Holger Reibold

Supply Chain Security Audit

Handbuch für prüfungssichere Lieferketten – NIS-2, DORA und ISO 28000 sicher umsetzen

BRAIN-MEDIA.DE

Holger Reibold

Supply Chain Security Audits

Handbuch für prüfungssichere Lieferketten – NIS-2, DORA und ISO 28000 sicher umsetzen

BRAIN-MEDIA.DE

ISBN: 978-3-95444-359-8

Cover: senivpetro / Freepik

Brain-Media.de

Dr. Holger Reibold – Huber-Müller-Str. 52 – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Vorwort

Lieferketten sind Ihr größtes Sicherheitsrisiko

Die Sicherheit von Lieferketten hat sich in den vergangenen Jahren von einem operativen Randthema zu einer der zentralen Herausforderungen moderner Unternehmen entwickelt. Globale Vernetzung, zunehmende Digitalisierung und eine steigende Abhängigkeit von Drittanbietern haben dazu geführt, dass Risiken längst nicht mehr nur innerhalb der eigenen Organisationsgrenzen entstehen. Vielmehr verlagern sich kritische Schwachstellen entlang komplexer, oft intransparenter Wertschöpfungsnetzwerke – mit erheblichen Auswirkungen auf die Resilienz, Compliance und Wettbewerbsfähigkeit von Unternehmen.

Cyberangriffe auf Software-Lieferketten, kompromittierte Updates, unsichere Drittanbieter oder mangelhaft kontrollierte Cloud-Dienste sind heute keine Ausnahme mehr, sondern Teil einer realen Bedrohungslage. Gleichzeitig erhöhen regulatorische Anforderungen wie NIS-2, DORA und der Cyber Resilience Act den Druck auf Organisationen, ihre Lieferketten nicht nur zu verstehen, sondern systematisch zu steuern, zu überwachen und vor allem nachweisbar abzusichern.

Genau an dieser Schnittstelle setzt dieses Buch an.

Ziel dieses Werkes ist es, Supply-Chain-Security nicht als abstraktes Konzept, sondern als konkret prüfbares und steuerbares System darzustellen. Der Fokus liegt dabei bewusst auf der Auditierbarkeit: Welche Kontrollen müssen etabliert sein? Wie lassen sich Risiken entlang der Lieferkette strukturiert bewerten? Und vor allem – wie kann ein Unternehmen gegenüber interner Revision, Wirtschaftsprüfern oder Aufsichtsbehörden belastbar nachweisen, dass die eigenen Lieferketten angemessen abgesichert sind?

Dieses Buch richtet sich an Fach- und Führungskräfte, die Verantwortung für Sicherheit, Risiko oder Compliance tragen. Dazu zählen insbesondere Auditoren, Informationssicherheitsbeauftragte, Chief Information Security Officers (CISOs), Risikomanager sowie Verantwortliche für Drittparteien-Management. Gleichzeitig ist es auch für Entscheider konzipiert, die strategische Leitplanken für den Umgang mit Lieferkettenrisiken definieren müssen.

Ein wesentliches Unterscheidungsmerkmal dieses Buches liegt in der konsequenten Verbindung von drei Perspektiven:

- Erstens: der regulatorischen Perspektive. Anforderungen aus NIS-2, DORA und relevanten ISO-Standards werden nicht isoliert betrachtet, sondern systematisch in den Kontext von Supply-Chain-Security eingeordnet. Ziel ist es, ein klares Verständnis dafür zu schaffen, welche regulatorischen Verpflichtungen konkret adressiert werden müssen – und wie diese praktisch umgesetzt werden können.

- Zweitens: der auditmethodischen Perspektive. Dieses Buch versteht sich ausdrücklich als Handbuch für prüfungssichere Lieferketten. Es geht nicht nur darum, „was" zu tun ist, sondern „wie" es geprüft wird. Auditmethoden, Evidenzanforderungen, Reifegradmodelle und strukturierte Prüfansätze bilden daher einen zentralen Bestandteil.
- Drittens: der technischen Perspektive. Insbesondere die Sicherheit von Software-Lieferketten – etwa durch den Einsatz von Software Bill of Materials (SBOM), Code-Signing oder automatisierte Prüfmechanismen – gewinnt zunehmend an Bedeutung. Diese Aspekte werden gezielt vertieft, da sie für die praktische Umsetzung regulatorischer Anforderungen entscheidend sind.

Um diese Perspektiven konsistent miteinander zu verbinden, folgt das Buch einer klar strukturierten Logik: Von den Grundlagen über Governance und Lieferantenbewertung bis hin zu konkreten Auditmethoden, technischen Kontrollen und operativen Prozessen. Ergänzt wird dies durch die Betrachtung internationaler Lieferketten sowie zukünftiger Entwicklungen wie Continuous Auditing oder KI-gestützte Prüfverfahren.

Ein zentrales Gestaltungsprinzip ist dabei der sogenannte „regulatorische rote Faden". Jedes Kapitel endet mit einer Management Summary, die nicht nur die wesentlichen Inhalte zusammenfasst, sondern diese explizit regulatorisch einordnet. Dadurch entsteht eine direkte

Verbindung zwischen implementierten Maßnahmen und den zugrunde liegenden Anforderungen aus NIS-2, DORA und anderen relevanten Regelwerken. Dieses Prinzip ermöglicht es, Inhalte unmittelbar in Auditkontexte zu übertragen und als Grundlage für Prüfberichte oder interne Bewertungen zu nutzen.

Darüber hinaus wurde besonderer Wert auf Praxisnähe gelegt. Checklisten, Beispielstrukturen und modellhafte Darstellungen – etwa zur Abbildung von Kontrollen in standardisierten Formaten – sollen dazu beitragen, die Inhalte nicht nur zu verstehen, sondern direkt anzuwenden. Das Buch ist somit nicht nur als Wissensquelle gedacht, sondern als Arbeitsinstrument für den täglichen Einsatz in Audit- und Compliance-Prozessen.

Gleichzeitig ist zu beachten, dass Supply-Chain-Security-Audits nicht ausschließlich eine technische oder regulatorische Disziplin sind. In der Praxis spielen auch organisatorische und zwischenmenschliche Faktoren eine entscheidende Rolle. Der Zugriff auf Informationen bei Drittanbietern, die Durchsetzung von Auditrechten oder der Umgang mit kritischen Abhängigkeiten erfordern neben methodischem Know-how auch kommunikative und strategische Fähigkeiten. Diese Dimension wird daher bewusst in die Betrachtung einbezogen.

Die vorliegende Struktur und inhaltliche Ausrichtung dieses Buches verfolgen ein klares Ziel: Organisationen in die Lage zu versetzen, ihre Lieferketten nicht nur zu sichern, sondern deren Sicherheit nachvollziehbar zu belegen. In einer Zeit zunehmender regulatorischer Anforderungen und wachsender Bedrohungen ist dies kein

optionaler Zusatz mehr, sondern eine grundlegende Voraussetzung für nachhaltigen Unternehmenserfolg.

Wenn dieses Buch dazu beiträgt, Audits strukturierter, Diskussionen fundierter und Entscheidungen belastbarer zu machen, hat es seinen Zweck erfüllt.

Herzlichst

Holger Reibold

1 Grundlagen der Supply-Chain-Security

Ohne Grundlagen kein Schutz – die wahren Risiken

Die Sicherheit von Lieferketten ist heute ein zentraler Bestandteil der Unternehmenssicherheit und geht weit über klassische IT-Sicherheitsansätze hinaus. Moderne Organisationen sind in komplexe Netzwerke aus Lieferanten, Dienstleistern und Technologiepartnern eingebunden, wodurch sich die Angriffsfläche erheblich erweitert. Risiken entstehen nicht mehr ausschließlich innerhalb der eigenen Organisation, sondern insbesondere an den Schnittstellen zu Drittparteien.

Supply-Chain-Security umfasst daher alle Maßnahmen, die darauf abzielen, diese erweiterten Abhängigkeiten systematisch zu identifizieren, zu bewerten und zu kontrollieren. Dabei stehen sowohl technische als auch organisatorische Aspekte im Fokus, ergänzt durch regulatorische Anforderungen, die zunehmend konkrete Vorgaben für den Umgang mit Lieferkettenrisiken machen.

Dieses Kapitel legt die konzeptionelle Grundlage für das Verständnis von Supply-Chain-Security. Es definiert zentrale Begriffe, grenzt das Themenfeld von angrenzenden Disziplinen ab und ordnet aktuelle Bedrohungen sowie regulatorische Entwicklungen ein. Darüber hinaus werden die wesentlichen Rollen, Verantwortlichkeiten und

Sicherheitsziele beschrieben, die für eine wirksame Steuerung und Auditierbarkeit von Lieferketten erforderlich sind.

1.1 Definition und Abgrenzung

Supply-Chain-Security bezeichnet die Gesamtheit aller strategischen, organisatorischen und technischen Maßnahmen, die darauf abzielen, Risiken entlang der Liefer- und Wertschöpfungskette eines Unternehmens zu identifizieren, zu bewerten und zu minimieren. Im Kern geht es darum, sicherzustellen, dass externe Abhängigkeiten – insbesondere zu Lieferanten, Dienstleistern und Technologiepartnern – kein unkontrolliertes Risiko für Verfügbarkeit, Integrität und Vertraulichkeit von Systemen, Daten und Prozessen darstellen.

Im Gegensatz zu klassischen Sicherheitsansätzen, die sich primär auf die interne IT-Infrastruktur konzentrieren, erweitert Supply-Chain-Security den Betrachtungsraum auf ein verteiltes Ökosystem. Dieses umfasst nicht nur direkte Vertragspartner (Tier-1-Lieferanten), sondern auch nachgelagerte Abhängigkeiten (Tier-n), die häufig nicht unmittelbar sichtbar sind. Gerade diese indirekten Verbindungen stellen in der Praxis ein erhebliches Risiko dar, da sie oft außerhalb direkter Kontrollmechanismen liegen.

Eine zentrale Herausforderung besteht darin, Transparenz über diese komplexen Abhängigkeiten herzustellen. Ohne ein klares Verständnis darüber, welche externen Komponenten, Dienstleistungen oder Softwarebausteine in die eigene Wertschöpfung einfließen, ist eine

fundierte Risikobewertung nicht möglich. Supply-Chain-Security erfordert daher nicht nur technische Kontrollen, sondern auch strukturierte Governance-Mechanismen und belastbare Informationsflüsse.

Abzugrenzen ist Supply-Chain-Security von verwandten Disziplinen wie klassischer Informationssicherheit, IT-Risikomanagement oder Vendor Management. Während Informationssicherheit sich auf den Schutz von Informationen und Systemen innerhalb einer Organisation fokussiert, erweitert Supply-Chain-Security diesen Fokus auf externe Einflüsse. IT-Risikomanagement wiederum betrachtet Risiken häufig auf aggregierter Ebene, ohne notwendigerweise die Tiefe und Spezifität von Drittparteienbeziehungen abzubilden. Vendor Management konzentriert sich primär auf wirtschaftliche und operative Aspekte der Lieferantensteuerung, während sicherheitsrelevante Fragestellungen dort oft nur eine untergeordnete Rolle spielen.

Eine weitere wichtige Abgrenzung besteht zur physischen Lieferkettensicherheit, wie sie beispielsweise in der Logistik oder im industriellen Umfeld betrachtet wird. Während dort Themen wie Transport, Lagerung oder physischer Zugriff im Vordergrund stehen, liegt der Schwerpunkt dieses Buches auf der digitalen beziehungsweise informationsbezogenen Supply-Chain-Security. Dennoch bestehen in vielen Fällen Überschneidungen, insbesondere wenn physische und digitale Komponenten miteinander verknüpft sind, etwa in industriellen Steuerungssystemen oder bei vernetzten Produktionsumgebungen.

Mit der zunehmenden Digitalisierung verschiebt sich der Fokus immer stärker auf die sogenannte Software Supply Chain. Hierbei geht es um die Herkunft, Integrität und Sicherheit von Softwarekomponenten, Bibliotheken und Entwicklungsprozessen. Die Verwendung von Open-Source-Komponenten, automatisierten Build-Prozessen und Continuous-Integration-/Continuous-Delivery-Pipelines führt zu einer erheblichen Dynamik, aber auch zu neuen Risiken. Konzepte wie die Software Bill of Materials (SBOM) gewinnen in diesem Kontext an Bedeutung, da sie Transparenz über eingesetzte Komponenten schaffen und somit eine Grundlage für Sicherheitsbewertungen bilden.

Ein wesentliches Merkmal von Supply-Chain-Security ist ihre interdisziplinäre Natur. Sie vereint Aspekte aus Informationssicherheit, Risikomanagement, Compliance, Einkauf, Vertragsrecht und operativem Betrieb. Effektive Sicherheitsmaßnahmen erfordern daher eine enge Zusammenarbeit zwischen verschiedenen Organisationseinheiten sowie klare Verantwortlichkeiten. Ohne diese Integration besteht die Gefahr von blinden Flecken, insbesondere an den Schnittstellen zwischen Fachbereichen.

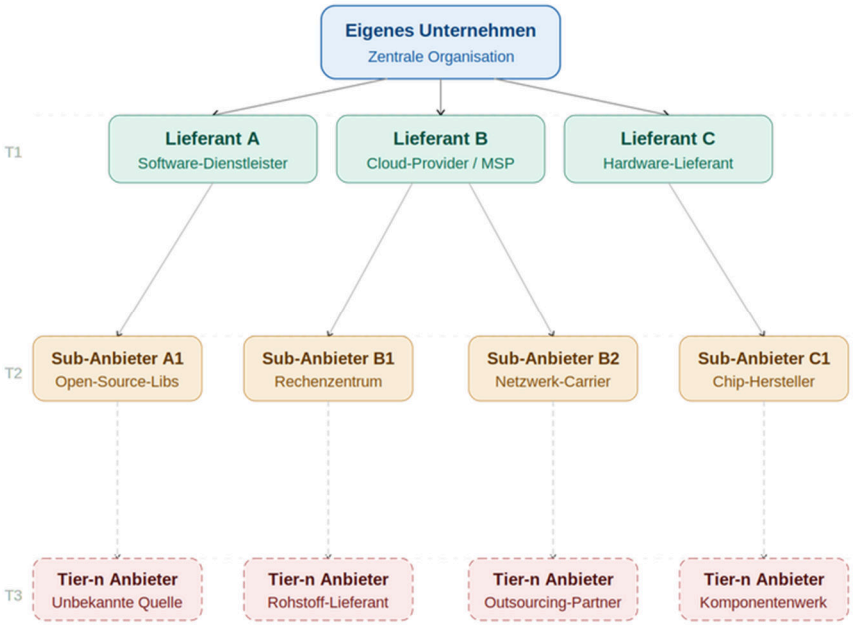


Abbildung 1: Die Struktur moderner Lieferketten mit direkten und indirekten Abhängigkeiten (Tier-1 bis Tier-n) und verdeutlicht die zunehmende Intransparenz sowie die wachsende Angriffsfläche durch externe Partner.

1.2 Bedrohungslandschaft

Die Bedrohungslandschaft im Kontext der Supply-Chain-Security hat sich in den letzten Jahren signifikant verändert und zeichnet sich durch eine zunehmende Professionalisierung sowie eine stärkere Fokussierung auf indirekte Angriffsvektoren aus. Angreifer nutzen gezielt die Tatsache aus, dass Organisationen ihre eigenen Systeme häufig besser absichern als die ihrer Lieferanten. Dadurch wird die Lieferkette selbst zum bevorzugten Einstiegspunkt.

Ein zentrales Angriffsszenario sind Kompromittierungen von Software-Lieferketten. Dabei werden beispielsweise Entwicklungsumgebungen, Build-Systeme oder Update-Mechanismen manipuliert, um schädlichen Code in legitime Softwareprodukte einzuschleusen. Da diese Software anschließend über reguläre Distributionskanäle verbreitet wird, erreicht ein erfolgreicher Angriff potenziell eine große Anzahl von Zielsystemen. Die Integrität von Softwareartefakten und die Vertrauenswürdigkeit von Update-Prozessen stehen daher im Fokus moderner Angriffe.

Neben softwarebasierten Angriffen spielen auch klassische Drittparteirisiken eine wesentliche Rolle. Externe Dienstleister, Managed Service Provider oder Cloud-Anbieter verfügen häufig über privilegierte Zugriffe auf Systeme und Daten. Werden diese Zugänge kompromittiert oder unzureichend abgesichert, können Angreifer weitreichende Auswirkungen erzielen. Besonders kritisch sind dabei Konstellationen mit hoher Abhängigkeit von einzelnen Anbietern, da hier ein Ausfall oder eine Kompromittierung unmittelbare Auswirkungen auf zentrale Geschäftsprozesse haben kann.

Ein weiteres relevantes Risiko ergibt sich aus mangelnder Transparenz in mehrstufigen Lieferketten. Während direkte Vertragspartner in der Regel bekannt sind, bleiben nachgelagerte Abhängigkeiten oft unklar. Diese sogenannten Tier-n-Lieferanten können jedoch erhebliche Risiken bergen, insbesondere wenn sie sicherheitskritische Komponenten oder Dienstleistungen bereitstellen. Angreifer nutzen

gezielt diese Intransparenz, um über weniger geschützte Glieder der Kette Zugang zu höherwertigen Zielen zu erlangen.

Auch Insider-Bedrohungen innerhalb von Lieferantenorganisationen gewinnen an Bedeutung. Fehlverhalten, Fahrlässigkeit oder gezielte Sabotage durch Mitarbeitende externer Partner können ebenso gravierende Auswirkungen haben wie externe Angriffe. Da diese Personen häufig legitimen Zugriff auf Systeme besitzen, sind solche Szenarien besonders schwer zu erkennen und zu verhindern.

Darüber hinaus führen geopolitische Spannungen und regulatorische Fragmentierung zu neuen Risikodimensionen. Abhängigkeiten von Anbietern in bestimmten Regionen können mit politischen oder rechtlichen Unsicherheiten verbunden sein, etwa im Hinblick auf Datenzugriff, Exportkontrollen oder staatliche Einflussnahme. Diese Faktoren müssen zunehmend in die Bedrohungsanalyse einbezogen werden.

Die Dynamik der Bedrohungslandschaft wird zusätzlich durch technologische Entwicklungen verstärkt. Automatisierung, Cloud-Computing und der verstärkte Einsatz von Open-Source-Komponenten erhöhen die Komplexität und Geschwindigkeit von Entwicklungs- und Betriebsprozessen. Gleichzeitig erweitern sie die potenzielle Angriffsfläche. Angreifer sind in der Lage, Schwachstellen in großem Maßstab zu identifizieren und auszunutzen, während Organisationen oft Schwierigkeiten haben, den Überblick über ihre eigenen Abhängigkeiten zu behalten.

Insgesamt ist die Bedrohungslandschaft durch eine Verschiebung von direkten zu indirekten Angriffen gekennzeichnet. Die Lieferkette fungiert dabei als Multiplikator, über den einzelne Schwachstellen weitreichende Auswirkungen entfalten können. Für Unternehmen bedeutet dies, dass klassische Schutzmaßnahmen nicht mehr ausreichen und eine systematische Einbeziehung externer Risiken zwingend erforderlich ist.

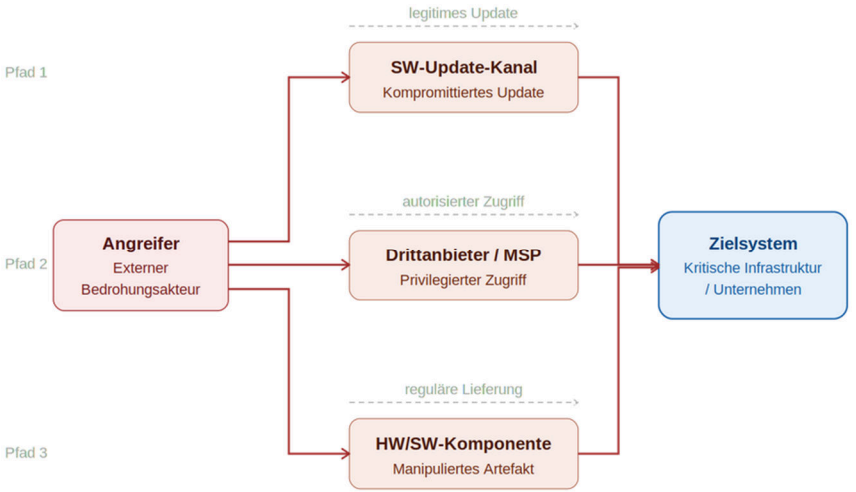
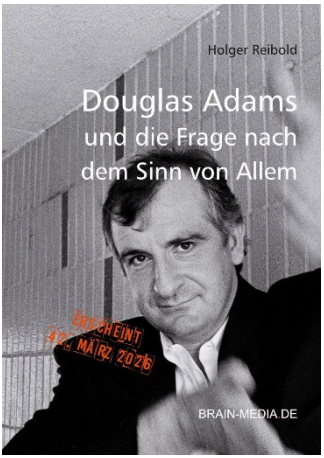


Abbildung 2: Visualisierung typischer Angriffspfade über Drittanbieter, Software-Updates oder kompromittierte Komponenten, die zeigen, wie Angreifer indirekt in Zielsysteme eindringen können.

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

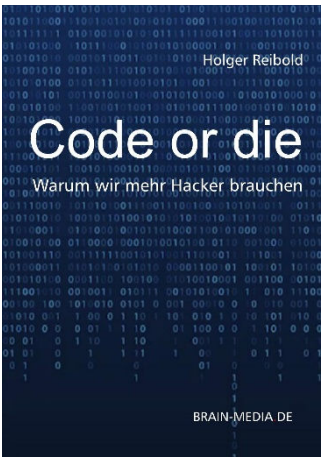
Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 14,99 EUR

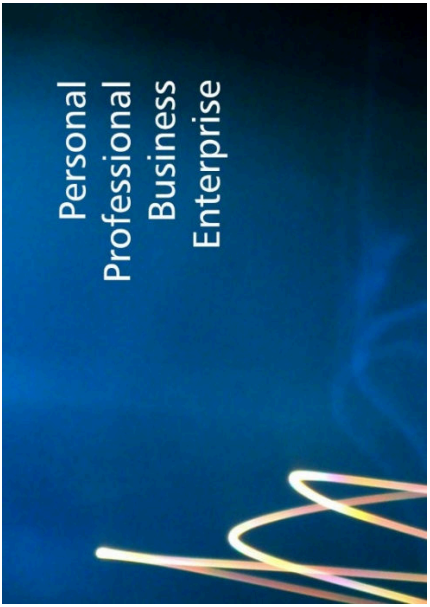
Erscheint Frühjahr 2026

Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

RAG- und LLM-Plattformen mit klarer Architektur, Guardrails, Monitoring und Governance kontrolliert und resilient betreiben.

Umfang: 270 Seiten

Preis: 29,99 EUR



Knowledge as a Service (KaaS)

Compliance als operativer Vorteil

NIS-2, DORA, EU AI Act, CRA – der regulatorische Druck wird zum Geschäftsrisiko. KaaS (Knowledge as a Service) macht Ihr Unternehmen sicher und audit-ready – schnell, strukturiert und ohne externe Beratungsabhängigkeit. Statt fragmentierter Anforderungen und schwer umsetzbarer Vorgaben erhalten Sie ein System, das Compliance in operative Umsetzung überführt:

- klare, priorisierte Anforderungen
- direkt umsetzbare Templates
- auditfähige Dokumentation
- kontinuierlich aktualisierte Inhalte

Von Unsicherheit und Einzelmaßnahmen zu strukturierter, prüfbarer Umsetzung. KaaS reduziert Ihre Risiken, beschleunigt die Umsetzung und schafft Transparenz auf allen Unternehmensebenen.

Vier Varianten – für jeden Bedarf die passende Lösung

KaaS ist in vier Tarifen verfügbar: von Personal für Einzelpersonen und IT-Leiter über Team (empfohlen) für Compliance-Abteilungen und Berater bis zu Business für Mittelstand und IT-Dienstleister – und Enterprise für größere Unternehmen und KRITIS-Betreiber mit unbegrenzter Nutzerzahl. Ihren Fragen beantwortet unsere FAQ. Für Kunden steht eine 20seitige Einleitung zur Nutzung von KaaS bereit.

Individuelle Anforderungen

Kein Unternehmen ist wie das andere – Branche, Größe, Reifegrad und regulatorisches Umfeld unterscheiden sich signifikant. Sie haben individuelle Anforderungen? Wir setzen diese gerne um.