

Sachbericht zum Vorhaben FKZ 16KIS1972 „OdySecure“

Laufzeit: 01.10.2023 – 28.02.2025

Zuwendungsempfänger: Cybervize Operations GmbH

Erstellt von Alexander Busse, 18.12.2025

Table of Contents

1. Ausgangssituation und Zielsetzung des Vorhabens	3
2. Geplante Ziele und deren Erreichung.....	5
3. Durchgeführte Arbeiten und Projektverlauf.....	6
3.1 Überblick über den Projektverlauf.....	6
3.2 AP1 – Webseite für den Demonstrator	7
3.3 AP2 – Back-End-Entwicklung (AP2.1–AP2.3)	7
AP2.1 Datenstrukturen und Algorithmen.....	7
AP2.2 APIs und Schnittstellen	8
AP2.3 Semantische Technologien	8
3.4 AP3 – Front-End-Entwicklung (AP3.1–AP3.3).....	8
3.5 AP4 – Security-Maßnahmen erstellen	9
3.6 AP5 – Schaffung und Betrieb der digitalen Infrastruktur.....	10
3.7 AP6 – Tests und Qualitätssicherung (AP6.1–AP6.2)	10
3.8 AP7 – Community-Forum (AP7.1–AP7.2).....	11
3.9 AP8 – Marketingkonzept (AP8.1–AP8.3)	11
3.10 AP9 – Kommunikationsinhalte (AP9.1–AP9.2)	12

3.11 AP10 – Validierung der Benutzererfahrung und Optimierung aus Anwendersicht	13
3.12 AP11 – Technischer Support (AP11.1–AP11.2)	13
3.13 AP12 – Umsetzung technischer Optimierungsvorschläge	14
3.14 AP13 – Messe- und Kundenauftritte	14
3.15 AP14 – Kommunikationsschulung und Wissenstransfer	15
3.17 AP16 – Projektkoordination	15
4. Kooperationen und Dissemination	16
5. Verwertung und wirtschaftliche Perspektive	17
6. Wissenschaftliche und technische Ergebnisse sowie Anschlussfähigkeit	17
7. Lessons Learned und Gründe für ausbleibende Investitionen	18
7.1 NIS2 als Managementaufgabe – und der „Tool-Reflex“ im Mittelstand	18
7.2 Lehren aus Testkunden- und Pilotakquise	20
7.3 Technische und architektonische Lessons Learned	21
7.4 Investorenperspektive und Finanzierbarkeit	21
7.5 Zusammenfassung der Gründe für das Ausbleiben eines Investments	22
8. Zusammenfassung	23

1. Ausgangssituation und Zielsetzung des Vorhabens

Kleine und mittlere Unternehmen (KMU) in Deutschland sind in besonderem Maße von Cyberangriffen betroffen. Studien von Branchenverbänden und Sicherheitsbehörden weisen seit Jahren hohe Schadenssummen und eine Zunahme von Datendiebstahl, Sabotage und Erpressung aus. Gleichzeitig verfügen KMU in der Regel weder über eine eigene IT-Sicherheitsabteilung noch über ausreichend Budget, um spezialisierte Fachkräfte dauerhaft zu beschäftigen.

In der Praxis führt dies häufig zu einem fragmentierten Sicherheitsniveau:

- Es werden einzelne technische Maßnahmen eingeführt (z. B. Firewalls, Endpoint-Protection, Backup-/Recovery-Lösungen oder SIEM-Systeme).
- Ein durchgängiges Managementsystem für Informationssicherheit (ISMS) fehlt jedoch.
- Regulatorische Anforderungen (z. B. ISO/IEC 27001, IT-Grundschutz, NIS2) werden nur teilweise, projektbezogen oder gar nicht umgesetzt.

Gleichzeitig steigt der Druck auf Unternehmen:

- Auf **regulatorischer Seite** durch Vorgaben aus der NIS2-Richtlinie, dem IT-Sicherheitsgesetz, branchenspezifischen Regulierungskonzepten und internationalen Standards.
- Auf **geschäftlicher Seite** durch steigende Abhängigkeit von IT-gestützten Prozessen, Lieferkettenverflechtungen und Kundenanforderungen (z. B. Sicherheitsanforderungen in Ausschreibungen oder Lieferantenbewertungen).
- Auf **versicherungstechnischer Seite** durch strengere Anforderungen von Cyber-Versicherern an Governance, Informationssicherheitsmanagement und Risikotransparenz.

Moderne Standards und Regulierungen betrachten Cybersicherheit primär als Managementsystem-Thema. Es geht darum, einen kontinuierlichen Plan-Do-Check-Act-Zyklus (PDCA) zu etablieren und Verantwortung im Management zu verankern – nicht nur in der IT. Cybersicherheit muss als kontinuierlicher Prozess verstanden werden, in dem:

- Risiken aus der Perspektive der Geschäftsprozesse identifiziert werden,
- Rollen und Verantwortlichkeiten definiert und gelebt werden,
- organisatorische und technische Maßnahmen geplant, priorisiert und umgesetzt werden,
- Wirksamkeit, Reifegrad und Restrisiko laufend überwacht und verbessert werden.

In vielen KMU fehlen jedoch die Kombination aus:

- fachlichem Know-how zu Normen und Regulierung,
- methodischer Kompetenz zum Aufbau eines ISMS,
- und geeigneten Werkzeugen, um einen solchen Managementprozess effizient zu etablieren.

Beratungsleistungen können diese Lücke teilweise schließen, sind aber kostenintensiv und skalieren schlecht – insbesondere für kleinere Unternehmen. Zudem ist es schwierig, das einmal aufgebaute Wissen dauerhaft im Unternehmen zu verankern, wenn es nicht in Prozesse, Rollen und Werkzeuge überführt wird.

Vor diesem Hintergrund verfolgte das Vorhaben **OdySecure** das Ziel, eine **kosteneffiziente, KI-gestützte Cyber-Sicherheitslösung für KMU** und auch mittelständische Unternehmen zu entwickeln, die folgende Bausteine verbindet:

- ein AI-basiertes Expertensystem auf Basis eines Wissensgraphen und einer Ontologie für Informationssicherheit,
- eine mandantenfähige SaaS-Lösung zur strukturierten Erfassung von Risiken, Prozessen, Assets und Maßnahmen,
- eine Community-Funktion, die Wissen bündelt und Erfahrungsaustausch ermöglicht,
- die Einbindung menschlicher Beratung (z. B. im Rahmen eines Virtual-CISO-Services), um Kunden bei der Umsetzung zu begleiten.

Ziel war es, KMU eine Lösung zur Verfügung zu stellen, mit der sie ohne umfangreiche externe Projektschemata ein wirksames Management der Cybersicherheit etablieren

können, mit Fokus auf Transparenz, Nachvollziehbarkeit und einer deutlichen Reduktion des Aufwands gegenüber klassischen ISMS-Einführungen.

2. Geplante Ziele und deren Erreichung

Im Förderantrag wurden die wissenschaftlich-technischen und wirtschaftlichen Ziele in mehreren Teilzielen konkretisiert. Im Kern sollten erreicht werden:

1. Entwicklung eines AI-basierten Expertensystems auf Basis eines Wissensgraphen (Ontologie, semantische Technologien).
2. Konzeption und Implementierung einer benutzerfreundlichen, sicheren und skalierbaren SaaS-Lösung für KMU.
3. Aufbau eines Community-Forums zur Unterstützung und zum Wissensaustausch.
4. Integration menschlicher Beratung (z. B. als Virtual-CISO-Dienstleistung) in das Angebot.
5. Entwicklung und Inbetriebnahme eines funktionsfähigen Demonstrators.
6. Entwicklung eines Marketingkonzepts, Kommunikationsinhalten und Go-to-Market-Ansatzes.
7. Pilotierung mit Testkunden und Validierung der Nutzererfahrung.

Zielerreichung im Überblick

- Das geplante **AI-basierte Expertensystem** wurde technisch weiterentwickelt und in Form einer **GraphRAG-basierten Architektur** umgesetzt. Die ursprüngliche Idee eines rein regelbasierten Expertensystems wurde im Projekt durch eine Kombination aus Wissensgraph und Large Language Models ersetzt. Die Zielrichtung, eine KI-gestützte Auswertung des Wissensgraphen und Vorschlag von Maßnahmen, wurde erreicht, die technische Umsetzung ist moderner und nachhaltiger als im Antrag beschrieben.
- Die **SaaS-Plattform** wurde mandantenfähig implementiert und als Demonstrator produktiv lauffähig bereitgestellt.
- Die **Community-Funktion** wurde technisch realisiert, konnte aber mangels ausreichender Testkunden nur eingeschränkt genutzt und validiert werden.

- Die Einbindung menschlicher Beratung wurde durch die Konzeption und Umsetzung eines **Virtual-CISO-Services** erreicht; bei einem Kunden kommt die Plattform im Rahmen einer laufenden Betreuung produktiv zum Einsatz.
- Ein **Demonstrator** der Gesamtlösung liegt vor und wurde in Pitches, bei einem Pilotkunden und in Gesprächen mit Investoren demonstriert.
- **Marketingkonzept und Kommunikationsinhalte** wurden in wesentlichen Teilen umgesetzt (Brand Story, Pitch-Decks, Webtexte, Präsentationen). Eine ursprünglich geplante umfangreiche Serie von Erklärvideos wurde zugunsten von Produktentwicklung und Vertrieb teilweise zurückgestellt.
- Die **Pilotierung** mit einem Unternehmen (ADVISORI FTC GmbH) wurde durchgeführt; weitere Testkunden konnten innerhalb der Projektlaufzeit nicht dauerhaft gewonnen werden. Somit konnte ein breiter Product-Market-Fit noch nicht nachgewiesen werden.

Insgesamt wurden die **fachlichen und technischen Ziele** des Vorhabens erreicht. Die Ziele hinsichtlich **Marktdurchdringung und Investorenfinanzierung** konnten mangels ausreichender Traktion (Kundenanzahl, Umsätze) nicht vollständig realisiert werden.

3. Durchgeführte Arbeiten und Projektverlauf

Im Antrag wurde der Arbeitsplan in die Arbeitspakete **AP1 bis AP16** gegliedert. Nachfolgend wird die tatsächliche Durchführung je Arbeitspaket beschrieben.

3.1 Überblick über den Projektverlauf

- In der **Startphase** (Q4/2023) lagen die Schwerpunkte auf technischer Architektur, Auswahl der Technologien (Graphdatenbank, semantische Frameworks, LLM-Integration), Planung der Ressourcennutzung und Aufbau der Infrastruktur.
- **2024** stand im Zeichen der Entwicklung von Backend und Frontend, des Aufbaus der Wissensbasis, der Implementierung der GraphRAG-Komponenten, interner Tests sowie der Pilotierung beim ersten Kunden. Parallel wurden Marketingkonzept, Kommunikationsinhalte und Messeauftritte vorbereitet und durchgeführt.
- In der **Abschlussphase** (Ende 2024 bis Februar 2025) erfolgten Stabilisierung, Dokumentation, Auswertung der Pilotierung, Investorengespräche sowie die

Zusammenführung der Projektergebnisse in Demonstrator, Fachbeitrag und Abschlussberichte.

3.2 AP1 – Webseite für den Demonstrator

Plan: Konzeption, Design und Entwicklung einer Webseite für den Demonstrator mit ansprechender Nutzerführung und Einbettung in die Corporate Identity.

Umsetzung und Ergebnisse:

- Entwicklung einer **Landing-Page** für OdySecure mit Beschreibung des Nutzens für KMU, Erläuterung des Ansatzes (Managementprozess, KI-gestützte Empfehlungen) und Optionen zur Kontaktaufnahme.
- Integration von **Screenshots und vereinfachten Darstellungen** der Plattform zur Visualisierung des Demonstrators.
- Einbindung von Kontakt- und Terminformularen zur Vereinbarung von Erstgesprächen bzw. Demos.

Das Arbeitspaket wurde wie geplant umgesetzt; die Webseite fungiert als Einstiegs- und Informationskanal für Interessenten.

3.3 AP2 – Back-End-Entwicklung (AP2.1–AP2.3)

AP2 umfasste die Teilpakete Datenstrukturen und Algorithmen (AP2.1), APIs und Schnittstellen (AP2.2) sowie semantische Technologien (AP2.3).

AP2.1 Datenstrukturen und Algorithmen

- Entwurf der **Kern-Datenmodelle** für Mandanten, Benutzer, Geschäftsprozesse, Assets, Risiken, Maßnahmen, Kontrollen und Nachweise.
- Implementierung der **Speicherschicht** unter Nutzung einer Graphdatenbank und ergänzender relationaler Speicherstrukturen, um sowohl graphbasierte Auswertungen als auch klassische Listen- und Reportingfunktionen zu ermöglichen.

- Entwicklung von **Algorithmen zur Risikobewertung** (Kombination aus Eintrittswahrscheinlichkeit und Schadenshöhe) und zur Aggregation von Kennzahlen (Risikoprofile auf Prozess- und Unternehmensebene).

AP2.2 APIs und Schnittstellen

- Definition und Implementierung einer REST-basierten **API-Schicht**, über die das Frontend und externe Komponenten auf Funktionen der Plattform zugreifen.
- Implementierung von Endpunkten für CRUD-Operationen (Create, Read, Update, Delete) auf den wichtigsten Entitäten (Prozesse, Assets, Risiken, Maßnahmen, Nachweise).
- Entwurf erster **Schnittstellenkonzepte** für spätere Partnerintegrationen (z. B. Breach-Informationendienste, SOC-Anbieter).

AP2.3 Semantische Technologien

- Modellierung einer **Ontologie für Informationssicherheit** auf Basis offener Standards (RDF/OWL).
- Abbildung der Anforderungen aus ISO 27001 und IT-Grundschutz in Form von Ontologieklassen und -relationen (Controls, Maßnahmen, Anforderungen, Nachweisbeziehungen).
- Integration des Wissensgraphen in die Plattform, so dass Normanforderungen, Risiken und Maßnahmen im Graphen referenziert und ausgewertet werden können.

AP2 bildet die technische Grundlage für Expertensystem und GraphRAG-Komponenten. Die ursprünglich vorgesehenen statischen Regelwerke wurden zugunsten des GraphRAG-Ansatzes modernisiert.

3.4 AP3 – Front-End-Entwicklung (AP3.1–AP3.3)

AP3 umfasste Framework-Auswahl, Nutzererlebnis/Design und Qualitätssicherung des Frontends.

Umsetzung und Ergebnisse:

- Auswahl eines modernen Web-Frameworks und Aufbau einer **modularen Frontend-Architektur**, die eine schrittweise Erweiterung ermöglicht.
- Gestaltung einer **übersichtlichen Navigation** entlang der zentralen Use Cases:
 - Unternehmens- und Organisationsstammdaten,
 - Risikoregister,
 - Maßnahmenpläne,
 - Berichte und Dashboards.
- Erstellung von **Prototypen und Klick-Dummies**, die intern und mit dem Pilotkunden getestet wurden. Das Feedback floss in Anpassungen von Benennungen, Gruppierungen und der Anzahl erforderlicher Eingabefelder ein.
- Einführung von grundlegenden **automatisierten und manuellen Tests** zur Sicherstellung der Funktionalität und Darstellungsqualität in unterschiedlichen Browsern.

Das Frontend unterstützt heute die durchgängige Erfassung und Auswertung von Informationen und wurde im Verlauf der Pilotierung iterativ verfeinert.

3.5 AP4 – Security-Maßnahmen erstellen

Plan: Aufbau und Pflege eines Katalogs von Security-Maßnahmen, die als Vorschläge des Expertensystems dienen und im Wissensgraphen hinterlegt werden.

Umsetzung und Ergebnisse:

- Zusammenführung von **Best-Practice-Maßnahmen** aus ISO 27001, IT-Grundschutz, gängigen Branchenstandards und eigener Beratungserfahrung.
- Strukturierung der Maßnahmen nach **Kontrollbereichen** (z. B. Organisation, Technik, physische Sicherheit, Awareness, Notfallmanagement).
- Verknüpfung der Maßnahmen mit **Risiken, Prozessen, Assets und Normanforderungen** im Wissensgraphen, so dass für identifizierte Risiken passende Maßnahmenpakete vorgeschlagen werden können.
- Kennzeichnung der Maßnahmen mit **Aufwandsklassen**, Verantwortlichkeiten und Fälligkeitsattributen zur besseren Planung.

Der Maßnahmenkatalog bildet die inhaltliche Basis für Risikobehandlung und Reifegradentwicklung.

3.6 AP5 – Schaffung und Betrieb der digitalen Infrastruktur

Plan: Aufbau der technischen Infrastruktur (Backend-Systeme, Graphdatenbank, Community-Plattform) und Sicherstellung von Skalierbarkeit, Sicherheit und Verfügbarkeit.

Umsetzung und Ergebnisse:

- Aufbau einer Cloud-basierten Infrastruktur mit Entwicklungs-, Test- und Staging-Umgebungen auf Basis einer containerisierten Docker-Architektur. Die Anwendungskomponenten (Backend, Frontend, Graphdatenbank) werden in separaten Containern betrieben und können so unabhängig voneinander aktualisiert und skaliert werden.
- Bereitstellung und Betrieb der Graphdatenbank, der Anwendungsserver und der Authentifizierungskomponenten innerhalb dieser Docker-Umgebung; Konfiguration standardisierter Images und Deploymentskripte, um reproduzierbare Rollouts zu gewährleisten.
- Implementierung grundlegender Sicherheitsmechanismen (TLS-Verschlüsselung, Rollen- und Rechtemodell, Protokollierung kritischer Aktionen) auf Applikations- und Infrastrukturebene, einschließlich sicherer Konfiguration der Container-Kommunikation.
- Einrichtung der technischen Basis für die Community-Funktion (Forenmodul, Benutzer- und Rechtestruktur) als weiterer Dienst in der Docker-Architektur, so dass auch diese Komponente getrennt deployt und gewartet werden kann.

Die auf Docker-Containern basierende Infrastruktur erwies sich im Projektbetrieb als stabil und wartungsfreundlich und bildet die Grundlage für den Weiterbetrieb und die schrittweise Erweiterung des Demonstrators.

3.7 AP6 – Tests und Qualitätssicherung (AP6.1–AP6.2)

Umsetzung und Ergebnisse:

- Erstellung von **Testplänen** für zentrale Funktionen (Risikomanagement, Maßnahmenverfolgung, Mandantenfähigkeit, Rechtekonzept).
- Durchführung von **funktionalen Tests** in mehreren Iterationen während der Entwicklung.
- Dokumentation und Nachverfolgung von Fehlern und Abweichungen.
- Einführung einfacher **Regressionstests** und Code-Reviews zur Qualitätssicherung.

Aufgrund der begrenzten Teamgröße konnte kein vollumfängliches QA-Team aufgebaut werden; die wesentlichen Qualitätssicherungsmaßnahmen wurden jedoch umgesetzt.

3.8 AP7 – Community-Forum (AP7.1–AP7.2)

Plan: Aufbau einer Community-Plattform, in der Fragen zur Cybersicherheit diskutiert werden können und ein Belohnungssystem für aktive Nutzer etabliert wird.

Umsetzung und Ergebnisse:

- Konzeption einer **Forenstruktur** mit Kategorien (z. B. NIS2, ISO 27001, technische Maßnahmen, Erfahrungen aus Audits).
- Implementierung der notwendigen **Berechtigungsstrukturen** für Moderation und Qualitätssicherung.
- Entwurf eines einfachen **Belohnungssystems** (Badges, sichtbare Rollen) für aktive Nutzer.
- Erstellung von Grundlagentexten und ersten FAQ-Beiträgen.

Die technische Plattform wurde fertiggestellt, konnte aber aufgrund der geringen Zahl aktiver Testkunden nur sehr begrenzt aktiviert werden. Das Ziel, eine lebendige Community aufzubauen, wurde daher nur teilweise erreicht.

3.9 AP8 – Marketingkonzept (AP8.1–AP8.3)

Umsetzung und Ergebnisse:

- Durchführung einer **Markt- und Wettbewerbsanalyse** auf Basis verfügbarer Studien und Marktbeobachtungen.
- Schärfung der Zielgruppenpositionierung:
 - KMU und Mittelstand mit 150–1000 Mitarbeitenden als Kernzielgruppe,
 - mittelfristige Erweiterung auf größere Unternehmen ohne eigenen CISO.
- Entwicklung eines **Marketing- und Kommunikationskonzepts** mit Kernbotschaften („Cybersicherheit als Managementprozess, nicht nur als Tool“), Value Proposition und Nutzenargumentation für Geschäftsführung und ISB.
- Erstellung von **Präsentationen, Pitch-Unterlagen und Textbausteinen** für Website, E-Mail-Ansprache und Veranstaltungen.
- Die geplante kontinuierliche Umsetzung einer breiten Kampagne (z. B. Paid-Ads, umfassende Videoreihe) konnte aufgrund begrenzter Ressourcen nur in Ansätzen realisiert werden.

3.10 AP9 – Kommunikationsinhalte (AP9.1–AP9.2)

Umsetzung und Ergebnisse:

- Erstellung von **Texten, Grafiken und Visualisierungen** zur Darstellung des OdySecure-Ansatzes (Managementprozess, Wissensgraph, Nutzen gegenüber klassischen ISMS-Einführungen).
- Produktion ausgewählter **Präsentationsgrafiken und kurzer Videosequenzen** für Pitches und Online-Formate.
- Überarbeitung der Inhalte hinsichtlich Zielgruppenorientierung (Technik vs. Management) und Corporate Identity.

Eine große Serie von Erklärvideos im ursprünglich angedachten Umfang wurde nicht vollständig umgesetzt; hier wurden zugunsten von Produktentwicklung und Investorengesprächen Prioritäten verschoben.

3.11 AP10 – Validierung der Benutzererfahrung und Optimierung aus Anwendersicht

Umsetzung und Ergebnisse:

- Identifikation und Onboarding von **Pilotkunden** (insbesondere ADVISORI FTC GmbH).
- Durchführung von **Usability-Tests** im Rahmen gemeinsamer Workshops und Remote-Sessions.
- Systematische Sammlung von Feedback zur Benutzerführung, Terminologie und zur Ausrichtung von Dashboards und Reports.
- Auf Basis des Feedbacks wurden u. a. folgende Anpassungen vorgenommen:
 - Vereinfachung von Formularen,
 - bessere Strukturierung von Maßnahmenlisten,
 - Ergänzung von Hilfetexten und Tooltips.
- Parallel wurden zentrale Elemente des **Markenkerns** (Positionierung, Tonalität, visuelles Erscheinungsbild) geschärft.

AP10 lieferte wesentliche Impulse für die Weiterentwicklung der Plattform in Richtung Praxistauglichkeit.

3.12 AP11 – Technischer Support (AP11.1–AP11.2)

Umsetzung und Ergebnisse:

- Einrichtung von **Support-Kanälen** (E-Mail, Telefon) für Testnutzer und Pilotkunden.
- Erstellung erster **Anleitungen** für das Onboarding sowie interner FAQ-Dokumente.
- Dokumentation wiederkehrender Fragen zur Verbesserung von Produkt und Hilfetexten.

Aufgrund der begrenzten Anzahl an Pilotnutzern blieb das Supportvolumen überschaubar, lieferte aber wertvolle Hinweise zur Verständlichkeit der Anwendung.

3.13 AP12 – Umsetzung technischer Optimierungsvorschläge

Umsetzung und Ergebnisse:

- Zusammenführung der aus Tests, Pilotierung, Investoren- und Partnergesprächen abgeleiteten **Optimierungsvorschläge**.
- Umsetzung von Verbesserungen in Frontend und Backend, u. a.:
 - Performance-Optimierungen bei komplexen Abfragen,
 - Anpassungen der Datenmodellierung zur besseren Erweiterbarkeit,
 - Verbesserungen im Berechtigungsmodell.
- Integration der GraphRAG-Struktur in den bestehenden Code, inkl. Anpassung bisheriger Logik.

AP12 diente der Konsolidierung und Stabilisierung der Lösung.

3.14 AP13 – Messe- und Kundenauftritte

Umsetzung und Ergebnisse:

- Teilnahme an mehreren Konferenzen und Veranstaltungen, u. a.:
 - Bits & Pretzels 2024 und 2025,
 - AI Week Frankfurt 2025,
 - Hinterland of Things 2024.
- Teilnahme an **Pitch-Formaten**, u. a.:
 - ECSO Investor Days (Berlin 2024, Bochum 2025),
 - Veranstaltungen des CISP Helmholtz-Zentrums für Informationssicherheit in Saarbrücken und Berlin.

- **Messeauftritt am CISPA-Stand auf der it-sa 2024 in Nürnberg**, bei dem der OdySecure-Ansatz und die GraphRAG-Architektur gegenüber Fachpublikum aus IT-Sicherheit, Beratung und Industrie vorgestellt wurden.
- Durchführung individueller **Kundengespräche und Demos** mit potentiellen Pilotkunden und Partnern.

Diese Aktivitäten dienen sowohl der Testkundenakquise als auch der Schärfung der Marktpositionierung.

3.15 AP14 – Kommunikationsschulung und Wissenstransfer

Umsetzung und Ergebnisse:

- Durchführung von **Coachings für die Geschäftsführung**, insbesondere zu Investorengesprächen, Storytelling und zielgruppenorientierter Kommunikation im KMU-Segment.
- Interner Wissenstransfer zu Methoden wie Risikoermittlung, Vorgehen in Assessments und Einsatz von OdySecure im Beratungs- und Virtual-CISO-Kontext.
- Erarbeitung einheitlicher **Argumentationslinien** für Gespräche mit Kunden, Investoren und Partnern.

3.16 AP15 – Kontaktverwaltung / Aufbau einer CRM-Datenbank

Umsetzung und Ergebnisse:

- Einrichtung einer **einfachen CRM-Lösung** zur strukturierten Erfassung von Kontakten, Leads, Veranstaltungen und Gesprächsständen.
- Erfassung von Testkunden-, Interessenten- und Investorendaten sowie der jeweiligen Historie (Pitches, Follow-ups, Feedback).
- Nutzung des CRM als Basis für Nachfassaktionen und Priorisierung von Vertriebsaktivitäten.

3.17 AP16 – Projektkoordination

Umsetzung und Ergebnisse:

- Planung, Steuerung und Überwachung des Projektfortschritts durch die Projektleitung (Zeitplanung, Budgetüberwachung, Abstimmung mit dem Projektträger).
- Koordination der internen und externen Ressourcen (Entwicklung, Marketing, Coaching, Dienstleister).
- Organisation der Meilensteinplanung und der regelmäßigen internen Statusrunden.

AP16 gewährleistete einen geordneten Projektverlauf und die fristgerechte Erstellung der Berichte und Nachweise.

4. Kooperationen und Dissemination

Während im Antrag zunächst keine formale Zusammenarbeit mit Dritten für die Demonstratorentwicklung vorgesehen war, wurden im Projektverlauf mehrere **Kooperationsbeziehungen** aufgebaut bzw. vertieft:

- **Pilotkunde:** ADVISORI FTC GmbH (Frankfurt). Einsatz der Plattform im eigenen ISMS-Kontext, regelmäßige Feedbackschleifen mit dem Informationssicherheitsbeauftragten.
- Potentielle Marktplatzpartner: Gespräche mit
 - einem Anbieter von Breach-Informationen (Darknet-Monitoring),
 - einem Beratungsunternehmen für Security-Assessments,
 - zwei SOC-Anbietern (SOC-as-a-Service und On-Premises-Lösungen), mit grundsätzlicher Kooperationsbereitschaft bei ausreichender Kundenbasis.

Dissemination und Sichtbarkeit:

- Präsentationen und Pitches auf den genannten Veranstaltungen (Bits & Pretzels, AI Week Frankfurt, Hinterland of Things, ECSO Investor Days, CISPA-Formate).
- **Messeauftritt am CISPA-Stand auf der it-sa 2024 in Nürnberg**, bei dem OdySecure als Beispiel für einen GraphRAG-basierten Ansatz im Bereich Cybersecurity-Management vorgestellt wurde.

- Fachbeitrag „GraphRAG für transparente KI“ im Sammelband „KI-Transformation in Deutschland“ (UVK Verlag, ISBN 978-3-8252-6538-0).
 - Präsenz in sozialen Medien, insbesondere LinkedIn, mit inhaltlichen Beiträgen zum Thema Cybersicherheitsmanagement und NIS2.
-

5. Verwertung und wirtschaftliche Perspektive

Die Verwertung der Ergebnisse erfolgt über die **Cybervize Operations GmbH**:

- Die Plattform wird im Rahmen eines **Virtual-CISO-Services** eingesetzt und ist bei einem Kunden produktiv in Nutzung.
- Kurzfristig liegt der Schwerpunkt auf der **direkten Kundenansprache** (Netzwerk, LinkedIn, Website, Fachveranstaltungen) und der Nutzung der Plattform in Beratungsmandaten (z. B. ISO 27001, IT-Grundschutz, NIS2).
- Mittelfristig ist der Aufbau eines **Partnernetzwerks** (Beratungen, Virtual-CISO-Dienstleister, SOC-Anbieter, Datenprovider) geplant.
- Zur Finanzierung einer intensiveren Marktbearbeitung wird die Aufnahme eines **Förderdarlehens** geprüft.

Die wirtschaftliche Skalierung hängt maßgeblich von der Gewinnung weiterer Kunden und der Etablierung eines wiederholbaren Vertriebsprozesses ab.

6. Wissenschaftliche und technische Ergebnisse sowie Anschlussfähigkeit

Wesentliche wissenschaftlich-technische Beiträge des Projekts sind:

- Kombination einer **Ontologie für Informationssicherheit** mit semantischen Technologien und einer Graphdatenbank.
- Einsatz einer **GraphRAG-Architektur**, die Wissensgraph und Large Language Models so verbindet, dass erklärbare und auditierbare Empfehlungen entstehen.

- Übertragbarkeit des Ansatzes auf weitere Anwendungsfelder, in denen Governance-, Risiko- und Compliance-Themen strukturiert und KI-gestützt bearbeitet werden sollen.

Die Anschlussfähigkeit besteht insbesondere in:

- einer Weiterentwicklung zu einer **Plattform**, die zusätzliche Dienste (Breach-Informationen, Assessments, SOC-Leistungen) integriert,
- einer Nutzung der Wissensbasis in **anderen Domänen** (z. B. Datenschutz-Management, Compliance-Management),
- der wissenschaftlichen Weiterbearbeitung des GraphRAG-Ansatzes in Kooperation mit Forschungseinrichtungen.

7. Lessons Learned und Gründe für ausbleibende Investitionen

Die im Projekt gemachten Erfahrungen betreffen drei Ebenen:

1. Kunden- und Marktverständnis von NIS2 und Informationssicherheit,
2. technische und architektonische Entscheidungen,
3. die Perspektive von Investoren und Finanzierbarkeit.

Gemeinsam erklären sie, warum trotz guter technischer Ergebnisse kein Investment zustande kam und warum die Plattform im Markt häufig zunächst als „nur ein weiteres GRC-Tool“ wahrgenommen wird.

7.1 NIS2 als Managementaufgabe – und der „Tool-Reflex“ im Mittelstand

In Gesprächen mit mittelständischen Unternehmen, sowohl im Rahmen von Vertriebsaktivitäten als auch auf Messen und Veranstaltungen, zeigte sich über die Projektlaufzeit ein wiederkehrendes Muster:

- Sobald NIS2 oder Informationssicherheitsmanagement angesprochen wird, lautet der erste Impuls vieler Unternehmen:
„Wir holen uns jetzt ein GRC-Tool, dann sind wir für NIS2 sicher.“

Die Erwartung ist, dass sich die Anforderungen im Wesentlichen durch **Einführung einer weiteren Software** lösen lassen, ohne tiefgreifende Veränderung von Rollen, Prozessen und Entscheidungswegen. Aus Sicht des Projekts führt dieser Ansatz zu mehreren Problemen:

1. **Potemkinsche Compliance**

Es entstehen **Compliance-Silos**: In einem GRC-Tool werden Maßnahmen, Risiken und Policies dokumentiert, während die tatsächlichen Abläufe im Incident-Fall (z. B. Ransomware, Produktionsausfall) zwischen IT, Fachbereichen, HR, Rechtsabteilung und Geschäftsführung kaum geübt sind.

Auf dem Papier ist vieles „grün“, im Ernstfall fehlt jedoch die gelebte Routine – genau das, was NIS2 eigentlich erzwingen soll.

2. **Alibi-IT und Doppelpflege von Daten**

In vielen Unternehmen werden sicherheitsrelevante Informationen **zweifach gepflegt**:

- im IT-Service-Management-System (Tickets, Changes, Assets),
- im GRC-Tool (Risiken, Kontrollen, Maßnahmen).
Der Fokus verschiebt sich von **Risikoreduktion** hin zu „Systempflege“.
Diese Entkopplung verstärkt den Eindruck, Sicherheit sei ein IT-Thema und kein Management-Thema.

3. **Scheinsicherheit für die Geschäftsführung**

Wird ein GRC-Tool mit Berichten und Ampeln eingeführt, entsteht schnell der Eindruck, man habe das Thema „unter Kontrolle“.

Tatsächlich bleibt die **Haftung bei der Geschäftsführung**, insbesondere nach NIS2, solange:

- keine klaren Risk Owner benannt,
- keine regelmäßigen Risikoberichte im Management verankert,
- keine geübten Melde- und Notfallprozesse etabliert sind.
Mehrere Gespräche im Projektverlauf zeigten, dass diese Diskrepanz zwischen Tool-Status und realer Governance vielen Verantwortlichen nicht bewusst ist.

Für OdySecure hat dies eine doppelte Konsequenz:

- Einerseits bestätigt es die Grundannahme des Projekts, dass NIS2 und Informationssicherheit **Chefsache und Managementprozess** sind.
- Andererseits führt der Wunsch nach „dem einen Tool“ dazu, dass die Plattform bei Erstkontakten häufig zunächst als **weiteres GRC-Tool** eingeordnet wird, das lediglich eine bestehende Tool-Landschaft ergänzt. Der eigentliche Mehrwert, die Integration von Managementprozess, Wissensgraph und begleitender Beratung, muss zunächst ausführlich erläutert werden.

7.2 Lehren aus Testkunden- und Pilotakquise

Aus der konkreten Arbeit mit Testkunden und Interessenten ergeben sich weitere Lessons Learned:

- **Abstraktes Problem, konkreter Aufwand**
Das Risiko „Cyberangriff“ ist zwar präsent, wirkt aber abstrakt, solange kein gravierender Vorfall eingetreten ist. Der Aufwand, einen strukturierten Managementprozess aufzubauen, ist dagegen unmittelbar sichtbar. Viele Unternehmen verschieben Entscheidungen oder reduzieren den Umfang auf minimale Compliance-Erfüllung.
- **Erwartung schneller technischer Effekte**
Testkunden wünschen sich „spürbare“ Ergebnisse in Form von technischen Maßnahmen, die unmittelbar Angriffe verhindern. Ein Managementsystem entfaltet seinen Nutzen jedoch über **Struktur, Priorisierung und Entscheidungsfähigkeit**. Dieser Nutzen zeigt sich mittel- bis langfristig, was die Bereitschaft zur aktiven Mitarbeit in Pilotprojekten reduziert.
- **Rollen- und Verantwortungsunklarheit**
Häufig ist unklar, **wer** im Unternehmen das Thema Informationssicherheit fachlich führen soll: IT-Leitung, Geschäftsführung, Compliance, Datenschutz oder externer Dienstleister. Ohne klare Rollenzuordnung bleibt das Problem „zwischen den Stühlen“ und kommt nicht in die Umsetzung.

Diese Faktoren erschweren es, ausreichend Testkunden zu gewinnen, die bereit sind, Zeit und interne Ressourcen in einen strukturierten Pilotbetrieb zu investieren. Für OdySecure bedeutet dies, dass die Lösung fachlich als sinnvoll wahrgenommen wird, die **organisatorische Aufnahmefähigkeit** in vielen Unternehmen aber (noch) begrenzt ist.

7.3 Technische und architektonische Lessons Learned

Auf technischer Ebene ist die wichtigste Erkenntnis:

- Ein **statisches, regelbasiertes Expertensystem** skaliert nicht mit der Dynamik von Normen, Bedrohungen und internen Policies.
- Die Umstellung auf eine **GraphRAG-Architektur** – also die Kombination aus Wissensgraph und Sprachmodell – bietet:
 - bessere Erweiterbarkeit bei neuen Normkapiteln, Branchenanforderungen oder internen Regelwerken,
 - höhere Erklärbarkeit, da Entscheidungen auf Pfade im Graphen zurückgeführt werden können,
 - geringere Wartungskosten, weil nicht jede Änderung in Form von Einzelregeln kodiert werden muss.

Diese Entscheidung hat den initialen Architektur- und Implementierungsaufwand erhöht, verbessert aber die **Langzeitstabilität und Wartbarkeit** der Lösung deutlich. Sie trägt dazu bei, dass OdySecure nicht als weiteres Formular- oder GRC-Frontend, sondern als inhaltlich fundierte Wissensbasis und Entscheidungsunterstützung verstanden werden kann – auch wenn dies in der Marktkommunikation zunächst erklärt werden muss.

7.4 Investorenperspektive und Finanzierbarkeit

Die Gespräche mit Investoren im Rahmen von Veranstaltungen (u. a. Bits & Pretzels, ECSO Investor Days, CISPA-Formate, it-sa) führten zu einem konsistenten Bild:

- **Traktion vor Technologie**
Investoren betonen, dass sie primär in belastbare Marktbeweise investieren, also in wiederkehrende Umsätze, wachsende Kundenbasis und skalierbare Vertriebsprozesse. Die vorhandene Traktion (ein produktiv betreuter Kunde, laufende Gespräche und Pilotinitiativen) genügte für ein klassisches VC-Investment nicht.
- **Komplexe Story, schwierige Kategorisierung**
OdySecure bewegt sich an der Schnittstelle von ISMS, Risikomanagement, GRC und KI-gestützter Beratung. Für viele Investoren ist es einfacher, in klar

umrissene Kategorien zu investieren (z. B. Endpoint-Security, SOC-Dienstleistung, einzelnes SaaS-Tool). Ein integrierter Managementansatz, der Organisationsentwicklung, Prozesse und Technologie kombiniert, lässt sich schwerer in bestehende Portfolios einordnen.

- **Wahrnehmung eines „vollen“ Security-Marktes**

Von Investorensseite wird der Security-Markt regelmäßig als stark belegt beschrieben. Die tatsächliche Lücke, die **organisatorische Prozessseite von Cyber-Governance**, wird in vielen Investmentthesen noch nicht explizit adressiert. Dadurch ist es schwierig, das spezifische Differenzierungsmerkmal von OdySecure klar zu verankern.

7.5 Zusammenfassung der Gründe für das Ausbleiben eines Investments

Aus der Kombination dieser Ebenen lassen sich die wesentlichen Gründe ableiten, warum es im Projektzeitraum nicht zu einer Investorenfinanzierung gekommen ist:

1. **Zu geringe Marktdurchdringung und Traktion**

Die Anzahl der zahlenden Kunden und die Umsatzdynamik reichten nicht aus, um klassische VC-Kriterien zu erfüllen, obwohl die technische Basis des Produkts solide ist.

2. **Erklärungsbedürftige Positionierung und Tool-Missverständnis**

OdySecure wird in Erstgesprächen häufig als weiteres GRC-Tool wahrgenommen. Der eigentliche Mehrwert – die Verbindung von Managementprozess, Wissensgraph, NIS2-Governance und begleitender Beratung (Virtual CISO) – erschließt sich erst nach ausführlicher Erklärung. Das erhöht den Aufwand in der Akquise und erschwert eine schnelle Skalierung.

3. **Strukturelle Marktbarrieren im Mittelstand**

Viele Unternehmen behandeln NIS2 noch nicht oder lediglich als **Tool- oder IT-Projekt**. Die notwendige Verankerung als **integriertes Managementthema** (inklusive Risk Ownern, regelmäßigen Risikoberichten und geübten Notfallprozessen) ist noch nicht flächendeckend vorhanden. Damit fehlt ein breiter Markt, der eine stark wachstumsorientierte Investmentstory kurzfristig tragen könnte.

Für die Cybervize Operations GmbH bedeutet dies, dass in der nächsten Phase weniger ein reines Technologierisiko, sondern vor allem ein **Go-to-Market- und**

Organisationsreife-Problem adressiert werden muss: Unternehmen müssen dabei unterstützt werden, NIS2 und Informationssicherheit tatsächlich als Managementaufgabe zu verstehen und nicht nur als weiteres Toolprojekt. Die Kombination aus Virtual-CISO-Service und Plattform ist hierfür ein Ansatz, der über die Projektlaufzeit hinaus weiterverfolgt wird.

8. Zusammenfassung

Mit OdySecure wurde im Rahmen des Vorhabens FKZ 16KIS1972 eine **GraphRAG-basierte SaaS-Plattform** entwickelt, die KMU und mittelständische Unternehmen dabei unterstützt, Cybersicherheit als Managementprozess zu verstehen und zu steuern.

Die im Antrag formulierten **fachlichen und technischen Ziele** – Aufbau eines AI-gestützten Expertensystems, Entwicklung eines Demonstrators, Integration semantischer Technologien, Community-Funktion und Einbindung menschlicher Beratung – wurden im Kern erreicht, wobei die Expertensystem-Architektur bewusst zugunsten eines moderneren GraphRAG-Ansatzes weiterentwickelt wurde.

Die **wirtschaftliche Skalierung** und der Nachweis eines breiten Product-Market-Fit stehen noch aus. Die im Projekt gewonnenen Erkenntnisse zu Markt, Kundenverhalten, Technologiearchitektur und Investorenanforderungen bilden eine belastbare Grundlage für die weitere Entwicklung und Verwertung durch die Cybervize Operations GmbH.