

Kurzbericht zum Vorhaben FKZ 16KIS1972 „OdySecure“

Laufzeit: 01.10.2023 – 28.02.2025

Zuwendungsempfänger: Cybervize Operations GmbH

1. Ausgangssituation und Zielsetzung

Viele kleine und mittlere Unternehmen (KMU) in Deutschland sehen Cybersicherheit weiterhin überwiegend als technisches Thema. Investiert wird vor allem in Einzelmaßnahmen wie Firewalls, Endpoint-Protection oder Backup-Lösungen. Moderne Standards und Regulierungen (u. a. ISO/IEC 27001, IT-Grundschutz, NIS2) fordern jedoch ein **Managementsystem für Informationssicherheit**, das Risiken aus Geschäftsprozess-Sicht betrachtet und klare Verantwortlichkeiten im Management etabliert.

In Gesprächen mit Unternehmen zeigte sich ein wiederkehrender „Tool-Reflex“: NIS2 und Informationssicherheit werden häufig als **GRC- oder IT-Projekt** verstanden („Wir kaufen ein Tool, dann sind wir compliant“). Dies führt zu „potemkinscher Compliance“: Auf dem Papier sind Ampeln grün, im Ernstfall fehlen jedoch geübte Abläufe zwischen IT, Fachbereichen und Geschäftsführung.

Ziel des Vorhabens **OdySecure** war es daher, eine **kosteneffiziente, KI-gestützte Lösung** zu entwickeln, mit der KMU und auch mittelständische Unternehmen ein wirksames Management der Cybersicherheit aufbauen können, nicht als weiteres isoliertes Tool, sondern als Unterstützung eines integrierten Managementprozesses. Geplant waren:

- ein AI-basiertes Expertensystem auf Basis eines Wissensgraphen,
 - eine mandantenfähige SaaS-Plattform zur strukturierten Erfassung von Risiken, Prozessen, Assets und Maßnahmen,
 - eine Community-Funktion zum Wissensaustausch,
 - die Integration menschlicher Beratung, z. B. als Virtual-CISO-Service.
-

2. Wesentliche Arbeiten und Projektverlauf

Die Arbeiten gliederten sich in 16 Arbeitspakete (AP1–AP16).

- In den AP2 und AP3 wurden **Backend und Frontend** der Plattform entwickelt: Datenmodelle, Graphdatenbank, APIs, Mandantenfähigkeit, Rollen- und Rechtemodell sowie Benutzeroberfläche für Risikoregister, Maßnahmenpläne und Management-Dashboards.

- In AP2.3 und AP4 wurde eine **Ontologie für Informationssicherheit** auf Basis von ISO 27001 und IT-Grundschutz modelliert und ein Maßnahmenkatalog aufgebaut, der Risiken, Prozesse und Normanforderungen miteinander verknüpft.
- Die ursprünglich geplante regelbasierte Expertensystem-Architektur wurde im Verlauf durch eine **GraphRAG-Architektur** ersetzt: Ein Wissensgraph bildet Normen, Risiken und Maßnahmen ab; ein Large Language Model generiert darauf aufbauend erklärbare Empfehlungen.
- In AP5, AP6 und AP11 wurden **Infrastruktur, Tests und Supportprozesse** aufgebaut, um einen stabilen Betrieb des Demonstrators sicherzustellen.
- AP7, AP8, AP9 und AP10 adressierten **Community, Marketing, Kommunikationsinhalte und User Experience**. Die Community-Funktion wurde technisch umgesetzt, konnte mangels aktiver Testkunden jedoch nicht in die Breite wachsen.
- In AP13 erfolgte die **Präsentation des Projekts** auf Fachveranstaltungen (u. a. Bits & Pretzels, AI Week Frankfurt, Hinterland of Things, ECSO Investor Days, CISPAs-Formate, it-sa 2024 am CISPAs-Stand in Nürnberg).
- AP14 bis AP16 umfassten **Kommunikationscoaching, CRM-Aufbau und Projektkoordination**.

Ein Pilotkunde (ADVISORI FTC GmbH, Frankfurt) setzte die Plattform in seinem eigenen ISO-27001-Kontext ein. In regelmäßigen Feedbackrunden wurden Funktionsumfang, Benutzerführung und Berichtslogik iterativ verbessert.

3. Ergebnisse und Zielerreichung

Die im Antrag formulierten **fachlichen und technischen Ziele** wurden im Kern erreicht:

- Es liegt eine **mandantenfähige SaaS-Plattform** vor, mit der Unternehmen Geschäftsprozesse, Assets, Risiken, Maßnahmen und Nachweise strukturiert erfassen und auswerten können.
- Die im Projekt entwickelte **Ontologie und der Wissensgraph** bilden zentrale Anforderungen aus ISO 27001 und IT-Grundschutz ab und können perspektivisch um weitere Normen erweitert werden.
- Das geplante Expertensystem wurde als **GraphRAG-Lösung** umgesetzt: Empfehlungen sind an konkrete Pfade im Wissensgraphen gekoppelt und damit nachvollziehbar und auditierbar.
- Die Plattform ist in einen **Virtual-CISO-Service** integriert und wird bei einem Kunden produktiv genutzt.
- Die Community-Funktion wurde technisch realisiert; aufgrund zu geringer Nutzerzahlen konnte ihre Wirksamkeit jedoch noch nicht validiert werden.
- Ein **funktionsfähiger Demonstrator** wurde in Pitches, bei Kunden und auf Messen eingesetzt.

Nicht vollständig erreicht werden konnte der geplante **Product-Market-Fit über mehrere zahlende Kunden**. Trotz positiver Rückmeldungen zu Konzept und Technologie gelang es innerhalb der Projektlaufzeit nicht, eine ausreichende Zahl von KMU zu einem aktiven, zahlenden Einsatz der Lösung zu bewegen. Gründe hierfür lagen u. a. im starken Fokus vieler Unternehmen auf Tool-Beschaffung statt Managementprozess, in begrenzten Vertriebskapazitäten sowie in der hohen Erklärungsbedürftigkeit des Ansatzes.

4. Verwertung, Anschlussfähigkeit und Veröffentlichungen

Die Verwertung der Projektergebnisse erfolgt durch die **Cybervize Operations GmbH**:

- Die Plattform wird im Rahmen eines **Virtual-CISO-Services** eingesetzt und soll künftig verstärkt in Beratungsprojekten (ISO 27001, IT-Grundschutz, NIS2) genutzt werden.
- Kurzfristig liegt der Schwerpunkt auf **direkter Kundenansprache** und der Einbettung in Beratungsleistungen; 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.

Wissenschaftlich-technisch sind insbesondere hervorzuheben:

- die Kombination einer **Ontologie für Informationssicherheit** mit einer Graphdatenbank und KI-gestützten Auswertungen,
- die Umsetzung einer **GraphRAG-Architektur** für erklärbare Empfehlungen im Kontext Informationssicherheitsmanagement.

Die Anschlussfähigkeit besteht in der Erweiterung der Plattform um zusätzliche Dienste (Breach-Informationen, Assessments, SOC) sowie in der Übertragung des Ansatzes auf andere Governance- und Compliance-Domänen.

Veröffentlichungen und Außenwirkung:

- Fachbeitrag „GraphRAG für transparente KI“ im Sammelband „KI-Transformation in Deutschland“ (UVK Verlag, ISBN 978-3-8252-6538-0).
- Präsentationen und Pitches auf verschiedenen Veranstaltungen (Bits & Pretzels, AI Week Frankfurt, Hinterland of Things, ECSO Investor Days, CISPA-Formate, it-sa 2024 in Nürnberg).
- Laufende Kommunikation über LinkedIn mit Beiträgen zu NIS2, Cybersicherheitsmanagement und der Abgrenzung zwischen Tool-Fokus und Managementprozess.

Insgesamt hat das Projekt gezeigt, dass der Bedarf an integrierten Managementlösungen für Cybersicherheit vorhanden ist, das Verständnis und daraus resultierende Bedarf vieler KMU und mittelständischer Unternehmen jedoch noch nicht ausreicht, um einen breiten, skalierbaren Einsatz kurzfristig zu erreichen. Die im Projekt aufgebauten technischen Grundlagen und Erfahrungen bilden eine belastbare Basis für die weitere Produkt- und Marktentwicklung.