity. Die Projektvorstellung erfolgte gemeinschaftlich durch mehrere Projektpartner, darunter die Universität der Bundeswehr München, das AIT Austrian Institute of Technology sowie der VDE e.V.

Als Beitrag zur Fachöffentlichkeit stellte der VDE das Projekt CONTAIN am 03.04.2025 durch den VDE auf der Hannover Messe auf der Energy 4.0 Conference Stage vor. Dabei wurden insbesondere die Serious Games sowie der Projektansatz und ausgewählte Inhalte aus dem Rahmenwerk einer breiten Öffentlichkeit vorgestellt.

Darüber hinaus wurde im Projekt eine Online-Durchführung eines Serious Games gemeinsam mit Partnern aus dem CERT@VDE-Netzwerk erprobt. Die dabei gewonnenen Rückmeldungen wurden in den weiteren Austausch im Projekt eingebracht.

Ziel der Disseminationsaktivitäten war es, den Wissenstransfer zwischen Forschung, Normung und Praxis zu stärken, Feedback aus unterschiedlichen Anwendergruppen einzuholen und die Anschlussfähigkeit der Projektergebnisse an bestehende und zukünftige Normungs- und Standardisierungsaktivitäten sicherzustellen.

1.4. Vergleich mit der ursprünglichen Planung

Der Vergleich zwischen der ursprünglichen Teilvorhabenbeschreibung des VDE und der tatsächlichen Durchführung des Vorhabens zeigt, dass die geplanten Ziele, Inhalte und Arbeitsschwerpunkte im Wesentlichen wie vorgesehen umgesetzt wurden. Abweichungen ergaben sich insbesondere in einzelnen Aspekten der operativen Umsetzung, ohne dass dies zu einer Änderung der Zielsetzung, zu inhaltlichen Einschränkungen oder zu einer Beeinträchtigung der Qualität der erzielten Ergebnisse führte.

1.4.1. Arbeitspakete und inhaltliche Umsetzung

Die in der Teilvorhabenbeschreibung vorgesehenen Arbeitspakete AP 2 (Szenaranalyse), AP 3 (CONTAIN-Rahmenwerk), AP 4 (Anforderungen an Informationssicherheit), AP 5 (Demonstration und Evaluation) sowie AP 6 (Dissemination) wurden entsprechend der geplanten Zielsetzungen bearbeitet. Die inhaltlichen Schwerpunkte – Normenanalyse, Einbindung von Praxispartnern, Ableitung praxisorientierter Anforderungen, Aufbau eines Rahmenwerks sowie Einbindung in Normungs- und Standardisierungsgremien – konnten umgesetzt werden.

In der ursprünglichen Planung war vorgesehen, drei Interviews mit Partnern aus dem CERT@VDE-Netzwerk durchzuführen (AP 2.2). Im Projektverlauf konnten zwei Interviews realisiert werden. Mehrere angefragte Partner sagten aufgrund begrenzter zeitlicher und personeller Kapazitäten ab oder stellten Anfragen zurück.

Die durchgeführten Interviews lieferten dennoch ausreichende und qualitativ hochwertige Erkenntnisse, die in die Normenanalyse, die Ableitung von Anforderungen sowie die Weiterentwicklung des Rahmenwerks einfließen. Eine zusätzliche Durchführung weiterer Interviews wurde geprüft, war jedoch für die Zielerreichung nicht zwingend erforderlich. Aus Sicht des VDE ergaben sich durch die geringere Anzahl an Interviews weder Verzögerungen im Projektverlauf noch qualitative Einschränkungen der Ergebnisse.

Der VDE erbrachte seine vorgesehenen inhaltlichen, strukturellen und normungsbezogenen Beiträge vollständig. Die technische Bereitstellung und der Betrieb des CONTAIN-Frameworks in Form eines Wikis lag im Verantwortungsbereich des IT-Sicherheitsclusters e. V.

1.4.2. Zeitliche Planung und Umsetzung eines Framework-Distributionsaspekts

Ein im Gesamtprojekt vorgesehener Teilaspekt betraf die Bereitstellung des CONTAIN-Rahmenwerks in Form einer Distribution für einen Virtualisierungskontext. Dieser Aspekt war nicht Bestandteil des Teilvorhabens des VDE, sondern lag im Verantwortungsbereich anderer Projektpartner.

Im Projektverlauf kam es beim IT-Sicherheitscluster e. V. zu organisatorischen und finanziellen Rahmenbedingungen, die eine Weiterverfolgung dieses Umsetzungsschrittes im vorgesehenen Umfang nicht zuließen. Diese Entwicklungen lagen außerhalb des Einflussbereichs des VDE.

Die inhaltlichen Arbeiten des VDE konzentrierten sich auf die Ableitung, Strukturierung und Dokumentation der fachlichen Inhalte des Rahmenwerks. Der Umsetzungsstand einzelner technischer oder organisatorischer Komponenten des Frameworks war hiervon unabhängig. Die Bereitstellung einer Distribution konnte innerhalb der Projektlaufzeit nicht abgeschlossen werden und ist von der weiteren organisatorischen Ausrichtung des IT-Sicherheitsclusters abhängig.

1.4.3. Abweichungen bei Dienstreisen und Präsenzterminen

In der ursprünglichen Planung waren mehrere Präsenztermine und Dienstreisen vorgesehen. Aufgrund organisatorischer, terminlicher und pandemiebedingter Rahmenbedingungen konnten einzelne Termine nicht wie geplant vor Ort durchgeführt werden und wurden durch Online-Formate ersetzt oder entfielen. Die Nutzung von Online-Formaten hatte keinen nachteiligen Einfluss auf die inhaltliche Abstimmung, die Zusammenarbeit im Projektkonsortium oder die Qualität der erarbeiteten Ergebnisse.

1.4.4. Auswirkungen auf Zielerreichung und Qualität

Die im Projektverlauf aufgetretenen Abweichungen wirkten sich unterschiedlich auf die einzelnen Projektbestandteile aus. Die inhaltlichen Arbeiten des VDE, insbesondere die Analyse normativer Anforderungen, die Ableitung und Strukturierung von Anforderungen an die Informationssicherheit sowie deren Einbringung in die Projektarbeiten, konnten wie vorgesehen umgesetzt werden.

Einschränkungen ergaben sich hingegen bei projektweiten Umsetzungsaspekten, die außerhalb des Verantwortungsbereichs des VDE lagen, insbesondere bei der technischen Bereitstellung und vollständigen Ausgestaltung des webbasierten Frameworks durch andere Projektpartner. Diese Aspekte konnten innerhalb der Projektlaufzeit nicht vollständig realisiert werden.

Insgesamt blieb die Zielsetzung des Teilvorhabens des VDE unverändert bestehen. Die Qualität der vom VDE erbrachten inhaltlichen Ergebnisse wurde durch die genannten Abweichungen nicht beeinträchtigt.

1.4.5. Kostenneutrale Verlängerung der Projektlaufzeit

Im Projektverlauf wurde die Laufzeit des Verbundprojekts kostenneutral bis zum 31.08.2025 verlängert. Hintergrund war insbesondere die Verschiebung der förderierten Übung auf den 28.02.2025. Die Verlängerung ermöglichte die Auswertung der Ergebnisse der Übung sowie deren Integration in die Weiterentwicklung des CONTAIN-Rahmenwerks und von CONTAINplus.

Darüber hinaus ergaben sich Verzögerungen bei einzelnen Arbeitspaketen aufgrund notwendiger Abstimmungen im Projektkonsortium. Die Verlängerung diente der planmäßigen Fertigstellung der vorgesehenen Inhalte.

Zusätzliche Fördermittel wurden nicht beantragt.

1.5. Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die im Teilvorhaben des VDE im Projekt CONTAIN geleisteten Arbeiten sowie die erzielten Ergebnisse entsprechen den im Projektantrag definierten Zielen. Der Schwerpunkt des Teilvorhabens lag auf der Analyse, Einordnung und praxisnahen Aufbereitung normativer und standardisierungsbezogener Anforderungen zur Bewältigung von IT-Sicherheitsvorfällen, insbesondere im Kontext transnationaler Lieferketten.

Die durchgeführten Arbeiten waren erforderlich, um bestehende Normen und Standards im Kontext der Bewältigung von IT-Sicherheitsvorfällen systematisch einzuordnen und ihre Anwendbarkeit in der Praxis zu untersuchen. Auf dieser Grundlage wurden Anforderungen abgeleitet und in strukturierter Form in das CONTAIN-Rahmenwerk integriert. Dadurch wird insbesondere kleinen und mittleren Unternehmen eine praxisnahe Unterstützung bei der Vorbereitung auf IT-Sicherheitsvorfälle und beim Umgang mit Anforderungen an die Informationssicherheit geboten.

Die Einbindung von Experten aus Normungs- und Standardisierungsgremien sowie der Abgleich mit praktischen Erfahrungen aus dem CERT@VDE-Netzwerk waren notwendige Bestandteile der Arbeiten, um die fachliche Qualität, Aktualität und Anschlussfähigkeit der Ergebnisse sicherzustellen. Umfang und Tiefe der geleisteten Arbeiten waren insgesamt angemessen, um die Projektziele zu erreichen und nachhaltige, über das Projektende hinaus nutzbare Ergebnisse zu schaffen.

1.5.1. Einordnung des zahlenmäßigen Nachweises

Für das Teilvorhaben waren im Projektantrag insgesamt acht Projektmonate vorgesehen. Die geplanten Arbeiten konnten im vorgesehenen zeitlichen Rahmen umgesetzt werden. Die gewährte kostenneutrale Verlängerung bis zum 31.08.2025 hatte keine Auswirkungen auf die Ausgabenplanung. Es wurden keine zusätzlichen Mittel beantragt oder abgerufen. Ein im Projektverlauf entstandener zusätzlicher zeitlicher Aufwand ergab sich insbesondere aus der inhaltlichen Tiefe der Normenanalyse, dem redaktionellen und strukturellen Aufwand bei der Ausgestaltung des CONTAIN-Rahmenwerks sowie aus zusätzlichen fachlichen Abstimmungen innerhalb des Projektkonsortiums. Dieser Mehraufwand wurde vom VDE als Eigenleistung erbracht und nicht zu Lasten der Projektförderung abgerechnet.

Abweichungen bei den ursprünglich geplanten Dienstreisen ergaben sich insbesondere durch organisatorische und terminliche Rahmenbedingungen sowie durch den verstärkten Einsatz von Online-Formaten. Diese Abweichungen hatten keinen nachteiligen Einfluss auf den Projektverlauf oder die Qualität der erzielten Ergebnisse.

Weiterführende Angaben sind Bestandteil des Erfolgskontrollberichts.

1.6. Ergebnisse, Nutzen und Anschlussfähigkeit

Die Ergebnisse des Teilvorhabens leisten einen Beitrag zur Stärkung der Cyber-Resilienz von Unternehmen, insbesondere von kleinen und mittleren Unternehmen. Durch die strukturierte Aufbereitung von Anforderungen an die Informationssicherheit und deren Integration in ein praxisorientiertes Rahmenwerk wird der Transfer bestehender Normen und Standards in die Anwendung erleichtert und besser nachvollziehbar gemacht.

Auf Basis der Normenanalyse und der im Projekt gewonnenen Erkenntnisse wurde mit CONTAINplus ein strukturierter Fragenkatalog entwickelt, der Anforderungen an die Informationssicherheit in den Kontext der Vorbereitung und Bewältigung von IT-Sicherheitsvorfällen überführt. CONTAINplus ist Bestandteil des webbasierten CONTAIN-Rahmenwerks und unterstützt Unternehmen bei der Selbsteinschätzung des Umsetzungsstands sowie bei der Identifikation von Handlungsbedarfen.

Die technische Bereitstellung und der Betrieb des CONTAIN-Rahmenwerks liegen im Verantwortungsbereich des IT-Sicherheitsclusters e. V. Der VDE brachte seine Expertise insbesondere in Form inhaltlicher, struktureller und normungsbezogener Beiträge in die Konzeption und Ausgestaltung des Rahmenwerks sowie in die Ableitung und Einordnung von Anforderungen ein.

Eine kommerzielle Verwertung der Ergebnisse ist nicht vorgesehen. Vielmehr dienen die erarbeiteten Inhalte dem Wissenstransfer zwischen Forschung, Normung und Praxis, der Unterstützung von Normungs- und Standardisierungsprozessen sowie der nachhaltigen Stärkung des CERT@VDE-Netzwerks. Die Ergebnisse sind so angelegt, dass sie über das Projektende hinaus genutzt und in zukünftige Aktivitäten im Bereich Normung, Standardisierung und Wissensvermittlung eingebunden werden können.

Die Relevanz dieser Ergebnisse wird auch durch die während der Projektlaufzeit zu beobachtenden Entwicklungen im Bereich der IT-Sicherheitslage und der regulatorischen Rahmenbedingungen unterstrichen.

Eine Weiterverwendung ist insbesondere im Rahmen von Normungs- und Standardisierungsaktivitäten sowie im CERT@VDE-Netzwerk möglich.

1.7. Bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens

Die Bedeutung der IT-Sicherheit hat während der Laufzeit des Projekts CONTAIN weiter deutlich zugenommen. Der Lagebericht zur IT-Sicherheit in Deutschland 2024 des Bundesamts für Sicherheit in der Informationstechnik (BSI) beschreibt eine anhaltend angespannte Bedrohungslage, die durch eine hohe Dynamik und eine zunehmende Professionalisierung von Cyberangriffen gekennzeichnet ist. Insbesondere Ransomware stellt weiterhin eine der größten Bedrohungen für Unternehmen dar (BSI, Die Lage der IT-Sicherheit in Deutschland 2024 [1]).

Von dieser Entwicklung sind in besonderem Maße kleine und mittlere Unternehmen betroffen. Neben direkten Angriffen auf Unternehmen geraten zunehmend auch Dienstleister und Zulieferer in den Fokus, wodurch sich Risiken entlang von Lieferketten verstärken. Die Auswirkungen reichen von Störungen betrieblicher Abläufe über Ausfälle von Informations- und Produktionssystemen bis hin zu erheblichen wirtschaftlichen Schäden.

Parallel zur Bedrohungslage haben sich während der Projektlaufzeit auch die regulatorischen Rahmenbedingungen weiterentwickelt. Mit bestehenden und absehbaren gesetzlichen Anforderungen, insbesondere im Kontext europäischer Regelwerke, steigen die Erwartungen an Unternehmen hinsichtlich der Vorbereitung auf IT-Sicherheitsvorfälle, der Umsetzung organisatorischer Maßnahmen sowie der Einhaltung normativer Vorgaben. Diese Anforderungen wirken zunehmend auch mittelbar auf kleinere Unternehmen, etwa über vertragliche Verpflichtungen innerhalb von Lieferketten.

Diese Entwicklungen verdeutlichen den wachsenden Bedarf an strukturierten, praxisnahen Ansätzen zur Vorbereitung auf IT-Sicherheitsvorfälle sowie zur Einordnung und Umsetzung normativer Anforderungen. Vor diesem Hintergrund sind die im Projekt CONTAIN erarbeiteten Ergebnisse in einem sich dynamisch weiterentwickelnden fachlichen und regulatorischen Umfeld verortet und adressieren einen während der Projektlaufzeit weiter zunehmenden Bedarf in Wirtschaft und Praxis.

1.8. Erfolgte oder geplante Veröffentlichungen

Während der Laufzeit des Projekts CONTAIN wurden Ergebnisse des Teilvorhabens des VDE im Rahmen verschiedener Fachformate und Veröffentlichungen kommuniziert. Ziel war es, die Projektergebnisse in den fachlichen Austausch mit relevanten Akteuren aus Normung, Praxis und Öffentlichkeit einzubringen.

Hierzu zählen unter anderem:

- Projektvorstellungen und fachliche Beiträge im Umfeld von Normungs- und Standardisierungsgremien bei DIN und DKE
- Vorstellung des Projekts in den DIN-Mitteilungen (Maßnahme der Öffentlichkeitsarbeit)
- Präsentation des Projekts CONTAIN auf der Hannover Messe (Energy 4.0 Conference Stage)
- Einbindung und Diskussion von Projektergebnissen im CERT@VDE-Partnernetzwerk, unter anderem im Rahmen projektbegleitender Serious-Games-Formate
- Beiträge zu Fachveranstaltungen und projektbegleitenden Austauschformaten

1.9. Wesentliche Ergebnisse

Ziel des Teilvorhabens des VDE im Projekt CONTAIN war es, einen Beitrag zur Verbesserung der Vorbereitung auf und Bewältigung von IT-Sicherheitsvorfällen zu leisten, insbesondere durch die strukturierte Aufbereitung normativer und standardisierungsbezogener Anforderungen sowie durch die Ableitung praxisnaher Unterstützungsinstrumente für Unternehmen.

Dieses Ziel konnte im Projekt erreicht werden. Durch die systematische Analyse einschlägiger Normen und Standards, den Abgleich mit praktischen Erfahrungen aus dem CERT@VDE-Netzwerk sowie die Einbindung von Experten aus Normungs- und Standardisierungsgremien wurden Anforderungen an die Informationssicherheit im Kontext von IT-Sicherheitsvorfällen identifiziert, eingeordnet und aufbereitet.

Ein zentrales Ergebnis des Teilvorhabens ist das CONTAIN-Rahmenwerk als strukturierte Wissensbasis sowie der daraus abgeleitete Fragenkatalog CONTAINplus. CONTAINplus unterstützt insbesondere kleine und mittlere Unternehmen dabei, den eigenen Umsetzungsstand im Hinblick auf Anforderungen an die Informationssicherheit systematisch zu reflektieren und Handlungsbedarfe zu identifizieren. Die Ergebnisse sind bewusst so gestaltet, dass sie unabhängig von konkreten technischen Lösungen anwendbar sind.

Die im Teilvorhaben erarbeiteten Ergebnisse wurden in das Projektkonsortium eingebracht, im Rahmen von Demonstrations- und Austauschformaten diskutiert und für die weitere Nutzung dokumentiert. Damit stehen sie über das Projektende hinaus als Grundlage für weitere Aktivitäten im Bereich Normung, Standardisierung und Wissenstransfer zur Verfügung.

1.10. Quellenverzeichnis

- [1] BSI (2024): *Die Lage der IT-Sicherheit in Deutschland 2024*.
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html> (abgerufen am: 29.01.2026).