Bewertung des Security-Reifegrads der Lieferkette

Knowledge Graph als Grundlage für ein digitales Security-Lieferantenmanagement

#Security #Knowledge Graph #Lieferketten #KI

Der Beitrag stellt die aktuellen gesetzlichen und regulatorischen Security-Anforderungen an Unternehmen und deren komplexen Lieferketten zwischen Betreibern und Dienstleistern und Lieferanten dar. Die Beherrschung dieser Anforderungen erfordert effiziente Prozesse und eine semantische Modellierung der Informationen. Daher wird ein risikobasierter, plattformgestützter Prozess dargestellt, der den Security-Reifegrad der Lieferkette bewertet und überwacht. Eine wichtige Grundlage dieses Ansatzes ist das Know-how von Security-Experten. Um den manuellen Aufwand zu reduzieren, wird die Entwicklung eines Knowledge Graphen präsentiert, der zusammen mit generativer KI den Prozess unterstützen kann.

This article presents the current legal and regulatory security requirements for companies and their complex supply chains between operators, service providers, and suppliers. Mastering these requirements calls for efficient processes and semantic modeling of information. Therefore, a risk-based, platform-supported process is presented that evaluates and monitors the security maturity level of the supply chain. An important basis for this approach is the expertise of security experts. To reduce manual effort, the development of a knowledge graph is presented, which, together with generative AI, can support the process.

Christian Siegwart, ZeMA gGmbH;
Michael Krammel, K4 DIGITAL GmbH;
Felix Scherhag, ZeMA gGmbH,
Georg Frey, Universität des Saarlandes

▶ PEER-REVIEW: 20.12.2025

1. Einleitung und Motivation

Die zunehmende Digitalisierung in Unternehmen mit neuen digitalen Geschäftsmodellen, vernetzten Produktionen und stark automatisierten Prozessen steigert die Wettbewerbsfähigkeit bringt aber meist eine steigende Komplexität der Wertschöpfungskette mit sich. Prozesse oder Dienstleistungen werden global vernetzt mit darauffolgend steigender Abhängigkeit von externen Dienstleistern und Lieferanten. Daher ist es für alle Unternehmen wichtig, sich mit den Stakeholdern längs der eigenen Lieferkette auseinanderzusetzen. Der entsprechende Bereich nennt sich Supply Chain Management (SCM) und befasst sich mit dem Management aller Aktivitäten, inklusive Risikomanagement, die die Stakeholder der eigenen Lieferkette betreffen [1].

Die Bedrohung durch Cyberangriffe über die Lieferkette hat in den letzten Jahren stark zugenommen und stellt eine ernste Gefahr für viele Unternehmen dar. Angreifer nutzen dabei gezielt Schwachstellen bei externen Partnern aus, um Zugang zu sensiblen Systemen und Daten ihrer eigentlichen Zielunternehmen zu erlangen [2, 3]. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet diese Supply-Chain-Angriffe als ernstzunehmende Bedrohung für die deutsche produzierende Wirtschaft [4]. Vor diesem Hintergrund wird deutlich, dass das klassische Supply Chain Management um das Management von Informationssicherheitsrisiken erweitert werden muss.

1.1 Gesetzliche und regulatorische Anforderungen

Im Kontext der Informationssicherheit entlang der Lieferkette gewinnen gesetzliche Regelungen zunehmend an Bedeutung, insbesondere für Betreiber

kritischer Infrastrukturen (KRITIS, bspw. Energie, Wasser, Transport, Gesundheit oder Telekommunikation). Mit dem IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0 [5]) hat der deutsche Gesetzgeber auf die wachsende Bedrohungslage reagiert und für zugehörige Unternehmen verpflichtende Anforderungen zur Einführung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus definiert. Dazu zählen unter anderem Meldepflichten, die Einrichtung von Systemen zur Angriffserkennung oder auch die Betrachtung von Security-Aspekten für die eigenen Dienstleister und Lieferanten.

Auch auf europäischer Ebene wurde die zunehmende Gefahr durch Cyberangriffe erkannt. Die EU-Richtlinie NIS2 (Network and Information Security Directive [6]), die Anfang 2023 in Kraft trat, verpflichtet viele mittlere und große Unternehmen in systemrelevanten Branchen zur Umsetzung umfassender Maßnahmen im Bereich Informationssicherheit. Zur Umsetzung der EU-Verordnung wurde in Deutschland im Dezember 2025 das NIS2-Umsetzungsgesetz [7] verabschiedet. Besonders hervorzuheben ist Artikel 21 der NIS2-Richtlinie, der explizit die Risiken aus der Zusammenarbeit mit Drittparteien adressiert:

„Artikel 21: Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;“ [6]

Zur Erfüllung der gesetzlichen Anforderungen spielen nationale und internationale Normen eine zentrale Rolle. Sie bieten praxisorientierte Leitlinien, um Sicherheitsmaßnahmen strukturiert und nachvollziehbar umzusetzen. Besonders hervorzuheben ist in diesem Kontext die Normenreihe ISO/IEC 2700x, die als international anerkannter und zertifizierbarer Standard für Informationssicherheitsmanagementsysteme (ISMS) gilt. Der zentrale Teil, ISO/IEC 27001 [8], definiert Anforderungen an ein ISMS und behandelt im Annex A, einem umfangreichen Katalog mit 93 Maßnahmen (Controls). In vier spezifischen Controls werden Maßnahmen dargestellt, die sich mit Auswahl, Bewertung, Überwachung und Management von externen Dienstleistern und Lieferanten befassen. Diese Controls werden im Rahmen der ISO/IEC 27036 [9] weiter konkretisiert. Die ISO/IEC 27036 stellt damit eine spezifische Ergänzung dar, die sich auf Security-Anforderungen in Lieferantenbeziehungen konzentriert.

Weitere relevante Normen (vgl. Tabelle 1)., adressieren spezifische Aspekte des Security-Lieferantenmanagements. Diese Normen unterstützen Unternehmen nicht nur bei der Implementierung von Informationssicherheitsmaßnahmen, sondern dienen auch als Nachweis gegenüber Meldestellen und Geschäftspartnern.

Viele Unternehmen haben Schwierigkeiten bei der Etablierung eines Informationssicherheitsprozesses und der Umsetzung der damit verbundenen Informationssicherheitsanforderungen [14, 15]. Auch die europäische Union gibt dies als einen der Gründe für die Entwicklung der NIS2-Richtlinie an. Daher bemühen sich Verbände und Kooperationen Best-Practices und Mindestempfehlungen zu veröffentlichen. Hervorzuheben ist hierbei das National Institute of Standards and Technology (NIST), das mit dem NIST Cybersecurity Framework (CSF) [16] ein international

Tabelle 1: Relevante Normen, die spezifische Aspekte des Security Lieferantenmanagements adressieren.

Norm	Beschreibung
ISO/IEC 27001 [8]	Zentrales Rahmenwerk für den Aufbau eines Informationssicherheits-managementsystems (ISMS)
ISO/IEC 27002 [10]	Umsetzungsempfehlungen zu den Controls aus der ISO/IEC 27001
ISO/IEC 27036-2 [9]	Leitfaden zur Informationssicherheit in Lieferantenbeziehungen und ausgelagerten Dienstleistungen (Teil 2: Anforderungen)
TISAX® [11]	Branchenstandard in der Automobilindustrie zur Prüfung von Informationssicherheit
BSI IT-Grundschutz [12]	Der BSI IT-Grundschutz ist ein vom Bundesamt für Sicherheit in der Informationstechnik entwickeltes methodisches Vorgehen zur Identifikation und Umsetzung von Sicherheitsmaßnahmen in Organisationen.
DIN EN IEC 62443-2-4 [13]	Fokussiert auf industrielle Automatisierungssysteme, inklusive Supply Chain Security für die Rollen Hersteller, Integrator und Betreiber

anerkanntes Modell zur strukturierten Steuerung von Informationssicherheits-Risiken bereitstellt. Domänenspezifisch ergänzt wird das Framework durch den NIST Report 8276 (NIST IR 8276 [17]), der die Risiken entlang der Lieferkette risikobasiert betrachtet und entsprechende Empfehlungen darstellt.

Im deutschsprachigen Raum haben sich ergänzend praxisnahe Ansätze etabliert. Der VDMA hat eine Supply-Chain-Security-Dokumentenreihe veröffentlicht, in der unter anderem eine standardisierte Lieferanten-Selbstauskunft Mindestanforderungen an die Informationssicherheit von Dienstleistern und Lieferanten adressiert. Die UP-KRITIS-Empfehlungen erweitern diesen Ansatz um spezifische Anforderungen für Betreiber kritischer Infrastrukturen und deren Zulieferer und dienen als Best-Practice-Katalog für ein risikobasiertes Security-Lieferantenmanagement.

Diese Standards und Best-Practices helfen bei der Einschätzung des Problems, liefern aber noch keine zufriedenstellende Lösung für die Unternehmen im operationellen Umgang mit dem Risiko, das von der Lieferkette ausgeht.

1.2 Aufgaben und Ziele des Security-Lieferantenmanagements

In vielen Unternehmen, insbesondere in der produzierenden Industrie, wird das Thema Security-Lieferantenmanagement bislang nur unzureichend adressiert. Eine vom TÜV-Verband durchgeführte Studie [21] zeigt dass nur rund 30 % der befragten Unternehmen Security-Anforderungen an Unternehmen in der Lieferkette stellen. Konkrete Audits führen noch deutlich weniger Unternehmen durch. Während regulatorische Anforderungen und zunehmende Bedrohungen eine systematische Betrachtung und Bewertung der Partner erfordern, fehlt es in der Praxis häufig an effizienten Verfahren. Oft beschränkt sich die Security-Bewertung der Dienstleister und Lieferanten auf selbst erstellte Fragebögen, die ohne tiefergehende Betrachtung von Unternehmen der Lieferkette beantwortet und zurückgesendet werden. Danach erfolgt auf Betreiberseite durch die mangelnde Standardisierung meist keine systematische Prüfung oder Plausibilisierung der zurückgesendeten Ergebnisse. Dies führt zu einer geringen Aussagekraft der Ergebnisse, da weder eine objektive Bewertung noch eine systematische Risikoeinschätzung möglich ist. Eine kontinuierliche Überwachung und Überprüfung der Lieferantenbeziehungen, wie es die Standards fordern, ist so kaum umzusetzen. Auch ist es mit dieser Vorgehensweise schwierig auf die Ressourcenprobleme in Form von fehlender Zeit und Know-how bei Unternehmen in der Lieferkette einzugehen.

Die Aufgabe des Security-Lieferantenmanagements ist es, Informationssicherheitsrisiken entlang der Lieferkette systematisch zu erkennen und zu bewerten, um anschließend geeignete Maßnahmen treffen zu können. Dabei steht nicht nur die Einhaltung regulatorischer Anforderungen im Vordergrund, sondern auch der Aufbau vertrauensvoller Partnerschaften innerhalb der Lieferkette, die das eigene Informationssicherheitsniveau weiterentwickeln. Die konkreten Ziele lassen sich wie folgt zusammenfassen:

- Kontinuierliches Monitoring des Security-Reifegrades der Dienstleister und Lieferanten in der Lieferkette zur Erkennung Security-relevanter Veränderungen
- Priorisierung der Zusammenarbeit mit Partnern, die ihre Informationssicherheitsanforderungen nachweisen können oder bereit sind, diese weiterzuentwickeln
- Integration von Security in der Lieferkette als kontinuierlicher, auswertbarer Prozess statt punktueller Prüfungen
- Vertrauensvolle Weiterentwicklung des Security-Reifegrades in der Lieferkette durch partnerschaftliche Zusammenarbeit mit Lieferanten, Dienstleistern und Security-Experten

2. Plattformgestütztes Security-Lieferantenmanagement

Um die oben beschriebenen Ziele des Security-Lieferantenmanagements zu erreichen, ist eine stärkere Automatisierung der Auswertung und die Zusammenarbeit aller Beteiligten notwendig. Dies erfordert einen Ansatz, der auf einer digitalen Platt-

Tabelle 2: Empfehlungen und Best Practices im Kontext Security Lieferantenmanagement.

Best Practice	Beschreibung
NIST IR 8276 [17]	Anforderungen und Empfehlungen zum Cyber Supply Chain Risk Management
IKT-Minimalstandard [18]	Mindestanforderungen im Bereich Informationssicherheit für Betreiber kritischer Infrastrukturen in der Schweiz, aufbauend auf dem NIST CSF
VDMA Selbstauskunft [19]	Standardisierte Selbsteinschätzung zur Informationssicherheit von Lieferanten
UP-KRITIS Empfehlungen [20]	Best-Practice-Anforderungen an Lieferanten Kritischer Infrastrukturen

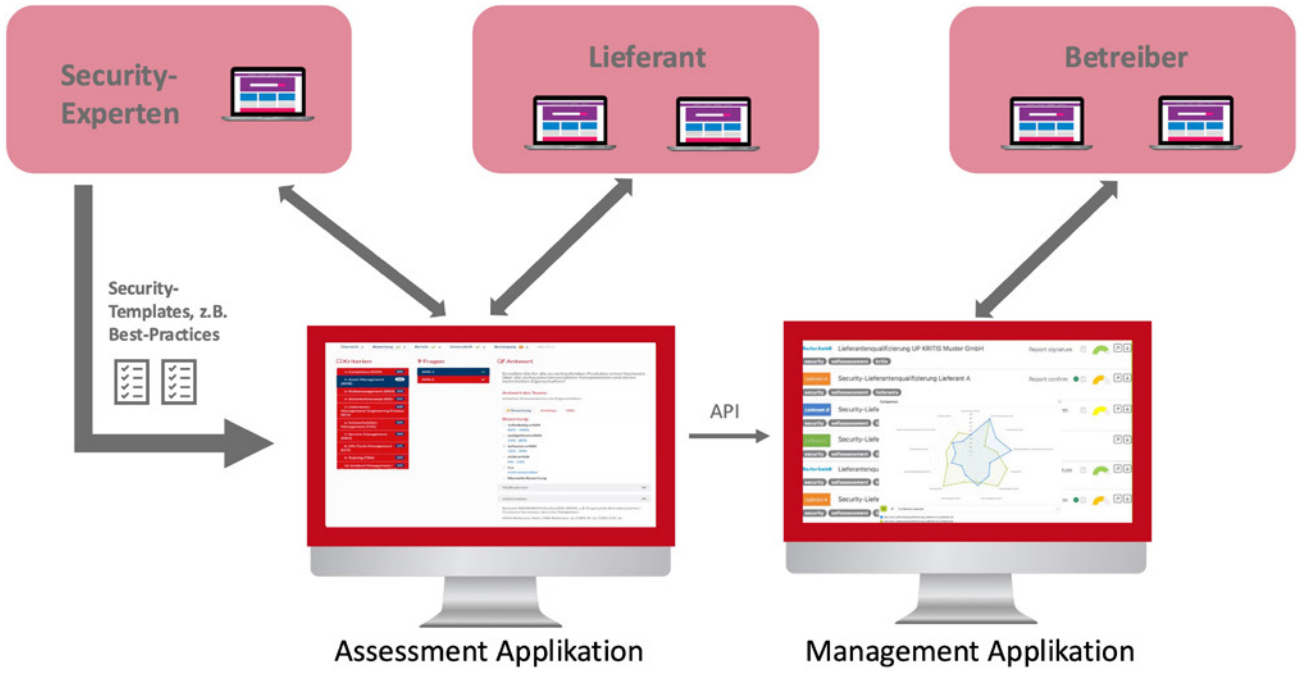

Abbildung 1: Aufbau der am MDZ Saarbrücken realisierten Demo-Plattform für digitales Security-Lieferantenmanagement.

form basiert, die es ermöglicht, entsprechende Security-Assessments in einem digitalen Prozess mit Betreiber, Lieferanten und externen Experten (Coaching) gemeinsam durchzuführen. Der Coaching-Ansatz bietet den enormen Vorteil, dass bei Problemen auf Betreiber- oder auch Lieferantenseite zeitnah und gezielt unterstützt werden kann, da eine Begleitung von der Entwicklung eines passenden Fragebogens über die Beantwortung und Bewertung bis zum Abschluss eines Assessments vorhanden ist.

Ein zentrales Gestaltungsprinzip des vorgestellten Ansatzes ist die konsequente Nutzung standardisierter Security-Informationen (z. B. VDMA, UP KRITIS). Durch Standardisierung und Zentralisierung im Rahmen der Plattform können Mehrfacherhebungen vermieden und Audit-Aufwände entlang der Lieferkette reduziert werden, da einmal erfasste Informationen nutzbar bleiben (z. B. unterschiedliche Betreiber, Standorte oder Abteilungen).

Für den Einsatz einer digitalen Plattform in diesem speziellen Kontext spielen die folgenden Kriterien eine zentrale Rolle:

- Kollaborative Durchführung der Security-Qualifizierungen (Assessments) mit der Möglichkeit des Austausches zwischen Betreiber, Lieferant und Security-Experten.
- Möglichkeit zur Erstellung und flexiblen Nutzung von standardisierten Anforderungskatalogen (Experten-Know-how).
- Integration von Hilfestellungen für die Lieferanten zur Beantwortung und Bewertung des Fragenkataloges.
- Entwicklung und Umsetzung eines möglichst einfachen Workflows abgestimmt auf das Szenario Security-Lieferantenmanagement.
- Steigerung der Effizienz durch eine automatisierte Reportgenerierung auf Basis anpassbarer Templates.
- Übersichtliche Möglichkeit für den Betreiber zur Darstellung des Security-Reifegrades der Partner in der Lieferkette.
- Möglichkeit zum Vergleich der Ergebnisse zwischen unterschiedlichen Lieferanten und Dienstleistern.

Abbildung 1 zeigt den Aufbau der entwickelten Plattform. Eine Assessment-Applikation mit entsprechenden Security-Templates zur gemeinsamen Durchführung der Lieferantenqualifizierungen und eine Management-Applikation, die die Verwaltung und die Darstellung der Ergebnisse für den Betreiber übernimmt. Im Folgenden wird die Funktionalität näher erläutert. Dazu gehören der dahinterliegende risikobasierte Ansatz, die Rollenbeschreibungen aller Beteiligter sowie der Prozess zur Durchführung der Assessments.

2.1 Risikobasierter Ansatz

Ein risikobasiertes Vorgehen im Security-Lieferantenmanagement erfordert die Etablierung eines strukturierten Prozesses im Unternehmen. Im ersten Schritt muss definiert werden, welche Risikostufen für die Klassifizierung von Dienstleistern und Lieferanten sinnvoll sind. Eine umfassende Bewertung des

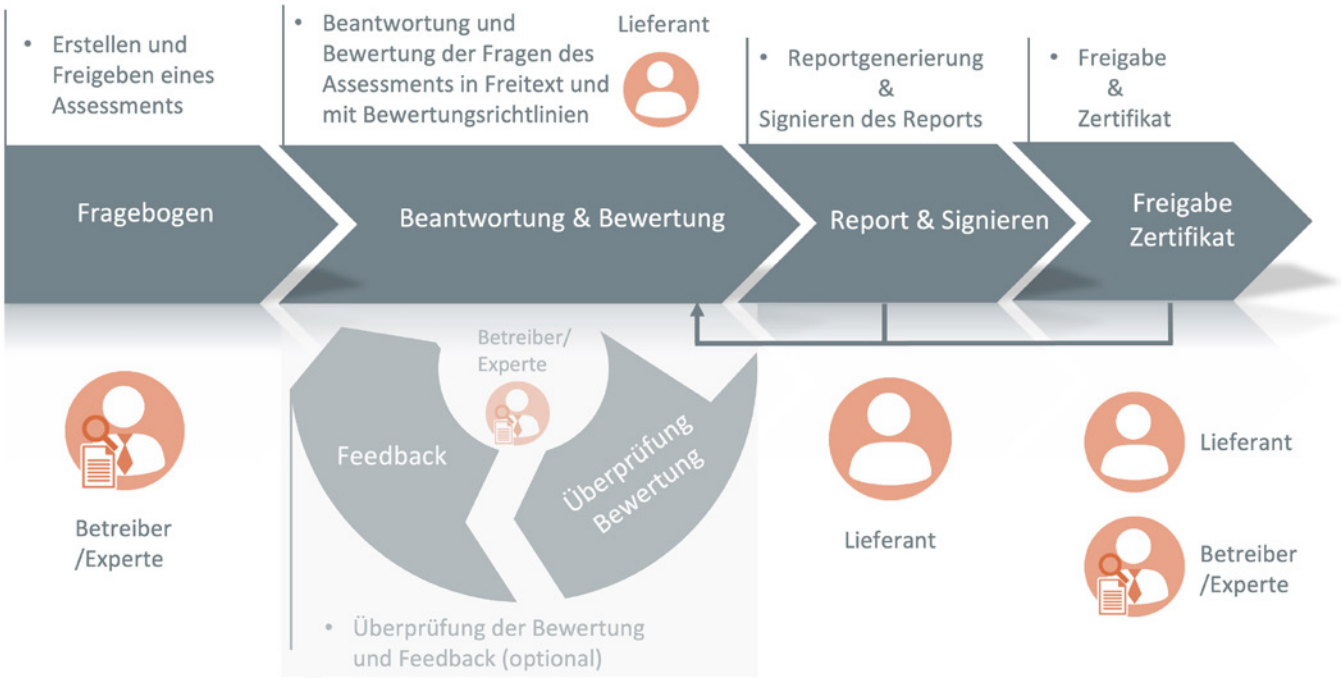

Abbildung 2: Darstellung des Prozesses zur Lieferantenqualifizierung auf der Plattform.

Security-Reifegrades aller Lieferanten ist meist mit einem unverhältnismäßig hohen Aufwand verbunden, weshalb eine gezielte Auswahl notwendig ist. Entscheidend ist daher zunächst die Identifikation der kritischen Lieferanten, die essenziell für den Betrieb der Geschäftsprozesse des Betreibers sind.

Im zweiten Schritt werden für diese Dienstleister und Lieferanten spezifische Security-Assessments erstellt, um den Reifegrad zu bewerten. Für bereits nach einem Security-Standard, z. B. ISO 27001, zertifizierte Unternehmen wird in diesem Schritt der Geltungsbereich der Zertifizierung überprüft und sie werden in das Monitoring aufgenommen. Der inhaltliche Aufbau der Security-Assessments kann durch Security-Experten unterstützt werden und wird in Abschnitt 3 näher beschrieben. Die Beantwortung und Bewertung liegen im Falle einer Selbstauskunft in der Verantwortung des Lieferanten, sie sollten jedoch beispielsweise durch Feedback-Möglichkeiten gemeinsam erfolgen, um eine vertrauensvolle Zusammenarbeit und aussagekräftige Ergebnisse zu gewährleisten.

Der dritte Schritt umfasst ein fortlaufendes Monitoring, um aus den Assessment-Ergebnissen Schlussfolgerungen zu ziehen, unterschiedliche Lieferanten miteinander zu vergleichen und eine transparente Übersicht über das Informationssicherheitsniveau der gesamten Lieferkette zu erhalten. Bestandteil dieses Monitorings sind die transparente Darstellung der Bearbeitungsstände, der Bewertungsergebnisse und der erzeugten Dokumente sowie die zeitliche Gültigkeit und Akzeptanz der Ergebnisse durch den Betreiber in Abhängigkeit von der Risikoeinstufung des Lieferanten. Durch diese risikobasierte Vorgehensweise wird das Security-Risiko entlang der Lieferkette effektiv minimiert.

2.2 Rollen

Im Security-Lieferantenmanagement stellen die unterschiedlichen Rollen der Beteiligten einen wichtigen Faktor für den erfolgreichen und effektiven Umgang mit Informationssicherheitsrisiken in der Lieferkette dar. Die Akteure sind Betreiber, Dienstleister und Lieferanten sowie externe Security-Experten. Jede dieser Rollen bringt spezifische Anforderungen und Erwartungen mit sich, die im Gesamtprozess berücksichtigt werden. Diese Anforderungen gehen von der Notwendigkeit eines kontinuierlichen Monitorings auf Betreiberseite über eine einfache und effektive Bearbeitung durch den Lieferanten bis zur Bereitstellung von Best-Practice Security-Inhalten und Feedback-Schleifen durch Security-Experten.

2.3 Durchführung der Assessments

Diese Anforderungen fließen in den digitalen Prozess zur Durchführung der Security-Lieferantenqualifizierung ein. Das in Abbildung 2 dargestellte Prozessbild visualisiert den Ablauf eines Security-Assessments im Rahmen des plattformbasierten Security Lieferanten-managements, der in vier Hauptphasen unterteilt ist. Jede Phase ist mit

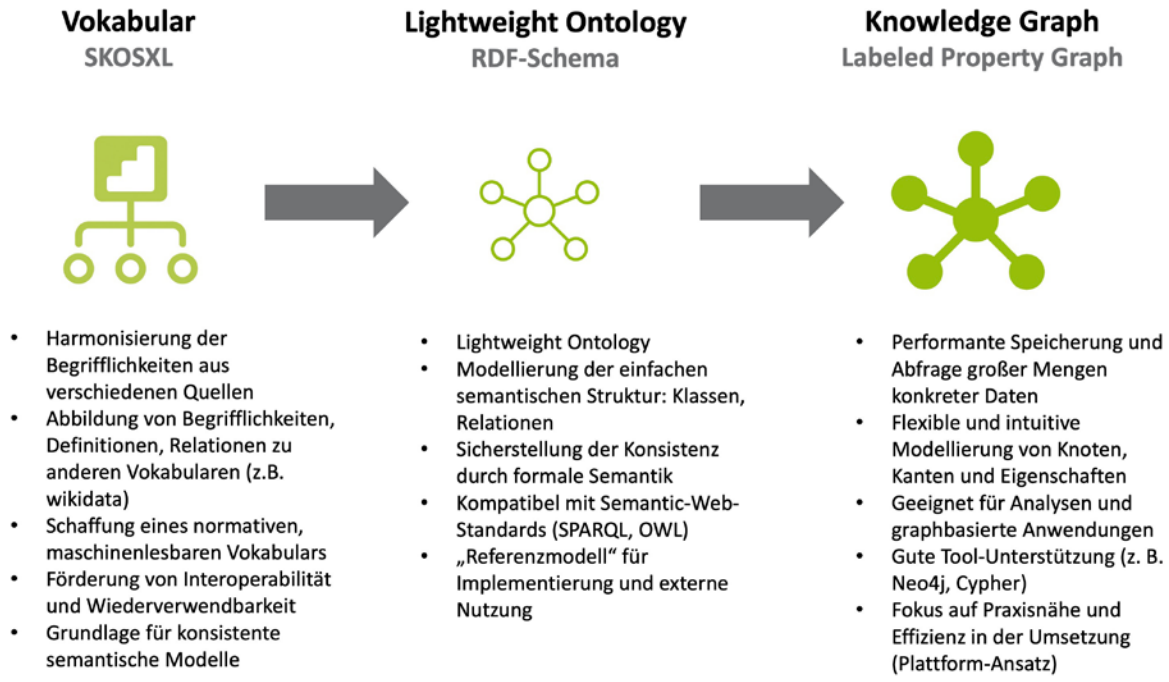

Abbildung 3: Entwicklungsschritte des Knowledge Graphen.

klar definierten Rollen und optionalen Feedbackschleifen versehen, um eine strukturierte und nachvollziehbare Durchführung zu gewährleisten. Zum Abschluss des Security-Assessments kann der Betreiber ein Zertifikat erstellen, das den Scope des Assessments festlegt, die Ergebnisse akzeptiert und eine risikobasierte zeitliche Gültigkeit definiert.

3. Semantische Modellierung von Security-Informationen mittels Knowledge Graph

Um den beschriebenen plattformbasierten Ansatz realisieren zu können, ist der effiziente Zugriff auf entsprechendes Know-how, wie beispielsweise passende Security-Fragebögen oder Best Practices zu den gestellten Security-Anforderungen notwendig.

Während bestehende Normen und Best-Practice-Dokumente (s. Abschnitt 1.1) inhaltliche Anforderungen an das Security-Lieferantenmanagement definieren, adressieren sie nur begrenzt deren operative, skalierbare Umsetzung. Der in diesem Beitrag vorgestellte Knowledge-Graph-Ansatz schließt diese Lücke bzw. bildet als semantisch strukturierte Wissensbasis die Grundlage für die plattformbasierte Umsetzung.

Der Knowledge Graph fungiert dabei nicht als weiterer Standard, sondern als Werkzeug, das eine standardisierte und automatisierbare Verarbeitung von Security-Informationen ermöglicht. Dadurch können manuelle Aufwände reduziert und der kontinuierliche Betrieb eines risikobasierten Security-Lieferantenmanagements unterstützt werden.

3.1 Entwicklung eines Knowledge Graphen

Zur systematischen Integration von Security-relevanten Informationen entlang der Lieferkette bietet sich der Einsatz eines semantisch strukturierten Knowledge Graphen an. Ein solcher Graph ermöglicht es, unterschiedliche Begriffe, Konzepte und Anforderungen aus Normen, Gesetzen oder Best Practices und Plattformprozessen in ein konsistentes, digitales Wissensmodell zu überführen. Besonders wertvoll für einen Austausch und die Nutzung ist die Berücksichtigung von Standards (z. B. für Vokabulare, Ontologien), wie sie im Rahmen des Semantic Web [22] definiert sind. Hierzu werden Konzepte wie RDF (Resource Description Framework [23]), RDFS (Resource Description Framework Schema [24]) und SKOS (Simple Knowledge Organization System [25]) des World Wide Web Consortiums (W3C) eingesetzt.

Im Kontext des Security-Lieferantenmanagements dient der Knowledge Graph als strukturierte Wissensbasis, in der Security-relevante Informationen formalisiert vorliegen. Dies bildet die Grundlage für gezieltes Prompt Engineering und die Nutzung der Inhalte auf der dargestellten digitalen Plattform.

Die Entwicklung des Knowledge Graphen erfolgt in drei Schritten (vgl. Abbildung 3). Diese bilden einen iterativen Prozess, der kontinuierlich erweitert und angepasst werden kann.

SKOS-Vokabular zur Begriffsvereinheitlichung: Im ersten Schritt wird ein kontrolliertes Vokabular erstellt, das zentrale Security-Begriffe formalisiert und deren Relationen (u. a. Definitionen, Ober-/Unterbegriffe, verwandte Konzepte) strukturiert beschreibt. Die Umsetzung erfolgt im maschinenlesbaren Standardformat SKOS/SKOSXL. Ziel ist die Vereinheitlichung der Begriffe, wie sie beispielsweise in der DIN SPEC 27076 [26], dem UP-KRITIS-Katalog [20] oder bereits bestehenden Wissensdatenbanken (z. B. wikidata [27]) auftreten. Das Vokabular [28] bildet somit die semantische Grundlage für die weitere Modellierung. SKOS bietet Relationen, um Begriffe (skos:Concept) semantisch miteinander in Verbindung zu setzen. Für das entwickelte Vokabular wurden unter anderem folgende Relationen verwendet:

- **skos:broader:** Diese Relation stellt eine hierarchische Oberbeziehung dar und wird verwendet, um allgemeinere Konzepte anzugeben. Sie hilft dabei, thematische Überbegriffe zu strukturieren. Das Concept „Ressource“ hat z. B. die Relation skos:broader zum Concept „Service“.
- **skos:narrower:** Das Gegenstück zu skos:broader. Diese Relation verweist auf spezifischere, untergeordnete Konzepte.
- **skos:definition:** Diese Relation beinhaltet eine kurze Definition bzw. Beschreibung des Concepts in mehreren Sprachen (deutsch und englisch)
- **skos:related:** Diese Relation wird genutzt, um assoziative, thematisch verwandte Begriffe zu verknüpfen, ohne dass eine Hierarchie besteht. Sie ist hilfreich, um Querbezüge innerhalb des Vokabulars abzubilden. Das Concept „Ressource“ hat z. B. die Relation skos:related zum Concept „Securityanforderung“
- **skosxl:prefLabel:** Diese Relation ist der präferierte Titel des Concepts in mehreren Sprachen. Es kann immer nur ein skosxl:prefLabel pro Concept geben. Das Concept „Bedrohung“ hat z. B. die Relation skosxl:prefLabel „Bedrohung“ und „Threat“
- **skos:closeMatch:** Referenzierung von inhaltlich ähnlichen/verwandten Concepts aus anderen Vokabularen (z.B. wikidata). Das Concept „Cyberrisiko“ hat z. B. die Relation skos:closeMatch zum wikidata Concept wd:Q104493

Lightweight Ontology: Aufbauend auf dem Vokabular wird im zweiten Schritt ein formales Schema entwickelt, das die strukturellen Beziehungen zwischen den Begriffen abbildet. Hierzu wird RDFS (RDF-Schema) verwendet, das die Definition von Klassen (z. B. „Anforderung“, „Risiko“, „Maßnahme“), deren Hierarchien und Relationen ermöglicht. Das Schema stellt damit eine „Lightweight Ontology“ dar (Ontologie, ohne komplexe logische Restriktionen. Durch die Verwendung von RDFS wird ein referenzierbares Modell [29] geschaffen, das die semantische Grundlage für den Knowledge Graph bildet.

Umsetzung Knowledge Graph: Im dritten Schritt erfolgt die Umsetzung des Modells durch die Integration konkreter Security-Informationen. Dabei sollen Entitäten (z. B. konkrete Anforderungen aus einem Fragenkatalog) als Knoten im Graphen angelegt und durch Relationen miteinander verknüpft werden. Diese Repräsentation erlaubt es, z. B. zu modellieren, welche Maßnahme eine spezifische Bedrohung adressiert oder welche Anforderungen aus welchem Normenrahmen stammen. Gleichzeitig können externe Quellen (z. B. Best-Practice-Empfehlungen) verlinkt und damit in ein übergreifendes semantisches Netz eingebettet werden. Die resultierende Wissensbasis kann anschließend für Analysen, Reifegradbewertungen und plattformgestützte Anwendungen genutzt werden.

3.2 Implementierung des Knowledge Graphen als Property Graph

Für die Implementierung des entwickelten semantischen Modells wurde Neo4j [30] verwendet, das auf dem Labeled Property Graph (LPG) Modell [31] basiert. Im Vergleich zu klassischen RDF-basierten Triple Stores bietet das LPG-Modell Vorteile für praxisorientierte Anwendungen im Kontext plattformbasierter Systeme [30] und ist daher in vielen industriellen Anwendungen im Einsatz [31]. Ziel ist es, nicht nur die semantischen Relationen zwischen Security-relevanten Informationen abzubilden, sondern auch Bewertungen und Abfragen effizient und ohne hohen Modellierungsaufwand realisieren zu können [32].

Ein Labeled Property Graph besteht aus Knoten (Nodes), Kanten (Relationships) und zugehörigen Eigenschaften (Properties), die sowohl Knoten als auch Kanten zugeordnet werden können. Dies ermöglicht eine direkte und performante Modellierung der Strukturen, wie sie bei Security-Anforderungen, Quellen oder Reifegradbewertungen auftreten.

3.3 Aufbereitung von Security-Informationen mittels generativer KI

Im letzten Abschnitt wurde deutlich, dass zur Aufbereitung relevanter Security Informationen in einem Knowledge Graph zur anschließenden Nutzung auf der Lieferantenmanagement Plattform enormer Aufwand in der Bereitstellung der praxiserprobten Informationen zur Security-Lieferantenbewertung liegt.

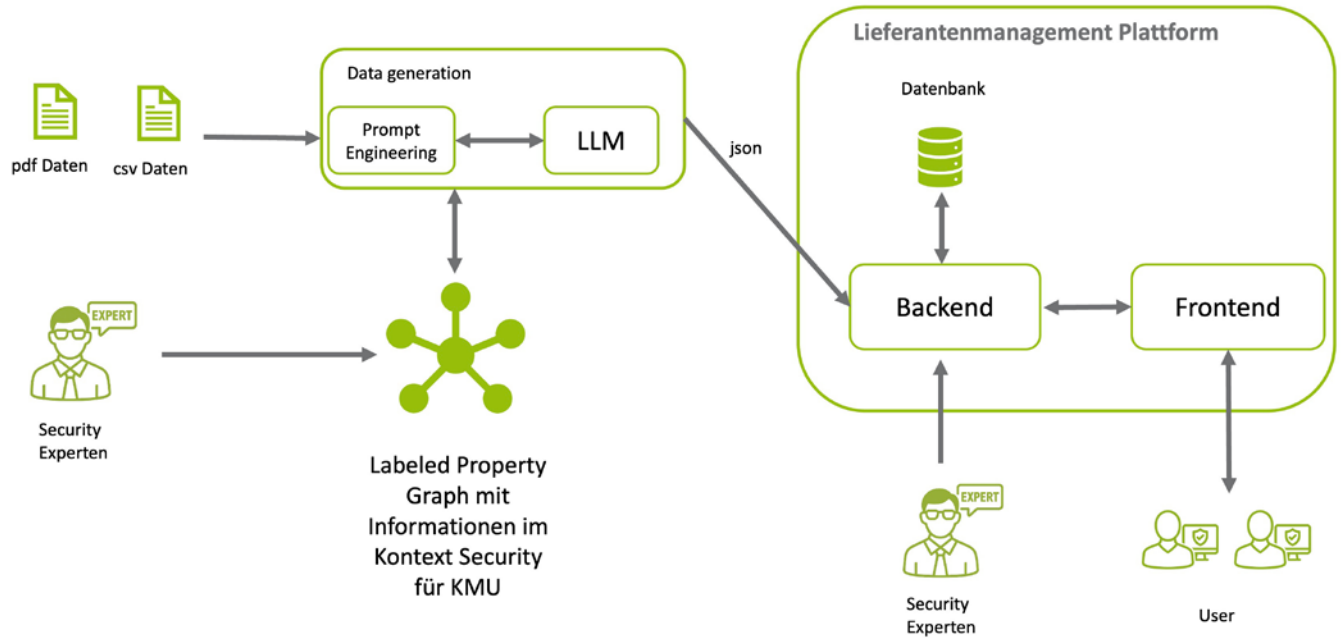

Abbildung 4: Darstellung des plattformbasierten Security Lieferantenmanagement Ansatzes mit Einsatz eines Knowledge Graphen und LLM-Unterstützung.

Viele Unternehmen haben zudem Schwierigkeiten bei der Beantwortung und Bewertung der jeweiligen Fragen, da das entsprechende Know-how fehlt. Je besser und detaillierter die Informationen von Security-Experten zusammengestellt werden, desto einfacher wird eine Bewertung auf Lieferantenseite und desto besser und aussagekräftiger sind die Ergebnisse für den Betreiber.

Da die manuelle Aufbereitung und Erstellung zeitintensiv ist und damit auch hohe Kosten verursacht, ist eine weitere Automatisierung von enormem Vorteil. In diesem Abschnitt wird daher näher erläutert, wie generative KI diesen manuellen Prozess beschleunigen kann. Abbildung 4 zeigt beide Wege im Rahmen des plattformbasierten Security Lieferanten-Management Ansatzes.

Der Einsatz von Large Language Models (LLMs) zur Unterstützung bei der Erstellung geeigneter Dokumente eröffnet neue Möglichkeiten, um komplexe Inhalte effizient, strukturiert und in hoher Qualität verfügbar zu machen. Ziel ist es, Informationsbausteine zu generieren, die auf anerkannten Standards und Best Practices basieren. Frühere Ergebnisse zeigen jedoch, dass beim LLM-Einsatz Probleme wie Halluzinationen [33], also das Erfinden von nicht vorhandenen Inhalten, oder ungenaue Extraktion von Informationen [34] auftreten können. Ziel des KI-Einsatzes ist im dargestellten Ansatz nicht die automatisierte Bewertung von Lieferanten oder der Ersatz von Security-Experten, sondern die strukturierte, standardkonforme Aufbereitung bestehender Inhalte. Generative KI wird eingesetzt, um den hohen manuellen Aufwand bei der Überführung und die inhaltliche Ergänzung umfangreicher Dokumente in maschinenlesbare, wiederverwendbare Informationsbausteine zu reduzieren. Aus diesem Grund wird die kombinierte Nutzung von Experten-Wissen in Form eines Knowledge Graphen und generativer KI vorgeschlagen und zur Erstellung eines strukturierten Fragebogens auf Basis des Best-Practice-Kataloges zum Security Lieferantenmanagement der UP KRITIS-Kooperation [20] eingesetzt.

Ziel und Herausforderungen: Im Folgenden werden die Herausforderungen und das Ziel für den KI-Einsatz zur automatisierten Erstellung von maschinenlesbaren Informationen im Kontext Security-Lieferantenmanagement dargestellt:

- Verarbeitung von pdf-Dokumenten
- Verarbeitung deutscher Texte
- Exakte Extraktion der folgenden Textbausteine aus dem Originaldokument: Security-Kriterium, Kurztitel der Security-Anforderung, Zusätzliche Informationen zur Anforderung
- Generierung zusätzlicher Inhalte, insbesondere: Leitfragen zur Security-Anforderung und Beschreibungen und Handlungsempfehlungen für vier Reifegrad-Stufen (vollständig erfüllt, weitgehend erfüllt, teilweise erfüllt, nicht erfüllt)
- Bereitstellung des Ergebnisses im maschinenlesbaren JSON-Format

Betrachtete KI-Modelle und Ergebnisse: Im Rahmen dieses Projekts wurden die Large Language Modelle (LLM) von OpenAI (GPT-4o, GPT-5) und Mistral AI (Mistral Large) analysiert. Die betrachteten LLMs zeigen vergleichbare Fähigkeiten in Bezug auf Textverständnis

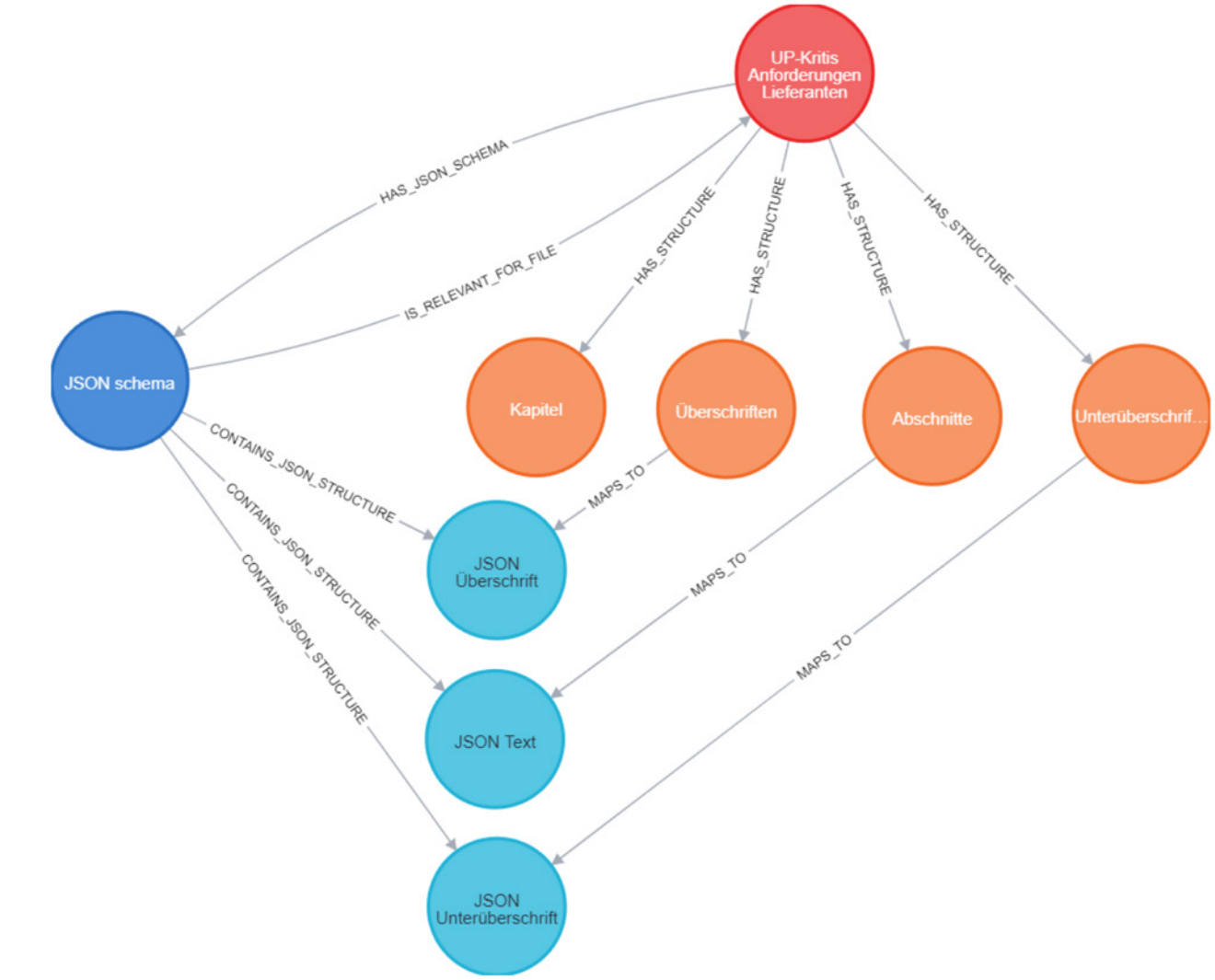

Abbildung 5: Ausschnitt aus dem LPG mit dem Mapping der Strukturinformationen einer Datei zur gewünschten JSON-Struktur zur Nutzung auf der dargestellten Plattform.

deutscher Texte und die Erstellung maschinenlesbarer Outputs. Aufgrund der Vorteile im Bereich Datenschutz und einer möglichen Open-Source-Nutzung von Mistral-Sprachmodellen [35, 36] wird im Weiteren die Nutzung des Mistral Modells dargestellt.

Um die maschinenlesbaren Informationen zu generieren und auszuwerten, wurde folgendes Vorgehen gewählt:

- 1. Integration Dokumentenstruktur und Mapping zur Zielstruktur im LPG (s. Abbildung 5)
- 2. Upload des Originaldokuments (UP-KRITIS Katalog) in die KI-Umgebung
- 3. Automatisierte Cypher Abfrage auf den Labeled Property Graphen (LPG) für Strukturinformationen der gewünschten Datei (z.B. Kapitel, Überschriften, Zeilen, Spalten, Tabelle, Dateityp, JSON-Mapping)
- 4. Erstellung eines gezielten Prompts mit den oben beschriebenen Zielen. Anwendung von Methoden aus Bereich Prompt Engineering (u.a. Few-Shot Prompting [37])
- 5. Analyse der generierten Ergebnis-Datei hinsichtlich Genauigkeit der übernommenen Originalinhalte und Qualität der generierten Zusatzinformationen
- 6. Prüfung der Strukturkonformität des JSON-Outputs

Das Originaldokument des UP-KRITIS-Verbands [20] umfasst 28 Seiten und kann mit dem dargestellten Vorgehen ohne Einteilung in einzelne Abschnitte verwendet werden. Für die Prompt-Formulierung lag der Fokus auf den folgenden Punkten:

- Die Oberkapitel ab Kapitel 3 des UP-KRITIS Dokumentes liefern die Kriterien des zu erstellenden Fragebogens

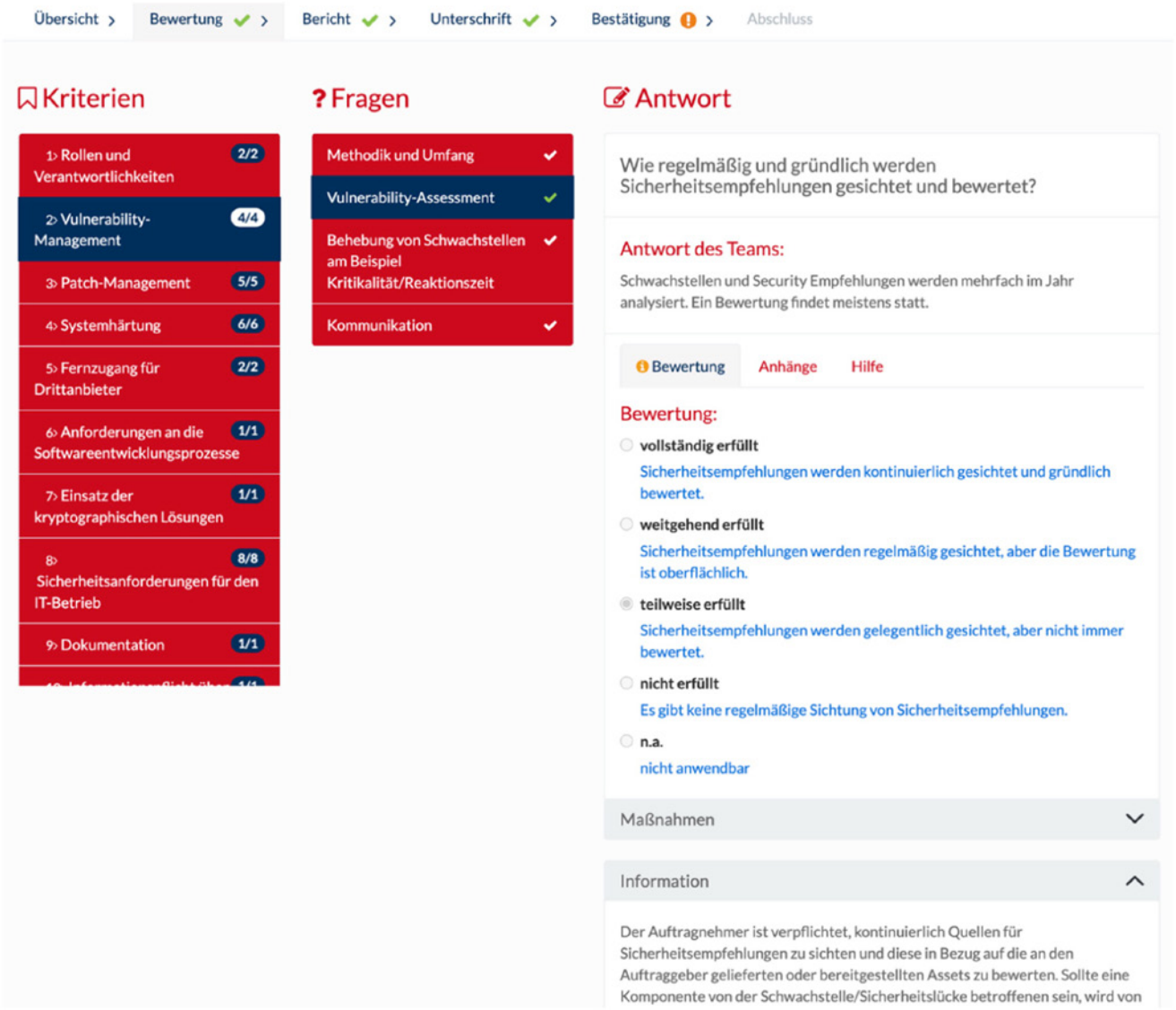

Abbildung 6: Beispiel einer Lieferantenbewertung auf der Demo-Plattform für digitales Lieferantenmanagements des Mittelstand-Digital Zentrums Saarbrücken auf Basis eines KI-generierten Fragebogens.

- Die darunterliegenden Unterkapitel stellen die Kurztitel der Security-Anforderungen dar
- Die Textpassagen sollen exakt übernommen werden und stellen die zusätzlichen Informationen dar
- Für jede Security-Anforderung soll eine Leitfrage für den Lieferanten generiert werden
- Für die vier Reifegrade sollen jeweils passende Beschreibungen und Handlungsempfehlungen generiert werden
- Bereitstellung der gewünschten Struktur des Outputs anhand eines Beispiels

Für die Ausführung des oben beschriebenen Vorgehens und des erstellten Prompts wird der von Mistral AI bereitgestellte KI-Assistent Le Chat [36] verwendet.

Die Extraktionsgenauigkeit der Originalinhalte ist mit 99,22 % sehr hoch und der JSON-Output ist konform zum Standard. Geringfügige Abweichungen resultieren aus Rechtschreibfehlern im Originaldokument oder nicht zu 100 % korrekt übernommenen kleineren Textstellen. Die generierten Inhalte wie Leitfragen, Beschreibungen und Handlungsempfehlungen sind inhaltlich passend zur jeweiligen Security-Anforderung und damit gut geeignet, um auf der Plattform zur Security-Lieferantenbewertung eingesetzt zu werden. In Einzelfällen empfiehlt sich eine Ergänzung bzw. Detaillierung durch Security-Experten, um die generierten Inhalte (z. B. die erstellten Leitfragen) noch spezifischer an die jeweiligen Security-Anforderungen anzupassen. Stellenweise kann zudem eine Layout-Anpassung der aus dem Originaldokument extrahierten Textbausteine sinnvoll sein. Die fachliche Verantwortung ver-

bleibt dabei bewusst beim Menschen, insbesondere bei der Validierung und Feinjustierung der generierten Inhalte.

In Abbildung 6 ist das Ergebnis nach Upload des generierten json-Outputs und anschließender Erstellung eines Assessments auf dessen Basis auf der Demo-Plattform zu sehen.

4. Fazit

Dieser Beitrag thematisiert das zunehmende Cyber-Risiko für Unternehmen, das von Angriffen über die Lieferkette ausgeht. Mit Hilfe eines digitalen Plattformansatzes wird die Möglichkeit geschaffen, Unternehmen effizient bei der Einschätzung des Security-Reifegrades der Lieferanten und Dienstleister zu unterstützen. Dabei wird ein effizienter, risikobasierter Prozess dargestellt, der die beteiligten Rollen Betreiber, Lieferanten und Security-Experten berücksichtigt und den weiter steigenden Aufwänden (u.a. NIS2) entgegenwirkt.

Durch die strukturierte Modellierung der Security-relevanten Informationen, Anforderungen, Dokumentstrukturen und deren semantischen Beziehungen in Form eines Labeled Property Graphen, lassen sich die Daten effizient abbilden sowie maschinenlesbar und automatisiert nutzen.

Die für eine aussagekräftige Bewertung des Security-Reifegrades erforderlichen Informationen werden in der Praxis überwiegend aufwändig manuell durch Security-Experten bereitgestellt. Eine gezielte Unterstützung durch generative KI kann diesen Aufwand reduzieren, indem bestehende Inhalte strukturiert, standardkonform und maschinenlesbar aufbereitet werden. Der im Beitrag vorgestellte, mittels eines Large Language Models erzeugte Fragebogen zeigt, dass generative KI insbesondere bei der strukturierten Dokumentengenerierung einen messbaren Mehrwert leisten kann.

Obwohl der Fokus dieses Beitrags auf dem Security-Lieferantenmanagement liegt, ist der vorgestellte Ansatz grundsätzlich domänenoffen konzipiert. Die zugrunde liegende semantische Modellierung erlaubt es, weitere Aspekte des Lieferantenmanagements, wie beispielsweise Umwelt- oder Nachhaltigkeitsanforderungen auf Basis entsprechender standardisierter Informationen zu integrieren.

Dieser Beitrag ist eine Erweiterung von [38]. Die beschriebenen Arbeiten basieren auf Ergebnissen eines Forschungsprojektes, das vom Ministerium für Wirtschaft, Innovation, Digitales und Energie des Saarlandes gefördert wurde. Die Demonstrationsmöglichkeit erfolgte im Rahmen des Mittelstand-Digital Zentrum Saarbrücken gefördert vom Bundesministerium für Wirtschaft und Energie.

Referenzen

[1] Council of Supply Chain Management Professionals. (2013). Supply Chain Management Terms and Glossary. Verfügbar unter: https://cscmp.org/CSCMP/cscmp/educate/scm_definitions_and_glossary_of_terms.aspx, abgerufen am: 24.04.2025

[2] The MITRE Corporation. (2020). Supply Chain Compromise: Compromise Software Supply Chain (ID:T1195.002). Verfügbar unter: https://attack.mitre.org/techniques/T1195/002/, abgerufen am: 23.01.2026

[3] The MITRE Corporation. (2020). Supply Chain Compromise (ID:T0862). Verfügbar unter: https://attack.mitre.org/techniques/T0862/, abgerufen am: 23.01.2026

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2022). Die Lage der IT-Sicherheit in Deutschland 2022. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410, abgerufen am: 17.04.2023

[5] Bundesgesetzblatt. (2021). Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. IT-SiG 2.0.

[6] Europäische Union. (2022). Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. NIS2 2022/2555.

[7] Bundesgesetzblatt. (2025). Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.

[8] ISO. (2022). ISO/IEC 27001:2022-10. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

[9] ISO. (2022). ISO/IEC 27036-2:2022-06. Cybersecurity — Supplier relationships Part 2: Requirements

[10] ISO. (2022). ISO/IEC 27002:2022-02. Information security, cybersecurity and privacy protection — Information security controls

[11] Verband der Automobilindustrie e.V. (2025). Information Security Assessment

[12] [12] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2023). IT-Grundschutz-Kompendium Edition 2023.

[13] IEC. (2018). IEC 62443-2-4. Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

[14] Siegwart, C., Scherhag, F., Pervölz, K., Frey, G. (2022). Geschäftsmodelle-Stärkung der Cyber-Resilienz in KMU. In Automation 2022. VDI Verlag 2022, S. 691–702.

[15] Siegwart, C., Rosenhauer, C., Krammel, M. u. Frey, G. (2023). Informationssicherheit für den Mittelstand – Lessons Learned. In: Automation 2023. VDI Verlag 2023, S. 973–984.

[16] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

[17] National Institute of Standards and Technology. (2021). Key practices in cyber supply chain risk management.

[18] Bundesamt für wirtschaftliche Landesversorgung. (2023). Minimalstandard zur Verbesserung der IKT-Resilienz, Bundesamt für wirtschaftliche Landesversorgung

[19] Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA). (2023). VDMA-SCS-Lieferantenselbstauskunft.

[20] Bundesamt für Sicherheit in der Informationstechnik (BSI). (2023). UP KRITIS: Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen

[21] TÜV-Verband e.V. (2025). TÜV Cybersecurity Studie 2025. Cybersicherheit in deutschen Unternehmen, Neue Bedrohungslage – besserer Schutz.

[22] Berners-Lee, T., Hendler, J., & Lassila, O. (2023). The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities. In Linking the world's information: essays on Tim Berners-Lee's invention of the World Wide Web (pp. 91-103).

[23] World Wide Web Consortium. (2014). W3C Recommendation: RDF 1.1 Concepts and Abstract Syntax, 2014. Verfügbar unter: https://www.w3.org/TR/rdf11-concepts/, abgerufen am: 08.12.2025

[24] World Wide Web Consortium. (2014). W3C Recommendation: RDF Schema 1.1, 2014. Verfügbar unter: https://www.w3.org/TR/rdf11-schema/, abgerufen am: 17.12.2025

[25] World Wide Web Consortium. (2009). W3C Recommendation: SKOS Simple Knowledge Organization System. Reference, 2009. Verfügbar unter: https://www.w3.org/TR/2009/REC-skos-reference-20090818/, abgerufen am: 08.12.2025

[26] DIN Deutsches Institut für Normung e. V. (2023). DIN SPEC 27076 - IT-Sicherheitsberatung für Klein- und Kleinstunternehmen. IT-Sicherheitsberatung für Klein- und Kleinstunternehmen

[27] Wikimedia Foundation: Wikidata. https://www.wikidata.org, abgerufen am: 23.01.2026

[28] Siegwart, C., Scherhag, F. https://purl.org/secsmevoc, abgerufen am: 08.12.2025

[29] Siegwart, C., Scherhag F. https://purl.org/secsmeschema, abgerufen am: 08.12.2025

[30] Packer, D. (2021). A Brief Introduction to Graph Data Platforms.

[31] Kondylakis, H., Dumbrava, S., Lissandrini, M., Yakovets, N., Bonifati, A., Efthymiou, V., ... Ymeralli, E. (2025). Property Graph Standards: State of the Art & Open Chal-

lenges. Proceedings of the VLDB Endowment, 18(12), 5477-5481.

[32] Monteiro, J., Sá, F., & Bernardino, J. (2023). Experimental evaluation of graph databases: Janusgraph, nebula graph, neo4j, and tigergraph. Applied Sciences, 13(9), 5770.

[33] Nadeau, D., Kroutikov, M., McNeil, K., & Baribeau, S. (2024). Benchmarking llama2, mistral, gemma and gpt for factuality, toxicity, bias and propensity for hallucinations. arXiv preprint arXiv:2404.09785.

[34] Han, R., Yang, C., Peng, T., Tiwari, P., Wan, X., Liu, L., & Wang, B. (2023). An empirical study on information extraction using large language models. arXiv preprint arXiv:2305.14450.

[35] Jiang, A. Q., Sablayrolles, A., Roux, A., Mensch, A., Savary, B., Bamford, C., ... & Sayed, W. E. (2024). Mixtral of experts. arXiv preprint arXiv:2401.04088.

[36] Yu, P. (2025). Le Chat vs ChatGPT: How Mistral AI is Redefining European AI Standards, 2025. Verfügbar unter: https://blog.chathub.gg/le-chat-vs-chatgpt-how-mistral-ai-is-redefining-european-ai-standards/, abgerufen am: 24.04.2025

[37] Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., ... Amodei, D. (2020). Language models are few-shot learners. Advances in neural information processing systems, 33, 1877-1901.

[38] Siegwart, C., Krammel, M., Scherhag, F., Frey, G. (2025). Security Lieferantenmanagement zur Absicherung der Lieferkette. In Automation 2025, S. 629–643.

Christian Siegwart ist wissenschaftlicher Mitarbeiter und Promotionsstudent am Zentrum für Mechatronik und Automatisierungstechnik in Saarbrücken. Nach Abschluss seines Studiums in Computer- und Kommunikationstechnik an der Universität des Saarlandes betreut er Forschungs-und Industrieprojekte im Forschungsbereich Industrial Security am ZeMA. Seit 2021 ist er ebenfalls als Cyber Security Consultant bei der K4 DIGITAL GmbH beschäftigt.

Christian Siegwart M.Sc.
ZeMA gGmbH
Eschberger Weg 46
Gewerbepark, Gebäude 9
66121 Saarbrücken
+49 6 81 85 787 540
christian.siegwart@zema.de

Felix Scherhag hat 2019 einen Master-Abschluss im Studiengang Computer- und Kommunikationstechnik an der Universität des Saarlandes in Saarbrücken erlangt. Bereits in seiner Master-Thesis widmete er sich dem ganzheitlichen Security-Management. Seit Juli 2020 arbeitet er als wissenschaftlicher Mitarbeiter am Zentrum für Mechatronik und Automatisierungstechnik (ZeMA) und wirkt dort an Projekten im Forschungsbereich Industrial Security mit.

Michael Krammel ist Geschäftsführer und Gründer der K4 DIGITAL GmbH. Er zählt zu den profiliertesten Vordenkern von Industrial Security in Deutschland. Er ist in vielen Gremien, Verbänden und Organisationen engagiert. Michael Krammel gilt als ausgewiesener Experte, Berater und Coach für Industrial & Cyber Security und ist in den Themen Prozessautomations- und Steuerungssysteme, sowie systemische Aspekte der Digitalen Transformation in Industrie 4.0 zuhause.

Univ.-Prof. Dr.-Ing. Georg Frey ist Universitätsprofessor und Inhaber des Lehrstuhls für Automatisierungs- und Energiesysteme an der Universität das Saarlandes in Saarbrücken. Zudem leitet er den Forschungsbereich Industrial Security am ZeMA. Seine Forschungsschwerpunkte sind modellbasierte Entwurfsverfahren für Automatisierungs- und Energiesysteme, Steuerungstechnik, Simulation, Safety und Security.