

Abschlussbericht des Forschungsvorhabens ML Policy

Teil I: Kurzbericht

Aufgabenstellung des Vorhabens: Das Vorhaben ML Policy wurde im Rahmen des Förderprogramms Start Up Secure Phase 1 (Entwicklungsphase) gefördert. Die Kernidee des Vorhabens ML Policy war die Unterstützung und weitgehende Selbstbefähigung von kleinen und mittelständischen Unternehmen beim Aufbau von Informationssicherheitsrichtlinien. Oft unterliegen Unternehmen Anforderungen aus mehreren Rahmenwerken (darunter BSI Grundschutz, ISO 27001, SWIFT, TARGET, B3S, TISAX, PCI-DSS etc.), die es in einer Richtlinie zu vereinen gilt. Derzeit fängt nahezu jedes Unternehmen bei der Erstellung von Sicherheitsrichtlinien bei Null an - die relevanten Anforderungen müssen herausgesucht, nebeneinander gelegt und verknüpft werden, um daraus eine eigene Policy zu erstellen. Für Unternehmen ist es sehr zeitaufwändig, sich durch die Rahmenwerke durchzuarbeiten und zudem sind betroffene Mitarbeiter oft durch interne Projekt- und Linientätigkeiten ausgelastet. Externe Mitarbeiter, die dabei operativ unterstützen und begleitend beraten, sind hingegen kostspielig. Das Vorhaben ML Policy verfolgte das Ziel, eine SaaS-Anwendung zu entwickeln, die Unternehmen bei der Erstellung und Harmonisierung von Sicherheitsrichtlinien unterstützt, um Zeit und Kosten zu sparen und für viele kleinere Unternehmen kostenmäßig überhaupt erst zu ermöglichen.

Anknüpfung an wissenschaftlichen und technischen Stand: Das Vorhaben konnte an den folgenden wissenschaftlichen und technischen Stand anknüpfen:

- 1.) Stand der Technik in textbasierter AI: Die hochdynamische technische Entwicklung im Bereich Machine Learning, insbesondere Natural Language Processing (NLP) durch Embeddings und Transformer-Modelle wie BERT und GPT bietet Anknüpfungspunkte mit hohem Potenzial. Die Möglichkeit, diese Technologien durch Feinabstimmung an spezifische Anforderungen anzupassen, bietet Unternehmen und Forschern wertvolle Chancen, um in einzelnen Anwendungsbereichen effiziente, skalierbare und intelligente Lösungen zu entwickeln, so auch in Form einer Unterstützung der Analyse von Informationssicherheitsrichtlinien sowie deren Erstellung.
- 2.) Stand der technischen Erstellung von Informationssicherheitsrichtlinien in der Praxis: Hier findet eine weitgehend manuelle Herangehensweise, manchmal unterstützt durch Templates, in einer Kombination aus Eigenleistung und Einkauf von Beratungswissen statt.

Ablauf des Vorhabens. Entsprechend der Konzeption des Programms Start Up Secure Phase 1 (Entwicklungsphase) war das Vorhaben im Wesentlichen ein Entwicklungsprojekt. Das Team bestand aus einem Product Owner, einem Frontend-

Entwickler, einem Backend-Entwickler, einem Data Scientist und dem Projektleiter. Das Team hat mit einer agilen Softwareentwicklungsmethode gearbeitet; dabei wurden Anforderungen in Sprints definiert, priorisiert und implementiert. Um Anforderungen zu erheben und Umsetzungen zu validieren, wurde regelmäßig Rücksprache mit Auditoren, IT-Sicherheitsspezialisten und potentiellen Anwendern gehalten.

Das Projekt wurde aus zwei Gründen kostenneutral um 6 Monate verlängert: 1.) Der Projektfortschritt hat sich bereits zu Beginn verzögert, da Personal gesucht werden musste. 2.) Im Projektverlauf haben wir festgestellt, dass wir die Anwender noch einen Schritt vorher abholen müssen mit einer initialen Einschätzung, wie viel Aufwand auf sie zukommt, so dass es notwendig wurde, eine entsprechende Funktion in den Demonstrator einzubauen.

Durch die kostenneutrale Verlängerung um 6 Monate konnte das Vorhaben in Qualität, Quantität und Kostenrahmen abgeschlossen werden.

Ergebnisse. Das wesentliche Ergebnis besteht in der Entwicklung eines Demonstrators. Der Demonstrator beinhaltet drei Artefakte, dies sind 1.) der *Policy Association Graph*, 2.) darauf aufbauend die Implementierung des Moduls *Policy Explorer*, und 3.) des Moduls *Policy Customizer*.

Zu 1.) Der *Policy Association Graph* beinhaltet die Verbindungen zwischen Informationssicherheitsrahmenwerken (z.B. ISO 27001 und PCI-DSS) und wird mit Hilfe von NLP-Ansätzen befüllt. Im *Policy Association Graph* wurden über die Projektlaufzeit die Verbindungen von mehreren Rahmenwerken zum zentralen Rahmenwerk ISO 27001 identifiziert und manuell überprüft.

Zu 2.) Der *Policy Explorer* erlaubt es Anwendern, die Zusammenhänge zwischen den Rahmenwerken zu explorieren. Dabei können Anwender ausgehend von Einstiegspunkten den *Policy Association Graph* interaktiv erkunden.

Zu 3.) Der *Policy Customizer* unterstützt den Anwender dabei, auf einfache Weise individuell zugeschnittene Informationssicherheitsrichtlinien zu erstellen.

Abschlussbericht des Forschungsvorhabens ML Policy

Teil II: Eingehende Darstellung

Inhaltsverzeichnis

Ziel des Vorhabens	2
Durchgeführte Arbeiten mit erzielten Ergebnissen	2
Ergebnisbereich 1: Grundsystem des Demonstrators (AP 9, AP 12, AP 15, AP 5).....	2
Ergebnisbereich 2: Policy Association Graph (AP 1, AP 4, AP 6-8, AP 17).....	4
Ergebnisbereich 3: Modul Policy Explorer (AP 2, AP 10, AP 13).....	5
Ergebnisbereich 4: Modul Policy Customizer (AP 3, AP 11, AP 14).....	6
Ergebnisbereich 5: Nicht-technische Ergebnisse.....	6
Abweichungen im Vergleich zum ursprünglichen Projektplan	6
Wichtigste Positionen des zahlenmäßigen Nachweises.....	7
Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten	8
Voraussichtlicher Nutzen und Verwertung	9
Stand der Verwertung	9
Nutzen für Anwender	9
Schutzrechte und Patente	10
Fortschritt auf dem Gebiet während der Projektlaufzeit.....	10

Ziel des Vorhabens

Die Kernidee des Vorhabens ML Policy war die Unterstützung und weitgehende Selbstbefähigung von kleinen und mittelständischen Unternehmen beim Aufbau von Informationssicherheitsrichtlinien. Oft unterliegen Unternehmen Anforderungen aus mehreren Rahmenwerken (darunter BSI Grundschutz, ISO 27001, SWIFT, TARGET, B3S, TISAX, PCI-DSS etc.), die es in einer Richtlinie zu vereinen gilt. Derzeit fängt nahezu jedes Unternehmen bei der Erstellung von Sicherheitsrichtlinien bei Null an - die relevanten Anforderungen müssen herausgesucht, nebeneinander gelegt und verknüpft werden, um daraus eine eigene Policy zu erstellen. Für Unternehmen ist es sehr zeitaufwändig, sich durch die Rahmenwerke durchzuarbeiten und zudem sind betroffene Mitarbeiter oft durch interne Projekt- und Linientätigkeiten ausgelastet. Externe Mitarbeiter, die dabei operativ unterstützen und begleitend beraten, sind hingegen kostspielig. Das Vorhaben ML Policy verfolgte das Ziel, eine SaaS-Anwendung zu entwickeln, die Unternehmen bei der Erstellung und Harmonisierung von Sicherheitsrichtlinien unterstützt, um Zeit und Kosten zu sparen und für viele kleinere Unternehmen kostenmäßig überhaupt erst zu ermöglichen.

Durchgeführte Arbeiten mit erzielten Ergebnissen

Das Ziel des Vorhabens ML Policy war die Entwicklung eines Demonstrators, der Unternehmen bei der Erstellung und Harmonisierung von Informationssicherheitsrichtlinien unterstützt.

Die Darstellung der Arbeiten eignet sich anhand der zentralen Ergebnisse, die erzielt wurden: 1.) Grundgerüst des Demonstrators, 2.) Policy Association Graph, 3.) Policy Explorer, 4.) Policy Customizer und 5.) nicht-technische Ergebnisse. Den Ergebnissen werden die jeweiligen Tätigkeiten der Arbeitspakete zugeordnet.

Ergebnisbereich 1: Grundsystem des Demonstrators (AP 9, AP 12, AP 15, AP 5)

Der entwickelte Demonstrator bietet als Natural Language Processing (NLP)-gestützte SaaS-Anwendung ein neuartiges Empowerment für Unternehmen, um Sicherheitsrichtlinien ohne großen Aufwand oder externe Berater selbst erstellen zu

können. Die Anwendung wurde mit einer Microservice-Architektur umgesetzt. Dies bringt die Möglichkeit der einfachen Skalierbarkeit und flexiblen Erweiterung.

Durchgeführte Arbeiten in AP 9:

In AP 9 wurde ein Grundgerüst für das Frontend in React gebaut. Der Prototyp wurde mandantenfähig ausgebaut und mit einem Authentifizierungsmechanismus versehen. Es wurde die Entwicklungsumgebung und Deploymentumgebung aufgesetzt.

Durchgeführte Arbeiten in AP 12:

In AP 12 wurde analog zu AP 9 ein Grundgerüst für das Backend gebaut. Zunächst wurde eine nicht-relationale Datenbank (MongoDB) verwendet, jedoch später nach erneuter Abwägung von Vor- und Nachteilen durch eine relationale Datenbank (PostgreSQL) ersetzt.

Durchgeführte Arbeiten in AP 15:

In AP 15 wurde ein Konzept zur Umsetzung in Microservices erarbeitet und umgesetzt. Die Umsetzung mit Microservices stellt sicher, dass die Software mit wachsender Nutzerzahl, zunehmender Datenmenge und der steigenden Komplexität Schritt halten kann.

Als Kernbestandteile des Demonstrators wurden entwickelt (Abbildung 1):

- Der *Policy Association Graph*, der die Verbindungen zwischen verschiedenen Rahmenwerken (z.B. ISO 27001 und branchenspezifischen Rahmenwerken) in einer Datenbank abbildet, darauf aufbauend
- das Modul *Policy Explorer*, das es Anwendern erlaubt, die Zusammenhänge zwischen den Rahmenwerken interaktiv zu explorieren
- das Modul *Policy Customizer*, das den Anwender befähigt, auf einfache Weise individuell zugeschnittene Policies zu erstellen.

Durchgeführte Arbeiten in AP 5:

In AP 5 wurden Friendly User Tests mit Experten und potentiellen Anwendern durchgeführt.

Ergebnisbereich 2: Policy Association Graph (AP 1, AP 4, AP 6-8, AP 17)

Der *Policy Association Graph* stellt die inhaltlichen Verbindungen der Informationssicherheitsanforderungen zwischen verschiedenen Rahmenwerken dar. Zum Aufbau des *Policy Association Graphs* wurden über Embeddings und Vektorisierungsmethoden ähnliche Anforderungen aus verschiedenen Rahmenwerken transparent und halbautomatisch vergleichbar gemacht. Durch den Vektorisierungsansatz wurden ähnliche Anforderungen halbautomatisiert in thematischen Zusammenhang gebracht.

Durchgeführte Arbeiten in AP 1:

In AP 1 wurden initiale Anforderungen für den Policy Association Graph definiert, der ein Mapping zwischen verschiedenen Rahmenwerken darstellt. Es wurde ein Product Backlog erstellt, welches aus den Anforderungen abgeleitet wurde.

Durchgeführte Arbeiten in AP 6 bis AP 8:

In AP 6 hat der Data Scientist die Datenbank für den Policy Association Graph aufgebaut und ein Data Preprocessing durchgeführt, um die Textdaten der Rahmenwerke zu bereinigen und vorzubereiten.

Mit den bereinigten Daten wurden in AP 6 initiale Modelle trainiert und fortlaufend iterativ verbessert (AP 7 und AP 8). Dabei konnten mit dem Embeddings-Ansatz die beiden Hürden überwunden werden 1.) die Verknüpfung zwischen Rahmenwerken (z.B. ISO 27001, TISAX, B3S, BSI Grundschutz) herzustellen und Anforderungen erstmalig automatisiert vergleichbar zu machen und 2.) die Veränderung von Anforderungen durch verschiedene Versionsstände desselben Rahmenwerks trotz Umstrukturierung über die Zeit im Blick zu behalten.

Die Unterstützung der Erstellung von unternehmensspezifischen Policies durch NLP und Embeddings war in der Informationssicherheitsdomäne neu. Auch ein vollständiges Mapping zwischen Anforderungen aus verschiedenen Frameworks auf Ähnlichkeitsbasis existierte zuvor nicht.

Die gefundenen Verbindungen mussten manuell qualitätsgesichert werden, um eine hohe Datenqualität zu gewährleisten, da die automatisch gefundenen Verbindungen

oft nur teilweise richtig waren. Die qualitätsgesicherten Daten konnten nachfolgend die für das Training verfügbaren Daten anreichern, um in weiteren Iterationen bessere Erkennungsraten zu ermöglichen.

Durchgeführte Arbeiten in AP 4:

Es wurden insgesamt 18 Rahmenwerke zum Aufbau des Policy Association Graph analysiert.

Durchgeführte Arbeiten in AP 17:

In AP 17 wurde mittels Clustering, manueller Strukturierung und manueller Validierung ein Codewörterbuch erstellt, das die Informationssicherheitsdomäne abbildet.

Ergebnisbereich 3: Modul Policy Explorer (AP 2, AP 10, AP 13)

Dieses Modul visualisiert die komplexen Beziehungen zwischen den Anforderungen verschiedener Sicherheitsnormen durch eine intuitive grafische Darstellung. Es erleichtert das Verständnis der Verflechtungen und Abhängigkeiten zwischen verschiedenen Sicherheitsstandards. Durch diese visuelle Klarheit können Sicherheitsexperten effektiver entscheiden, wie sie die Anforderungen aus unterschiedlichen Rahmenwerken in einer einheitlichen und kohärenten Sicherheitsrichtlinie zusammenführen können.

Durchgeführte Arbeiten in AP 2:

In AP 2 wurden die Anforderungen in Form eines Backlogs für das Modul Policy Explorer definiert. Es wurden passende Screens in Figma entworfen.

Der Policy Explorer wurde derart ausgestaltet, dass er die Exploration des Policy Association Graphs durch den Anwender ermöglicht. Der Anwender kann beispielsweise anschauen, wie sich die ISO 27001 von der Version 2017 auf 2022 verändert hat oder wie die ISO 27001 mit branchenspezifischen Rahmenwerken inhaltlich verknüpft ist. Der Graph wird übersichtlich in thematischen Gruppierungen dargestellt.

Durchgeführte Arbeiten in AP 10 und 13:

In AP 10 und AP 13 wurde die Implementierung des Moduls Policy Explorer durchgeführt (Frontend AP 10 und Backend AP 13).

Ergebnisbereich 4: Modul Policy Customizer (AP 3, AP 11, AP 14)

Ergänzend zum Explorer bietet das zweite Modul eine AI-gestützte Interaktion durch einen fortschrittlichen Chatbot, der die Automatisierung der Zusammenführung von Anforderungen aus verschiedenen Normen ermöglicht. Dieser Chatbot führt in Interaktion mit dem Benutzer Anforderungen aus verschiedenen branchenrelevanten Rahmenwerken zusammen und erstellt daraus eine unternehmensspezifische Sicherheitsrichtlinie. Durch den Einsatz künstlicher Intelligenz wird die Genauigkeit der Anpassungen erhöht und der Prozess der Richtlinienerstellung beschleunigt.

Durchgeführte Arbeiten in AP 3:

In AP 3 wurden die Anforderungen in Form eines Backlogs für das Modul Policy Customizer definiert. Der Policy Customizer wurde mit einem Chatbot umgesetzt auf Basis mehrerer Modelle. Es wurden passende Screens in Figma entworfen.

Durchgeführte Arbeiten in AP 11 und 14:

In AP 11 und AP 14 wurde die Implementierung des Moduls Policy Explorer durchgeführt (Frontend AP 11 und Backend AP 14).

Der Policy Customizer wurde derart umgesetzt, dass er die Erstellung einer unternehmensspezifischen Informationssicherheitsrichtlinie mit Hilfe eines Chatbots ermöglicht. Das zentrale Element bildet die halbautomatische Interaktion mit dem Chatbot. Hier werden verschiedene branchenrelevante Anforderungen zusammengeführt. Eine Seitenleiste enthält unternehmensinternes Expertenwissen zu der spezifischen Anforderung.

Ergebnisbereich 5: Nicht-technische Ergebnisse

In AP 16 wurde ein Transferkonzept erstellt. Dazu war der Input von externen Dienstleistern notwendig, darunter einem professionellen ISO 27001 Lead-Auditor, um die optimale Passung des Demonstrators in die Zertifizierungspraxis zu erarbeiten.

Abweichungen im Vergleich zum ursprünglichen Projektplan

Es gab zwei nennenswerte Abweichungen zum ursprünglichen Projektplan:
1.) Das Vorhaben begann mit Zeitverzug, da zu Beginn noch Personal gefunden werden musste und die Prozesse an der Universität keine schnelle Reaktion

ermöglichen. In kurzer Zeit qualifiziertes Personal zu finden, das sich für eine unterjährige Beschäftigung interessiert, war eine Herausforderung. Teile des Teams mussten in Teilzeit eingestellt werden.

2.) Im Projektverlauf haben wir festgestellt, dass wir die Anwender noch einen Schritt vorher abholen müssen mit einer initialen Einschätzung, wie viel Aufwand auf sie zukommt, so dass es notwendig wurde, eine entsprechende Funktion in den Demonstrator einzubauen.

Beide Abweichungen konnten mit einer kostenneutralen Projektverlängerung erfolgreich adressiert werden.

Wichtigste Positionen des zahlenmäßigen Nachweises

0812 Personalkosten

Das Vorhaben konnte mit den 5 geplanten Stellen Projektleiter, Product Owner, Data Scientist, Frontend Entwickler und Backend Entwickler abgewickelt werden.

0822 Beschäftigungsentgelte

Es wurde eine studentische Hilfskraft eingestellt.

0835 Vergabe von Aufträgen

Um projektnotwendiges, aber nicht intern vorhandenes Wissen zu erlangen, wurden zwei externe Dienstleister einbezogen. Zum einen benötigten wir die Hilfe eines professionellen ISO 27001 Lead-Auditors, um mit diesem gemeinsam ein Konzept zu entwickeln, wie wir unseren Demonstrator optimal in die Zertifizierungspraxis einbinden können. Zum anderen haben wir Unterstützung durch einen erfahrenen Business Coach angefordert, der sehr großen Erfolg mit der Entwicklung ähnlicher Produkte vorweisen kann.

Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die durchgeführten Arbeiten im Projekt ML Policy sowie die dafür aufgewandten Ressourcen entsprechen den im Projektantrag dargestellten Vorhaben und waren notwendig und angemessen.

Die Zuwendung wurde hauptsächlich für Personalkosten verwendet. Eine nahezu vollständige Entwicklung mit internen Ressourcen war deutlich kostengünstiger als mit extensivem Einbezug externer Ressourcen und hat einen deutlich besseren Knowhow-Aufbau ermöglicht. Zudem ist bei interner Entwicklung das Risiko eines Knowhow-Abflusses deutlich geringer. Eine Entwicklung mit internen Ressourcen erscheint deswegen angemessen, kosteneffizient und strategisch sinnvoll.

Notwendig war die Entwicklung aus zwei Aspekten:

- 1.) Notwendigkeit des Gesamtprojektes: Der normative Wert der ISO 27001 verpufft im Mittelstand derzeit weitgehend, weil die Umsetzung in vielen Fällen prohibitiv teuer ist oder zumindest im Vergleich zu anderen Investitionen nicht attraktiv erscheint. Im Sinne einer Stärkung der Resilienz des Mittelstandes ist es deswegen notwendig, die Hürden beim Aufbau eines ISMS abzubauen und Kosten zu senken.
- 2.) Notwendigkeit der Projektarbeiten: Innerhalb des Projektes war es über die Entwicklung mit internen Ressourcen hinaus notwendig, zwei Dienstleister mit Spezialwissen einzubeziehen, das an einer Universität nicht erworben werden kann, zum einen Wissen aus der ISO 27001 Zertifizierungspraxis und zum anderen ein Coaching durch einen erfolgreichen Gründer, welches die Chancen auf eine erfolgreiche Marktpositionierung erhöht.

Durch die Kombination aus interner Entwicklung und gezieltem Einbezug externen Wissens konnte der Ressourcenverbrauch auf ein notwendiges und angemessenes Maß reduziert werden.

Voraussichtlicher Nutzen und Verwertung

Stand der Verwertung

Der Demonstrator ist zum Ende des Vorhabens noch nicht in einem vermarktungsfähigen Zustand und benötigt technische Reifung und Weiterentwicklung zu einem marktfähigen Produkt. Der Demonstrator kann in der vorliegenden Form deswegen nicht direkt an Anwender lizenziert werden, sondern muss eine Weiterentwicklung erfahren. Deswegen findet die Verwertung im Anschluss an das Vorhaben in Form einer Rechteeinräumung zur Weiterentwicklung statt.

Nutzen für Anwender

Der entwickelte Demonstrator adressiert drei Zielgruppen, um die Entwicklung eines ISMS und eine Zertifizierung nach ISO 27001 niedrigschwelliger zu gestalten.

Nutzen für Zielgruppe Erstzertifizierung Mittelstand: Der primäre Zielmarkt besteht aus mittelständischen Unternehmen, die sich auf eine Zertifizierung in der Informationssicherheit vorbereiten wollen, oder anderweitig Konformität zu IT-Grundschutz, ISO 27001 oder weiteren Rahmenwerken erreichen wollen. Während große Unternehmen meistens genügend finanzielle Ressourcen haben, um große Auditierungsgesellschaften mit der Zertifizierung zu beauftragen, können mit dem Demonstrator kleine und mittelständige Unternehmen angesprochen werden, die oft nicht die erforderlichen Mittel haben, um die Zertifizierung in externe Hände zu geben. Die fehlende Expertise und die hohen externen Kosten stellen eine enorme Barriere für den Mittelstand dar. Statt Aufgaben an Externe abzugeben, sollen Unternehmen weitestgehend selbst befähigt werden. Eine Reduzierung der externen Beratungskosten um ein Drittel stellt für diese Zielgruppe bereits einen signifikanten Vorteil dar.

Nutzen für Zielgruppe Rezertifizierung: Einen zweiten Zielmarkt stellen Unternehmen dar, die bereits zertifiziert sind und die Änderung in den Rahmenwerken und die Weiterentwicklung ihres ISMS tool-unterstützt begleiten wollen, insbesondere mit dem Ziel einer leichtgängigen Rezertifizierung. Weltweit existieren 44.500 gültige

ISO 27001-Zertifizierungen¹, davon in Deutschland ca. 1500². Für bestehende Zertifizierungen sind jährliche Überwachungsaudits und alle drei Jahre eine Rezertifizierung notwendig.

Nutzen für Zielgruppe Auditierungsgesellschaften: Ein weiterer Zielmarkt sind Auditierungsgesellschaften, die ihren Kunden unsere Lösung im Bündel mit ihren Dienstleistungen anbieten können, und die mit der Software neue Mitarbeiter effizienter einsetzen zu können.

Schutzrechte und Patente

Schutzrechte und Patente sind nicht angemeldet worden.

Fortschritt auf dem Gebiet während der Projektlaufzeit

Im Bereich Machine Learning und darin insbesondere im Bereich Natural Language Processing (NLP) werden in einem rasanten Tempo, teilweise unterjährig, Meilensteine erreicht. Während der Projektlaufzeit gab es bedeutende Fortschritte im NLP-Bereich. Ein herausragendes Ereignis war die Veröffentlichung von GPT-4o durch OpenAI im Mai 2024. Ein weiterer wichtiger Meilenstein war die Einführung von GPT-4 Turbo im November 2023. Dieses Modell ermöglichte es Nutzern, eigene Chatbots zu erstellen, sogenannte "Custom GPTs", und konnte bis zu 128.000 Tokens auf einmal verarbeiten. Zusätzlich wurden Open-Source-Modelle wie Mixtral 8x7b von Mistral AI im Januar 2024 veröffentlicht.

Diese technologischen Entwicklungen geben Rückenwind und haben neue Möglichkeiten geboten, die Projektziele zu erreichen.

Fortschritt auf dem konkreten Anwendungsgebiet der automatisierten Verbindung von Informationssicherheitsanforderungen über verschiedene Rahmenwerke hinweg ist während der Laufzeit nicht bekannt geworden.

¹ <https://de.statista.com/statistik/daten/studie/829313/umfrage/bestand-an-vergebenen-iso-27001-zertifikaten-weltweit>

² <https://de.statista.com/statistik/daten/studie/829353/umfrage/bestand-an-vergebenen-iso-27001-zertifikaten-in-deutschland/>