Hochschule Niederrhein

HSNR

Hochschule Niederrhein
Fachbereich 08 - Wirtschaftswissenschaften

Masterarbeit

„Cyber Resilience Act und Softwareentwicklung – Herausforderungen und Lösungsansätze für Softwareentwicklung deutscher Unternehmen“

Frédéric Noppe - 1520686

Master Cybersecurity Management
MCSM 9000: Masterarbeit

Masterarbeit **21. September 2025 – SS 25**

Prüfer: **Prof. Dr. René Treibert**
Prof. Dr. Matthias Mehrtens

Entstanden an der

Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Zusammenfassung

Die vorliegende Arbeit untersucht den Stand der getroffenen Sicherheitsmaßnahmen in softwareentwickelnden Organisationen und der Awareness der Softwareentwickler bezüglich der Anforderungen des Cyber Resilience Acts (CRA) der Europäischen Union mit einem Fokus auf die Softwareentwicklung. Die im Zuge einer Umfrage erhobenen Daten zeigen, dass in Bezug auf die durch den CRA geforderten Sicherheitsmaßnahmen Nachholbedarf in verschiedensten Feldern wie etwa dem Security by Design, dem Schwachstellenmanagement, der Schwachstellenkommunikation, der Erstellung konformer SBOMs und der Softwareversionierung besteht. Um die vom CRA betroffenen Organisationen zu unterstützen, werden in dieser Arbeit Maßnahmen erarbeitet, um die Anforderungen der Gebiete mit dem höchsten festgestellten Nachholbedarf zu erfüllen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BSI Bundesamt für Sicherheit in der Informationstechnik 1

C5 Cloud Computing Compliance Controls Catalogue 27
CALMAS Culture, Automation, Lean, Measurement, Added Value, Sharing 8
CAMS Culture, Automation, Measurement, Sharing 8
CD Continuous Delivery 9
CI Continuous Integration 9
CNA CVE Numbering Authority 73
CNC Computerized Numerical Control 19
CPE Common Platform Enumeration 72
CRA Cyber Resilience Act 1
CSAF Common Security Advisory Framework 14, 73
CSIRT Computer Security Incident Response Team 75
CVD Coordinated vulnerability disclosure 73
CVE Common Vulnerabilities and Exposures 12
CWE Common Weakness Enumeration 12

DCS Distributed Control System 19
DevSecOps Development, Security and Operations 7, 9

ENISA European Union Agency for Cybersecurity 15
EU Europäische Union 1
EUVD ENISA European Vulnerability Database 73

HIPAA Health Insurance Portability and Accountability Act 27
HSM Hardware Security Module 19

IAC Industrial Automation and Control System 19

IaC Infrastructure as code 10

IIoT Industrial Internet of Things 19

IoT Internet of Things 1

ISMS Informationssicherheitsmanagementsystems 28

KPI Key Performance Indicators 8

KRITIS Kritische Infrastrukturen 27

NVD National Vulnerability Database 32

PCI-DSS Payment Card Industry Data Security Standard 27

PLC Programmable Logic Controller 19

PSIRT Product Security Incident Response Team 74

SaaS Software as a Service 34

SCADA Supervisory Control and Data Acquisition 19

SDLC Software Development Lifecycle 10

SIEM Security Information and Event Management 18

SSDF Secure Software Development Framework 11

TISAX Trusted Information Security Assessment Exchange 27

URI Uniform Resource Identifier 72

URL Uniform Resource Locator 71

UTC Universal Time Coordinated 71

VEX Vulnerability Exploitability eXchange 14

1 Einleitung

Angriffe auf IT-Infrastrukturen, Software und die Ausnutzung von Schwachstellen in Produkten mit digitalen Elementen nehmen seit mehreren Jahren in Folge zu [1], [2]. Im Bereich der Software rücken Angriffe auf deren Lieferkette, wie in den prominenten Sicherheits-Vorfällen um SolarWinds in 2021 [3], XZ Utils in 2024 [4] und zahlreichen Angriffen auf die npm-library [5], [6], [7] immer häufiger in den Vordergrund. So wurde 2023 eine laut Bundesamt für Sicherheit in der Informationstechnik (BSI) die besorgniserregend hohe Zahl von 78 neuen Schwachstellen pro Tag gemeldet [1], welche dann bereits im folgenden Jahr 2024 mit 110 neuen Schwachstellen pro Tag deutlich übertroffen wurde [8]. Ebenso sind im Bereich der Regulatorik von Softwareprodukten auf der europäischen Ebene noch Lücken und Ungleichheiten in den Sicherheitsanforderungen an diese „Produkte mit digitalen Elementen“ vorhanden, die es notwendig machen, dass die EU diese durch zusätzliche Regulatoriken adressiert [2]. Unter anderem wurde der Cyber Resilience Act (CRA) aus diesem Grund als erste europäische Verordnung für eine horizontale Regulation der Sicherheitsanforderungen für Produkte mit digitalen Elementen am 23.10.2024 durch das Europäische Parlament verabschiedet und ist am 11.12.2024 in Kraft getreten [2]. Das Ziel des CRA ist es ein flächendeckendes Mindestmaß an Cybersicherheit für alle vernetzten Produkte wie Software und Internet of Things (IoT) Geräte festzulegen, die auf dem Markt der Europäischen Union (EU) zum Kauf durch Unternehmen und Privatpersonen erhältlich sind und er erweitert das bisher von z. B. Elektrogeräten, Spielzeug oder Medizinprodukten bekannte CE-Kennzeichen auf den Bereich der vernetzten Software und Hardware [9]. Ziel ist es, die Cybersicherheit für Unternehmen sowie die Bürger und Bewohner in allen EU-Mitgliedstaaten zu erhöhen, in denen die Anforderungen des CRA bis zum Stichtag des 11.12.2027 komplett umgesetzt und eingehalten werden muss.[10]

1.1 Problemvorstellung

Bislang erfolgt bei Unternehmen aus dem Bereich der Softwareentwicklung überwiegend eine Kenntnisnahme der neuen Auflagen ohne direkte Umsetzungsvorhaben. Dies ist womöglich auf die als zeitlich fern wahrgenommene Frist bis 2027 zurückzuführen. Doch ist der Geltungsbereich des CRA sehr umfassend und betrifft nahezu jeden Softwarehersteller, der im Vorfeld nicht bereits anderen Regularien zur Cyber- und Softwaresicherheit unterliegt (z. B. NIS-2, Medizinprodukte oder in der Luftfahrt) [2]. Aufgrund einer der Aktualität der Thematik geschuldeten, dünnen Forschungslage, die auch die These der

wahrgenommenen Ferne des Themas unterstreicht, ist es weitgehend noch unklar, inwieweit die betroffenen Unternehmen auf die Einhaltung des CRA vorbereitet sind sowie die Art der Anforderungen, die durch die betroffenen Unternehmen bisher nicht erfüllt werden.

1.2 Zielsetzung der Arbeit

Ziel der vorliegenden Arbeit ist es, den allgemeinen Kenntnisstand zum CRA im Umfeld der Industrien und Organisationen, speziell der softwareentwickelnden Organisationen, zu untersuchen, welche direkt von den Vorgaben des CRA betroffen sind. Es wird analysiert, in welchem Maße der CRA innerhalb der Unternehmen bereits thematisiert und priorisiert wird. Der Schwerpunkt liegt hierbei in der Untersuchung des aktuellen Umsetzungsgrades der CRA-Vorgaben innerhalb der betroffenen Organisationen mittels einer anonymen Befragung per Online-Fragebogen. Durch die Befragung der Umfrageteilnehmer wird somit überprüft, inwiefern bereits vor Inkrafttreten des CRA die in ihm geforderten Maßnahmen in den Arbeitsabläufen der jeweiligen Organisationen integriert wurden und mit den Anforderungen der Verordnung übereinstimmen bzw. diese zumindest teilweise erfüllen.

Auf Basis der während der Arbeit gewonnenen Umfrageergebnisse werden nach der Ergebnisanalyse Handlungsempfehlungen erarbeitet, die es Unternehmen ermöglichen sollen, die im CRA und dessen Annex definierten Anforderungen möglichst effizient und zielgerichtet umzusetzen. Die Ergebnisse dieser Arbeit können damit als praxisorientierte Unterstützung verwendet werden, um betroffene Organisationen bei der strategischen und operativen Anpassung an die neuen regulatorischen Rahmenbedingungen zu begleiten.

1.3 Forschungsfragen

Beim Cyber Resilience Act handelt es sich um eine bisher nicht vollumfänglich umgesetzte Verordnung der Europäischen Union [10]. Dementsprechend ist der Forschungsstand bezüglich der Ergebnisse und Herausforderungen dieser Verordnung nicht sonderlich groß und setzt sich aus wenigen Papern und Betrachtungen der Materie durch Institutionen wie das Fraunhofer Institut zusammen [11]. Daher sind in diesem Forschungsfeld noch viele Fragen weitgehend unbeantwortet. Diese Arbeit soll mit der Beantwortung der folgenden Fragen zum Beginn der Forschung beitragen. Der Fokus wird primär auf der Softwareentwicklung liegen.

1. Inwieweit sind die Softwareentwicklungsabteilungen deutscher Unternehmen bereits auf das Inkrafttreten des CRA und dessen Anforderungen vorbereitet?

2. Wie ist der Kenntnisstand der Softwareentwickler über die jeweiligen, sie betreffenden Anforderungen im Sinne der Compliance Awareness?
3. Welche Maßnahmen können ergriffen werden, um tendenziell nicht erfüllte Anforderungen (basierend auf den Umfrageergebnissen) des CRA zu erfüllen?

1.4 Abgrenzung

In der vorliegenden Arbeit stehen die im Anhang geforderten Maßnahmen des Cyber Resilience Act (CRA) für die Softwareentwicklung und die Planung von Softwarekomponenten im Mittelpunkt. Aspekte, die die Entwicklung, Planung und Dokumentation speziell von Hardwaretechnologien betreffen, sind hingegen nicht Teil des Untersuchungsrahmens. Damit erfolgt eine bewusste thematische Eingrenzung, um die Analyse auf den softwarebezogenen Kernbereich der Regulierung zu konzentrieren und eine ausreichende Tiefe der Untersuchung zu gewährleisten. Ebenso wird in dieser Arbeit nicht auf das stufenweise Inkrafttreten des CRA eingegangen, sondern es werden alle zum finalen Datum des 11. Dezembers 2027 umzusetzenden Vorgaben betrachtet.

Darüber hinaus ist der zeitliche Rahmen dieser Arbeit klar definiert. Es kann ausschließlich auf Datenquellen und Erkenntnisse zurückgegriffen werden, die bis zum Abschluss der Arbeit verfügbar waren. Entwicklungen im Themenfeld des CRA, die nach dem 15. September 2025 eintreten, werden keinen Einfluss auf die Ergebnisse, Interpretationen und Schlussfolgerungen dieser Untersuchung haben.

2 Theoretische Grundlagen

Dieses Kapitel soll das Grundlagenwissen vermitteln, das notwendig ist, um die Ergebnisse der Untersuchung erfassen und interpretieren zu können.

2.1 Einführung in die Softwaresicherheit

In diesem Unterkapitel wird die Grundlage geschaffen, um das Feld der sicheren Softwareentwicklung zu verstehen. Dazu werden die historischen und aktuellen Wege der Softwareentwicklung erläutert. Im Anschluss wird anhand von modernen Sicherheitspraktiken vermittelt, wie dort der Aspekt der Sicherheit integriert werden kann.

2.1.1 Moderne Softwareentwicklung

Die moderne Softwareentwicklung ist von einem stetigen Wandel geprägt, der aus einer Vielzahl an technologischen Fortschritten, daraus resultierender wachsender Systemkomplexität und durch entsprechende Gewöhnungseffekte gestiegene Erwartungen von Kunden und Anwendern resultiert. Während bis in die 1990er hauptsächlich plangetriebene, lineare Vorgehensmodelle zur Umsetzung von Softwareprojekten verwendet wurden, sind mittlerweile flexiblere und iterative Ansätze auch in großen Entwicklungsprojekten etabliert. Allerdings gibt es kein universelles Modell, welches auf jedes einzelne Projekt gleichermaßen als Best-Practice anwendbar ist. Da sich die Anforderungen auch bei gut durchgeplanten Projekten in deren Verlauf ändern können, ist eine kontinuierliche Anpassung der Methoden an die jeweiligen Projektanforderungen erforderlich, um den aus Dynamik, Unsicherheit und Geschwindigkeit der Softwareentwicklung resultierenden Herausforderungen adäquat zu begegnen. [12], [13]

2.1.1.1 Traditionelle Entwicklung: Das Wasserfallmodell

Das Wasserfallmodell ist eines der ältesten und bekanntesten Vorgehensmodelle der Softwareentwicklung. Um 1970 wurde es von Winston Royce das erste Mal beschrieben und orientiert sich an einem streng sequentiellen Ablauf von Phasen wie Anforderungsanalyse, System- & Softwaredesign, Implementierung, Test, Betrieb und Wartung (siehe

Abbildung 2.1. Die Ergebnisse einer Phase fließen nach ihrem jeweiligen Abschluss direkt in die nächste ein und werden dort für die nächsten Arbeitsschritte aufgenommen. Dies begründet die Namensgebung, da die Arbeitsweise einem Wasserfall gleicht, dessen Fließrichtung unumkehrbar ist. [14], [13]

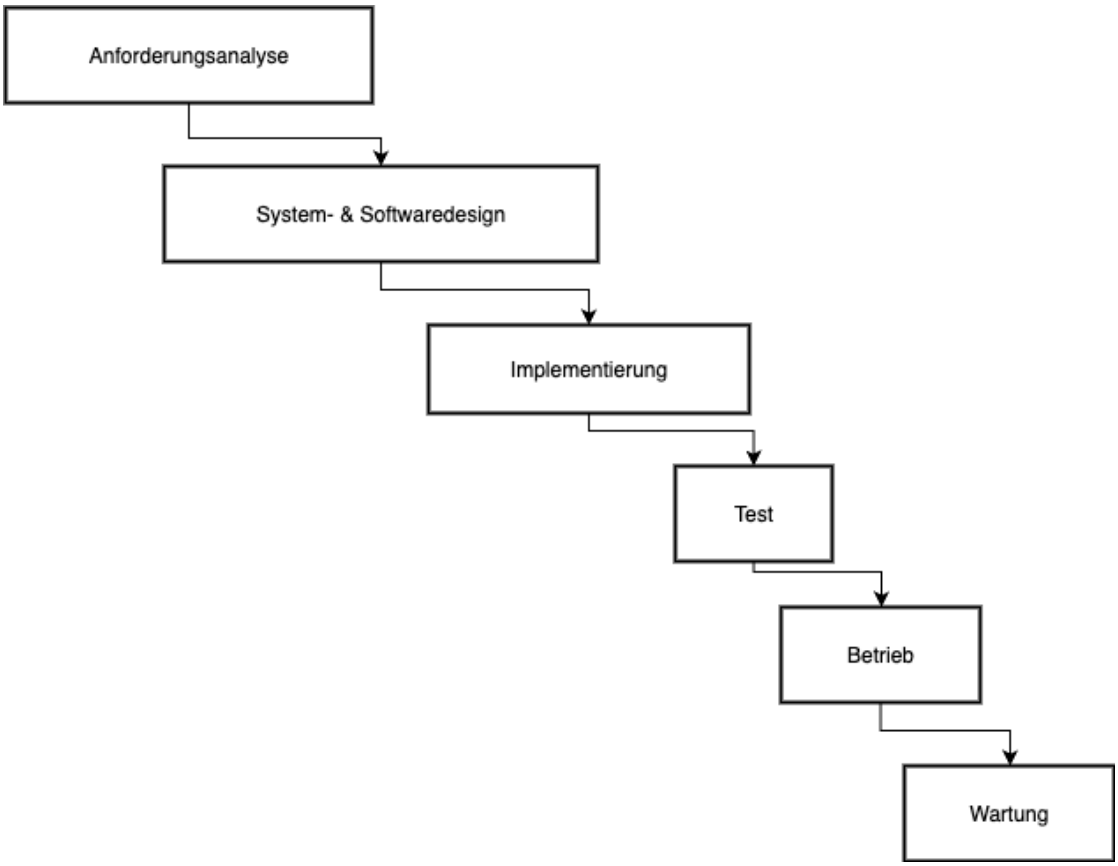


Abbildung 2.1: *Grafische Darstellung des Ablaufes der Phasen des Wasserfallmodells*

Die zentralen Merkmale des Wasserfallmodells sind dessen Einfachheit, die klare Strukturierung und die Nachvollziehbarkeit der jeweiligen Prozessschritte [14]. Insbesondere in Projekten mit stabilen und gut abschätzbaren Anforderungen kann diese Form des Vorgehens Vorteile bieten, da sie Transparenz und ein hohes Maß an Dokumentationsmöglichkeiten sicherstellt [13].

In der Realität moderner Softwareprojekte stößt das Modell allerdings schnell an Grenzen. Eine der größten Schwächen besteht darin, dass sich plötzlich ergebende Änderungen an Anforderungen oder Entwürfen z. B. durch neue Kundenanforderungen nach Abschluss einer Phase kaum mehr berücksichtigen lassen können. Da iterative Arbeitszyklen oder Rücksprünge im klassischen Modell nicht vorgesehen sind, kommt es zu teilweise schwerwiegenden Problemen, sobald sich Annahmen im Projektverlauf ändern.

Zudem ist die starre Abfolge oft unvereinbar mit der Realität, in der Anforderungen selten zu Beginn vollständig vorliegen und sich im Laufe der Zeit durch beispielsweise das Aufkommen einer neuen Technologie oder sich verändernden Regularien weiterentwickeln. Dadurch ist das Wasserfallmodell nur eingeschränkt für komplexe und dynamische Projekte geeignet und eignet sich in der heutigen Zeit insbesondere für kleinere genau planbare Entwicklungsprojekte. [14], [13]

Trotz dieser Kritikpunkte bleibt das Wasserfallmodell eine wertvolle und nicht zu vernachlässigende Arbeitsweise, da es die Phasen des Softwarelebenszyklus klar isoliert und Einsteigern in der Softwareentwicklung eine gute Grundlage bietet, um die grundlegenden Abläufe eines Entwicklungsprojektes zu verstehen [13].

2.1.1.2 Agile Softwareentwicklung

Als Reaktion auf die Schwächen der plangetriebenen Modelle wie dem Wasserfallmodell entstand zu Beginn der 2000er-Jahre die Bewegung der agilen Softwareentwicklung. Ihr Ursprung liegt im „Agilen Manifest“ von 2001, in dem führende Vertreter der modernen Softwareentwicklung zentrale Werte und Prinzipien für die agile Entwicklung von Software formulierten. [12], [13]

Bei der agilen Softwareentwicklung steht der Wert funktionierender Software über dem einer umfassenden Dokumentation. Die Zusammenarbeit mit dem Kunden wird über die starren und vorab komplett ausformulierten Vertragsbedingungen gestellt. Ebenso wird die Fähigkeit zur Anpassung über das strikte Festhalten an festgelegten Projektplänen priorisiert. Im Zentrum steht hier die kontinuierliche Auslieferung von lauffähiger Software sowie die enge Kommunikation und Abstimmung mit dem Kunden im kompletten Verlauf des Entwicklungsprozesses. [13]

Im Unterschied zum Wasserfallmodell, welches wie beschrieben auf Vollständigkeit und lineare Abläufe setzt, versteht sich die agile Softwareentwicklung als eine Antwort auf die Schnelllebigkeit und Unvorhersehbarkeit von Softwareprojekten. Agile Methoden ermöglichen es, iterativ und inkrementell zu arbeiten. Anforderungen an die Software werden in kleinen Zyklen umgesetzt und regelmäßig mit den jeweiligen Stakeholdern abgestimmt. Auf diese Weise werden Fehler oder Missverständnisse früh erkannt und Anpassungen können ohne großen Aufwand und vor allem schnell im laufenden Projekt umgesetzt werden. [12], [13]

Die diversen seither entstandenen Agile Methoden wie Scrum, Kanban oder Extreme Programming sind dabei nicht als starres Regelwerk, sondern vielmehr als Rahmen zu verstehen. Entwicklungsteams können die Methoden nutzen, um ihre Zusammenarbeit selbstständig zu organisieren und an neue Vorgänge anzupassen. Jede der agilen Methoden legt besonderen Wert auf die Kommunikation, Flexibilität, Verantwortung und die aktive Mitarbeit der Entwickler, aber auch der weiteren Stakeholder. [12]

2.1.1.3 DevOps

DevOps ist ein integrativer Ansatz der modernen Softwareentwicklung, der darauf abzielt, die Entwicklung und Betrieb von Software innerhalb eines Zykluses, wie in Abbildung 2.2 dargestellt, zu verschmelzen, um eine nachhaltig schnellere, zuverlässigere und kontinuierliche Softwarebereitstellung zu ermöglichen [15]. Der Begriff leitet sich aus der Begrifflichkeiten des „Development“ und der „Operations“ ab und verdeutlicht, dass bei der Arbeitsmethode enge Kooperation, kontinuierliche Iteration und Automatisierung zentrale Rollen spielen [16]. Erweiterungen wie die DevSecOps Praktiken, welche in 2.1.2 näher beschrieben werden, zeigen, dass auch zusätzliche spezifischere Aspekte wie Sicherheit in die Methodik integriert und innerhalb des kontinuierlichen Entwicklungsprozesses genutzt werden können [16].

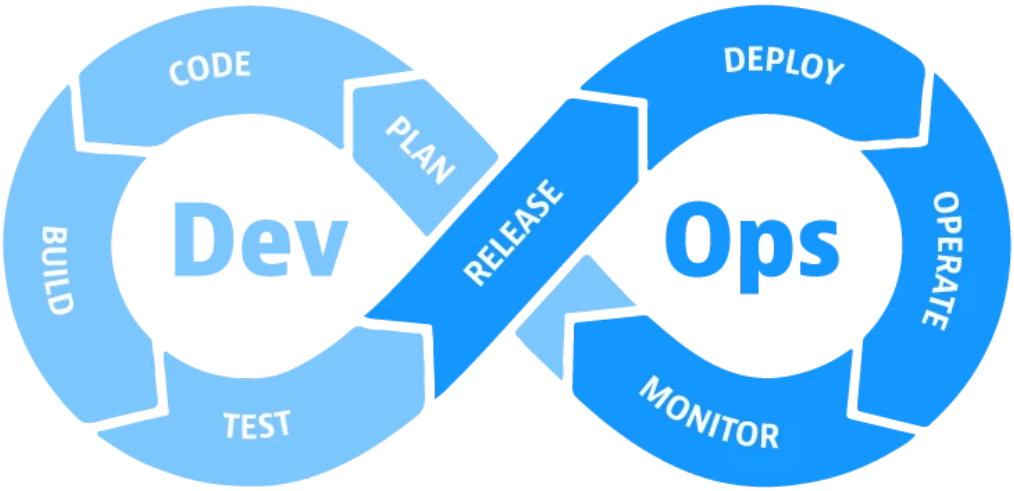


Abbildung 2.2: *Darstellung eines DevOps Zyklus*

Zielsetzung und Motivation Das Ziel der DevOps Methodik liegt in der Optimierung und Verzahnung der Zusammenarbeit zwischen unterschiedlichen Bereichen eines Unternehmens oder einer Organisation. Traditionelle Organisationen arbeiten im Bereich der Entwicklung von Software und der Bereitstellung für deren Anwender häufig in isolierten Silos, deren Prozesse schwerfällig und wenig flexibel sind. DevOps adressiert diese Herausforderung durch interdisziplinäre Teams, die sich gemeinsam um die für einen Projekterfolg notwendigen Aufgaben kümmern, Verantwortung teilen und den Anwender- bzw. Kundennutzen maximieren [17]. Das Ziel ist, die Geschwindigkeit und Stabilität der Softwareauslieferung zu erhöhen, Risiken zu reduzieren und kontinuierliche Verbesserungen im gesamten Entwicklungszyklus zu ermöglichen [15].

Grundprinzipien von DevOps Das Kernkonzept von DevOps lässt sich durch die Säulen Culture, Automation, Measurement, Sharing (CAMS) sowie ergänzend Lean und Added Value (CALMAS) beschreiben [17]:

Culture (Kultur):
Eine Kultur der Zusammenarbeit ist für den Projekterfolg entscheidend. Entscheidungen sollten subsidiär getroffen und die entsprechende Verantwortung für die Entscheidung auf die Ebene delegiert werden, die am besten für die Aufgabenerfüllung geeignet ist. Kulturwandel wird im Optimalfall durch das Vorleben durch das Management und die Stärkung bereits funktionierender Einheiten gefördert. [17]

Automation (Automatisierung):
Software-Pipelines die zwischen einzelnen Arbeitsschritten automatisiert ablaufen erleichtern die Umsetzung und beschleunigen die Bereitstellung von Software. Automatisierung reduziert so die Anzahl der notwendigen manuellen Arbeitsschritte und fördert die flexible Zusammenarbeit zwischen Entwicklung und Betrieb. [17], [16]

Lean:
Lean-Prinzipien, wie Work-in-Progress-Limits, Visualisierung von Arbeit wie z.B. Scrum-Boards und Eliminierung nicht-wertschöpfender Aktivitäten, werden auf Softwareentwicklungsprozesse sowie die Bereitstellungsschritte von Softwareprojekten adaptiert. [17]

Measurement (Messung):
DevOps stützt sich ebenfalls auf Kennzahlen auch Key Performance Indicators (KPI) gennant, die sowohl technische Aspekte wie z.B. Verfügbarkeit und Fehlerbehebungszeiten als auch geschäftlichen Nutzen abbilden, um den Teammitgliedern fundierte Entscheidungen zu ermöglichen. [17]

Added Value (Mehrwert):
DevOps betrachtet ebenfalls die Schaffung eines messbaren Mehrwerts, etwa durch eine schnellere Softwareauslieferung, die verkürzte Reaktionszeiten auf Fehler oder eine sich durch Verbesserungen und Features ergebende höhere Kundenzufriedenheit. [17]

Sharing (Teilen):
Ein besonders wichtiger Aspekt von DevOps ist der Wissensaustausch innerhalb und zwischen den verschiedenen Teams. Der Wissensaustausch muss in einer in einer blame-free culture erfolgen, da das Teilen von Fehlern das Lernen aus Erfahrungen (positiven sowie negativen) eine kontinuierliche Verbesserung der Arbeitsleistung der Teams fördert. [17]

Kontinuierliche Integration, kontinuierliches Deployment und Verbesserung:
Zentrale Elemente von DevOps sind die kontinuierliche Integration im Fachterminus

Continuous Integration (CI) genannt und das kontinuierliche Deployment genannt Continous Deployment(CD). Diese verzahnen Entwicklung, Test und Deployment eng miteinander, indem sie die jeweiligen Arbeitsergebnisse zentral zusammenführen und stetig neue Versionen der Software veröffentlichen. So ermöglichen sie schnelle, funktionsfähige und iterative Releases. Die kontinuierliche Verbesserung (Continuous Improvement) stellt sicher, dass Feedback aus allen Phasen der Entwicklung und der Bereitstellung genutzt wird, um Prozesse zu optimieren und Best Practices zu implementieren. [15], [16]

Abgrenzung zu anderen Konzepten
DevOps stellt kein standardisiertes Framework wie ITIL oder Scrum dar und ist nicht als reines Automatisierungstool zu verstehen [17]. Ebenso ersetzt es die in der jeweiligen Organisation etablierten Vorgehensmodelle nicht grundsätzlich, sondern transformiert sie zu einem übergreifenden, optimierten Prozess. Wesentlich ist vor allem der Kulturwandel durch die enge Verzahnung von Entwicklung, Betrieb und Business sowie die Förderung einer konstruktiven Zusammenarbeit und des Informationsaustauschs [17].

2.1.2 Sicherheit in der Softwareentwicklung

In der Softwareentwicklung stellt die Sicherheit und deren Integration in die Entwicklungsprozesse sowie den Softwarebetrieb zwar nur einen Teilaspekt in der Erstellung von Softwareprojekten dar. Sie bildet jedoch eine grundlegende Voraussetzung für die Verlässlichkeit und Vertrauenswürdigkeit moderner IT-Systeme und der zugrundeliegenden Software. Unsichere Software kann nicht nur Fehler in den Systemen und für den Nutzer erkennbare technische Qualitätsmängel erzeugen, sondern wie beim in der Einleitung erwähnten Solarwinds-Vorfall auch schwerwiegende technische, wirtschaftliche und gesellschaftliche Schäden verursachen [4]. Ziel sicherer Softwareentwicklung und der Nutzung von Methodiken zur sicheren Softwareentwicklung ist es, Sicherheitsaspekte von Beginn an in den gesamten Entwicklungsprozess zu integrieren, anstatt diese erst im Nachhinein bei bereits in Produktion befindlichen Systemen nachzubessern. Im Folgenden wird das Prinzip der modernen sicheren Softwareentwicklung anhand aktuell verwendeter Methodiken näher erläutert.

2.1.2.1 Sichere Softwareentwicklung im Kontext von DevSecOps

Ein zentrales Paradigma sicherer Softwareentwicklung ist das auf DevOps aufbauende Konzept der Development-Security-Operations (DevSecOps). Das DevSecOps Konzept erweitert den DevOps-Ansatz um die Dimension der Sicherheit. Während DevOps die enge und kontinuierliche Verzahnung von Entwicklung und Betrieb als Arbeitsweise etabliert, werden bei DevSecOps wie die Abbildung 2.3 beispielhaft darstellt aufbauend auf dem DevOps-Zyklus Sicherheitsmechanismen in allen Phasen des Software-

lebenszyklus, oder auch Software Development Lifecycles (SDLC) genannt, integriert. [15]

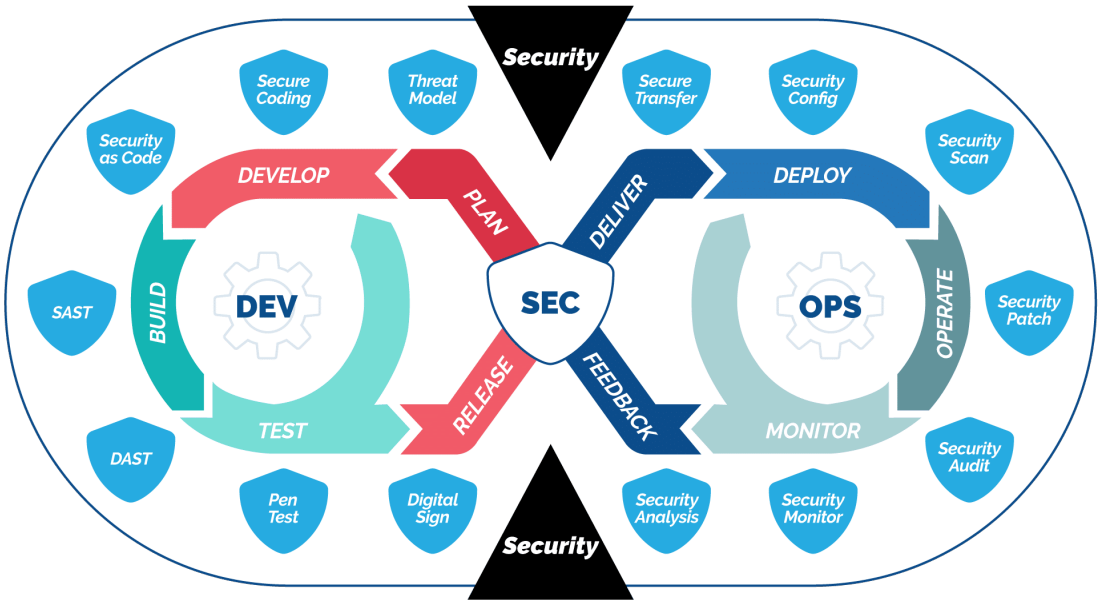


Abbildung 2.3: *Darstellung eines DevSecOps Zyklus mit möglichen Sicherheitsmaßnahmen*

Das Kernprinzip wird als „Shift-Left“ bezeichnet und besagt, dass Sicherheitsprüfungen und Bedrohungsanalysen so früh wie möglich und von da an kontinuierlich in den Entwicklungsprozess integriert werden. Statt Sicherheit erst kurz vor dem Release der Software oder gar danach zu adressieren, erfolgt die Berücksichtigung bereits in der Planungs- und Designphase der Software- und Betriebsarchitektur. Typische Methoden sind etwa das Threat Modeling (z. B. STRIDE) oder die Integration von automatisierten Sicherheitstests wie SAST, DAST oder SCA in die CI/CD Pipelines sowie die kontinuierliche Überwachung der Produktionsumgebungen und der darauf laufenden Software. [18]

Kulturelle und organisatorische Aspekte
Ebenso wie DevOps fordert DevSecOps eine Kultur, in der Sicherheit als gemeinsame Verantwortung wahrgenommen wird. Alle Beteiligten – Entwickler, Sicherheitsteams und Betrieb – tragen gleichermaßen dazu bei, sichere Software zu entwickeln und diese im Anschluss bereitzustellen. Dieser Kulturwandel erfordert Schulungen, offene Kommunikation und den Abbau von bestehenden Silo-Strukturen zwischen Fachbereichen. [19]

Automatisierung und Tooling
Ein wesentliches Charakteristikum von DevSecOps ist die Automatisierung von Sicherheitstests in der CI/CD-Pipeline. Tools für Secret-Scanning, Infrastructure-as-Code (IaC)-Prüfungen oder Container-Security-Scans stellen sicher, dass kontinuierlich auf

Schwachstellen geprüft und diese schnellstmöglich adressiert werden, ohne den Entwicklungsfluss zu verlangsamen. Dies ermöglicht es, den Widerspruch zwischen schnellem Time-to-Market und hohem Sicherheitsniveau aufzulösen und verbessert gleichzeitig die Qualität der ausgelieferten Software. [18]

2.1.2.2 Einordnung in bestehende Frameworks

Während DevSecOps vor allem die technische und kulturelle Umsetzung adressiert, existieren etablierte Frameworks, die ergänzend eine strukturierte Vorgehensweise für sichere Softwareentwicklung bereitstellen.

NIST Secure Software Development Framework (SSDF)
Das NIST SSDF (SP 800-218) bietet eine Sammlung bewährter Praktiken, die Organisationen bei der Integration von Sicherheit in den Entwicklungsprozess unterstützen. Es ist technologieunabhängig und beschreibt Maßnahmen wie:

- Etablierung organisatorischer Richtlinien und Standards,
- Integration von Sicherheitsanforderungen in jede Entwicklungsphase,
- kontinuierliches Testen und Validieren der Sicherheit,
- Monitoring und schnelle Reaktion auf Sicherheitsvorfälle.

Das SSDF ist vor allem in den USA als Referenzrahmen für staatliche Softwareprojekte etabliert und wird zunehmend auch international berücksichtigt. [20]

Secure Development Lifecycle (SDL)
Der von Microsoft entwickelte SDL stellt eine praxisnahe Ergänzung zu DevSecOps dar. Er beschreibt konkrete Schritte, um Sicherheit systematisch in den Softwarelebenszyklus zu integrieren. Dazu gehören u. a.:

1. Bedrohungsmodellierung bereits in der Designphase,
2. Festlegung kryptografischer Standards,
3. Sicherung der Software-Lieferkette,
4. verpflichtende Sicherheitstests vor Freigabe.

Der SDL ist seit über 20 Jahren in Microsoft-Produkten etabliert und gilt als Blaupause für Security by Design [21], [22].

2.2 Schwachstellen / Vulnerabilities

Die NIS2 Richtlinie der EU definiert eine Schwachstelle in Artikel 6 Paragraph 15 folgendermaßen: „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann [23]. Im deutschen Sprachgebrauch ist in der Softwareentwicklung eine Schwachstelle mit einer Sicherheitslücke gleichzusetzen. Im Englischen unterscheidet man hier spezifischer zwischen einer Schwachstelle „Weakness“, einem Fehler in der Software, der die Funktionalität beeinträchtigen kann, die u.a. im Common Weakness Enumeration (CWE) Katalog [24] aufgelistet werden. Sicherheitslücke „Vulnerabilities“, bezeichnet eine Schwachstelle, die durch einen Angreifer ausgenutzt werden kann, welche u.a. im Common Vulnerabilities and Exposures (CVE Katalog [25]) aufgelistet werden.

2.3 Software Bill of Materials (SBOM)

Eine Anforderung innerhalb des CRA ist das Vorhandensein einer Software Bill of Materials (SBOM). Diese wird im folgenden Abschnitt basierend auf dem zweiten Teil der aktuellen Version 2.1 (Veröffentlichung 20.08.2025) der technischen Richtlinie BSI TR-03813 des BSI grundlegend vorgestellt.

2.3.1 Definition und Bestandteile einer SBOM

Eine SBOM ist eine maschinenverarbeitbare Datei, die die Komponenten eines Softwareprodukts sowie deren Beziehungen innerhalb der Lieferkette dokumentiert und in einer einheitlichen Struktur auflistet. Der Begriff „maschinenverarbeitbar“ bedeutet, dass die SBOM automatisch erstellt, ausgelesen, verarbeitet und analysiert werden kann. Auf der Basis der in ihr enthaltenen Daten können die enthaltenen Software-Komponenten und die darauf aufbauenden Abhängigkeiten transparent dargestellt werden. Die SBOM zeichnet sich vor allem dadurch aus, dass sie klar definiert und standardisiert strukturiert ist. [26]

Zweck einer SBOM ist es also, Transparenz über die verwendeten Softwarekomponenten zu schaffen, sowohl für die primäre Komponente – also das eigentliche Softwareprodukt – als auch für externe oder Drittanbieter-Komponenten, die damit verbundenen transitiven Abhängigkeiten und daraus ableitbare mögliche Verwundbarkeiten der Software. Jede SBOM muss bestimmte Mindestinformationen enthalten, um als konform zu gelten, kann aber zusätzlich detaillierte Informationen aufnehmen, solange diese nicht zu Widersprüchen führen. Für jede Version eines Softwareprodukts muss eine eigene SBOM erstellt werden. Wird eine Komponente geändert oder werden Fehler in der

SBOM korrigiert, muss die SBOM aktualisiert und die Versionierung entsprechend angepasst werden. Informationen über mögliche Sicherheitslücken dürfen nicht direkt enthalten sein, da diese im Softwarebereich häufig dynamischer Natur sind und sich über die Zeit ändern, während die SBOM statische und für die jeweilige Version der Software unveränderliche Informationen über die verbauten Softwarekomponenten enthält. [26]

Komponenten und Abstraktionsebenen

- Eine in der SBOM aufgelistete Komponente der Software kann ein einzelnes ausführbares Programm, ein Archiv oder eine logische Einheit sein. Zu den ausführbaren Dateien zählen beispielsweise kompilierte Binärdateien, interpretierte Scripte oder Bibliotheken. Dateien wie Konfigurationsdateien oder Dokumentationen gelten hingegen nicht als ausführbar. [26]
- Ein Archiv fasst mehrere Komponenten zusammen und kann strukturiert oder unstrukturiert sein. Strukturierte Archive (z. B. Container-, ZIP- oder TAR-Dateien) enthalten Metadaten, die die ursprünglichen Komponenten erkennbar machen. Unstrukturierte Archive wie Firmware-Images oder statisch verlinkte Binärdateien erlauben dies hingegen nicht. Selbstextrahierende Archive sind zugleich ausführbar, archiviert und strukturiert. [26]
- Logische Komponenten dienen als Abstraktionsebene, um mehrere Dateien zu einem Produkt zu bündeln und Referenzen zu anderen SBOMs zu ermöglichen. Beispiele sind Betriebssysteme oder Anwendungen. [26]
- Externe Komponenten stammen von einem anderen Ersteller als die primäre Komponente.[26]
- Referenzierte Komponenten werden in einer anderen SBOM beschrieben und in der eigenen SBOM lediglich durch Name, Version und Ersteller sowie die Referenz zur ursprünglichen SBOM angegeben. Im Fall von Widersprüchen gelten die Angaben der referenzierten SBOM. [26]
- Identifizierte Komponenten müssen nicht vollständig beschrieben sein; es genügen Name, Version, Ersteller und eindeutige Kennungen. [26]

Abhängigkeiten
Eine Abhängigkeit beschreibt die gerichtete Beziehung einer Komponente zu einer anderen. Dabei wird nicht unterschieden, ob die Abhängigkeit technisch enthalten, statisch verlinkt oder dynamisch eingebunden ist. Für jede Abhängigkeit existiert ein Pfad von der primären zur abhängigen Komponente, der die Kette der beteiligten Komponenten eindeutig darstellt.[26]

Lizenzinformationen
SBOMs enthalten Informationen zu Lizenzen der Komponenten, um die rechtliche Nutzung zu klären:

- **Originallizenz:** vom Ersteller der Komponente vergeben. [26]
- **Distributionslizenz:** Lizenz, unter der eine Komponente weitergegeben werden darf. [26]
- **Effektive Lizenz:** Lizenz, unter der die Komponente tatsächlich vom SBOM-Ersteller genutzt wird. [26]

Diese Unterscheidung ist insbesondere dann relevant, wenn verschiedene Lizenzoptionen bestehen oder unterschiedliche Lizenzinformationen entlang der Lieferkette vorliegen. [26]

Rollen innerhalb einer SBOM

Die SBOM unterscheidet zwischen Creator (Ersteller der Komponente) und Vendor/Supplier (Anbieter der Software). Der Creator entwickelt die Software, während der Vendor sie bereitstellt, unabhängig davon, ob er sie selbst erstellt hat. [26]

Zusätzliche Aspekte
Idealerweise sollten SBOMs digital signiert sein, um die Authentizität der enthaltenen Informationen zu gewährleisten. Referenzen auf externe SBOMs müssen vom Ersteller so bereitgestellt werden, dass sie dieselben Informationen enthalten, als wären sie vollständig in der eigenen SBOM integriert. Da SBOMs statisch sind, enthalten sie keine direkten Informationen zu Schwachstellen. Diese sollen über separate Formate wie das Common Security Advisory Framework (CSAF)/ Vulnerability Exploitability eXchange (VEX) verteilt werden. [26] CSAF & VEX sind spezielle maschinenlesbare Austauschformate für Schwachstellen, die den Austausch von Informationen über die Ausnutzbarkeit bestimmter Schwachstellen und deren entsprechende Priorisierung stark vereinfachen und beschleunigen sollen. [27], [28]

2.4 Vorstellung des regulatorischen Rahmenwerkes: Cyber Resilience Act

Mit dem CRA hat die Europäische Union erstmals einen einheitlichen Rechtsrahmen geschaffen, der grundlegende Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen festlegt. Ziel dieser Verordnung ist es, das insgesamt niedrige Sicherheitsniveau der vernetzten Produkte zu erhöhen und somit sowohl Verbraucher als auch Unternehmen besser vor den Folgen von Schwachstellen und Sicherheitsvorfällen zu schützen. Hier fehlt bisher ein horizontaler Rechtsrahmen, was einen Flickenteppich aus nationalen und sektorspezifischen Regelungen zur Folge hat und zu Rechtsunsicherheit sowie einer unnötigen Belastungen für Hersteller führt. [2]

Der Begriff „Produkt mit digitalen Elementen" umfasst in der Definition des CRA sowohl Hardware- als auch Softwareprodukte, die mit anderen Geräten oder Netzwerken wie dem Internet verbunden werden können. Zu diesen Produkten zählen alltägliche Konsumgüter wie Smartphones, Laptops oder Smart-Home-Geräte ebenso wie industrielle Systeme und sicherheitskritische Produkte wie Firewalls oder Passwort-Manager sowie reine Softwareprodukte, die nicht als SaaS Anwendung an Kunden ausgeliefert werden. Von den Anforderungen ausgenommen sind lediglich nicht-kommerzielle Open-Source-Software und bereits regulierte Softwareprodukte. [10],[2]

Das Ziel des CRA besteht darin, die Entwicklung sicherer Produkte nach den Prinzipien „Secure by Design" und „Secure by Default" zu fördern. Dazu müssen Hersteller über den gesamten Lebenszyklus hinweg eine systematische Risikobewertung vornehmen, ein Schwachstellenmanagement betreiben, Sicherheitsupdates bereitstellen und die Angriffsfläche ihrer Produkte durch geeignete Maßnahmen wie Verschlüsselung oder sichere Konfigurationen minimieren. [29], [10]

Einer der zentralen Bestandteile des CRA ist die Verpflichtung für Hersteller und Vertreiber von Produkten mit digitalen Elementen, eine Konformitätserklärung vorzulegen. Diese muss den Nachweis erbringen, dass die Produkte die grundsätzlich für alle Hersteller digitaler Produkte geltenden Anforderungen des CRA erfüllen. Ebenso verpflichtet der CRA Hersteller zur Meldung von aktiv ausgenutzten Schwachstellen und schwerwiegenden Sicherheitsvorfällen an eine zentrale europäische Plattform wie die etwa die Schwachstellendatenbank der European Union Agency for Cybersecurity (ENISA) sowie zur Unterstützung der Nutzer durch Bereitstellung von Sicherheitsupdates während eines definierten Supportzeitraums. Für die meisten Produktkategorien erfolgt dies durch eine Selbsterklärung des Herstellers. Für besonders kritische Produkte, die in 2.4.2 aufgeführt sind, wird durch den CRA jedoch eine Prüfung durch externe Stellen auf deren Konformität notwendig. Die Produkte erhalten im Anschluss auf die Selbsterklärung oder die Prüfung als sichtbares Zeichen für die Einhaltung dieser Anforderungen die CE-Kennzeichnung, die nun auch Cybersicherheitsaspekte umfasst. [10], [29]

2.4.1 Zielsetzung des Rahmenwerkes

Mit dem CRA verfolgt die EU das Ziel, sowohl den Schutz der Gesellschaft vor den Folgen von Cyberangriffen zu verbessern als auch die Wettbewerbsfähigkeit des Binnenmarkts zu stärken. Die Dringlichkeit einer Verordnung wie des CRA ergibt sich aus der zunehmenden Häufigkeit und Intensität von Cyberangriffen auf Hardware- und Softwareprodukte. Cyberangriffe stellen laut BSI und EU eine erhebliche Bedrohung für Wirtschaft und Gesellschaft und sogar das demokratische Zusammenleben dar. Schätzungen der EU zufolge beliefen sich die jährlichen Kosten der Cyberkriminalität bereits im Jahr 2021 auf 5,5 Billionen Euro. Die bestehenden Herausforderungen resultieren insbesondere aus zwei zentralen Problembereichen [2], [1]:

1. Viele der aktuell in der EU entwickelten und vertriebenen Produkte mit digitalen Elementen weisen ein unzureichendes Cybersicherheitsniveau auf. Dies zeigt sich in verbreiteten Schwachstellen und einer inkonsistenten Bereitstellung von Sicherheitsaktualisierungen.
2. Den Nutzern dieser digitalen Produkte fehlt es an Transparenz und Information bezüglich der Sicherheit der Produkte, wodurch sie weder fundierte Entscheidungen treffen noch Sicherheitsmaßnahmen angemessen umsetzen können.

Sicherheitsvorfälle können, vor allem im Bereich der vom CRA als kritisch definierten Produkte 2.4.2, in einem vernetzten digitalen Umfeld und Infrastruktur binnen kürzester Zeit grenzüberschreitende Auswirkungen entfalten, Lieferketten unterbrechen und kritische Infrastrukturen gefährden. Vor diesem Hintergrund verfolgt die vorgeschlagene EU-Verordnung zwei übergeordnete Zielsetzungen [2]:

1. Es sollen Rahmenbedingungen geschaffen werden, die eine Entwicklung sicherer Produkte mit digitalen Elementen gewährleisten, sodass Hersteller bereits in der Konzeptions- und Entwicklungsphase Sicherheitsaspekte berücksichtigen und über den gesamten Lebenszyklus hinweg angemessene Schutzmaßnahmen implementieren.
2. Die Transparenz in Bezug auf die Sicherheitsmerkmale digitaler Produkte soll erhöht werden, um Unternehmen und Verbraucher in die Lage zu versetzen, informierte Entscheidungen hinsichtlich der Cybersicherheit zu treffen.

Durch die Harmonisierung der Anforderungen werden gleiche Bedingungen für alle Marktteilnehmer geschaffen, was insbesondere kleinen und mittleren Unternehmen den Zugang zum europäischen Markt erleichtert [2].

Um diese übergeordneten Ziele zu erreichen, definiert die Verordnung vier spezifische Maßnahmen [2]:

1. Die Verankerung von Cybersicherheitsanforderungen über den gesamten Lebenszyklus eines Produkts hinweg,
2. Die Schaffung eines kohärenten regulatorischen Rahmens zur Vereinfachung der Einhaltung von Cybersicherheitsvorgaben durch Hersteller,
3. Die Verbesserung der Transparenz hinsichtlich der Sicherheitsmerkmale von Produkten mit digitalen Elementen sowie
4. Die Befähigung von Unternehmen und Verbrauchern zur sicheren Nutzung dieser Produkte.

Da Cyberbedrohungen nicht an nationalstaatliche Grenzen gebunden sind aber durch die nationalstaatlichen Gesetzgebungen die Gefahr einer Fragmentierung durch unterschiedliche nationale Vorschriften besteht, ist eine einheitliche Regulierung auf EU-Ebene erforderlich. Eine uneinheitliche Gesetzgebung innerhalb der Mitgliedstaaten könnte den

EU-Binnenmarkt erheblich durch die notwendigen Einzelprüfungen der Produkte stark beeinträchtigen. Diese Prüfungen können den zügigen Warenaustausch behindern und somit die Wettbewerbsfähigkeit europäischer Unternehmen stark schwächen. Ein harmonisierter Rechtsrahmen mit horizontal konzipierten und weitgehend allgemeingültigen Sicherheitsanforderungen soll daher die Cybersicherheit innerhalb der Europäischen Union stärken, das Vertrauen in digitale Produkte aus der EU erhöhen und gleiche Wettbewerbsbedingungen für alle in der EU vertretenen Anbieter schaffen. Die Notwendigkeit eines solchen abgestimmten Vorgehens wird zudem durch gesellschaftspolitische Forderungen bekräftigt, wie sie unter anderem im Abschlussbericht der Konferenz zur Zukunft Europas formuliert worden ist. [2]

Da bisherige Regulierungen Lücken in Bezug auf die spezifischen Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen oder nicht eingebetteter Software aufgewiesen haben. Ergänzt der CRA unter anderem die folgenden bestehenden horizontal ausgerichteten EU-Rechtsvorschriften [2]:

- Richtlinie über Angriffe auf Informationssysteme (2013/40/EU),
- NIS-Direktive (2016/1148),
- NIS2-Direktive (2022/2555),
- EU-Rechtsakt zur Cybersicherheit (2019/881),
- Delegierte Verordnung (EU) 2022/30.

Beim CRA handelt es sich um eine vom Europäischen Parlament und Europäischen Rat verabschiedete Verordnung, die am 11. Dezember 2024 in Kraft getreten ist. Die Anforderungen des CRA müssen ab dem Stichtag 11.Dezember 2027 eingehalten werden (siehe Abbildung 2.4).

Die Zielgruppe des Rahmenwerks, die die Anforderungen des CRA umsetzen müssen, besteht aus folgenden Akteuren [2]:

- **Hersteller von Produkten mit digitalen Elementen**:
  Verantwortlich für die Cybersicherheit von Produkten während der Konzeption, Entwicklung und des gesamten Lebenszyklus.
- **Einführer und Händler**:
  Verpflichtet, sicherzustellen, dass Produkte, die in Verkehr gebracht werden, den Anforderungen entsprechen.

2.4.2 Kategorisierung der kritischen Produkte mit digitalen Elementen

Die im CRA aufgeführten kritischen Produkte mit digitalen Komponenten werden in zwei Klassen unterteilt. Die Unterteilung wird im Anhang 3 des CRA aufgelistet und ist wie folgt aufgebaut [30]:

Abbildung 2.4: *CRA Einführungszeitplan [10]*

Klasse I

1. Software für Identitätsmanagementsysteme und Software für die Verwaltung des privilegierten Zugangs;
2. eigenständige und eingebettete Browser;
3. Passwort-Manager;
4. Software für die Suche, Entfernung und Quarantäne von Schadsoftware;
5. Produkte mit digitalen Elementen mit der Funktion eines virtuellen privaten Netzes (VPN);
6. Netzmanagementsysteme;
7. Instrumente für die Netzkonfigurationsverwaltung;
8. Systeme für die überwachung des Netzverkehrs;
9. Verwaltung der Netzressourcen;
10. Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM);
11. Aktualisierungs- und Patchverwaltung, einschließlich Bootmanager;
12. Systeme für die Anwendungskonfigurationsverwaltung;
13. Software für Fernzugriff und gemeinsame Datennutzung;
14. Software für die Mobilgeräteverwaltung;

15. physische Netzschnittstellen;
16. Betriebssysteme, die nicht zur Klasse II gehören;
17. Firewalls, Angriffserkennungs- und/oder -präventionssysteme, die nicht zur Klasse II gehören;
18. Router, Modems für die Internetanbindung und Switches, die nicht zur Klasse II gehören;
19. Mikroprozessoren, die nicht zur Klasse II gehören;
20. Mikrocontroller;
21. anwendungsspezifische integrierte Schaltungen (ASIC) und Field Programmable Gate Array (FPGA), die zur Verwendung durch wesentliche Einrichtungen der in [Anhang I der Richtlinie NIS2] genannten Art bestimmt sind;
22. industrielle Automatisierungs- und Steuerungssysteme (IACs), die nicht zur Klasse II gehören, wie z. B. speicherprogrammierbare Steuerungen (PLC), verteilte Steuerungssysteme (DCS), computergestützte numerische Steuerungen für Werkzeugmaschinen (CNC) und Prozesssteuerungs- und Datenerfassungssysteme (SCADA);
23. industrielles Internet der Dinge (IIoT), das nicht zur Klasse II gehört.

Klasse II

1. Betriebssysteme für Server, Desktops und Mobilgeräte;
2. Hypervisoren und Container-Runtime-Systeme, die eine virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen;
3. Public-Key-Infrastrukturen und Aussteller digitaler Zertifikate;
4. Firewalls, Angriffserkennungs- und/oder -präventionssysteme für den industriellen Einsatz;
5. Allzweck-Mikroprozessoren;
6. Mikroprozessoren, die für die Integration in speicherprogrammierbare Steuerungen (PLC) und Sicherheitselemente bestimmt sind;
7. Router, Modems für die Internetanbindung und Switches für den industriellen Einsatz;
8. Sicherheitselemente;
9. Hardware-Sicherheitsmodule (HSM);
10. sichere Kryptoprozessoren;
11. Chipkarten, Chipkartenleser und Token;

12. industrielle Automatisierungs- und Steuerungssysteme (IACS), die zur Verwendung durch wesentliche Einrichtungen der in [Anhang I der Richtlinie NIS2] genannten Art bestimmt sind, wie z. B. speicherprogrammierbare Steuerungen (PLC), verteilte Steuerungssysteme (DCS), computergestützte numerische Steuerungen für Werkzeugmaschinen (CNC) und Prozesssteuerungs- und Datenerfassungssysteme (SCADA);
13. Geräte für das industrielle Internet der Dinge (IIoT), die zur Verwendung durch wesentliche Einrichtungen der in [Anhang I der Richtlinie NIS2] genannten Art bestimmt sind;
14. Sensor- und Aktuatorkomponenten von Robotern und Robotersteuerungen;
15. intelligente Zähler.

2.5 Analyse der Anforderungen des Cyber Resilience Act im Bezug auf die Softwareentwicklung

2.5.1 Für die Softwareentwicklung relevante Anforderungen

Die Anforderungen für die Softwareentwicklung können dem Anhang 1 des CRA entnommen werden [30]:

Kapitel 1: Sicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

1. Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten;
2. Produkte mit digitalen Elementen werden ohne bekannte ausnutzbare Schwachstellen ausgeliefert;
3. Auf der Grundlage der Risikobewertung gemäß Artikel 10 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend:
    - a) mit einer sicheren Standardkonfiguration ausgeliefert werden und ermöglichen, das Produkt in seinen ursprünglichen Zustand zurückzusetzen,
    - b) durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme,
    - c) die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z. B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen,

- d) die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung schützen sowie deren Beschädigung melden,
- e) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und relevant sind, und auf das für die bestimmungsgemäße Verwendung des Produkts erforderliche Maß beschränken („Datenminimierung“),
- f) die Verfügbarkeit wesentlicher Funktionen, einschließlich der Abwehrfähigkeit gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe) und deren Eindämmung gewährleisten,
- g) ihre eigenen negativen Auswirkungen auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste minimieren,
- h) so konzipiert, entwickelt und hergestellt werden, dass sie – auch bei externen Schnittstellen – möglichst geringe Angriffsflächen bieten,
- i) so konzipiert, entwickelt und hergestellt werden, dass die Auswirkungen eines Vorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden,
- j) sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen,
- k) sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Aktualisierungen und die Benachrichtigung der Nutzer über verfügbare Aktualisierungen.

Kapitel 2: Anforderungen an die Behandlung von Schwachstellen

1. Die Hersteller der Produkte mit digitalen Elementen müssen Schwachstellen und Komponenten des Produkts ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten des Produkts hervorgehen;
2. Im Hinblick auf die Risiken im Kontext der Produkte mit digitalen Elementen unverzüglich Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen;
3. Die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam testen und überprüfen;
4. Sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Elementen, die Auswirkungen der Schwachstellen und ihre Schwere

erkennen können, sowie Informationen, die den Nutzern helfen, die Schwachstellen zu beheben;

5. Eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen;
6. Maßnahmen ergreifen, um den Austausch von Informationen über mögliche Schwachstellen in ihrem Produkt mit digitalen Elementen und darin enthaltenen Komponenten Dritter zu erleichtern, und dazu u. a. eine Kontaktadresse für die Meldung der in dem Produkt mit digitalen Elementen entdeckten Schwachstellen angeben;
7. Mechanismen für die sichere Verbreitung von Aktualisierungen für Produkte mit digitalen Elementen bereitstellen, damit ausnutzbare Schwachstellen rechtzeitig behoben oder eingedämmt werden;
8. Dafür sorgen, dass Sicherheits-Patches oder -Aktualisierungen, die zur Bewältigung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich und kostenlos verbreitet werden, zusammen mit Hinweisen und einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.

3 Methodik

Zur Beantwortung der Forschungsfragen wird eine Mixed Methods Methodik eingesetzt, da es sich um eine vergleichsweise unerforschte Thematik handelt. Das methodische Vorgehen wird im Folgenden näher erläutert.

3.1 Methodisches Vorgehen

Zur Beantwortung der in dieser Arbeit formulierten Forschungsfragen wird ein Mixed Methods Ansatz gewählt, bei dem quantitative und qualitative Verfahren in einem sequenziellen Design miteinander kombiniert werden. Dieses Vorgehen ist deshalb sinnvoll, da die Verordnung zum Cyber Resilience Act (CRA) bisher weder in der Forschung noch in der industriellen Praxis umfassend behandelt wurde. Aus diesem Grund ist eine explorative Erhebung notwendig. Ergänzend müssen die Ergebnisse aber auch mit aktuellen Best-Practice-Empfehlungen verglichen werden.

3.1.1 Quantitative Datenerhebung mittels Fragebogen

Zur Erhebung relevanter Daten im Rahmen der quantitativen Umfrage, im eingebetteten Design, da auch offene Fragen vorhanden sein sollen, mit einer Zielgröße der befragten Gruppe von ca. 50 Teilnehmern. Primäre Zielgruppe der befragten Personen sind Softwareentwickler und Leiter von Softwareentwicklungsabteilungen sowie Produktverantwortliche.

Der Fragebogen wird inhaltlich entlang der ersten beiden Forschungsfragen konzipiert:

- **Forschungsfrage 1**: Der Fragebogen erfasst den Vorbereitungsgrad der Softwareentwicklungsabteilungen auf die Anforderungen des CRA. Dazu werden Fragen zu organisatorischen Prozessen, vorhandenen Compliance-Strukturen sowie bereits implementierten technischen Maßnahmen formuliert.
- **Forschungsfrage 2**: Der Fragebogen erhebt den Kenntnisstand der Befragten über die für sie relevanten Vorschriften im Sinne einer Compliance Awareness. Hierbei werden sowohl Fragen zum allgemeinen Wissen als auch zur persönlichen Einschätzung der eigenen Verantwortlichkeiten integriert.

Die Umfrage an sich wird auf Basis der ersten Sondierungen mit möglichen Umfrageteilnehmern, die im Vorfeld der Exposé-Erstellung befragt wurden, anonym stattfinden. Dies geschieht aus dem Grund, dass die mögliche Offenlegung von Sicherheitsmechanismen bzw. deren Nichtvorhandensein, ein Sicherheitsrisiko in den Augen der Befragten darstellen und somit zu einer geringeren Teilnahmebereitschaft führen kann. Es sollen lediglich (optionale) Angaben zur Position und der Branche abgefragt werden, um auch hier mögliche Trends erkennen zu können. Die Auswertung erfolgt mittels deskriptiver und, sofern sinnvoll, inferenzstatistischer Verfahren. Als wissenschaftliche Grundlage wird sich an Empfehlungen zur Umfrageforschung in der Softwaretechnik als Strategie zur Erhöhung der Validität und Reliabilität orientiert. [31], [32]

3.1.2 Qualitative Analyse und Ableitung von Maßnahmen

Im zweiten Schritt werden die quantitativen Ergebnisse qualitativ ausgewertet und in den Kontext aktueller Best-Practices und Handlungsempfehlungen der Softwareentwicklung gestellt. Dieser Teil richtet sich primär an Forschungsfrage 3, die auf die Entwicklung von Maßnahmen zur Schließung identifizierter Lücken abzielt.

Die Analyse folgt dabei drei Schritten:

1. Die im Fragebogen erhobenen Defizite und Herausforderungen werden innerhalb der Einordnung der Ergebnisse in den Forschungskontext 5.1 systematisch identifiziert.
2. Diese Ergebnisse werden mit einschlägigen Best-Practices, regulatorischen Vorgaben sowie technischen Richtlinien (z. B. des BSI) abgeglichen.
3. Auf dieser Grundlage werden konkrete Maßnahmenvorschläge entwickelt, die Unternehmen als Orientierung dienen können, um bestehende Anforderungen des CRA umzusetzen.

Durch diese Kombination quantitativer und qualitativer Methoden soll sichergestellt werden, dass die Untersuchung nicht nur eine Bestandsaufnahme liefert, sondern auch als Ergebnis der Arbeit praxisnahe Handlungsempfehlungen. Das methodische Vorgehen soll damit sowohl zur explorativen Grundlagenforschung in einem noch jungen Themenfeld beitragen als auch zur praktischen Unterstützung von Softwareentwicklungsabteilungen und softwareentwickelnden Organisationen dienen, die mit der Implementierung des CRA konfrontiert sind.

3.2 Literaturrecherche

Zunächst erfolgt eine qualitative Analyse des regulatorischen Dokumentes (CRA) auf dessen Anforderungen an die Softwareentwicklung in 2.4 sowie wissenschaftlicher Literatur und spezifischer Fachartikel, um die spezifischen Sicherheitsanforderungen des

CRA zu erfassen. Ebenso werden entsprechend den Anforderungen mögliche Herangehensweisen auf Basis etablierter Best-Practices zur Erfüllung der Anforderungen recherchiert.

3.3 Datenerhebung

Die Datenerhebung erfolgte wie in 3.1.1 durch den Einsatz eines standardisierten Fragebogens, dessen Aufbau und Inhalte in Kapitel 3.4 detailliert dargestellt werden. Die Wahl dieses Erhebungsinstruments basiert auf der Möglichkeit, innerhalb kurzer Zeit eine größere Anzahl an Personen befragen zu können und damit den quantitativen Teil des Mixed-Methods-Designs ausreichend zu erfüllen.

Die Rekrutierung der Teilnehmenden erfolgte über verschiedene Kanäle, um eine möglichst breite und diversifizierte Stichprobe sicherzustellen. Dazu zählten digitale Plattformen wie themenspezifische Discord-Server und direkte Kontaktaufnahmen über LinkedIn. Ergänzend wurde der Fragebogen auf einschlägigen Fachveranstaltungen verbreitet, namentlich dem OSS-Bonn-Event am 12.08.2025 sowie der FrOSCon 20 am 16. und 17.08.2025. Darüber hinaus fand eine Verteilung im erweiterten fachlichen Bekanntenkreis statt. Um potenzielle Verzerrungen der Ergebnisse durch organisationale oder persönliche Nähe zu vermeiden, wurden Personen aus dem unmittelbaren Arbeitsumfeld von der Teilnahme ausgeschlossen.

Angesichts der spezialisierten und zeitlich stark beanspruchten Zielgruppe der Softwareentwickelnden wurde ein Erhebungszeitraum von zwei Monaten (01.07.2025–31.08.2025) festgelegt.

3.4 Instrumentenerstellung - Fragebogen

Für die Erhebung der Daten wurde ein Fragebogen entwickelt, der sowohl quantitative als auch qualitative Informationen erfasst. Zum einen wurden Hintergrundinformationen der Befragungsteilnehmer sowie die von den jeweiligen Organisationen implementierten Sicherheitsmaßnahmen über Multiple-Choice-Fragen (quantitativ) erhoben. Zum anderen wurden offene Fragen mit Freitextfeldern eingesetzt, um vertiefte qualitative Einblicke zu gewinnen. Im Anschluss wurden die einzelnen Fragen sowie die vorgesehenen Antwortoptionen detailliert dargestellt. Falls einzelne Fragen unmittelbar auf Anforderungen des CRA Bezug nehmen, wird in der folgenden Aufzählung eine explizite Zuordnung (Mapping) zu den entsprechenden Passagen des CRA[2] oder dessen Annex [30] vorgenommen.

1. **Haben Sie bereits vom CRA (Cyber Resilience Act gehört)?**
   (Ja/ Nein)

Hintergrund der Frage: Durch diese Frage soll festgestellt werden, wie viele der Umfrageteilnehmer bereits Vorkenntnisse über den CRA besitzen.

2. **Ist der CRA in Ihrer Firma bereits ein Gesprächsthema?**
Haben Sie mitbekommen, dass der CRA von Ihren Kollegen oder dem Management bereits besprochen wurde, oder waren Sie selbst an solchen Gesprächen beteiligt?
(Ja/ Nein/ Ist mir nicht bekannt)

   Hintergrund der Frage: Durch diese Frage soll festgestellt werden, wie viele der Umfrageteilnehmer möglicherweise bereits beruflich mit dem CRA und dessen Anforderungen in Kontakt gekommen sind.

3. **Welche der angegebenen Berufsbezeichnungen trifft auf Sie zu?**
Wählen Sie eine oder mehr Antworten

   - Softwareentwickler:in
   - Softwarearchitekt:in
   - ISB/ ISO
   - CISO
   - Geschäftsführer:in
   - IT-Administrator:in
   - Cybersecurity Berater:in
   - Ich möchte keine Angabe machen
   - Andere (bitte geben Sie an)

   Hintergrund der Frage: Diese Frage soll klären, welchen beruflichen Hintergrund und damit verbundenes mögliches Vorwissen die Umfrageteilnehmer besitzen.

4. **Wie alt sind Sie? (optional)**
Wählen Sie eine Antwort

   - <25
   - 25 - 35
   - 35 - 45
   - 45 - 55
   - 55 - 65
   - >65

   Hintergrund der Frage: Diese Frage soll klären, ob das Alter möglicherweise einen Einfluss auf den Kenntnisstand zum CRA haben kann.

5. **In welcher Branche ist Ihr Unternehmen tätig?**
   Wählen Sie eine Antwort
   - Informationstechnologie
   - Finanzen & Versicherungen
   - Gesundheitswesen
   - Industrie & Produktion
   - Transport & Logistik
   - Energie & Versorgung
   - Bildung & Forschung
   - Öffentlicher Dienst
   - Medien & Kommunikation
   - Beratung & Dienstleistungen
   - Ich möchte keine Angabe machen
   - Andere (bitte geben Sie an)

   Hintergrund der Frage: Diese Frage soll den Arbeitshintergrund der Umfrageteilnehmer im Generellen klären.

6. **Handelt es sich bei Ihrem Unternehmen um kritische Infrastruktur (KRITIS)? (optional)**
   Wählen Sie eine Antwort
   (Ja/ Nein/ Ist mir nicht bekannt)

   Hintergrund der Frage: Diese Frage soll den Hintergrund der Umfrageteilnehmer im Bezug auf das Arbeitsumfeld in der kritischen Infrastruktur aufzeigen.

7. **Ist Ihr Unternehmen von einer dieser Regularien betroffen bzw. muss diese erfüllen? (optional)**
   Wählen Sie eine oder mehr Antworten
   - BSI-Grundschutz
   - NIS-2
   - PCI-DSS
   - HIPAA
   - TISAX
   - C5

- ISO 27001 (ISMS)
- NIST Cybersecurity Framework
- Mir sind keine bekannt
- Mein Unternehmen unterliegt keiner dieser Anforderungen
- Ich möchte hierzu keine Angaben machen
- Andere (bitte geben Sie an)

Hintergrund der Frage: Diese Frage soll es ermöglichen, einen Zusammenhang bereits vorhandener Sicherheitsmaßnahmen oder eines hohen Sicherheitsbewusstseins bei den Teilnehmern auf das Unterliegen diverser Regularien zu mappen.

8. **Ist Softwaresicherheit ein priorisiertes Thema in Ihrem Unternehmen?**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

   Hintergrund der Frage: Durch diese Frage soll geklärt werden, ob die Umfrageteilnehmer in ihrem Arbeitskontext Sicherheit priorisieren sollen. Mapping: CRA Verordnung Paragraphen (1) und (4) [2].

9. **Ist Softwaresicherheit für Sie persönlich ein priorisiertes Thema?**
Wählen Sie eine Antwort
(Ja/ Nein)

   Hintergrund der Frage: Diese Frage soll klären, ob die Umfrageteilnehmer sich auch persönlich für Sicherheitsthemen (in der Softwareentwicklung) interessieren.

10. **Wie hoch schätzen Sie die Relevanz von Softwaresicherheit für Ihre tägliche Arbeit ein?**
Geben Sie an, zu welchem Wert Sie tendieren
Auswahl eines Zahlenwertes zwischen -5 = Nicht relevant & 5 = Sehr relevant

    Hintergrund der Frage: Durch diese Frage soll ermittelt werden, welchen Stellenwert Sicherheit in der täglichen Arbeit der Umfrageteilnehmer im Durchschnitt hat.

11. **Werden Sicherheitsmaßnahmen bei der Konzeption, Entwicklung oder im Betrieb der durch Sie entwickelten Software integriert?**
Bitte auswählen, wo Integration stattfindet. Wählen Sie eine oder mehr Antworten.

    - Konzeption/ Design
    - Entwicklung
    - Im Betrieb

- Sicherheitsmaßnahmen werden nur nach Bedarf integriert
- Sicherheitsmaßnahmen werden nicht integriert
- Ist mir nicht bekannt

Hintergrund der Frage: Diese Frage soll klären, wie häufig Sicherheitsmaßnahmen in der Softwareentwicklung integriert werden. Mapping: CRA Annex 1 Anforderung 1.1. [30].

12. **Findet eine Bedrohungsanalyse der Software statt, um Schwachstellen in der Architektur der Software ausfindig zu machen? Z. B. ein Threat-Modeling mittels STRIDE Methodik.**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

    Hintergrund der Frage: Diese Frage soll klären, ob Security by Design Methoden verwandt werden. Mapping: CRA Artikel 10 (2) und CRA Annex 1 Anforderung 1.3 [30].

13. **Falls ja, wird diese Bedrohungsanalyse regelmäßig während des Lebenszyklus der Software wiederholt? (optional)**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

    Hintergrund der Frage: Diese Frage soll klären, inwieweit die Sicherheitsmaßnahmen in den Unternehmen iterativ angelegt sind (Sicherheitsbedrohungen während des Lebenszyklusses) Mapping: CRA Artikel 10 (2) [2] und CRA Annex 1 Anforderung 1.3 [30].

14. **Wird Software in Ihrem Unternehmen auf bekannte Schwachstellen (CVEs) überprüft? Z. B. durch einen SCA Scan (Software Composition Analysis)**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

    Hintergrund der Frage: Diese Frage soll klären, ob die Unternehmen Schwachstellenscans durchführen, die auf bekannte Schwachstellen testen. Mapping: CRA Annex 1 Anforderung 1.2 & 2.3 [30].

15. **Falls ja, werden diese Scans regelmäßig wiederholt? (optional)**
Wählen Sie eine Antwort

    - Ja, automatisiert
    - Ja, manuell getriggert
    - Ja, bei Produktabnahme

- Nein
- Ist mir nicht bekannt

Hintergrund der Frage: Diese Frage zielt auf die im CRA geforderte Regelmäßigkeit der Sicherheitsüberprüfungen ab. Mapping: CRA Annex 1 Anforderung 1.2 & 2.3 [30].

16. **Welche Sicherheitsmaßnahmen werden noch zur Erhöhung der Sicherheit der durch Ihr Unternehmen gebaute Software durchgeführt? (optional)**
Stichpunkte genügen. Ausführliche Antworten sind ebenfalls willkommen!
Textfeldeingabe (maximal 1.000 Zeichen)

Hintergrund der Frage: Diese qualitative Frage soll den Befragten die Möglichkeit geben, die weiteren durch Ihr Unternehmen in der Entwicklung getroffenen Sicherheitsmaßnahmen über die Schwachstellenscans hinaus zu nennen. Mapping: CRA Annex 1 Anforderung 1.1 [30].

17. **Werden alle ausnutzbaren Schwachstellen geschlossen, bevor die Software an den Kunden/ Nutzer ausgeliefert wird?**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

Hintergrund der Frage: Diese Frage zielt darauf ab, ob die durch den CRA geforderte Freiheit von ausnutzbaren Schwachstellen zum Zeitpunkt der Auslieferung gewährleistet wird. Mapping: CRA Annex 1 Anforderung 1.2 [30].

18. **Wird von der Software eine SBOM (Software-Bill-of-Materials) angefertigt und für Nutzer/ Kunden erreichbar hinterlegt?**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

Hintergrund der Frage: Die Frage soll überprüfen, ob die Organisationen der Befragten bereits jetzt die Anforderungen des CRA hinsichtlich einer SBOM Erstellung nachkommen und diese den Nutzern bereitstellen. Mapping: CRA Annex 1 Anforderung 2.5 & Annex 2 Anforderung 6 [30].

19. **Falls ja, wird diese SBOM für jede ausgelieferte Version der Software erstellt und hinterlegt? (optional)**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

Hintergrund der Frage: Diese Frage hat den Hintergrund zu überprüfen, ob die SBOM für jede Version der Software immer wieder neu erstellt wird, da sich bei Versionsupdates auch die verwendeten Komponenten der Software ändern können. Mapping: CRA Annex 1 Anforderung 2.5 [30].

20. **Wie lange dauert es in der Regel, eine ausnutzbare Schwachstelle oberhalb eines CVE Scores von 7.0 (high) zu beheben?**
Wählen Sie eine Antwort

    - Einen Tag
    - $<$ 3 Tage
    - $<$ 7 Tage
    - $<$ 14 Tage
    - $<$ 30 Tage
    - $>$ 30 Tage
    - Ist mir nicht bekannt
    - Andere (bitte geben Sie an)

    Hintergrund der Frage: Diese Frage zielt darauf ab, zu untersuchen, wie schnell Schwachstellen mit einem hohen Verbundenen Risiko (CVSS Score über 7 = hohes Risiko) durch die Organisationen der Befragten behandelt werden. Mapping: CRA Annex 1 Anforderung 2.2 [30].

21. **Werden Ihre Kunden/ Nutzer direkt über neue Schwachstellen informiert?**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt/ Anderes (bitte geben Sie an)

    Hintergrund der Frage: Diese Frage zielt darauf ab zu erfahren, ob die Information über die gefundenen Schwachstellen auch an die Nutzer der Software weitergeleitet werden. Mapping: CRA Annex 1 Anforderung 2.4 [30].

22. **Falls ja, über welchen Kommunikationskanal? (optional)**
Wählen Sie eine Antwort

    - Mail
    - Telefon
    - Die Software selbst (z. B. per Pop-Up)
    - Messenger
    - Vulnerability Exploitability eXchange (VEX)
    - Andere (bitte geben Sie an)

    Hintergrund der Frage: Diese Frage zielt darauf ab zu erfahren, was die jeweiligen Organisationen der Umfrageteilnehmer als geeigneten Kommunikationskanal zur Schwachstellenoffenlegung betrachten bzw. welchen sie nutzen. Mapping: CRA Annex 1 Anforderung 1.3.k & Annex 1 Anforderung 2.4 [30].

23. **Falls ja, existiert für die Kommunikation der Schwachstelle ein geregelter Prozess? (optional)**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

    Hintergrund der Frage: Diese Frage soll in Erfahrung bringen, ob die Schwachstellenkommunikation einem geregelten Prozess folgt. Mapping: Annex 1 Anforderung 2.5 [30].

24. **Werden durch Ihr Unternehmen Zeitangaben bis zur erwarteten Behebung der Schwachstellen gegenüber den Nutzern/ Kunden angegeben?**
Wählen Sie eine Antwort

    - Ja - genaue Angaben
    - Ja - ungefähre Angaben
    - Nein
    - Ist mir nicht bekannt

    Hintergrund der Frage: Diese Frage zielt darauf ab in Erfahrung zu bringen, inwieweit bereits Zeitangaben zur Schwachstellenbehebung an die Nutzer kommuniziert werden. Mapping: Annex 2 Anforderung 8 [30]

25. **Sollte die Schwachstelle durch den Kunden/ Nutzer selbst behoben werden müssen. Wird eine detaillierte Anleitung/ Dokumentation mitgegeben.**
Wählen Sie eine Antwort
(Ja/ Nein/ Schwachstellen werden nicht durch den Kunden oder Nutzer behoben/Ist mir nicht bekannt)

    Hintergrund der Frage: Die Frage soll klären, ob, wenn machbar, die Schwachstellen durch die Nutzer selbst unter einer Anleitung behoben werden können und ob diese Anleitung durch den Hersteller mitgeliefert wird. Mapping: Annex 2 Anforderung 8 [30]

26. **Werden Schwachstellen in Ihrer Software nach Ihrer Behebung veröffentlicht? Z. B. in der NIST-NVD Database.**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt/ Anderes (bitte geben Sie an)

    Hintergrund der Frage: Diese Frage soll klären, ob Schwachstellen, die in Produkten der Organisation der Umfrageteilnehmer gefunden werden, koordiniert veröffentlicht werden. Dies ist vor insofern wichtig, da die Sicherheitslücken so durch die gängigen Sicherheitsscanner gefunden werden können. Mapping: Annex 1 Anforderung 2.6 [30]

27. **Falls ja, existiert für die Veröffentlichung der Schwachstelle ein geregelter Prozess? (optional)**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

Hintergrund der Frage: Diese Frage soll in Erfahrung bringen, bei wie vielen Organisationen, denen die Umfrageteilnehmer angehören, diese Offenlegung der Schwachstellen bereits ein koordinierter Prozess ist. Mapping: Annex 1 Anforderung 2.5 & 2.6 [30]

28. **Sollte eine Schwachstelle durch einen Dritten entdeckt werden. Ist eine Meldeadresse zur Meldung dieser entdeckten Schwachstellen an Ihr Unternehmen vorhanden? Z. B. per Responsible Disclosure.**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt/ Anderes (bitte geben Sie an)

Hintergrund der Frage: Diese Frage soll klären, ob sich Dritte, die eine Schwachstelle in den jeweiligen Produkten entdecken, im besten Falle anonymisiert, an die Organisationen wenden können, um die Schwachstelle zu kommunizieren. Mapping: Annex 1 Anforderung 2.6 [30]

29. **Falls ein Meldeweg vorhanden ist: Wie können durch Dritte entdeckte Schwachstellen an Ihr Unternehmen kommuniziert werden? (optional)**
Textfeldeingabe (maximal 1.000 Zeichen)

Hintergrund der Frage: Diese Frage dient der qualitativen Spezifizierung der vorherigen Frage (Frage 28). Mapping: Annex 1 Anforderung 2.6 [30]

30. **Wird die durch Ihr Unternehmen produzierte Software nach einem einheitlichen Schema versioniert? Z. B. Semantic Versioning 2.0.0**
Wählen Sie eine Antwort
(Ja/ Ja, verschiedene Projekte nutzen jedoch unterschiedliche Arten der Versionierung/ Nein/ Ist mir nicht bekannt)

Hintergrund der Frage: Diese Frage dient dazu herauszufinden, ob die Umfrageteilnehmer bei ihrer Arbeit bereits ein Versionierungsschema der Software verwenden, um eine genaue Identifizierung von möglicherweise vulnerablen Versionen zu ermöglichen. Mapping: Annex 2 Anforderung 3 [30]

31. **Existiert eine technische Dokumentation Ihrer Software?**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

Hintergrund der Frage: Diese Frage soll klären, ob eine technische Dokumentation der entwickelten Software angefertigt wird, die im Nachhinein den

Prüfern oder Nutzern zur Verfügung gestellt werden kann. Mapping: Annex 2 Anforderung 9 [30]

32. **Sollte der Kunde die Software selbst konfigurieren können oder müssen. Existiert eine dokumentierte und dem Kunden jederzeit verfügbare Anleitung zur sicheren Konfiguration der Software, die alle notwendigen Informationen zur sicheren Konfiguration enthält? (optional)**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

Hintergrund der Frage: Diese Frage zielt darauf ab, in Erfahrung zu bringen, wie viele der Organisationen, bei denen die Umfrageteilnehmer engagiert sind, eine Anleitung zur sicheren Konfiguration oder Schwachstellenbehebung ausgeben (wenn notwendig). Mapping: Annex 1 Anforderung 2.4 & Annex 2 Anforderung 4 & 9[30]

33. **Gehört die von Ihnen entwickelte Software zu einer der hier genannten Produktkategorien/ Verwendungszwecken oder wird in diesen durch Ihr Unternehmen verbaut?**
Hinweis: Sollte Ihr Produkt zu einer der Kategorien gehören, fällt es in die Kategorie „Kritische Produkte“ und muss besondere Anforderungen im Rahmen des CRA erfüllen.
Wählen Sie eine Antwort
Auswahl aus den Produktkategorien, die laut dem Annex des CRA unter die Klasse der „kritischen Produkte“ fallen. [30]

Hintergrund der Frage: Diese Frage soll anzeigen, wie viele der Umfrageteilnehmer Softwareprodukte der Kategorie „kritische Produkte mit digitalen Elementen“ herstellen. Mapping: Annex 3 [30]

34. **Handelt es sich bei der durch Sie vertriebenen Software um eine reine SaaS-Anwendung?**
Wählen Sie eine Antwort
(Ja/ Nein/ Ist mir nicht bekannt)

Hintergrund der Frage: Diese Frage soll herausfinden, wie viele der Umfrageteilnehmer SaaS Anwendungen entwickeln und somit nicht unter den CRA fallen, sondern eher von anderen Sicherheitsregularien betroffen sind. Mapping: CRA-Verordnung (9) [30]

35. **Gibt es etwas, was sie im Rahmen der Befragung noch unbedingt erwähnen möchten? (optional)**
Textfeldeingabe (maximal 1.000 Zeichen)

Hintergrund der Frage: Diese Frage soll es den Umfrageteilnehmern ermöglichen, weitere qualitative Antworten der Umfrage hinzuzufügen.

3.5 Datenanalyse

Nach Abschluss des im Vorfeld festgelegten Befragungszeitraums wurden die Ergebnisse der Befragung gesammelt und anschließend im Kapitel 4.1 einerseits grafisch präsentiert und in der anschließenden Diskussion teilweise näher interpretiert.

4 Ergebnisse

Dieses Kapitel dient der Darstellung der in der Umfrage gewonnenen Ergebnisse und eine Interpretation dieser.

4.1 Darstellung der Ergebnisse

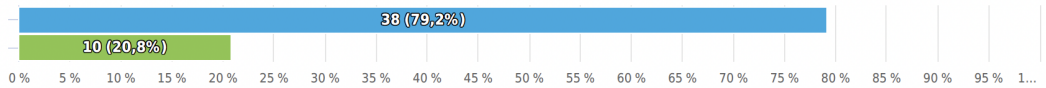
Die Umfrage war insgesamt 60 Tage vom 30.06.2025 bis zu 28.08.2025 geöffnet. Insgesamt haben 186 Teilnehmer die Umfrage besucht. Von diesen Teilnehmern haben jedoch nur 48 also 25,8 % die Umfrage abgeschlossen. Dies ist möglicherweise wie in 5.4 referenziert auf die Länge des Fragebogens oder auf das spezielle Thema zurückzuführen, vor dessen Beantwortung die Befragten möglicherweise zurückschreckten.

Im Folgenden werden die Umfrageergebnisse grafisch dargestellt. Der Fragebogen in seiner vollen Länge, aus dem die folgenden Grafiken stammen, ist dieser Arbeit in Anhang 1 angehängt.

1 Haben Sie bereits vom CRA (Cyber Resilience Act gehört)

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	38	79,2%
Nein	10	20,8%



2 Ist der CRA in Ihrer Firma bereits ein Gesprächsthema?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	23	47,9%
Nein	13	27,1%
Ist mir nicht bekannt	12	25,0%

Abbildung 4.1: *Antworten Frage 1 & 2*

3 Welche der angegebenen Berufsbezeichnungen trifft auf Sie zu?

Mehrfachauswahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Softwareentwickler:in	22	45,8%
Softwarearchitekt:in	5	10,4%
ISB/ ISO	3	6,3%
CISO	1	2,1%
Geschäftsführer:in	5	10,4%
IT-Administrator:in	8	16,7%
Cybersecurity Berater:in	8	16,7%
Ich möchte keine Angabe machen	1	2,1%
Andere (bitte geben Sie an)	9	18,8%

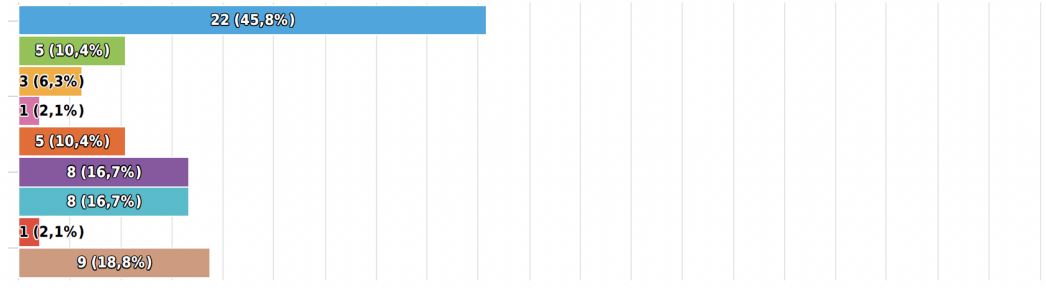


Abbildung 4.2: *Antwort Frage 2*

4 Wie alt sind Sie? (optional)

Einzelwahl , geantwortet 46 x, unbeantwortet 2 x

Antwort	Antworten	Verhältnis
<25	6	13,0%
25 - 35	17	37,0%
35 - 45	12	26,1%
45 - 55	5	10,9%
55 - 65	6	13,0%
>65	0	0,0%

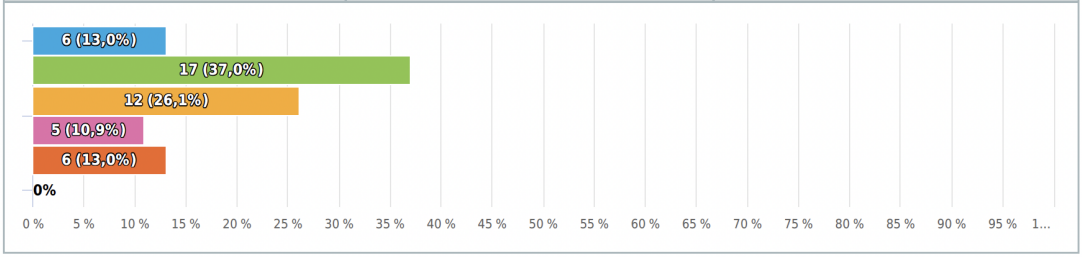


Abbildung 4.3: *Antwort Frage 4*

5 In welcher Branche ist Ihr Unternehmen tätig?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Informationstechnologie	17	35,4%
Finanzen & Versicherungen	3	6,3%
Gesundheitswesen	3	6,3%
Industrie & Produktion	1	2,1%
Transport & Logistik	3	6,3%
Energie & Versorgung	0	0,0%
Bildung & Forschung	1	2,1%
Öffentlicher Dienst	3	6,3%
Medien & Kommunikation	2	4,2%
Beratung & Dienstleistungen	12	25,0%
Ich möchte keine Angabe machen	0	0,0%
Andere (bitte geben Sie an)	3	6,3%

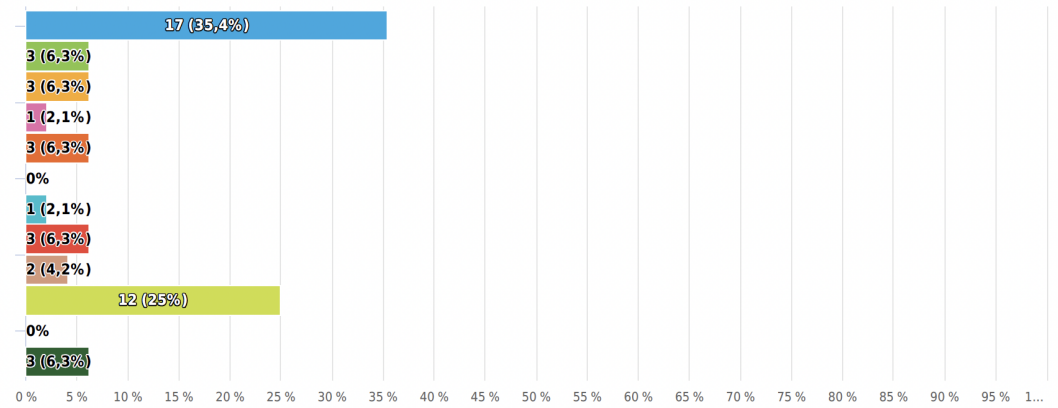


Abbildung 4.4: *Antwort Frage 5*

6 Handelt es sich bei Ihrem Unternehmen um kritische Infrastruktur (KRITIS)? (optional)

Einzelwahl , geantwortet 47 x, unbeantwortet 1 x

Antwort	Antworten	Verhältnis
Ja	10	21,3%
Nein	32	68,1%
Ist mir nicht bekannt	5	10,6%

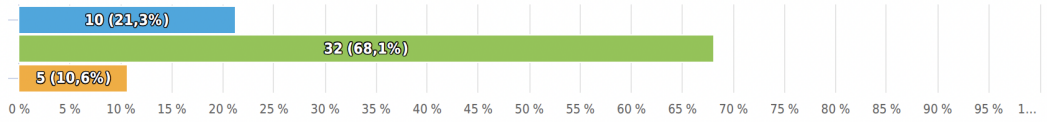


Abbildung 4.5: *Antwort Frage 6*

7 Ist Ihr Unternehmen von einer dieser Regularien betroffen bzw. muss diese erfüllen? (optional)

Mehrfachauswahl , geantwortet 47 x, unbeantwortet 1 x

Antwort	Antworten	Verhältnis
BSI-Grundschutz	19	40,4%
NIS-2	8	17,0%
PCI-DSS	1	2,1%
HIPAA	1	2,1%
TISAX	3	6,4%
C5	1	2,1%
ISO 27001 (ISMS)	25	53,2%
NIST Cybersecurity Framework	2	4,3%
Mir sind keine bekannt	12	25,5%
Mein Unternehmen unterliegt keiner dieser Anforderungen	6	12,8%
Ich möchte hierzu keine Angaben machen	2	4,3%
Andere (bitte geben Sie an)	1	2,1%

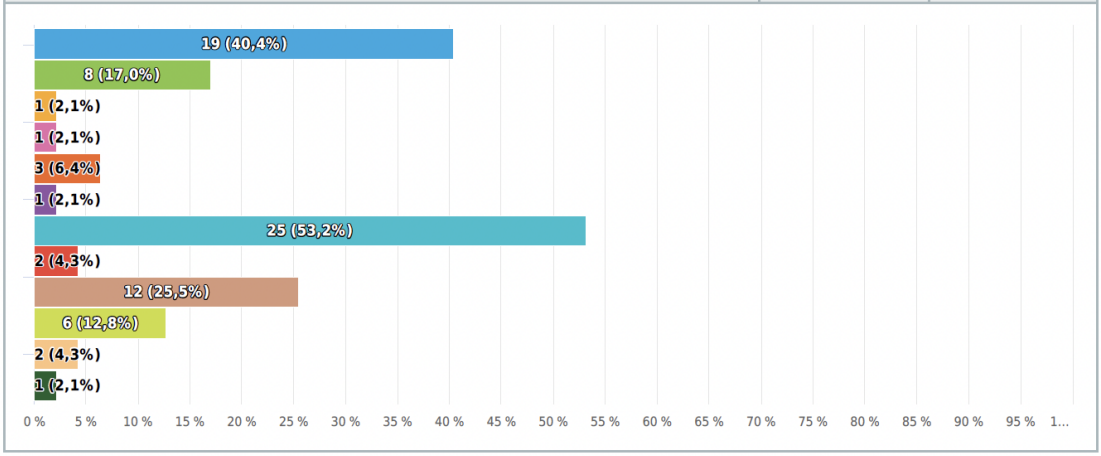
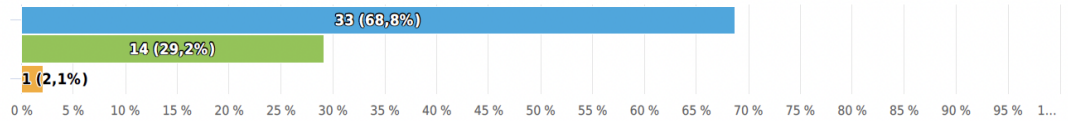


Abbildung 4.6: *Antwort Frage 7*

8 Ist Softwaresicherheit ein priorisiertes Thema in Ihrem Unternehmen?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

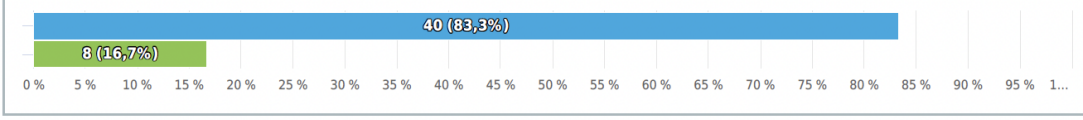
Antwort	Antworten	Verhältnis
Ja	33	68,8%
Nein	14	29,2%
Ist mir nicht bekannt	1	2,1%



9 Ist Softwaresicherheit für Sie persönlich ein priorisiertes Thema?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	40	83,3%
Nein	8	16,7%



10 Wie hoch schätzen Sie die Relevanz von Softwaresicherheit für Ihre tägliche Arbeit ein?

Semantisches Differential , geantwortet 48 x, unbeantwortet 0 x

Antwort	-5	-4	-3	-2	-1	0	1	2	3	4	5	
Nicht relevant	1 (2,1%)	0	1 (2,1%)	3 (6,3%)	0	1 (2,1%)	2 (4,2%)	6 (12,5%)	12 (25,0%)	11 (22,9%)	11 (22,9%)	Sehr relevant

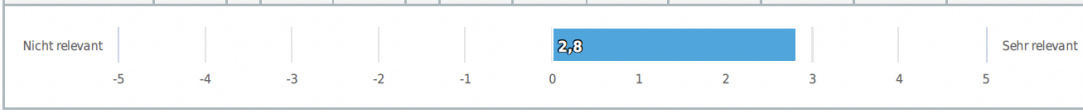
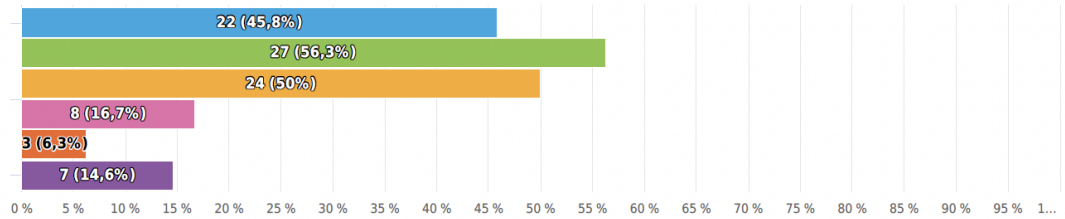


Abbildung 4.7: *Antworten Frage 8, 9 & 10*

11 Werden Sicherheitsmaßnahmen bei der Konzeption, Entwicklung oder im Betrieb der durch Sie entwickelten Software integriert?

Mehrfachauswahl, geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Konzeption/ Design	22	45,8%
Entwicklung	27	56,3%
Im Betrieb	24	50,0%
Sicherheitsmaßnahmen werden nur nach Bedarf integriert	8	16,7%
Sicherheitsmaßnahmen werden nicht integriert	3	6,3%
Ist mir nicht bekannt	7	14,6%



12 Findet eine Bedrohungsanalyse der Software statt, um Schwachstellen in der Architektur der Software ausfindig zu machen? Z. B. ein Threat-Modeling mittels STRIDE Methodik.

Einzelwahl, geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	21	43,8%
Nein	15	31,3%
Ist mir nicht bekannt	12	25,0%

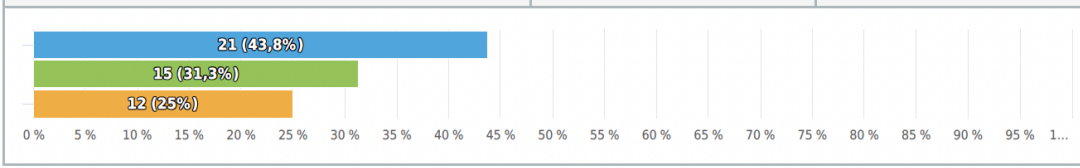
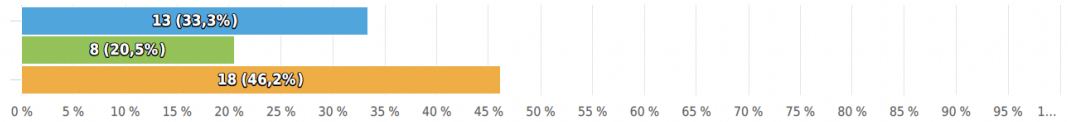


Abbildung 4.8: *Antworten Frage 11 & 12*

13 Falls ja, wird diese Bedrohungsanalyse regelmäßig während des Lebenszyklus der Software wiederholt? (optional)

Einzelwahl, geantwortet 39 x, unbeantwortet 9 x

Antwort	Antworten	Verhältnis
Ja	13	33,3%
Nein	8	20,5%
Ist mir nicht bekannt	18	46,2%



14 Wird Software in Ihrem Unternehmen auf bekannte Schwachstellen (CVEs) überprüft? Z. B. durch einen SCA Scan (Software Composition Analysis)

Einzelwahl, geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	31	64,6%
Nein	7	14,6%
Ist mir nicht bekannt	10	20,8%

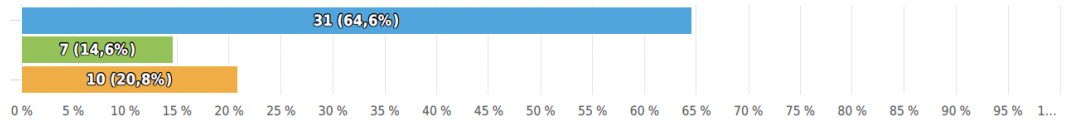
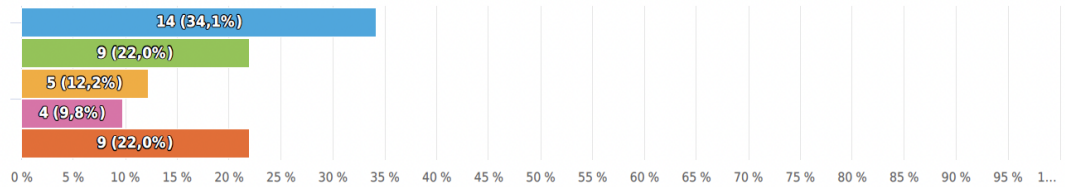


Abbildung 4.9: *Antworten Frage 13 & 14*

15 Falls ja, werden diese Scans regelmäßig wiederholt? (optional)

Einzelwahl , geantwortet 41 x, unbeantwortet 7 x

Antwort	Antworten	Verhältnis
Ja, automatisiert	14	34,1%
Ja, manuell getriggert	9	22,0%
Ja, bei Produktabnahme	5	12,2%
Nein	4	9,8%
Ist mir nicht bekannt	9	22,0%



16 Welche Sicherheitsmaßnahmen werden noch zur Erhöhung der Sicherheit der durch Ihr Unternehmen gebaute Software durchgeführt? (optional)

Text Frage , geantwortet 15 x, unbeantwortet 33 x

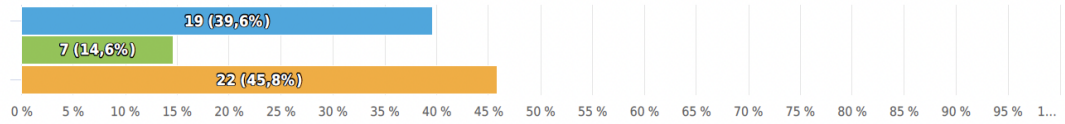
- Code Reviews (4 Augen Prinzip)
- Dependency updates mit renovate Trivy scan Sonarqube scans
- Es wird sich auf das Know-How der Entwickler verlassen ...
- Interne wie externe Audits
- Kryptographische Mechanismen aus eigener Entwicklung
- Lol
- Patches
- Pentests
- Pentests (extern)
- Regelmäßige Pen-tests
- Sast
- Schulungen der Mitarbeiter
- Schulungen durch die IT Abteilung
- Vorgaben für Frequent von SCA,CCA-scans. Verpflichtende jährliche pentests. Scan tools für produktive Infrastruktur via tools wie paloalto prisma cloud oder qualys.
- 4augenprinzip, immer Mal wieder pentest

Abbildung 4.10: *Antworten Frage 15 & 16*

17 Werden alle ausnutzbaren Schwachstellen geschlossen, bevor die Software an den Kunden/ Nutzer ausgeliefert wird?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	19	39,6%
Nein	7	14,6%
Ist mir nicht bekannt	22	45,8%



18 Wird von der Software eine SBOM (Software-Bill-of-Materials) angefertigt und für Nutzer/ Kunden erreichbar hinterlegt?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	10	20,8%
Nein	10	20,8%
Ist mir nicht bekannt	28	58,3%

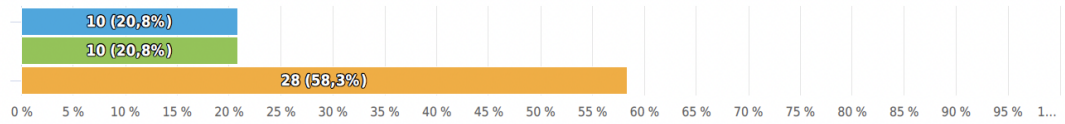


Abbildung 4.11: *Antworten Frage 17 & 18*

19 Falls ja, wird diese SBOM für jede ausgelieferte Version der Software erstellt und hinterlegt? (optional)

Einzelwahl , geantwortet 36 x, unbeantwortet 12 x

Antwort	Antworten	Verhältnis
Ja	7	19,4%
Nein	6	16,7%
Ist mir nicht bekannt	23	63,9%

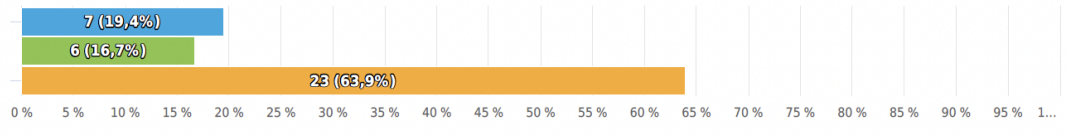


Abbildung 4.12: *Antwort Frage 19*

20 Wie lange dauert es in der Regel, eine ausnutzbare Schwachstelle oberhalb eines CVE Scores von 7.0 (high) zu beheben?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Einen Tag	3	6,3%
< 3 Tage	5	10,4%
< 7 Tage	6	12,5%
< 14 Tage	4	8,3%
< 30 Tage	0	0,0%
> 30 Tage	0	0,0%
Ist mir nicht bekannt	28	58,3%
Andere (bitte geben Sie an)	2	4,2%

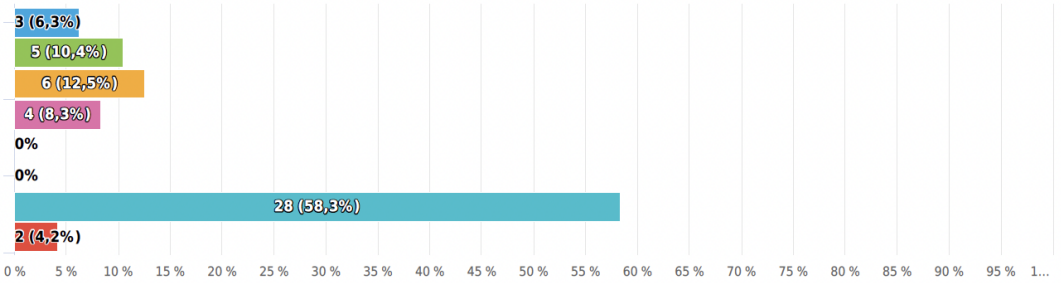
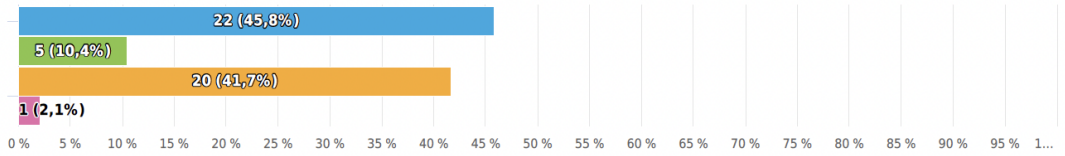


Abbildung 4.13: *Antwort Frage 20*

21 Werden Ihre Kunden/ Nutzer direkt über neue Schwachstellen informiert?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	22	45,8%
Nein	5	10,4%
Ist mir nicht bekannt	20	41,7%
Andere (bitte geben Sie an)	1	2,1%



22 Falls ja, über welchen Kommunikationskanal? (optional)

Einzelwahl , geantwortet 31 x, unbeantwortet 17 x

Antwort	Antworten	Verhältnis
Mail	18	58,1%
Telefon	2	6,5%
Die Software selbst (z. B. per Pop-Up)	2	6,5%
Messenger	1	3,2%
Vulnerability Exploitability eXchange (VEX)	2	6,5%
Andere (bitte geben Sie an)	6	19,4%

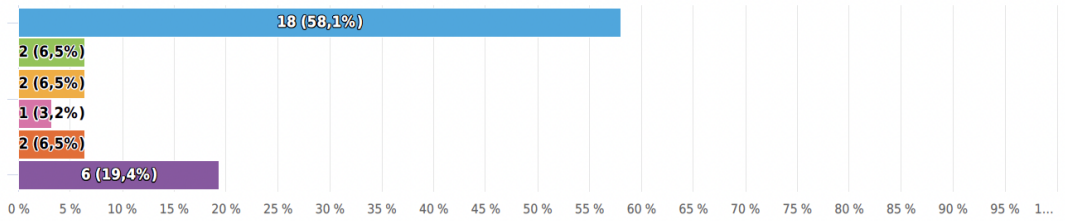
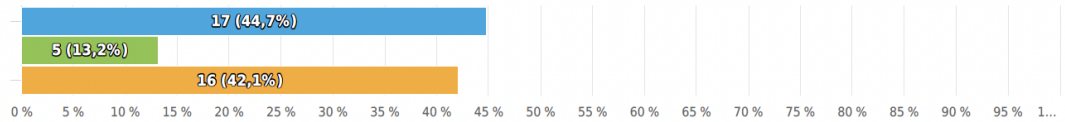


Abbildung 4.14: *Antworten Frage 21 & 22*

23 Falls ja, existiert für die Kommunikation der Schwachstelle ein geregelter Prozess? (optional)

Einzelwahl , geantwortet 38 x, unbeantwortet 10 x

Antwort	Antworten	Verhältnis
Ja	17	44,7%
Nein	5	13,2%
Ist mir nicht bekannt	16	42,1%



24 Werden durch Ihr Unternehmen Zeitangaben bis zur erwarteten Behebung der Schwachstellen gegenüber den Nutzern/ Kunden angegeben?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja - genaue Angaben	3	6,3%
Ja - ungefähre Angaben	15	31,3%
Nein	8	16,7%
Ist mir nicht bekannt	22	45,8%

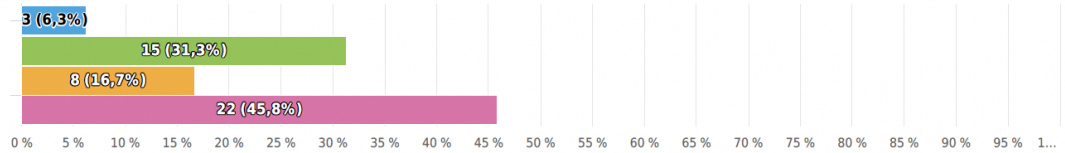
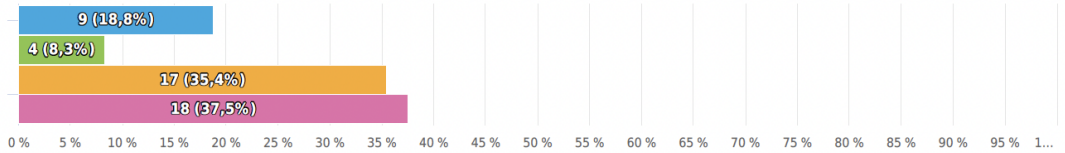


Abbildung 4.15: *Antworten Frage 23 & 24*

25 Sollte die Schwachstelle durch den Kunden/ Nutzer selbst behoben werden müssen. Wird eine detaillierte Anleitung/ Dokumentation mitgegeben.

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	9	18,8%
Nein	4	8,3%
Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	17	35,4%
Ist mir nicht bekannt	18	37,5%



26 Werden Schwachstellen in Ihrer Software nach Ihrer Behebung veröffentlicht? Z. B. in der NIST-NVD Database.

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	5	10,4%
Nein	9	18,8%
Ist mir nicht bekannt	33	68,8%
Andere (bitte geben Sie an)	1	2,1%

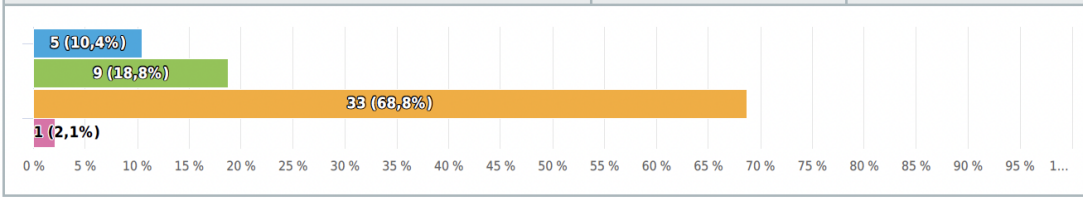
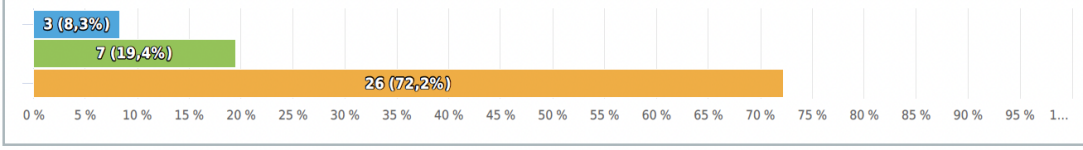


Abbildung 4.16: *Antworten Frage 25 & 26*

27 Falls ja, existiert für die Veröffentlichung der Schwachstelle ein geregelter Prozess? (optional)

Einzelwahl, geantwortet 36 x, unbeantwortet 12 x

Antwort	Antworten	Verhältnis
Ja	3	8,3%
Nein	7	19,4%
Ist mir nicht bekannt	26	72,2%



28 Sollte eine Schwachstelle durch einen Dritten entdeckt werden. Ist eine Meldeadresse zur Meldung dieser entdeckten Schwachstellen an Ihr Unternehmen vorhanden? Z. B. per Responsible Disclosure.

Einzelwahl, geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	24	50,0%
Nein	8	16,7%
Ist mir nicht bekannt	14	29,2%
Andere (bitte geben Sie an)	2	4,2%

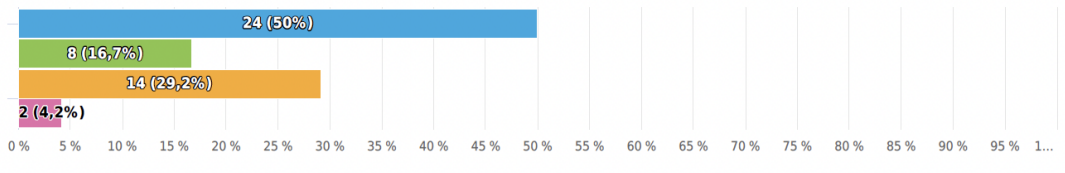


Abbildung 4.17: *Antworten Frage 27 & 28*

29 Falls ein Meldeweg vorhanden ist: Wie können durch Dritte entdeckte Schwachstellen an Ihr Unternehmen kommuniziert werden? (optional)

Text Frage , geantwortet 11 x, unbeantwortet 37 x

- E-Mail oder Issue post auf dem public GitHub repository.
- Gut dokumentierter prozess inklusive safe harbor erklärung. Hochladen von Berichten bei intigriti
- Jede Form vertraulicher Kommunikation wird akzeptiert
- Mail
- Mail an security@... oder über unser BugBounty-Programm
- Mailkontakt
- Nutzung des normalen Kontaktformulars
- security.txt
- Security.txt, E-Mail Kontakt
- Schlecht. Per anonymen Brief an den Hauptsitz wäre wahrscheinlich am besten. Ansonsten ist das eher schwer
- Verschlüsselte Email via security.txt direkt an das Operations Team

30 Wird die durch Ihr Unternehmen produzierte Software nach einem einheitlichen Schema versioniert? Z. B. Semantic Versioning 2.0.0

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	17	35,4%
Ja, verschiedene Projekte nutzen jedoch unterschiedliche Arten der Versionierung	12	25,0%
Nein	6	12,5%
Ist mir nicht bekannt	13	27,1%

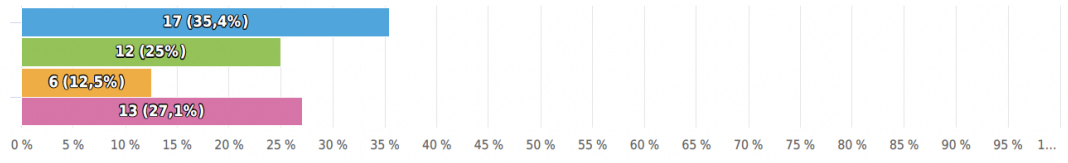
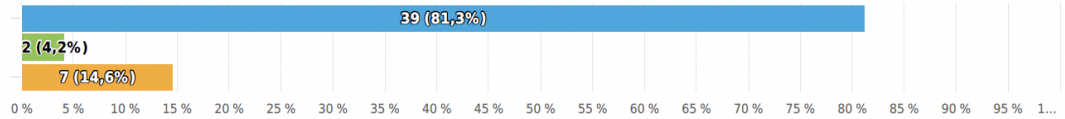


Abbildung 4.18: *Antworten Frage 29 & 30*

31 Existiert eine technische Dokumentation Ihrer Software?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	39	81,3%
Nein	2	4,2%
Ist mir nicht bekannt	7	14,6%



32 Sollte der Kunde die Software selbst konfigurieren können oder müssen. Existiert eine dokumentierte und dem Kunden jederzeit verfügbare Anleitung zur sicheren Konfiguration der Software, die alle notwendigen Informationen zur sicheren Konfiguration enthält? (optional)

Einzelwahl , geantwortet 42 x, unbeantwortet 6 x

Antwort	Antworten	Verhältnis
Ja	17	40,5%
Nein	10	23,8%
Ist mir nicht bekannt	15	35,7%

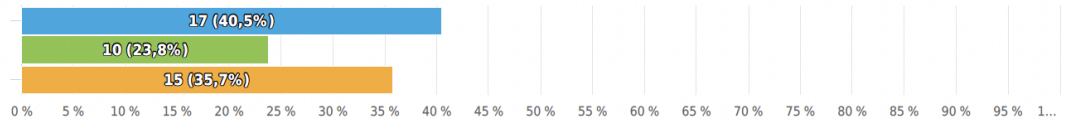
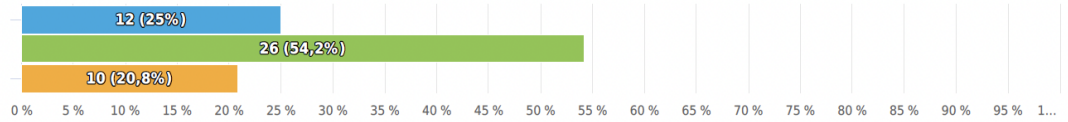


Abbildung 4.19: *Antworten Frage 31 & 32*

34 Handelt es sich bei der durch Sie vertriebenen Software um eine reine SaaS-Anwendung?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	12	25,0%
Nein	26	54,2%
Ist mir nicht bekannt	10	20,8%



35 Gibt es etwas, was sie im Rahmen der Befragung noch unbedingt erwähnen möchten? (optional)

Text Frage , geantwortet 8 x, unbeantwortet 40 x

- Bisher keinen Kontakt zu der Thematik gehabt...
- Bug bei Auswahl iam
- Die Fragen sind primär für Softwareentwickler gedacht. Ein Konzern hat aber wesentlich mehr Abteilungen die sich mit cra auseinandersetzen müssen.
- Ich bin als GF leider nicht so sehr in die Entwicklung involviert, denke aber, dass wir sichere Software bauen. Ich leite den Bogen an meine Entwickler weiter.
- Ich bin keine programmierende Person.UnserUnternehmen betreut Menschen in ihrer Lebensführung. Daten dieser zu schützen ist relevant.
- Ich bin selbst nicht an der Softwareentwicklung beteiligt, bin mir aber sicher, dass Vorgaben einghalten werden.

Abbildung 4.20: *Antworten Frage 34 & 35(1/2)*

- Wir sind eine Agentur für Softwareentwicklung und liefern verschiedenste Softwareprojekte an Kunden. Viele der Projekte sind unterschiedlich, daher sind keine 100 % igen Angaben möglich. Sicherheit ist bei vielen unserer Kunden leider kein Thema, für das sie Geld ausgeben.
- Wir sind noch in einem frühen Stadium der Entwicklung. Einige der Punkte werden ggf. noch adressiert.

Abbildung 4.21: *Antwort Frage 35(2/2)*

Die genauen Antworten auf die gestellten Fragen sind im Anhang 2 dieser Arbeit zu finden.

4.2 Ergebnisinterpretation

Im folgenden Abschnitt werden die Ergebnisse der Befragung interpretiert und es wird eine erste Auswertung vorgenommen.

4.2.1 Genereller Kenntnisstand zum CRA und Bedeutung von Softwaresicherheit

Es ist deutlich zu erkennen, dass fast 80 % der Befragten bereits vom CRA gehört haben. Von diesen Waren etwa 48 % Softwareentwickler. Betrachtet man die genauen Angaben der reinen Softwareentwickler genauer, haben 9 % dieser Gruppe noch nicht vom CRA gehört und bei 45 % besitzt dieser in der täglichen Arbeit keine Relevanz. Zwar fällt auf, dass die 9 % der Umfrageteilnehmer ohne Kenntnisstand über den CRA jeweils über 45 Jahre alt sind, eine direkte Korrelation zwischen Alter und Kenntnisstand zum CRA ist jedoch nicht zu erkennen. Ebenfalls ist kein Zusammenhang zwischen der Behandlung des CRA im Arbeitskontext zu erkennen. Was die generelle Einschätzung von Softwaresicherheit für die tägliche Arbeit anbelangt, so weist diese einen Durchschnittswert von 2,8 auf einer Skala von –5 (nicht relevant) bis 5 (sehr relevant) mit einem größeren Clustering hin zu den Werten 3, 4 und 5. Dies deutet darauf hin, dass ein Großteil der Befragten Softwaresicherheit hier eine hohe Relevanzwahrnehmung besitzt.

4.2.2 Compliancekontext der Teilnehmenden

Aus den Ergebnissen der Umfrage ist zu erkennen, dass mindestens 21,3 % der Umfrageteilnehmer aus dem KRITIS Umfeld stammen. Von diesen Teilnehmern gaben jeweils 20 % an, dass Sicherheit kein priorisiertes Thema innerhalb ihres Unternehmens und für sie persönlich sei. Hier schätzten aber nur die Teilnehmer die Relevanz von Softwaresicherheit für ihre tägliche Arbeit als gering oder sehr gering ein, die auch angaben, dass Sicherheit für sie persönlich kein priorisiertes Thema sei. Im Kontext der Integration von Sicherheitsmaßnahmen innerhalb der Software geht aus den Ergebnissen hervor, dass bei den Befragten im KRITIS Sektor bei nur 30 % Sicherheitsmaßnahmen während der Konzeption der Software integriert werden (genereller Schnitt 45,8 %). Bei etwa 30 % dieser Gruppe werden Sicherheitsmaßnahmen generell nicht in die Entwicklung integriert (genereller Schnitt 6,8 %). Bei insgesamt 53,2 % der Teilnehmer wird in der jeweiligen Organisation ein ISMS nach der DIN ISO/IEC 27001 betrieben und bei 40,4 % findet der BSI IT-Grundschutz Anwendung.

4.2.3 Relevanz des CRA für die Ausfüllenden

25 % der Befragten gaben an, dass es sich bei dem durch ihre Organisation entwickelten Produktes um eine SaaS Anwendung handelt. Dies bedeutet, dass der CRA laut der CRA-Verordnung Absatz (9) nicht auf die jeweiligen Produkte anwendbar ist [2]. Besondere Relevanz besitzt der CRA für „kritische Produkte“, die erhöhte Auflagen im Rahmen des CRA erfüllen müssen [2] und im Annex des CRA aufgelistet werden [30]. Insgesamt haben die Organisationen, denen die Befragten zugehörig sind, zu 33,6 % kritische Produkte hergestellt. Sicherheitselemente und industrielle Automatisierungssysteme (außerhalb des KRITIS-Bereichs) wurden von jeweils 6,3 % der Befragten hergestellt. 4,2 % nannten Internetbrowser, PKI- und Zertifikatinfrastrukturen her und jeweils 2,1 % fertigten Passwortmanager, Netzwerkmanagement-/Monitoringlösungen, Betriebssysteme, IoT Devices (nicht KRITIS), intelligente Zähler oder IAM Systeme. Letztere wurden aufgrund einer Fehlfunktion im Auswahlfeld als Freitextantwort zu Frage 35 angegeben und hier manuell hinzugezählt.

5 Diskussion

In diesem Kapitel werden die Ergebnisse mit Blick auf die in der Arbeit gestellten Forschungsfragen diskutiert und die sich daraus ergebenden Implikationen für die Praxis aufgeführt. Im Anschluss daran werden Maßnahmen erarbeitet, die den softwareentwickelnden Unternehmen, als Leitfaden dienen sollen, um die Anforderungen des CRA möglichst pragmatisch zu erfüllen.

5.1 Einordnung in den Forschungskontext

Im Bezug auf die Forschungsfragen lassen sich die folgenden Erkenntnisse aus den Ergebnissen der Umfrage ableiten.

5.1.1 Aktueller Stand der Vorbereitung auf den CRA

Die erste Forschungsfrage lautete „Inwieweit sind die Softwareentwicklungsabteilungen deutscher Unternehmen bereits auf das Inkrafttreten des CRA und dessen Anforderungen vorbereitet?“. Hierzu müssen die Ergebnisse der Fragen 8, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23, 24, 25, 26, 27, 28, 29, 31, 32 näher betrachtet werden. Die Ergebnisse der Beantwortung der Fragen werden im Folgenden logisch nach der jeweiligen Anforderung gruppiert. Im Folgenden wird die Forschungsfrage für jede dieser Gruppierungen im Einzelnen beantwortet.

1. **Security Awareness:**
   In der Betrachtung dieses Clusters wird das Ergebnis der Frage 8 zugrundegelegt. Diese Frage wurde mit dem Hintergrund der Erkennung, ob Sicherheit bei der Entwicklung von Softwareprodukten eine zentrale Rolle spielt in den Fragebogen eingebaut. Der CRA nennt in seinen Paragraphen (1) und (4) ein geringes Maß an Cybersicherheit als ein gesellschaftliches Problem und wurde unter anderem für den Zweck geschaffen, „umfassende Cybersicherheitsanforderungen an alle Produkte mit digitalen Elementen“ festzulegen [2]. Da der CRA Cybersicherheitsanforderungen für bisher unregulierte Produkte einführt und eine Priorisierung der Cybersicherheit für alle Hersteller von Softwareprodukten zur Folge hat, wurde untersucht, ob die Hersteller/Organisationen die Sicherheit ihrer Produkte bereits priorisieren oder diese Priorisierung in Folge des CRA zeitnah vornehmen/nachsteuern müssen.

Die Sicherheit der Software wird laut den Umfrageergebnissen in 68,8 % der Organisationen priorisiert.

2. **Security by Design:**
   In der Betrachtung dieses Clusters werden die Ergebnisse der Fragen 11, 12 und 13 einbezogen. Die hier geclusterten Fragen zielen darauf ab, zu erfahren, ob Sicherheitsüberlegungen und Risikoabschätzungen bereits in der Konzeptions- und Planungsphase sowie nachgelagert, wie im CRA Annex gefordert, iterativ durchgeführt werden. Diese Praxis lässt sich über dem Überbegriff Security by Design zusammenfassen [30].
   Bei der Betrachtung der Ergebnisse fällt auf, dass Sicherheitsmaßnahmen bei einem Großteil der Befragten in den Entwicklungsprozess integriert werden. Allerdings werden nur bei 45,8 % der Befragten Sicherheitsmaßnahmen ab der Konzeption eingesetzt und nur 43,8 % der Befragten führen die geforderten Risiko-/ Bedrohungsanalysen durch, die nur bei etwa 33,3 % regelmäßig wiederholt werden. Dies bedeutet, das nur ein Drittel der Befragten in ihrer Organisation die Anforderung des CRA (Artikel 10 Praragraph 2), die Sicherheit in jeder Phase des Lebenszyklus zu bewerten, nachkommt.

3. **Schwachstellenmanagement:**
   In der Betrachtung dieses Clusters werden die Ergebnisse der Fragen 14, 15, 16, 17 und 20 einbezogen. Die betrachteten Fragen zielen darauf ab, zu erfahren, wie die Befragten in ihren jeweiligen Organisationen mit der Behandlung von Schwachstellen in den entwickelten Softwareprojekten verfahren. Der CRA an sich fordert bereits in seiner Begründung als erstes Hauptziel, dass Hard- und Softwareprodukte mit weniger Schwachstellen auf den Markt gebracht werden sollen [2]. Die spezifische Anforderung 1.2 des Annex des CRA (Anhang 1) fordert: „Produkte mit digitalen Elementen werden ohne bekannte ausnutzbare Schwachstellen ausgeliefert“ [30]. 64,6 % der Befragten gaben an, dass die Software in ihren Organisationen auf bekannte Schwachstellen überprüft wird und diese Scans in den meisten Fällen mit einer gewissen Regelmäßigkeit wiederholt werden. Zur weiteren Absicherung gegen Schwachstellen gaben die Befragten an, dass ebenfalls auch Sicherheitsmaßnahmen wie Code Reviews oder Penetrationstests durchgeführt werden und die Mitarbeiter in Security Themen geschult werden. Es ist jedoch aus den Antworten zu erkennen, dass nur 39,6 % der Umfrageteilnehmer davon ausgehen, dass die ausnutzbaren Schwachstellen, wie im CRA gefordert, vor der Auslieferung an die Kunden und Nutzer geschlossen werden. Ebenso können lediglich 37,5 % der Befragten angeben, dass in der Regel, ausnutzbare Schwachstellen mit einem hohen Risiko für die Nutzer innerhalb der ersten 30 Tage behoben werden. Man kann somit erkennen, dass in der Breite die Überprüfung auf ausnutzbare Schwachstellen in Software durchgeführt wird jedoch die Schließung dieser Schwachstellen vor der Auslieferung und die Behebung neuer Schwachstellen nur bei einem Drittel der Befragten tatsächlich erfolgt.

4. **SBOM:**

In der Betrachtung dieses Clusters werden die Ergebnisse der Fragen 18 und 19 einbezogen. Diese Fragen zielen darauf ab, in Erfahrung zu bringen, ob die im CRA und dessen Annex geforderte SBOM nicht nur angefertigt wird, sondern auch für die Kunden und Nutzer erreichbar hinterlegt wird [2], [30]. Nur 20,8 % der Befragten konnten diese Frage positiv beantworten. Betrachtet man diese Gruppe der Befragten in ihren Antworten auf die Frage 19 genauer, so können nur 14,5 % (bereinigt, da nicht alle Teilnehmer der Umfrage diese Frage beantwortet haben) der Befragten eine Anfertigung und Auslieferung einer SBOM für jede von den Kunden und Nutzern genutzte Softwareversion positiv beantworten. Diese Antworten zeigen deutlich, dass die Veröffentlichung und vor allem die Veröffentlichung einer SBOM in jeder Version der Software nur bei einem kleinen Teil der Organisationen stattfindet. Die Veröffentlichung einer stets aktuellen SBOM ist aus dem Grund relevant, da sich mit jeder neuen Version der Software die in ihr verbauten fremden Softwarekomponenten und die damit verbundenen Abhängigkeiten ändern können, was einen erheblichen Einfluss auf die vorhandenen Schwachstellen haben kann.

5. **Schwachstellenkommunikation nach extern (Disclosure):**
In der Betrachtung dieses Clusters werden die Ergebnisse der Fragen 21, 23, 24, 26 und 27 einbezogen. Diese Fragen zielen darauf ab, in Erfahrung zu bringen, wie die Organisationen der Umfrageteilnehmer Nutzer und Nutzerinnen über die Schwachstellen, in den eigenen ausgelieferten Softwareprodukten informieren, bei deren Behebung unterstützen und die Schwachstellen im Anschluss veröffentlichen. Hier geben 45,8 % der Befragten an, dass Nutzer direkt über Schwachstellen in den Produkten informiert werden. Ein Großteil dieser Kommunikation (58,1 %) findet per Mail statt und bei 35,4 % (bereinigt) der Befragten ist die Kommunikation der Schwachstellen ein geregelter Prozess. Lediglich 37,6 % geben an, dass zur Behebungszeit der Schwachstellen Zeitangaben gegenüber Kunden und Nutzern getätigt werden, wovon nur 6,3 % genaue Zeitangaben machen. Ebenso geben nur 10,4 % an, dass Schwachstellen in den Softwareprodukten auf Datenbanken wie etwa der NIST-NVD Database veröffentlicht werden, was essenziell ist, um mögliche Nutzer weltweit zu warnen und die Auffindbarkeit der Schwachstellen durch etablierte Scanning-Tools zu gewährleisten. Nur 6,3 % (bereinigt) geben an, dass eine solche Veröffentlichung ein geregelter Prozess ist.
Diese Ergebnisse lassen erkennen, dass bei der Schwachstellenkommunikation der Unternehmen und vor allem der geforderten Veröffentlichung der Schwachstellen als geregeltem Prozess ein großer Nachholbedarf besteht.

6. **Externe Schwachstellenmeldung:**
In der Betrachtung dieses Clusters werden die Ergebnisse der Fragen 28 und 29 einbezogen. Diese Fragen zielen darauf ab, in Erfahrung zu bringen, ob die Organisationen der Befragten eine Möglichkeit etabliert haben, dass Dritte eine Meldung von Schwachstellen an Sie tätigen können. Eine solche Möglichkeit der Meldung wird nach dem Ergebnis der Befragung von 54,2 % auf dem Weg der Responsible Disclosure, Safe Harbor Optionen oder direkter Ticketanlage in der öffentlichen Repository-Entwicklungsumgebungen (z. B. GitHub) der Organisationen selbst er-

möglicht. Hier ist vor allem aus den individuell per Textfeld beantworteten Fragen zu erkennen, dass in diesem Fall eine vertrauliche Kommunikation, wenn per Responsible Disclosure möglich, präferiert wird. Allerdings ist eine solche Meldung als Sicherheitsmaßnahme nur etwa bei der Hälfte etabliert bzw. bekannt und somit noch nicht flächendeckend im Einsatz.

7. **Versionierung:**
   In der Betrachtung dieses Clusters wird das Ergebnis der Frage 30 zugrundegelegt. Diese Frage zielt darauf ab, in Erfahrung zu bringen, ob die Organisationen der Befragten eine einheitliche Versionierung in den durch sie entwickelten Softwareprojekten verwenden. Eine Versionierung, die zumindest im jeweiligen Projekt selbst einheitlich ist, wird durch 60,4 % der Organisationen eingesetzt. Eine solche Versionierung dient im Bezug auf Schwachstellen einer besseren Zuordnung und Auffindbarkeit vulnerabler Softwareversionen und sollte, wie durch den CRA gefordert, in jedem Softwareprojekt verwendet werden. Da es sich bei einer Versionierung der Software nicht um eine neue Technologie handelt, ist ein Ergebnis von 60,4 % nicht als ausreichend zu betrachten und sollte durch die Organisationen, die keine Versionierung nutzen definitiv nachgeholt werden.

8. **Dokumentation:**
   In der Betrachtung dieses Clusters werden die Ergebnisse der Fragen 31 und 32 einbezogen. Diese Fragen zielen darauf ab, in Erfahrung zu bringen, ob die Organisationen der Befragten eine technische Dokumentation ihrer in Umlauf gebrachten Software anfertigen. Dies wird von 81,3 % der Befragten mit Ja beantwortet. Bei der Zusatzfrage, ob die technische Dokumentation den Kunden bei Bedarf zur Verfügung gestellt werden kann, beantworten 40,9 % (bereinigt) mit ja. Dies lässt darauf deuten, dass das Hinterlegen einer technischen Dokumentation zur sicheren Konfiguration durch den Nutzer selbst, noch nicht so verbreitet ist, wie durch den Annex des CRA gefordert [30]. Allerdings ist auch hier zu erwähnen, dass die Möglichkeit besteht, dass die eigenständige Konfiguration nicht notwendig ist und somit ggf. aus diesem Grund mit „Nein“ geantwortet wurde.

5.1.2 Kenntnisstand der Softwareentwickler zum CRA

Betreffend des CRA muss in der Diskussion der Ergebnisse zwischen zwei Berufsgruppen unterschieden werden, um die zweite Forschungsfrage „Wie ist der Kenntnisstand der Softwareentwickler über die jeweiligen, sie betreffenden Anforderungen im Sinne der Compliance Awareness?“ genauer beantworten zu können. Zum einen werden die Gruppe der Softwareentwickler und Softwarearchitekten im Folgenden gesammelt und „Softwareentwickler“ zusammengezählt, da der Aufgabenbereich dieser beiden Berufsprofile primär die Konzeption und Entwicklung von Softwareprojekten darstellt. Zum anderen werden die weiteren Berufsbilder ebenfalls betrachtet, um hier mögliche Unterschiede festzustellen, und im Folgenden als „übrige Berufsbilder“ bezeichnet.

1. **Softwareentwickler:**
   - Gesamtgruppe: 23
   - Kennen den CRA bzw. haben bereits von ihm gehört: 20
   - Kennen den CRA nicht bzw. haben noch nicht von ihm gehört: 3
2. **Übrige Berufsbilder:**
   - Gesamtgruppe: 25
   - Kennen den CRA bzw. haben bereits von ihm gehört: 15
   - Kennen den CRA nicht bzw. haben noch nicht von ihm gehört: 10

Durch die Untersuchung der zwei Gruppen ist zu erkennen, dass ein Großteil der Softwareentwickler und Softwarearchitekten mit 87 % bereits vom CRA gehört haben und somit bekannt ist, dass diese Regulatorik Auswirkungen auf sie haben kann. Bei den übrigen Berufsfeldern ist zu erkennen, dass bisher etwa 60 % der Befragten Kenntnis über das Kommen des CRA besitzen. Somit ist der Kenntnisstand in den Berufsgruppen, die als softwareentwicklungsnah zu betrachten sind, weiter verbreitet als im Rest bzw. der Gesamtheit der Berufsgruppen, wo der Kenntnisstand nach den Ergebnissen der Umfrage 79,2 % beträgt.

5.1.3 Notwendige Maßnahmen zur CRA Anforderungserfüllung

Um die dritte Forschungsfrage „Welche Maßnahmen können ergriffen werden, um tendenziell nicht erfüllte Anforderungen (basierend auf den Umfrageergebnissen) des CRA zu erfüllen?“ zu beantworten, muss untersucht werden, bei welchen Maßnahmen, die im Fragebogen überprüft wurden, der Umsetzungsgrad in der Breite zu niedrig ist. Zwar sollten entsprechende Maßnahmen im Generellen umgesetzt sein, da bis zum finalen Zeitpunkt der Einhaltung der geforderten Maßnahmen des CRA noch mehr als 2 Jahre zum Zeitpunkt der Befragung bestehen, wird hier eine Grenze von zwei Dritteln (66,6 %) der Umsetzung als hoch genug zugrunde gelegt. Zu diesem Zweck werden die Ergebnisse der geclusterten Fragen aus der Betrachtung der vorangegangenen zweiten Forschungsfrage herangezogen.

Aus der Betrachtung der Cluster ergeben sich die folgenden Themengebiete an geforderten Maßnahmen, deren Umsetzung in der Breite noch eines weiteren Ausbaus bedarf:

1. Security by Design
2. Schwachstellenmanagement
3. SBOM
4. Schwachstellenkommunikation

5. Schwachstellenmeldung (Disclosure)
6. Versionierung

5.2 Implikationen für die Praxis

Aus der Beantwortung der Forschungsfragen ergeben sich für die Praxis mehrere wesentliche Implikationen. Die Ergebnisse verdeutlichen, dass die Einhaltung der im CRA formulierten Anforderungen in vielen Organisationen bislang nur in Teilbereichen umgesetzt ist und somit ein erheblicher Handlungsbedarf besteht.

Zunächst zeigt sich, dass insbesondere die Bereiche Security by Design, Schwachstellenmanagement sowie die Erstellung und Bereitstellung von SBOMs in der Breite noch unzureichend etabliert sind. Für die Praxis bedeutet dies, dass Unternehmen ihre Entwicklungs- und Sicherheitsprozesse frühzeitig anpassen und systematisch in den gesamten Softwarelebenszyklus integrieren müssen. Hierbei ist insbesondere sicherzustellen, dass Bedrohungs- und Risikoanalysen regelmäßig durchgeführt und dokumentiert werden, sowie geeignete technische und organisatorische Maßnahmen zur kontinuierlichen Schwachstellenprüfung und -behebung implementiert werden. Ebenso muss die Schwachstellenkommunikation sowohl in Bezug auf interne Prozesse als auch auf die externe Information von Kunden und die Veröffentlichung in anerkannten Datenbanken weiter ausgebaut werden. Ein hinzukommender geregelter Disclosure-Prozess, um Meldungen durch Dritte zu ermöglichen, stellt nicht nur die Erfüllung regulatorischer Anforderungen sicher, sondern fördert zugleich Transparenz und Vertrauen bei den Nutzern.

Des Weiteren müssen einheitliche und nachvollziehbare Versionskennzeichnungen sowie die Bereitstellung aktueller Dokumentationen umgesetzt werden, um Schwachstellen eindeutig zuordnen und Konfigurationssicherheit beim Nutzer gewährleisten zu können. Dies gilt gleichermaßen für die Veröffentlichung aktueller SBOMs, die eine Nachvollziehbarkeit verwendeter Komponenten sicherstellen.

Ebenso machen die Ergebnisse deutlich, dass der Kenntnisstand zum CRA insbesondere außerhalb der softwareentwicklungsnahen Berufsbilder noch ausgebaut werden sollte, bei den Softwareentwickelnden Berufsgruppen allerdings schon weit verbreitet ist. Um den Kenntnisstand aller Beteiligten zu erhöhen wäre es in der Praxis möglich, dass Organisationen gezielt Schulungs- und Awareness-Maßnahmen einführen, um sicherzustellen, dass alle relevanten Akteure über die Anforderungen informiert sind und diese in ihrem jeweiligen Aufgabenbereich umsetzen können.

5.3 Maßnahmen zur Erfüllung der regulatorischen Anforderungen

Da die Anforderungen, die gemäß des CRA ab dem 11.12.2027 erfüllt werden müssen, werden im Folgenden Maßnahmen näher beschrieben, die, basierend auf den im Abschnitt 5.2.3 herausgearbeiteten Themenfeldern, mit ihrer Umsetzung eine möglichst effiziente und vollständige Erfüllung der jeweiligen Anforderungen und somit der umsetzenden Organisation eine Konformität zum CRA gewährleisten können. Sie sollen als Leitfaden dienen, wie eine mögliche und konforme Umsetzung der geforderten Maßnahmen erreicht werden kann.

5.3.1 Security by Design

Die Umsetzung von Security by Design erfordert die konsequente Integration von umfassenden Sicherheitsmaßnahmen und entsprechend vorangehenden Sicherheitsüberlegungen in allen Phasen des Softwarelebenszyklus, von der Planung bis hin zum Betrieb. Ein zentrales Instrument hierfür stellt das sogenannte Threat Modeling als mögliche Form der Risikoanalyse dar, welches eine systematische Identifikation, Bewertung und Behandlung von Risiken ermöglicht. Insbesondere die Anwendung der STRIDE-Methode bietet einen strukturierten Ansatz, um Bedrohungen aus Angreiferperspektive zu erfassen, die entsprechenden Risiken abzuschätzen und geeignete Gegenmaßnahmen abzuleiten.

5.3.1.1 Threat Modeling per STRIDE-Methode

Das Threat Modeling dient der systematischen Bedrohungsanalyse und schafft die notwendige Grundlage, um die Anforderungen des CRA für eine Risikoanalyse proaktiv zu erfüllen. Dabei wird ein Software-System nicht aus Sicht des Softwareentwicklers bzw. Verteidigers, sondern aus Sicht eines Angreifers betrachtet. Dies ermöglicht es, potenzielle Schwachstellen frühzeitig zu erkennen und gezielt zu mitigieren.

1. **Scoping**
   Zunächst muss das zu analysierende System und dessen Umfang im Vorfeld der Modellierung festgelegt und verstanden werden. Dies umfasst die Erstellung von Datenflussdiagrammen (DFDs), in denen Systemkomponenten, Datenbewegungen, Schnittstellen und Vertrauensgrenzen dargestellt werden. Innerhalb dieses Schritts werden insbesondere Einstiegspunkte für Angreifer, kritische Assets sowie unterschiedliche Berechtigungsniveaus identifiziert. Auf Basis dieser Vorarbeit können die realistischen Missbrauchsszenarien abgeleitet werden, die eine Grundlage für die effektive Bedrohungsanalyse bilden.

2. **Identifikation von Bedrohungen (STRIDE)**
   Die STRIDE-Methode kategorisiert Bedrohungen systematisch nach sechs Dimensionen:

   - **Spoofing Identity** – unberechtigte Identitätsanmaßung,
   - **Tampering** – Manipulation von Daten oder Prozessen,
   - **Repudiation** – fehlende Nachweisbarkeit von Handlungen,
   - **Information Disclosure** – unautorisierter Informationsabfluss,
   - **Denial of Service** – Einschränkung oder Ausfall von Diensten,
   - **Elevation of Privilege** – unberechtigter Privilegiengewinn.

   Durch die Zuordnung dieser Kategorien zu den in den identifizierten Assets lassen sich die konkreten Bedrohungsszenarien für die Software oder die IT-Systeme ableiten. Ergänzend kann die Einbindung von Angreifer-Frameworks wie MITRE ATT&CK [33] erfolgen, um realitätsnahe Angriffsmuster zu berücksichtigen (siehe Abbildung 5.1).

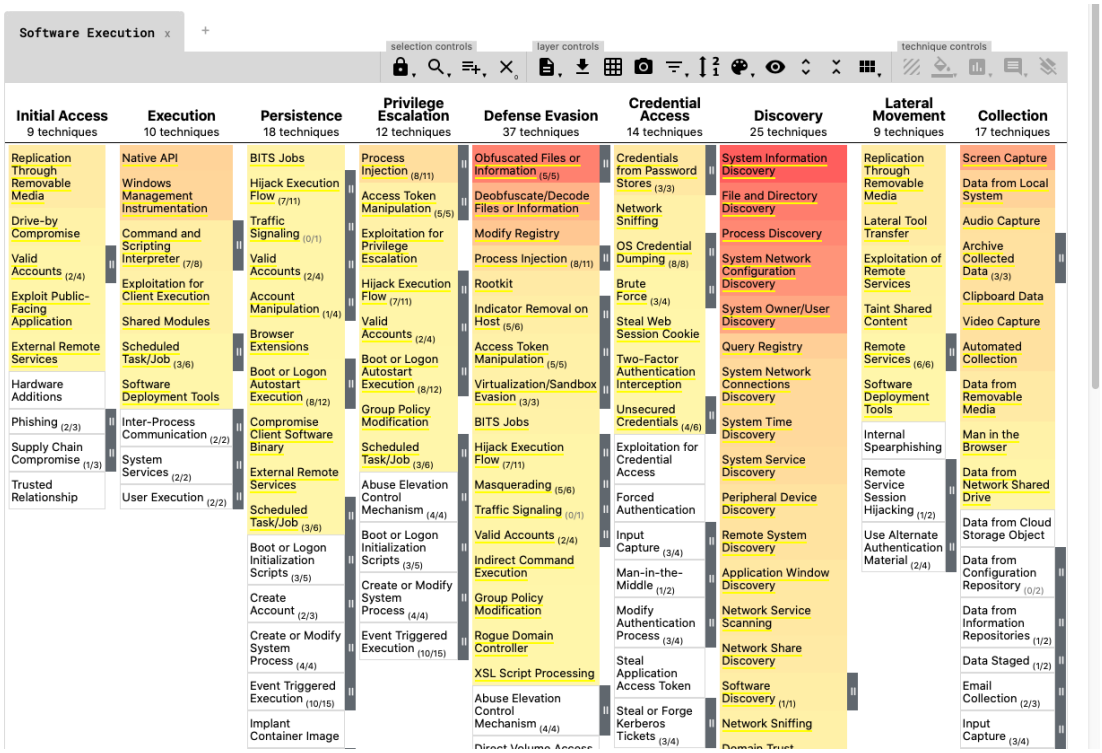


Abbildung 5.1: *Ausschnitt einer Übersicht über das MITRE Framework [34]*

3. **Risikobewertung und Gegenmaßnahmen**
   Die identifizierten Bedrohungen werden einer Risikoanalyse unterzogen, bei der Eintrittswahrscheinlichkeit, potenzieller Schaden und Kosten der Mitigation berücksichtigt werden. Auf Basis dieser Bewertung können die notwendigen Maßnahmen nach ihrer Wichtigkeit und der Einfachheit der Umsetzung priorisiert werden. Mögliche Behandlungsstrategien (Mitigationen) sind:

   - **Akzeptanz**: Belassen der Sicherheitslücke, wenn Risikowert als tolerierbar gilt
   - **Eliminierung**: Ausschließen des Risikos z. B. durch Verzicht auf unsichere Komponenten
   - **Minderung**: Verkleinerung des möglichen Risikoeintritts oder des zu erwartenden Schadens etwa durch zusätzliche Kontrollen wie Input-Validierung oder Verschlüsselung
   - **Übertragung**: Transfer des Risikos auf einen anderen Risikoträger, der sich um die Mitigation des Risikos kümmert, wie beispielsweise durch Dienstleisterverträge oder Versicherungen

4. **Review und Iteration**
   Der Bedrohungsmodellierungsprozess muss kontinuierlich überprüft und nach wesentlichen Änderungen im System erneut durchgeführt werden. Dies gilt insbesondere nach größeren Architekturänderungen, Releases oder der Integration neuer Abhängigkeiten. Regelmäßige Reviews stellen sicher, dass identifizierte Risiken dokumentiert, kontrolliert und durch wirksame Gegenmaßnahmen adressiert bleiben.

5.3.1.2 Praktische Relevanz für den CRA

Die regelmäßige Durchführung von Risikoanalysen mittels Threat Modeling und insbesondere der STRIDE-Methode ermöglicht es Unternehmen, den Anforderungen des CRA in Bezug auf die Bewertung der Sicherheit in allen Phasen des Lebenszyklus (Art. 10 Abs. 2 CRA) nachzukommen. Darüber hinaus stellt die strukturierte Dokumentation der Ergebnisse sicher, dass Nachweispflichten gegenüber Aufsichtsbehörden und Auditoren erfüllt werden können. Damit trägt die konsequente Implementierung von Security by Design Maßnahmen in den Softwarelebenszyklus durch Threat Modeling nicht nur zur Minimierung von Schwachstellen und Angriffsmöglichkeiten bei, sondern unterstützt Unternehmen auch unmittelbar bei der Erreichung regulatorischer Konformität und der nachhaltigen Verbesserung der Produktqualität.

5.3.2 Schwachstellenmanagement

Ein effektives Schwachstellenmanagement ist ein zentraler Bestandteil der Erfüllung der Anforderungen des CRA. Es verfolgt das Ziel, Sicherheitslücken frühzeitig zu erkennen,

deren Schweregrad zu bewerten und angemessene Gegenmaßnahmen einzuleiten. Hierbei gilt das Prinzip, dass Schwachstellen im Idealfall bereits während der Entwicklung automatisiert identifiziert und behoben werden, bevor sie in produktiven Systemen ausgenutzt werden können.

5.3.2.1 Kontinuierliches Scanning

Zur frühzeitigen Erkennung von Schwachstellen ist ein kontinuierliches Scanning erforderlich. Dies schließt sowohl Entwicklungs- als auch Produktionsumgebungen ein:

- **Während der Entwicklung:** Integrierte Sicherheitsprüfungen in der CI/CD-Pipeline (z. B. durch statische und dynamische Analysen, Software Composition Analysis und Container Scans) stellen sicher, dass Schwachstellen so früh wie möglich erkannt werden. Dies reduziert den Aufwand für Nachbesserungen erheblich.
- **In produktiven Systemen:** Laufende Infrastruktur- und Applikationsscans sorgen dafür, dass auch im Betrieb neue Bedrohungen erkannt und schnell adressiert werden können. Hierbei ist vor allem eine automatisierte Integration in zentrale Monitoring-Systeme sinnvoll.

5.3.2.2 Zentrales Schwachstellenmanagement

Alle erkannten Schwachstellen sollten in einem zentralen Schwachstellenmanagement-System (Vulnerability Management System, VMS) erfasst werden. Ein solches System ermöglicht:

1. die **Konsolidierung** aller gefundenen Schwachstellen aus unterschiedlichen Quellen (z. B. SAST, DAST, SCA, Infrastruktur-Scanner),
2. die **Priorisierung und Bewertung** nach Schweregrad, Ausnutzbarkeit und potenziellen Auswirkungen,
3. die **Nachvollziehbarkeit** der Maßnahmen, die zur Behebung eingeleitet wurden.

Besonders wichtig ist die Durchführung einer detaillierten Schwachstellen-Bewertung (Reachability-Analyse). Diese Analyse stellt sicher, dass nicht nur potenziell vorhandene Schwachstellen erfasst, sondern auch deren tatsächliche Ausnutzbarkeit durch den Angreifer im spezifischen Kontext des Systems, spezieller beim Aufruf der jeweiligen Komponenten-Funktion durch die Software selbst, bewertet wird. So wird vermieden, Ressourcen in Form von Arbeitskraft durch den Entwickler in die Behandlung theoretischer, aber praktisch irrelevanter Schwachstellen zu investieren.

5.3.2.3 Scanning-Pipeline im Entwicklungsprozess

Die Integration von Scanning-Mechanismen in den Entwicklungsprozess kann sich an den Empfehlungen der OWASP DevSecOps Guideline orientieren. Diese beschreibt, wie Sicherheitsmaßnahmen von Beginn an im Sinne einer Shift-Left-Security in die Entwicklungsprozesse, vor allem auf der technischen Ebene, implementiert werden können. Relevante Schritte sind [18] :

1. **Pre-Commit-Prüfungen:** Automatische Scans auf Secrets, unsicheren Code und Verstöße gegen Coding-Guidelines, bevor der Code in das Repository übernommen wird.
2. **Automatisiertes Vulnerability Scanning:** Integration von SAST, DAST, IAST, SCA, Infrastruktur- und Container-Scans in die Build- und Deployment-Pipelines (CI/CD Pipelines).
3. **Threat Modeling:** Systematische Bedrohungsanalyse (z. B. via STRIDE vgl. 2) pro Entwicklungsiteration, um neu eingeführte Risiken frühzeitig zu identifizieren.
4. **Kontinuierliche Überwachung:** Laufende Scans in produktiven Umgebungen, die mit den Ergebnissen der Entwicklungstests konsolidiert werden.

Das OWASP DevSecOps Maturity Model kann ergänzend eingesetzt werden, um den Reifegrad der implementierten Prozesse zu messen und schrittweise zu verbessern. Dadurch wird ein kontinuierlicher Verbesserungsprozess ermöglicht, der sich an internationalen Best Practices orientiert. [35], [36]

5.3.2.4 Endgültige Abnahmen und Bewertungen

Um die Sicherheit, nach dem Prozess der Schwachstellenbehandlung nachhaltig zu gewährleisten, sollten Schwachstellenprozesse mit klar definierten Abnahme- und Review-Schritten versehen sein. Diese umfassen:

- Die technische Verifizierung, ob die Schwachstelle tatsächlich behoben wurde. Dies kann in Form eines erneuten Schwachstellen-Scans und einem anschließenden Ergebnisabgleich erfolgen.
- Eine erneute Risikobewertung nach der Mitigation, sollte die Schwachstelle nicht vollends beseitigt werden können.
- Die Dokumentation der geschlossenen Schwachstellen im innerhalb des Schwachstellenmanagment-Logs für eine kontinuierliche Nachweisbarkeit und Auditierbarkeit.
- Die formale Freigabe der fertigen Software durch eine verantwortliche Stelle (z. B. Security Governance oder CISO). Dies ist insbesondere wichtig, sollten Sicherheitslücken per Risiko-Akzeptanz behandelt werden.

Ein gut aufgebautes Schwachstellenmanagement kombiniert automatisierte Security-Scans in der CI/CD Pipeline, zentrale Konsolidierung der Ergebnisse, Schwachstellen-Bewertungen wie etwa eine Reachability-Analyse sowie formale Abnahmen. In Verbindung mit einer DevSecOps-Arbeitsweise nach den OWASP-Guidelines wird sichergestellt, dass Schwachstellen systematisch und proaktiv über den gesamten Lebenszyklus hinweg erkannt, bewertet und geschlossen werden können. Dies stellt nicht nur die Konformität zum CRA sicher, sondern verbessert auch nachhaltig und in weiten Teilen automatisiert die Sicherheit und Vertrauenswürdigkeit der eingesetzten Softwareprodukte. [18]

5.3.3 SBOM

Eine SBOM muss gemäß der eigens zum Zweck der Erreichung einer CRA-Konformität entwickelten technischen Richtlinie BSI TR-03183 bestimmte Mindestinformationen enthalten, die sich nach dem jeweiligen Detaillierungsgrad der Komponenten richten. Ziel ist es, die Nachvollziehbarkeit von Abhängigkeiten innerhalb der Lieferkette zu gewährleisten und die automatisierte Verarbeitung zu ermöglichen. [26]

5.3.3.1 Geforderte Detailtiefe

Für eine konforme SBOM ist eine rekursive Auflösung aller Abhängigkeiten sämtlicher im Lieferumfang der Software enthaltenen/ verwendeten Komponente erforderlich. Diese geforderte Auflösung muss mindestens bis zur ersten Software-Komponente erfolgen, die nicht mehr Bestandteil des Lieferumfangs ist. Komponenten außerhalb des Lieferumfangs müssen mindestens als identifizierte Komponenten gekennzeichnet werden, um eine eindeutige Referenzierung zwischen verschiedenen SBOMs, wie etwa der SBOM des betrachteten Liefergegenstands und der SBOM der verwendeten Compiler oder Betriebsumgebungen, zu ermöglichen. [26]

Falls der Primärkomponente der Software mehrere Instanzen derselben Komponente mit unterschiedlichen Metainformationen zugeordnet sind, müssen alle Instanzen mit ihren individuellen Metadaten separat aufgeführt werden. Die SBOM kann auf die SBOMs der in der Software verwendeten Komponenten referenzieren, anstatt deren Informationen komplett zu integrieren, sofern diese referenzierten SBOMs ebenfalls konform zu den Anforderungen des CRAs an die SBOM Erstellung sind. Dabei trägt der Anbieter der Primärkomponenten-SBOM die Verantwortung für die Verfügbarkeit dieser referenzierten SBOMs. [26]

Die Reihenfolge zur Bestimmung der Datenfelder, die in einer SBOM aufzuzeichnen sind, ist wie folgt festgelegt [26]:

1. Referenzierte Komponenten

2. Identifizierte Komponenten
3. Vollständig beschriebene Komponenten

5.3.3.2 Erforderliche Datenfelder der SBOM selbst

Jede SBOM muss mindestens folgende Informationen enthalten [26]:

- **Ersteller der SBOM**: E-Mail-Adresse der erstellenden Entität oder alternativ eine URL, z. B. zur Homepage des Projekts.
- **Zeitstempel**: Datum und Uhrzeit der SBOM-Erstellung, empfohlen in UTC.

5.3.3.3 Erforderliche Datenfelder jeder Komponente

Für jede in der SBOM enthaltene Komponente müssen mindestens die folgenden Angaben erfasst werden [26]:

- **Komponenten-Ersteller**: E-Mail-Adresse oder URL des Erstellers bzw. Maintainers der Komponente.
- **Komponenten-Name**: Name der Komponente oder alternativ der Dateiname.
- **Komponenten-Version**: Version gemäß den Vorgaben des Erstellers; falls nicht vorhanden, das Änderungsdatum der Datei.
- **Dateiname der Komponente**: Tatsächlicher Dateiname der Komponente.
- **Abhängigkeiten**: Auflistung aller direkt abhängigen Komponenten oder enthaltener Unterkomponenten.
- **Distributionslizenzen**: Lizenzen, unter denen die Komponente genutzt werden darf.
- **Hashwert der deploybaren Komponente**: SHA-512 Prüfsumme der deploybaren Datei.
- **Ausführbare Eigenschaft**: Angabe, ob die Komponente ausführbar ist.
- **Archiv-Eigenschaft**: Angabe, ob die Komponente ein Archiv ist.
- **Strukturierte Eigenschaft**: Angabe, ob die Komponente strukturiert ist, d. h. Metadaten der enthaltenen Inhalte verfügbar sind.

5.3.3.4 Zusätzliche Datenfelder

Zusätzlich muss jede SBOM die URI der SBOM enthalten, sofern verfügbar. Für jede Komponente können weitere Datenfelder bereitgestellt werden [26]:

- **Source-Code-URI**: URI des Quellcodes der Komponente oder Repository-URL.
- **URI der deploybaren Komponente**: Direktlink zur deploybaren Version der Komponente.
- **Weitere eindeutige Kennungen**: z. B. CPE oder Package-URL.
- **Originallizenzen**: Vom Ersteller vergebene Lizenzinformationen.

5.3.3.5 Optionale Datenfelder

Optional können weitere Informationen aufgenommen werden, wenn diese verfügbar sind [26]:

- **Effektive Lizenz**: Lizenz, unter der die Komponente aktuell durch den SBOM-Ersteller genutzt wird.
- **Hashwert des Quellcodes**: Prüfsumme des Quellcodes der Komponente.
- **URL der security.txt**: URL zur Sicherheitsinformation des Komponentenerstellers.

Diese Struktur stellt sicher, dass SBOMs alle relevanten Informationen zur Nachverfolgbarkeit, Lizenzkonformität und Integrität der Softwarekomponenten enthalten. Dabei können die unterschiedlichen Detailstufen an die Komplexität der Darstellung und die jeweiligen Anforderungen angepasst werden. [26]

5.3.4 Schwachstellenkommunikation (Disclosure)

Ein weiterer Bestandteil, der notwendig ist, um die Anforderungen des CRA zu erfüllen ist eine transparente und nachvollziehbare Kommunikation neu entdeckter Schwachstellen gegenüber den Kunden, Nutzern und der breiteren Öffentlichkeit. Hersteller müssen Prozesse etablieren, die sowohl die rechtzeitige Meldung von Schwachstellen innerhalb der eigenen Produkte, als auch einen strukturierten Informationsablauf sicherstellen, um betroffene Parteien in die Lage zu versetzen, angemessene Gegenmaßnahmen zu ergreifen.

5.3.4.1 Etablierter Kommunikationsprozess

Für die konforme und koordinierte Schwachstellenkommunikation bietet es sich an, einen klar definierten und dokumentierten Prozess einzuführen, der auf den Prinzipien der Coordinated Vulnerability Disclosure (CVD) basiert. Ein möglicher Ablauf kann wie folgt gestaltet werden:

1. **Erkennung und Verifizierung**: Sobald eine Schwachstelle entdeckt oder gemeldet wurde, erfolgt eine technische Prüfung und Bewertung des Schweregrads.
2. **Kommunikation mit Kunden und Nutzern**: Hersteller sollten primär direkte Kommunikationskanäle wie E-Mail-Verteiler oder Kundenportale nutzen und auf ein standardisiertes Format der Schwachstellenbeschreibung zurückgreifen. Für eine standardisierte Weitergabe eignet sich das Vulnerability Exploitability eXchange (VeX)-Format, das beschreibt, ob und in welchem Umfang ein Produkt von einer bekannten Schwachstelle betroffen ist. Dadurch wird eine schnelle Risikobewertung durch die Nutzer unterstützt. Die Dokumentation der Schwachstelle sollte in einem etablierten Format wie dem CSAF erfolgen. CSAF erlaubt wie in 2.3.1 beschrieben eine strukturierte, maschinenlesbare Beschreibung der Schwachstelle, ihrer Auswirkungen sowie der verfügbaren Abhilfemaßnahmen. [27], [28]
3. **Veröffentlichung und kontinuierliche Aktualisierung**: Nach erfolgter Koordination wird die Schwachstelle öffentlich dokumentiert. Aktualisierungen oder Patches müssen zeitnah kommuniziert und über die gleichen Kanäle verteilt werden.

5.3.4.2 Meldung an Datenbanken

Neben der direkten Kundenkommunikation ist die Veröffentlichung in internationalen und europäischen Schwachstellendatenbanken von zentraler Bedeutung.

- **NIST-NVD (National Vulnerability Database)**: Hersteller können Schwachstellen über einen CVE Numbering Authority (CNA)-Partner registrieren lassen oder selbst als CNA auftreten. Nach erfolgreicher Registrierung einer CVE-ID wird die Schwachstelle in die NIST-NVD-Datenbank übernommen, wo sie maschinenlesbar und standardisiert zur Verfügung steht. [37]
- **ENISA European Vulnerability Database (EUVD)**: Im europäischen Kontext wird durch ENISA eine eigene Schwachstellendatenbank aufgebaut, die in engem Austausch mit MITRE und anderen CVE-Betreibern steht. Hersteller sowie CSIRTs können dort Schwachstellen im Rahmen einer koordinierten Offenlegung registrieren und veröffentlichen. Die EUVD stellt sicher, dass innerhalb der Europäischen Union eine zentrale Plattform für Schwachstelleninformationen verfügbar ist, die den Vorgaben der NIS2-Richtlinie entspricht. [38]

Durch die parallele Veröffentlichung in NIST-NVD und EUVD wird sowohl eine internationale Sichtbarkeit, als auch die Erfüllung europäischer regulatorischer Anforderungen sichergestellt. Unternehmen sollten daher Prozesse etablieren, die eine Meldung an beide Plattformen vorsehen, um eine umfassende Transparenz und Konsistenz in der Schwachstellenkommunikation zu gewährleisten.

Ein standardisierter Disclosure-Prozess, der auf CSAF für strukturierte Meldungen, VeX für die konkrete Produktbetroffenheit sowie NIST-NVD und EUVD für die öffentliche Dokumentation setzt, ermöglicht eine einheitliche und nachvollziehbare Schwachstellenkommunikation. Damit können Hersteller nicht nur regulatorische Anforderungen des CRA erfüllen, sondern gleichzeitig auch das Vertrauen ihrer Kunden und Nutzer in die Sicherheit und Verlässlichkeit ihrer Produkte stärken.

5.3.5 Schwachstellenmeldung von extern

Ebenfalls zentraler Bestandteil zur Erfüllung der Anforderungen des CRA ist die Etablierung klarer und verlässlicher Prozesse zur Meldung von Schwachstellen. Hierbei muss zwischen der internen Behandlung von Schwachstellen und der externen Meldung durch Dritte unterschieden werden.

5.3.5.1 Responsible Disclosure an das Unternehmen

Die sichere und strukturierte Bearbeitung von Schwachstellenmeldungen ist ein wesentlicher Bestandteil der vom CRA, aber auch von anderen Regularien geforderten Cyber-Resilienz von Herstellern und Produkten. Die technische Richtlinie des BSI TR-03183 definiert hierzu verbindliche Mindestanforderungen, die Hersteller erfüllen müssen, um einen konformen Prozess zur Annahme von Schwachstellenmeldungen zu etablieren. Die Richtlinie fordert, dass alle implementierten Maßnahmen, Testverfahren und Testergebnisse dokumentiert werden, um die Nachvollziehbarkeit und Auditierbarkeit des Prozesses sicherzustellen. Ergänzend zu den Mindestanforderungen können Hersteller zusätzliche Maßnahmen ergreifen, beispielsweise durch weitere Angaben in der security.txt, auf der Webseite für eingehende Meldungen oder in der Coordinated Vulnerability Disclosure (CVD) Policy. [39]

5.3.5.2 Vorbereitende Maßnahmen für den CVD-Prozess

Für eine effiziente Bearbeitung von Schwachstellenmeldungen müssen Hersteller zwei zentrale Rollen etablieren [39]:

- **Product Security Incident Response Team(PSIRT):** Zuständig für die Bearbeitung von Schwachstellen in Produkten und Dienstleistungen.

- **Computer Security Incident Response Team (CSIRT):** Zuständig für die Bearbeitung von Schwachstellen in der Infrastruktur des Herstellers.

Beide Rollen müssen eigene Kontaktmöglichkeiten (z. B. E-Mailpostfächer) besitzen, getrennt personell besetzt sein (außer bei kleinen Unternehmen) und miteinander eng kommunizieren. Für die E-Mail-Kommunikation müssen dedizierte OpenPGP-Schlüssel bereitgestellt werden. Zudem müssen den Rollen ausreichend personelle Ressourcen zur Verfügung gestellt werden, um die garantierten Reaktionszeiten gemäß der CVD-Policy einzuhalten. [39]

5.3.5.3 Website des Herstellers

Hersteller müssen eine öffentlich zugängliche Website betreiben, auf der mindestens sicherheitsrelevante Informationen zu ihrem Unternehmen und deren Produkten bereitgestellt werden. Diese Informationen müssen ohne jegliche Zugangsbeschränkungen für jeden Internetnutzer zugänglich sein. Alle sicherheitsrelevanten Inhalte, inklusive der CVD-Policy und einer Möglichkeit für das Einreichen einer Schwachstellenmeldung, müssen in einer für Nutzer und Marktüberwachungsbehörden leicht verständlichen Sprache bereitgestellt werden. [39]

5.3.5.4 Security.txt nach RFC 9116

Um den Meldern von Schwachstellen die Kontaktaufnahme zu erleichtern, muss auf der Herstellerwebsite eine sogenannte security.txt-Datei nach RFC 9116 bereitgestellt werden. Die security.txt muss folgende Anforderungen erfüllen [39]:

- **Lokalisierung:** Die security.txt muss über den der Website angehängten Pfad /.well-known/security.txt bereitgestellt und über HTTPS abrufbar sein. Sie muss als ASCII- oder UTF-8-codierte Textdatei vorliegen.
- **Kannonische-URI:** Der Hersteller muss die kanonische URI angeben, die direkt (ohne Redirects) auf die security.txt verweist.
- **Kontaktinformationen:** Die security.txt muss eine Liste von Kontaktmöglichkeiten enthalten, beginnend mit der Kontaktmöglichkeit des PSIRT, gefolgt von der Kontaktmöglichkeit zum CSIRT und optional der URI der Webseite für eingehende Meldungen.
- **OpenPGP-Schlüssel:** Die Verschlüsselungsoptionen für die sichere Kommunikation müssen bereitgestellt werden, inklusive Web-URI der öffentlichen Schlüssel im ASCII-Format und Angabe der Fingerprints.

- **Anerkennung und bevorzugte Sprachen:** Die security.txt sollte eine Web-URI für die Danksagungen an Meldende und die bevorzugten Sprachen für Meldungen enthalten (mindestens Englisch).
- **CVD-Policy und Sicherheitswarnungen:** Die security.txt muss die URI der CVD-Policy und optional CSAF-Sicherheitswarnungen enthalten.
- **Ablaufdatum:** Die security.txt muss ein Ablaufdatum gemäß RFC 3339 enthalten, maximal ein Jahr in der Zukunft, und vierteljährlich überprüft werden.
- **Digitale Signatur:** Die security.txt muss mit OpenPGP digital signiert werden, wobei dedizierte Schlüssel genutzt werden sollten und die Signatur den Anforderungen der aktuellen BSI-Richtlinien (BSI TR-03116-4 [40]) entspricht.
- **Automatische Auffindbarkeit:** Die security.txt muss für Web-Crawler auffindbar sein, um automatisierte Entdeckung durch Plattformen wie etwa findsecurity-contacts.com zu ermöglichen.

5.3.5.5 Webformular für Schwachstellenmeldungen

Hersteller müssen ein zentrales Webformular für die Einreichung von Schwachstellenmeldungen bereitstellen, das anonym nutzbar und mindestens in englischer Sprache verfügbar ist. Das Formular sollte den Nutzer strukturiert durch die Meldung führen und eine hohe Verfügbarkeit gewährleisten. [39]

5.3.5.6 CVD-Policy

Die CVD-Policy beschreibt den gesamten Prozess der Bearbeitung von Schwachstellenmeldungen und enthält[39]:

- Sichtbarkeit des letzten Änderungsdatums und eindeutige Zuweisung zur Herstellerorganisation.
- Jährliche Überprüfung und Aktualisierung der Policy.
- Benachrichtigung des nationalen CSIRT bei aktiv ausgenutzten Schwachstellen.
- Bereitstellung der Kontaktinformationen der funktionalen Mailboxen.
- Zusicherung der Vertraulichkeit, Schutz personenbezogener Daten und keine Verfolgung der meldenden Person bei Einhaltung der Richtlinien.
- Veröffentlichung validierter Schwachstellen innerhalb von 90 Tagen oder in Abstimmung mit nationalen CSIRTs, gegebenenfalls auf der European Vulnerability Database.

5.3.5.7 Kommunikationsanforderungen und garantierte Reaktionszeiten

Hersteller müssen sicherstellen, dass eingehende Meldungen innerhalb von fünf Arbeitstagen eine erste Rückmeldung und innerhalb von zehn Arbeitstagen ein detailliertes Feedback erhalten. Es muss die Möglichkeit bestehen, Meldungen anonym einzureichen, wobei der Umfang der Bearbeitung eingeschränkt sein kann. Während des gesamten CVD-Prozesses müssen Hersteller einen vertrauensvollen Austausch mit den meldenden Personen gewährleisten, inklusive Empfehlungen zur verschlüsselten und signierten Kommunikation. [39]

5.3.5.8 Webseite für eingehende Meldungen

Eine zentrale Webseite für eingehende Meldungen muss folgende Anforderungen erfüllen [39]:

- Leicht auffindbar, ohne Login oder Client-Script-Restriktionen.
- Klar strukturierte Darstellung aller relevanten Informationen.
- Einfach zugänglicher Link zur CVD-Policy.
- Veröffentlichung der Kontaktoptionen inklusive der OpenPGP-Schlüssel-URIs und deren Fingerprints.
- Angabe des Ablaufdatums der Kontaktinformationen, maximal ein Jahr im Voraus.

Die Einhaltung dieser Anforderungen gewährleistet eine effiziente, sichere und nachvollziehbare Verarbeitung von Schwachstellenmeldungen sowie eine transparente und vertrauenswürdige Kommunikation mit meldenden Entitäten. [39]

5.3.6 Versionierung

Eine einheitliche und nachvollziehbare Versionierung ist ein wesentliches Element, um die Anforderungen des CRA zu erfüllen. Sie gewährleistet die eindeutige Identifikation von Softwareständen und ermöglicht somit eine transparente Zuordnung von Schwachstellen, Patches und Sicherheitsupdates. Insbesondere im Hinblick auf die Nachvollziehbarkeit sicherheitsrelevanter Änderungen ist eine konsistente Versionierung unerlässlich.

Ein in der Praxis weit verbreiteter und bewährter Standard ist das Semantic Versioning in der Version 2.0.0. Das Modell basiert auf einem dreiteiligen Versionsschema `MAJOR.MINOR.PATCH` und folgt klaren Regeln [41]:

- **MAJOR** (X.y.z): Erhöhung bei inkompatiblen Änderungen der API oder wesentlichen funktionalen Umstellungen.

- **MINOR** (x.Y.z): Erhöhung bei abwärtskompatiblen Funktionserweiterungen.
- **PATCH** (x.y.Z): Erhöhung bei abwärtskompatiblen Fehler- und Sicherheitsbehebungen.

Zusätzlich erlaubt Semantic Versioning die Verwendung von Pre-Release-Kennzeichnungen (z. B. `1.0.0-alpha`) sowie Build-Metadaten (z. B. `1.0.0+build201`), die insbesondere in Entwicklungs- und Testphasen eine klare Unterscheidung ermöglichen.

Die Anwendung von Semantic Versioning 2.0.0 bringt für die Praxis mehrere Vorteile:

1. **Transparenz und Nachvollziehbarkeit:** Nutzer, Auditoren und Aufsichtsbehörden können auf Basis der Version unmittelbar erkennen, ob es sich um funktionale Erweiterungen, sicherheitsrelevante Patches oder grundlegende Änderungen handelt.
2. **Sicherheitsrelevante Updates:** Durch die konsistente Erhöhung der PATCH-Version können sicherheitskritische Änderungen eindeutig gekennzeichnet und schnell kommuniziert werden.
3. **Kompatibilitätsmanagement:** Das klare Regelwerk unterstützt Entwickler und Nutzer bei der Einschätzung, ob eine Aktualisierung ohne Anpassungen vorgenommen werden kann oder ob größere Umstellungen erforderlich sind.
4. **Automatisierbarkeit:** Durch die Sortierbarkeit der jeweiligen Versionen fällt eine Automatisierbarkeit weiterer sich anschließender Prozesse in der Praxis deutlich leichter.

Um die CRA-Anforderungen zu erfüllen, muss Semantic Versioning konsequent und projektübergreifend angewendet werden. Nur so ist eine eindeutige Zuordnung von Schwachstellen zu spezifischen Softwareständen möglich und eine transparente Dokumentation der vorgenommenen Änderungen kann gewährleistet werden. Darüber hinaus sollte die Versionierung eng mit der technischen Dokumentation sowie gegebenenfalls mit einer Software Bill of Materials (SBOM) verknüpft sein, um die geforderte Rückverfolgbarkeit vollständig sicherzustellen.

Die Implementierung von Semantic Versioning 2.0.0 ist somit nicht nur eine bewährte Praxis im Software-Engineering, sondern zugleich ein zentraler Baustein zur Einhaltung der regulatorischen Anforderungen des CRA.

5.4 Limitationen der Studie

Wie jede empirische Untersuchung unterliegt auch die vorliegende Studie bestimmten Limitationen, die bei der Interpretation der Ergebnisse zu berücksichtigen

sind. Die Limitationen betreffen methodische Aspekte der Datenerhebung, die Zusammensetzung der Stichprobe sowie inhaltliche Einschränkungen der erhobenen Daten.

5.4.1 Methodische Limitationen

Die Methodik der Untersuchung bringt mehrere Einschränkungen mit sich. So entstand für die Erhebung der Daten ein umfangreicher Fragebogen mit insgesamt 35 Fragen (siehe 3.4). Die dadurch erhöhte Länge des Instruments und die damit einhergehende längere Bearbeitungszeit durch die Befragten führten in der Praxis vermutlich zu einer erhöhten Abbruchquote von insgesamt 74,2 %. Diese Abbruchquote stellt insofern eine Limitation der Untersuchung dar, da sie die Menge an verwertbaren, vollständigen Datensätzen stark reduziert. So wird eine Aussagekraft der Ergebnisse durch eine kleinere Anzahl der abgegebenen Antworten beeinträchtigt. Die Erhebung von Individualantworten war durch eine technische Beschränkung in Form einer vorgegebenen Zeichenanzahl innerhalb der Freitextfelder limitiert. Dadurch war es den Teilnehmenden nicht möglich, differenzierte und ausführliche Antworten abzugeben. Diese hätten möglicherweise ein tieferes Verständnis über organisationale Sicherheitsmaßnahmen ermöglicht. Hinzu kommt die Möglichkeit, dass Zeitrestriktionen seitens der Befragten dazu führten, dass qualitative Angaben verkürzt oder gänzlich ausgelassen wurden. Diese Limitationen schränken die interpretative Tiefe der qualitativen Ergebnisse ein und verdeutlichen die Notwendigkeit, die vorliegenden Befunde stets im Kontext dieser Limitationen zu betrachten.

5.4.2 Stichprobenbezogene Limitationen

Ein weiterer in Bezug auf die Limitationen dieser Untersuchungen wichtiger Aspekt betrifft die Zusammensetzung und das Antwortverhalten der Gruppe der Befragten. Es ist davon auszugehen, dass die Befragten, die den relativ langen Fragebogen vollständig und ausführlich bearbeitet haben, ein überdurchschnittliches Interesse an den Themenbereichen Cybersecurity und dem CRA aufweisen. Dieses erhöhte Interesse kann sich möglicherweise in einer systematischen Verzerrung der Ergebnisse niederschlagen, da Personen mit geringerem Vorwissen oder einer geringeren Relevanzwahrnehmung die Befragung eher abbrachen und somit in den finalen Ergebnissen der Analyse unterrepräsentiert sind. In diesem Zusammenhang lässt sich auch die grundsätzliche Entscheidung zur Teilnahme an der Befragung interpretieren. Sie kann als Indikator dafür gewertet werden, dass bereits ein gewisses Maß an thematischem Vorwissen, Bewusstsein oder zumindest Interesse an dem Themengebiet der Untersuchung vorhanden war.

Die damit potenziell einhergehende begrenzte Zahl an vollständig abgeschlossenen Befragungen verstärkt diese Einschränkung zusätzlich. Die Ergebnisse sind daher primär im Kontext der untersuchten Stichprobe zu interpretieren und lassen sich nur eingeschränkt

auf die Grundgesamtheit der relevanten Zielgruppen wie etwa Softwareentwickler und Softwarearchitekten übertragen.

6 Fazit

In diesem Kapitel werden die zentralen Erkenntnisse der Arbeit zusammengefasst.

6.1 Zentrale Erkenntnisse

Die Arbeit und die ihr zugrunde liegende Untersuchung haben gezeigt, dass die Awareness bezüglich des Kommens des CRA zumindest bei den softwareentwicklungsnahen Berufsgruppen vorhanden ist. Damit handelt es sich zumindest nicht um eine Regulatorik, von der die betroffenen Unternehmen bei ihrem vollumfänglichen Inkrafttreten überrascht werden sollten. Was sich jedoch ebenfalls bei der Auswertung der Umfrageergebnisse gezeigt hat, ist, dass die Organisationen, die die Anforderungen des CRA erfüllen müssen, um ihre Softwareprodukte innerhalb der EU vertreiben zu können noch Lücken in deren Erfüllung aufweisen. Vor allem in den Bereichen Risikoanalyse, Schwachstellenmanagement, Kommunikation gefundener Schwachstellen an die Nutzenden, Meldung von extern gefundenen Schwachstellen an die Organisation selbst, Erstellung und Bereitstellung konformer SBOMs sowie Versionierung der Software selbst haben die Organisationen, in denen die Befragten tätig sind, noch Nachholbedarf. Um die Anforderungen, die durch den CRA gefordert werden möglichst effizient zu erfüllen, lässt sich wie in dieser Arbeit demonstriert, auf etablierte Best-Practices und technische Richtlinien zurückgreifen.

Der CRA stellt, wie in der Untersuchung des Dokuments zu erkennen war, eine bedeutende regulatorische Maßnahme dar, die die Cybersicherheit von Softwareprodukten in der Europäischen Union nachhaltig prägen und stark verbessern wird. Durch die Einführung der modernen und vor allem einheitlichen Sicherheitsanforderungen für Produkte mit digitalen Elementen auf der Softwareebene adressiert der CRA zentrale Herausforderungen der Softwareentwicklung. Von besonderer Relevanz ist hier die Konzeption von Sicherheitsmaßnahmen bereits in der Entwicklungsphase und deren Implementierung über den gesamten Produktlebenszyklus. Hier bietet der CRA einen guten Leitfaden, an dem sich die betroffenen Organisationen und Entwickelnden orientieren können, um ihren Kunden und Nutzenden sichere Produkte anbieten zu können. Der CRA sollte so von den zur Umsetzung der Anforderungen Betroffenen nicht lediglich als regulatorische Verpflichtung verstanden werden, sondern als Chance gesehen werden, die eigenen Entwicklungs- und Sicherheitsprozesse auf ein höheres Niveau zu heben. Organisationen, die frühzeitig entsprechende Maßnahmen implementieren, können hierdurch sowohl regulatorische

als auch aktuelle Sicherheitsrisiken minimieren als auch langfristig Wettbewerbsvorteile erzielen.

7 Ausblick

Dieses Kapitel gibt einen Ausblick auf die mögliche zukünftige Entwicklung des Forschungsfeldes und den Einfluss, den der CRA auf die europäische Cybersecurity-Landschaft haben kann.

7.1 Ausblick auf weiterführende Forschung und Entwicklungen

In den kommenden Jahren wird der CRA eine entscheidende Rolle spielen, da er bestehende Regulierungen im Bereich der Softwaresicherheit ergänzt und Lücken schließt. Die zukünftige wissenschaftliche Relevanz des untersuchten Themenfeldes ergibt sich maßgeblich daraus, dass der CRA bislang nicht vollständig in Kraft getreten ist und sich somit ein hohes Maß an Aktualität für die Forschung ergibt. Diese Aktualität impliziert zugleich ein erhebliches Potenzial für weiterführende wissenschaftliche Arbeiten, die auf den hier vorliegenden Ergebnissen aufbauen können. Im Zuge der sukzessiven Umsetzung und Veröffentlichung der Vorgaben bis zum 11. Dezember 2027 ist davon auszugehen, dass verstärkt Untersuchungen zum Kenntnisstand der betroffenen Akteure sowie zum Stand der praktischen Implementierung erfolgen werden. Dies betrifft einerseits die Unternehmen, die unmittelbar der Regulierung unterliegen, andererseits aber auch jene Organisationen, die begleitende Dienstleistungen wie Beratungsleistungen oder spezialisierte Sicherheitsprodukte im Kontext des CRA bereitstellen.

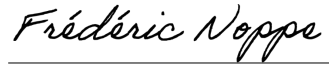
Von besonderem Interesse wird in diesem Zusammenhang die Analyse der Wirksamkeit der ergriffenen Maßnahmen sowie des jeweiligen Umsetzungsgrades sein. Aufbauend auf den hier dargestellten Ergebnissen erscheint es sinnvoll, diese künftigen Untersuchungen stärker zu fokussieren und spezifischer auszurichten. Wie in Kapitel 5.4 erläutert, bieten sich hierfür insbesondere differenzierte rein qualitative oder quantitative Forschungsansätze an. Während der in dieser Arbeit gewählte Mixed-Method-Ansatz vor allem für die Exploration des bisher weitgehend unerforschten Forschungsfeldes geeignet ist, kann eine vertiefte methodische Spezialisierung dazu beitragen, präzisere Aussagen über die Implementierungs- und Wirkungseffekte des CRA zu treffen. Die im Rahmen dieser Arbeit gewonnenen Ergebnisse stellen damit einen ersten Indikator für mögliche Entwicklungen dar. Auf dieser Grundlage lassen sich künftige Veränderungen nicht nur beobachten, sondern auch systematisch ableiten und in den wissenschaftlichen sowie praktischen Diskurs einordnen.

Im Bereich der Wirtschaft ist durch die Einführung der entsprechenden Maßnahmen eine Steigerung der Sicherheit der in der EU vertriebenen Software und der Produkte

mit digitalen Elementen zu erwarten. Dieses hohe Maß an Sicherheit kann einen entscheidenden positiven Einfluss auf die Produktqualität und die damit verbundene erhöhte Resilienz der in der EU eingesetzten IT-Systeme haben. So können durch das dadurch vermutete Ausbleiben von Schäden durch Cyberangriffe der EU-Binnenmarkt, aber auch die europäischen Unternehmen sowie deren Kunden durch die Vermeidung der mit diesen Angriffen verbundenen Kosten signifikant gestärkt werden. Ebenso können im Bereich der Cybersicherheit neue Wirtschaftszweige entstehen, in denen sich auch europäische Unternehmen als Zulieferer von Produkten und Dienstleistungen auf dem globalen Markt durch ihre hohe Qualität profilieren und somit wachsen können.

8 Eidesstattliche Erklärung

Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Die Stellen, die anderen Quellen dem Wortlaut oder dem Sinn nach entnommen sind, habe ich unter Angabe der Quellen kenntlich gemacht. Dies gilt sinngemäß auch für verwendete Zeichnungen, Skizzen, bildliche Darstellungen und dergleichen.



Bonn den 21. September 2025
Frédéric Noppe
Matrikelnummer: 1520686

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Die Lage der IT-Sicherheit in Deutschland 2024*. Die Lage der IT-Sicherheit in Deutschland 2024. 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html (besucht am 22. 12. 2024).

[2] *Cyber Resilience Act*. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. EU-Gesetzgebung zur Stärkung der Cybersicherheit von vernetzten Geräten und Software. 2024. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (besucht am 14. 10. 2024).

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Cybersicherheitswarnung 2021-234165-1032*. Cybersicherheitswarnung des BSI. 2021. URL: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-234165-1032.html (besucht am 14. 10. 2024).

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Cybersicherheitswarnung 2024-223608-1032*. Cybersicherheitswarnung des BSI. 2024. URL: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-223608-1032.pdf?__blob=publicationFile&v=3 (besucht am 14. 10. 2024).

[5] Liran Tal. *Maintainers of ESLint Prettier Plugin Attacked via npm Supply Chain Malware*. Snyk Blog. accessed: 2025-09-19. 2025. URL: https://snyk.io/blog/maintainers-of-eslint-prettier-plugin-attacked-via-npm-supply-chain-malware/.

[6] Infosecurity Magazine. *Open Source Community Thwarts Massive npm Supply Chain Attack Averted*. Infosecurity Magazine. accessed: 2025-09-19. 2025. URL: https://www.infosecurity-magazine.com/news/npm-supply-chain-attack-averted/.

[7] Melanie Staudacher. „Supply-Chain-Angriff trifft über 180 npm-Pakete: Wachsende Malware-Infektion“. In: *Security-Insider (Vogel Communications Group)* (2025). accessed: 2025-09-19. URL: https://www.security-insider.de/npm-pakete-supply-chain-angriff-malware-infektion-a-7058d3a07ba5184bbd66002da6001877/.

[8] Cybersecurity und Infrastructure Security Agency (CISA). *Known Exploited Vulnerabilities Catalog*. Online. Available: https://www.cisa.gov/known-exploited-vulnerabilities-catalog. 2024.

[9] IHK Mittlerer Niederrhein. *CE-Kennzeichnung*. https://mittlerer-niederrhein.ihk.de/de/wissenschaft-innovation/ce-kennzeichnung.html. Zugriff am 13. September 2025. 2025.

[10] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Cyber Resilience Act: Cybersicherheit EU-weit gedacht*. Online. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html. 2025.

[11] Fraunhofer SIT. *Der EU Cyber Resilience Act: Empfehlung zur Umsetzung technischer Anforderungen*. Available: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Whitepaper_CRA_EU-Cyber-Resilience-Act-Teil-II_v02c_digital.pdf?_=1731665657. 2023.

[12] Hans Brandt-Pook und Rainer Kollmeier. *Softwareentwicklung kompakt und verständlich. Wie Softwaresysteme entstehen*. 3. Aufl. 105 b/w illustrations, 3 illustrations in colour. Wiesbaden: Springer Vieweg, 2020, S. XI, 171. ISBN: 978-3-658-30631-1. DOI: 10.1007/978-3-658-30631-1. URL: https://doi.org/10.1007/978-3-658-30631-1.

[13] John F. Dooley. *Software Development, Design and Coding. With Patterns, Debugging, Unit Testing, and Refactoring*. 2. Aufl. 43 b/w illustrations, 22 illustrations in colour. Berkeley, CA: Apress, 2017, S. XXII, 320. ISBN: 978-1-4842-3153-1. DOI: 10.1007/978-1-4842-3153-1. URL: https://doi.org/10.1007/978-1-4842-3153-1.

[14] Philipp Winniewski. *Grundlagenwissen der Software-Entwicklung. IT-Konzepte und Fachbegriffe für das Projektmanagement*. 1. Aufl. IT kompakt. 3 b/w illustrations. Wiesbaden: Springer Vieweg, 2024, S. XI, 175. ISBN: 978-3-658-42659-0. DOI: 10.1007/978-3-658-42659-0. URL: https://doi.org/10.1007/978-3-658-42659-0.

[15] Eberhard Hechler, Martin Oberhofer und Thomas Schaeck. *Einsatz von KI im Unternehmen: IT-Ansätze für Design, DevOps, Governance, Change Management, Blockchain und Quantencomputing*. 1. Aufl. Berkeley, CA: Springer Vieweg, 2023, S. XXVI, 360. ISBN: 978-1-4842-9565-6. DOI: https://doi-org.printkr.hs-niederrhein.de:2443/10.1007/978-1-4842-9566-3.

[16] RedHat. *Was ist DevOps?* Apr. 2018. URL: https://www.redhat.com/de/topics/devops.

[17] Jürgen Halstenberg, Bernd Pfitzinger und Thomas Jestädt. *DevOps: Ein Überblick*. 1. Aufl. essentials. Wiesbaden: Springer Vieweg, 2020, S. X, 52. ISBN: 978-3-658-31404-0. DOI: https://doi-org.printkr.hs-niederrhein.de:2443/10.1007/978-3-658-31405-7.

[18] OWASP. *DevSecOps Guideline*. https://github.com/OWASP/DevSecOpsGuideline. accessed: 2025-09-19. 2025.

[19] IBM. *What is DevSecOps?* IBM Think Topics. accessed: 2025-09-19. 2025. URL: https://www.ibm.com/think/topics/devsecops.

[20] Murugiah Souppaya, Karen Scarfone und Donna Dodson. *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*. Special Publication SP 800-218. accessed: 2025-09-19. NIST, 2022. URL: https://csrc.nist.gov/pubs/sp/800/218/final.

[21] Microsoft. *Microsoft Security Development Lifecycle (SDL)*. https://learn.microsoft.com/de-de/compliance/assurance/assurance-microsoft-security-development-lifecycle. accessed: 2025-09-19; last updated: May 23, 2024 :contentReference[oaicite:0]index=0. 2024.

[22] Niklaus Schild und Alexander Neumann. „Sichere Softwareentwicklung nach dem "Security by Design"-Prinzip". In: *heise online* (2009). accessed: 2025-09-19. URL: https://www.heise.de/hintergrund/Sichere-Softwareentwicklung-nach-dem-Security-by-Design-Prinzip-403663.html.

[23] *EU NIS-2 Richtlinie*. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022L2555-20221227. Überarbeitete EU-Richtlinie zur Sicherheit von Netz- und Informationssystemen. 2022. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022L2555-20221227 (besucht am 14. 10. 2024).

[24] The MITRE Corporation. *Common Weakness Enumeration (CWE)*. https://cwe.mitre.org/. Website last updated August 19, 2025. MITRE, 2025.

[25] The MITRE Corporation. *Common Vulnerabilities and Exposures (CVE)*. https://www.cve.org/. Authentic reference for publicly known information-security vulnerabilities and exposures; maintained by MITRE, a U.S. cybersecurity FFRDC operated entity. MITRE, 2025.

[26] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Technical Guideline BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products, Part 2: Software Bill of Materials (SBOM)*. Technical Guideline TR-03183-2. Version 2.1.0. Bonn, Germany: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2025. URL: https://bsi.bund.de/dok/TR-03183-en.

[27] Langley Rock, Stefan Hagen und Thomas Schmidt. *Common Security Advisory Framework, Version 2.0*. OASIS Standard. OASIS, Nov. 2022. URL: https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html.

[28] Nicole Segerer. *Vulnerability Disclosure Report (VDR) und Vulnerability Exploitability eXchange (VEX)*. Abgerufen am 8. September 2025. 2024. URL: https://www.embedded-software-engineering.de/vulnerability-disclosure-report-vdr-und-vulnerability-exploitability-exchange-vex-a-8c00228d78bb991cfba596733ed9d5e2/ (besucht am 08. 09. 2025).

[29] Steven Arzt u. a. *Der EU Cyber Resilience Act: Empfehlung zur Umsetzung technischer Anforderungen*. Techn. Ber. Version 1.0. Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE. Darmstadt: Fraunhofer-Institut für Sichere Informationstechnologie SIT, 2024.

[30] Europäische Kommission. *Cyber Resilience Act: Annexes 1 to 6. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020*. COM(2022) 454 final. Brüssel, 2022. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM:2022:454:FIN.

[31] Ahmad Nauman Ghazi u. a. „Survey Research in Software Engineering: Problems and Mitigation Strategies“. In: *IEEE Access* 7 (2019), S. 24703–24718. DOI: 10.1109/ACCESS.2018.2881041.

[32] Marco Torchiano u. a. „Lessons Learnt in Conducting Survey Research“. In: (Feb. 2017). DOI: 10.48550/arXiv.1702.05744.

[33] MITRE ATT&CK. *MITRE ATT&CK Navigator Example*. Accessed: 11. Sept. 2025. n.d. URL: https://attack.mitre.org/.

[34] MITRE ATT&CK. *MITRE ATT&CK Navigator Example*. Accessed: 11. Sept. 2025. n.d. URL: https://attack.mitre.org/theme/images/navigator-example.png.

[35] OWASP. *DSOMM*. https://dsomm.owasp.org/. accessed: 2025-09-19. 2025.

[36] OWASP. *OWASP SAMM: The Model*. https://owaspsamm.org/model/. accessed: 2025-09-19; licensed under CC BY-SA 4.0 :contentReference[oaicite:0]index=0. 2025.

[37] *National Vulnerability Database (NVD)*. https://nvd.nist.gov/. U.S. Department of Commerce, National Institute of Standards and Technology. 2025.

[38] European Union Agency for Cybersecurity (ENISA). *About — Vulnerability Database (EUVD)*. https://euvd.enisa.europa.eu/about. Zugriff am 12. September 2025. 2025.

[39] *Technical Guideline BSI TR-03183: Cyber Resilience Requirements for Manufacturers and Products, Part 3: Vulnerability Reports and Notifications*. Techn. Ber. Version 1.0.0. Bonn, Germany: Bundesamt für Sicherheit in der Informationstechnik (BSI), Aug. 2025. URL: https://bsi.bund.de/dok/TR-03183-en.

[40] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Technische Richtlinie TR-03116-4*. Technical Guideline TR-03116-4. Downloaded YYYY-MM-DD. BSI – Bundesamt für Sicherheit in der Informationstechnik, 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile\&v=8.

[41] Tom Preston-Werner. *Semantic Versioning 2.0.0*. https://semver.org/. Letzte Änderung: 30. März 2013. 2013.

9 Anhang

Anhang 1

CRA Readiness deutscher Unternehmen

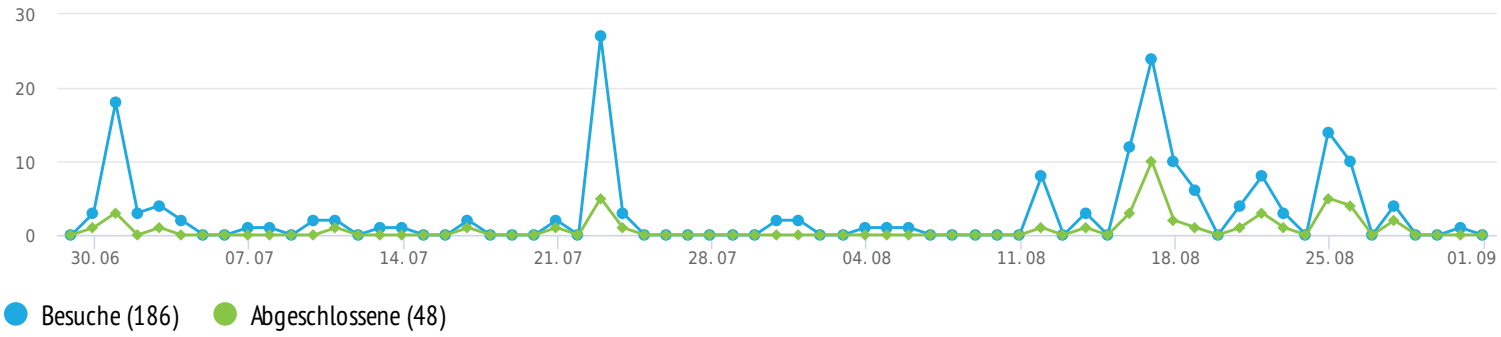
Allgemeines

Titel der Umfrage	CRA Readiness deutscher Unternehmen
Autor	Frédéric Noppe
Sprache der Umfrage	Deutsch
Öffentliche Web-Adresse der Umfrage (URL)	https://www.survio.com/survey/d/H2E2B6V7X1U9I8K4B
Erste Antwort	30. 06. 2025
Letzte Antwort	28. 08. 2025
Dauer	60 Tage

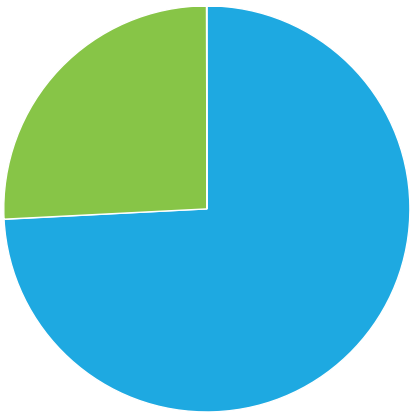
Umfrage Besucher

186	48	0	138	25,8%
Insgesamt Besuche	Fertige Antworten	Unvollendete Antworten	Nur gezeigt	Insgesamt Abschlussquote

Besuch Historie (30. 06. 2025 – 28. 08. 2025)

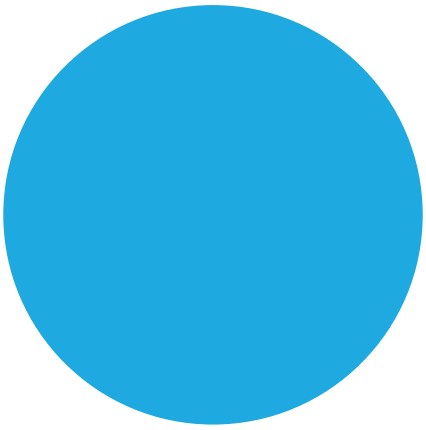


Besucher total



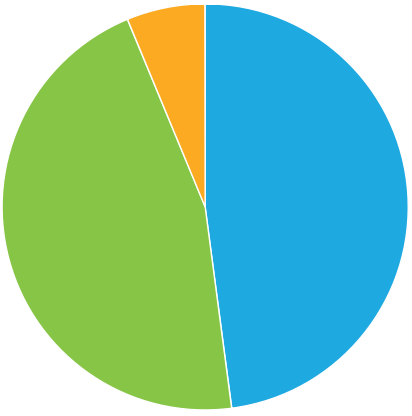
- Nur gezeigt (74,2 %)
- Abgeschlossene (25,8 %)
- Unvollständige (0,0 %)

Besuchen Quellen



- Direkter Link (100,0 %)

Durchschnittliche Zeit der Fertigstellung



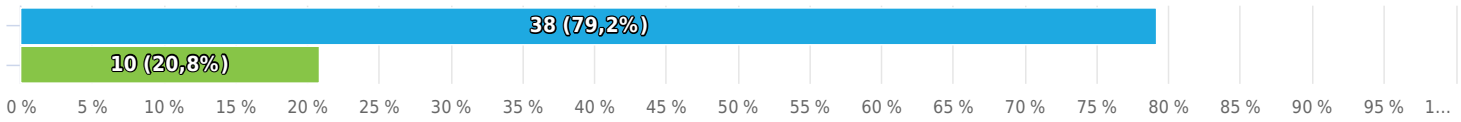
- 2-5 min. (47,9 %)
- 5-10 min. (45,8 %)
- 10-30 min. (6,3 %)

Ergebnisse

1 Haben Sie bereits vom CRA (Cyber Resilience Act gehört)

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

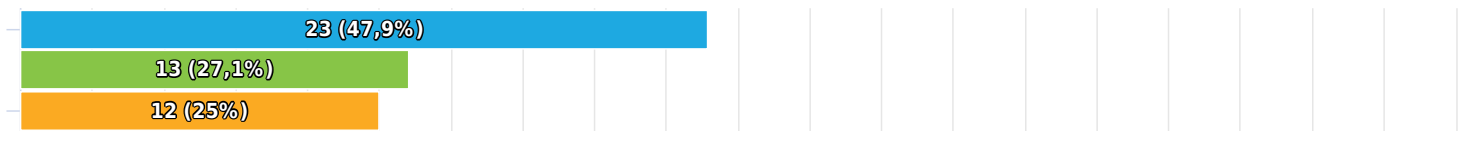
Antwort	Antworten	Verhältnis
Ja	38	79,2%
Nein	10	20,8%



2 Ist der CRA in Ihrer Firma bereits ein Gesprächsthema?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

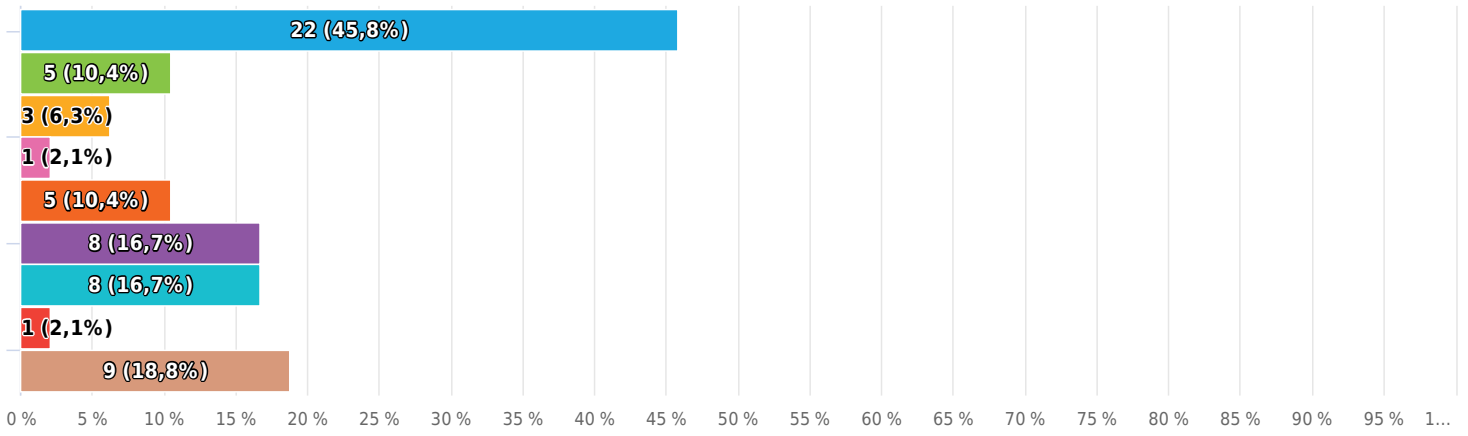
Antwort	Antworten	Verhältnis
Ja	23	47,9%
Nein	13	27,1%
Ist mir nicht bekannt	12	25,0%



3 Welche der angegebenen Berufsbezeichnungen trifft auf Sie zu?

Mehrfachauswahl , geantwortet 48 x, unbeantwortet 0 x

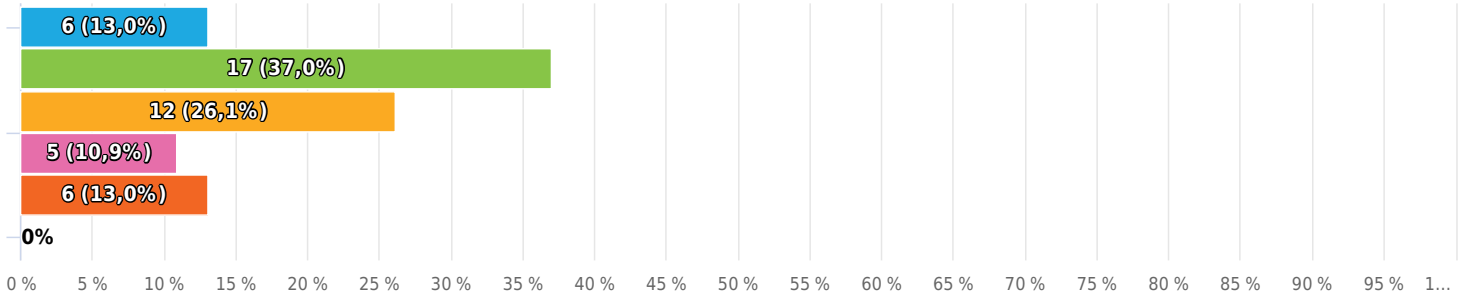
Antwort	Antworten	Verhältnis
Softwareentwickler:in	22	45,8%
Softwarearchitekt:in	5	10,4%
ISB/ ISO	3	6,3%
CISO	1	2,1%
Geschäftsführer:in	5	10,4%
IT-Administrator:in	8	16,7%
Cybersecurity Berater:in	8	16,7%
Ich möchte keine Angabe machen	1	2,1%
Andere (bitte geben Sie an)	9	18,8%



4 Wie alt sind Sie? (optional)

Einzelwahl , geantwortet 46 x, unbeantwortet 2 x

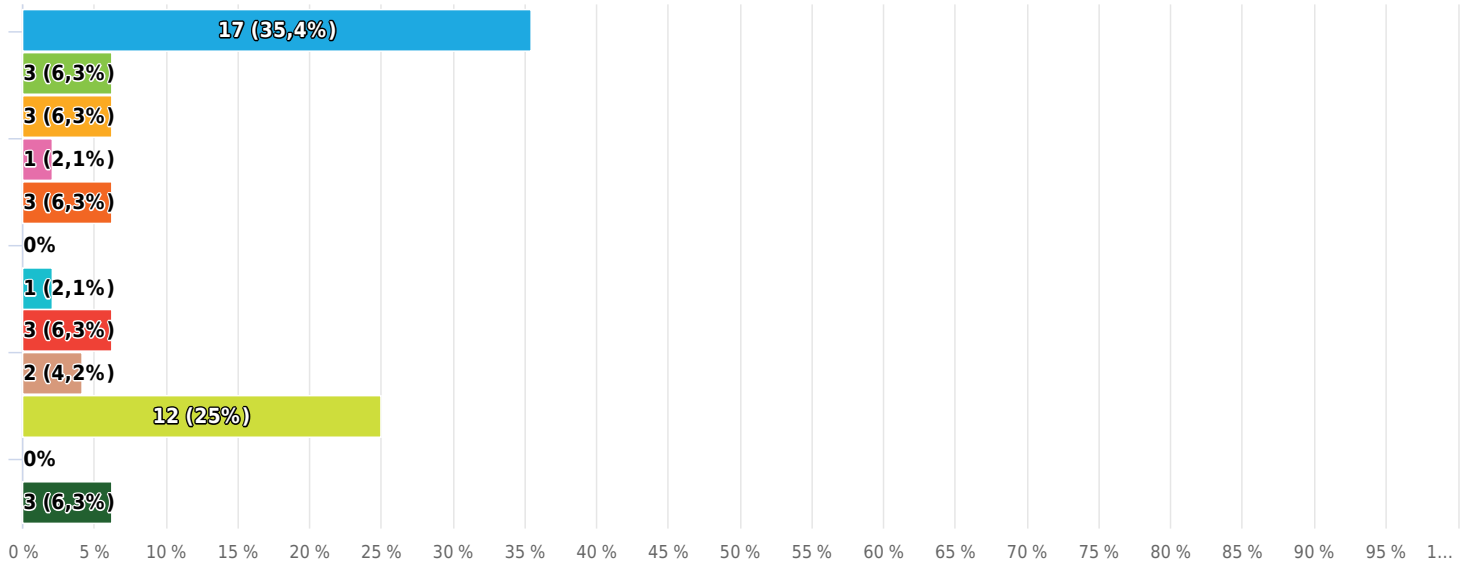
Antwort	Antworten	Verhältnis
<25	6	13,0%
25 - 35	17	37,0%
35 - 45	12	26,1%
45 - 55	5	10,9%
55 - 65	6	13,0%
>65	0	0,0%



5 In welcher Branche ist Ihr Unternehmen tätig?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

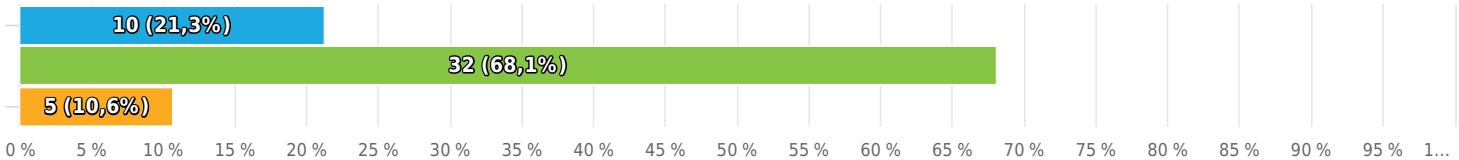
Antwort	Antworten	Verhältnis
Informationstechnologie	17	35,4%
Finanzen & Versicherungen	3	6,3%
Gesundheitswesen	3	6,3%
Industrie & Produktion	1	2,1%
Transport & Logistik	3	6,3%
Energie & Versorgung	0	0,0%
Bildung & Forschung	1	2,1%
Öffentlicher Dienst	3	6,3%
Medien & Kommunikation	2	4,2%
Beratung & Dienstleistungen	12	25,0%
Ich möchte keine Angabe machen	0	0,0%
Andere (bitte geben Sie an)	3	6,3%



6 Handelt es sich bei Ihrem Unternehmen um kritische Infrastruktur (KRITIS)? (optional)

Einzelwahl , geantwortet 47 x, unbeantwortet 1 x

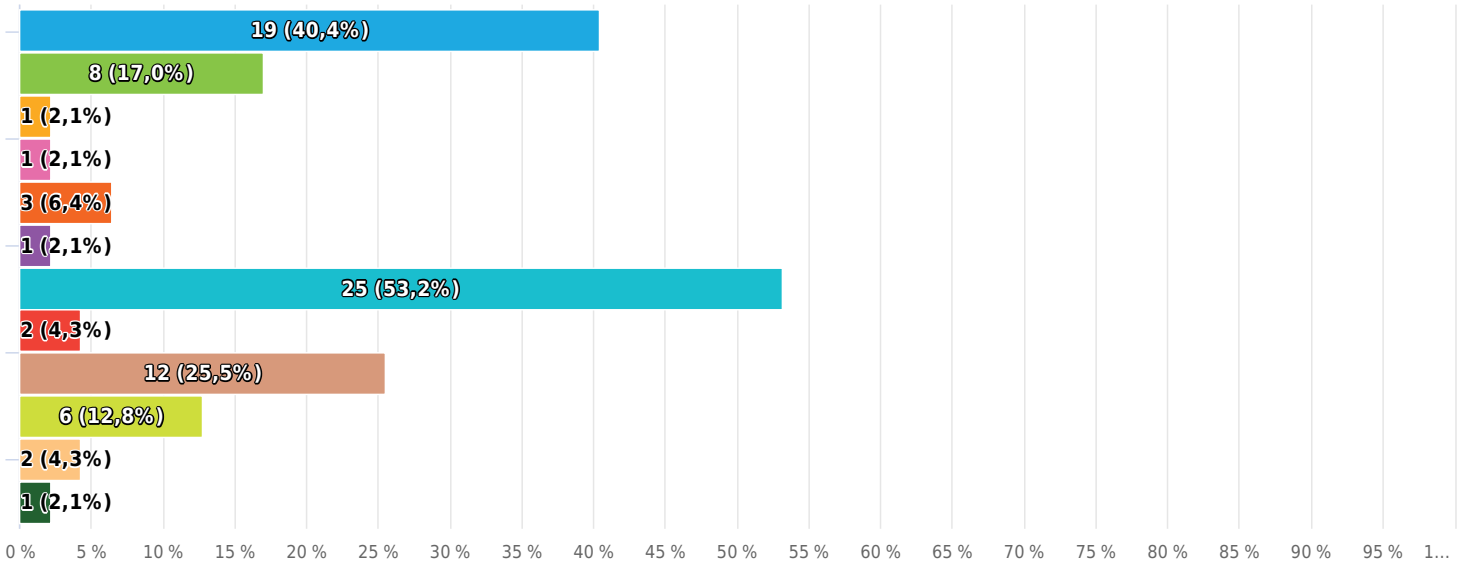
Antwort	Antworten	Verhältnis
Ja	10	21,3%
Nein	32	68,1%
Ist mir nicht bekannt	5	10,6%



7 Ist Ihr Unternehmen von einer dieser Regularien betroffen bzw. muss diese erfüllen? (optional)

Mehrfachauswahl , geantwortet 47 x, unbeantwortet 1 x

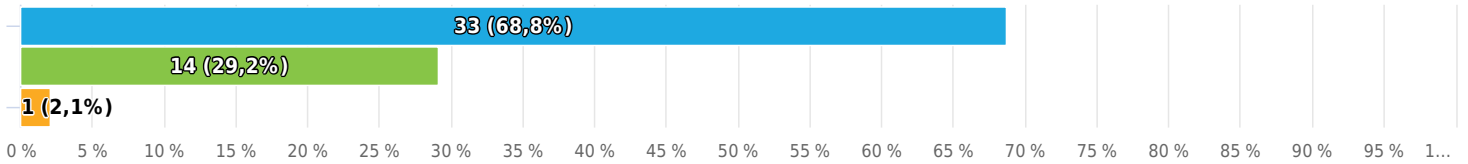
Antwort	Antworten	Verhältnis
BSI-Grundschutz	19	40,4%
NIS-2	8	17,0%
PCI-DSS	1	2,1%
HIPAA	1	2,1%
TISAX	3	6,4%
C5	1	2,1%
ISO 27001 (ISMS)	25	53,2%
NIST Cybersecurity Framework	2	4,3%
Mir sind keine bekannt	12	25,5%
Mein Unternehmen unterliegt keiner dieser Anforderungen	6	12,8%
Ich möchte hierzu keine Angaben machen	2	4,3%
Andere (bitte geben Sie an)	1	2,1%



8 Ist Softwaresicherheit ein priorisiertes Thema in Ihrem Unternehmen?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

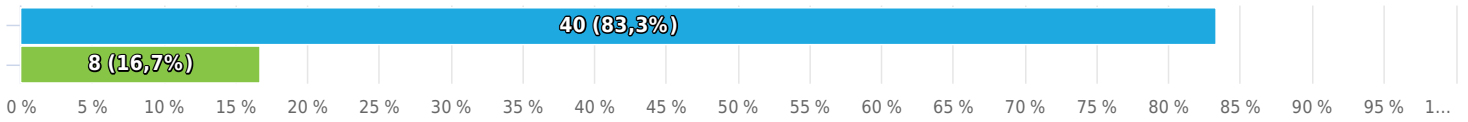
Antwort	Antworten	Verhältnis
Ja	33	68,8%
Nein	14	29,2%
Ist mir nicht bekannt	1	2,1%



9 Ist Softwaresicherheit für Sie persönlich ein priorisiertes Thema?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

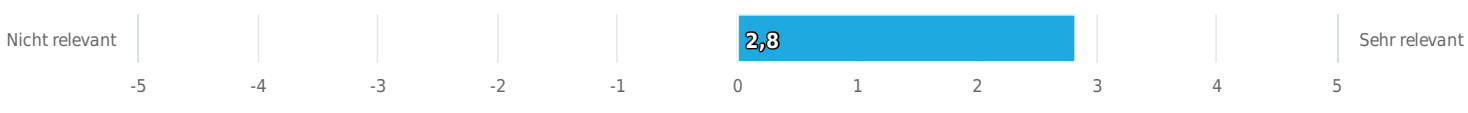
Antwort	Antworten	Verhältnis
Ja	40	83,3%
Nein	8	16,7%



10 Wie hoch schätzen Sie die Relevanz von Softwaresicherheit für Ihre tägliche Arbeit ein?

Semantisches Differential , geantwortet 48 x, unbeantwortet 0 x

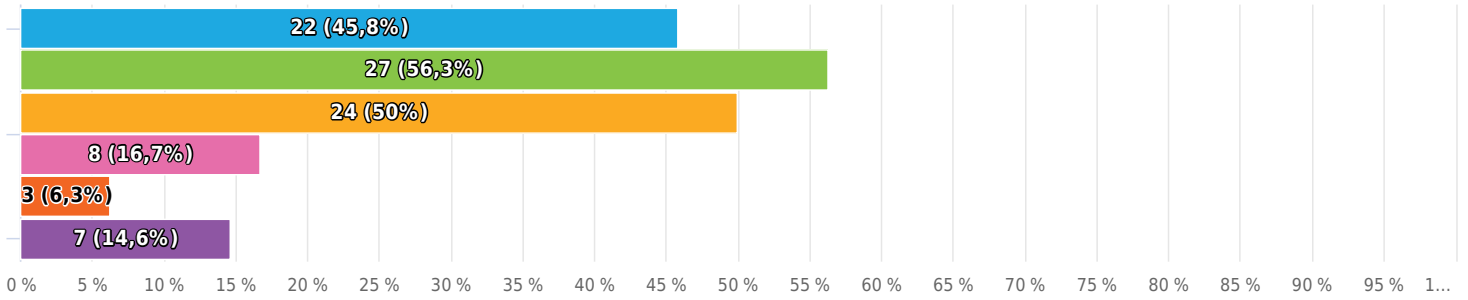
Antwort	-5	-4	-3	-2	-1	0	1	2	3	4	5	
Nicht relevant	1 (2,1%)	0	1 (2,1%)	3 (6,3%)	0	1 (2,1%)	2 (4,2%)	6 (12,5%)	12 (25,0%)	11 (22,9%)	11 (22,9%)	Sehr relevant



11 Werden Sicherheitsmaßnahmen bei der Konzeption, Entwicklung oder im Betrieb der durch Sie entwickelten Software integriert?

Mehrfachauswahl , geantwortet 48 x, unbeantwortet 0 x

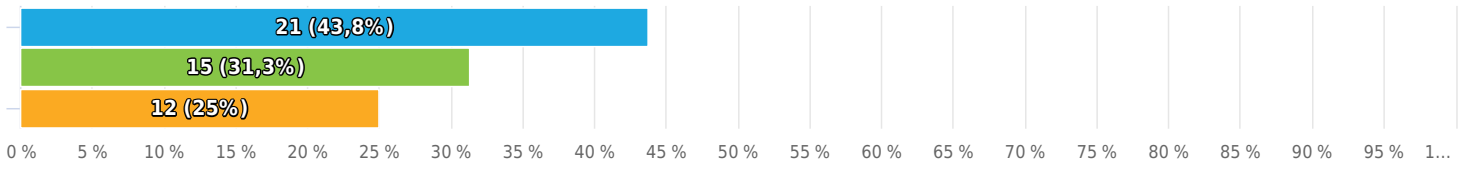
Antwort	Antworten	Verhältnis
Konzeption/ Design	22	45,8%
Entwicklung	27	56,3%
Im Betrieb	24	50,0%
Sicherheitsmaßnahmen werden nur nach Bedarf integriert	8	16,7%
Sicherheitsmaßnahmen werden nicht integriert	3	6,3%
Ist mir nicht bekannt	7	14,6%



12 Findet eine Bedrohungsanalyse der Software statt, um Schwachstellen in der Architektur der Software ausfindig zu machen? Z. B. ein Threat-Modeling mittels STRIDE Methodik.

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

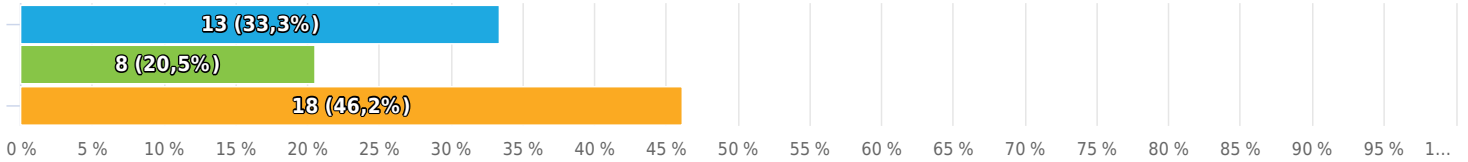
Antwort	Antworten	Verhältnis
Ja	21	43,8%
Nein	15	31,3%
Ist mir nicht bekannt	12	25,0%



13 Falls ja, wird diese Bedrohungsanalyse regelmäßig während des Lebenszyklus der Software wiederholt? (optional)

Einzelwahl , geantwortet 39 x, unbeantwortet 9 x

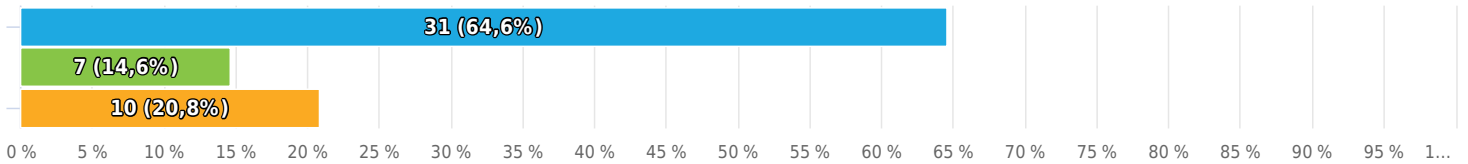
Antwort	Antworten	Verhältnis
Ja	13	33,3%
Nein	8	20,5%
Ist mir nicht bekannt	18	46,2%



14 Wird Software in Ihrem Unternehmen auf bekannte Schwachstellen (CVEs) überprüft? Z. B. durch einen SCA Scan (Software Composition Analysis)

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

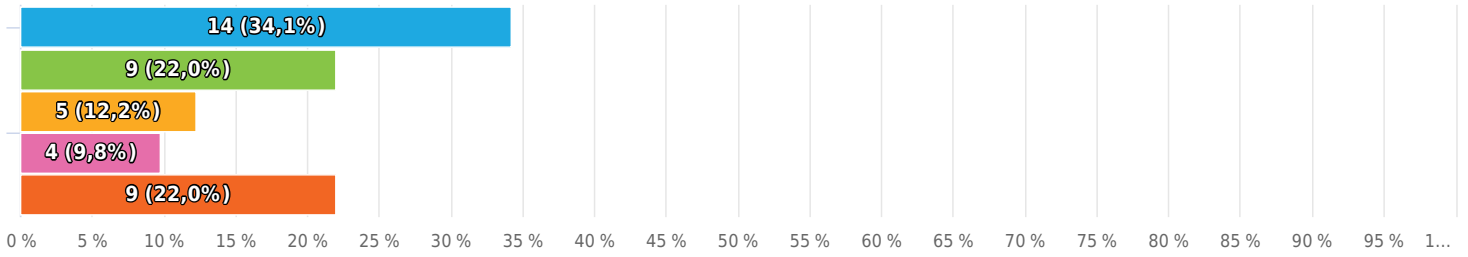
Antwort	Antworten	Verhältnis
Ja	31	64,6%
Nein	7	14,6%
Ist mir nicht bekannt	10	20,8%



15 Falls ja, werden diese Scans regelmäßig wiederholt? (optional)

Einzelwahl , geantwortet 41 x, unbeantwortet 7 x

Antwort	Antworten	Verhältnis
Ja, automatisiert	14	34,1%
Ja, manuell getriggert	9	22,0%
Ja, bei Produktabnahme	5	12,2%
Nein	4	9,8%
Ist mir nicht bekannt	9	22,0%



16 Welche Sicherheitsmaßnahmen werden noch zur Erhöhung der Sicherheit der durch Ihr Unternehmen gebaute Software durchgeführt? (optional)

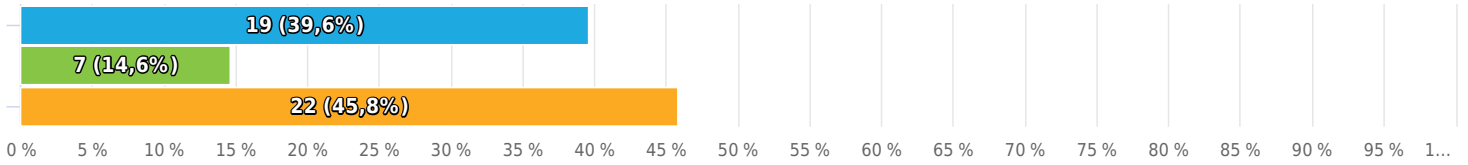
Text Frage , geantwortet 15 x, unbeantwortet 33 x

- Code Reviews (4 Augen Prinzip)
- Dependency updates mit renovate Trivy scan Sonarqube scans
- Es wird sich auf das Know-How der Entwickler verlassen ...
- Interne wie externe Audits
- Kryptographische Mechanismen aus eigener Entwicklung
- Lol
- Patches
- Pentests
- Pentests (extern)
- Regelmäßige Pen-tests
- Sast
- Schulungen der Mitarbeiter
- Schulungen durch die IT Abteilung
- Vorgaben für Frequent von SCACCA-scans. Verpflichtende jährliche pentests. Scan tools für produktive Infrastruktur via tools wie paloalto prisma cloud oder qualys.
- 4augenprinzip, immer Mal wieder pentest

17 Werden alle ausnutzbaren Schwachstellen geschlossen, bevor die Software an den Kunden/ Nutzer ausgeliefert wird?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

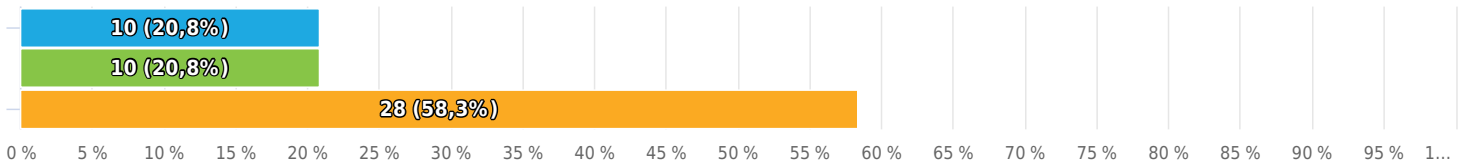
Antwort	Antworten	Verhältnis
Ja	19	39,6%
Nein	7	14,6%
Ist mir nicht bekannt	22	45,8%



18 Wird von der Software eine SBOM (Software-Bill-of-Materials) angefertigt und für Nutzer/ Kunden erreichbar hinterlegt?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

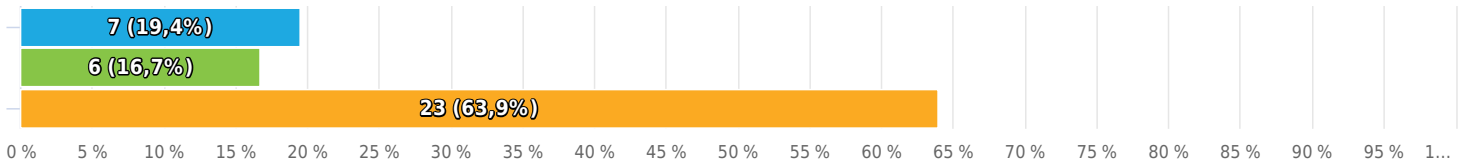
Antwort	Antworten	Verhältnis
Ja	10	20,8%
Nein	10	20,8%
Ist mir nicht bekannt	28	58,3%



19 Falls ja, wird diese SBOM für jede ausgelieferte Version der Software erstellt und hinterlegt? (optional)

Einzelwahl , geantwortet 36 x, unbeantwortet 12 x

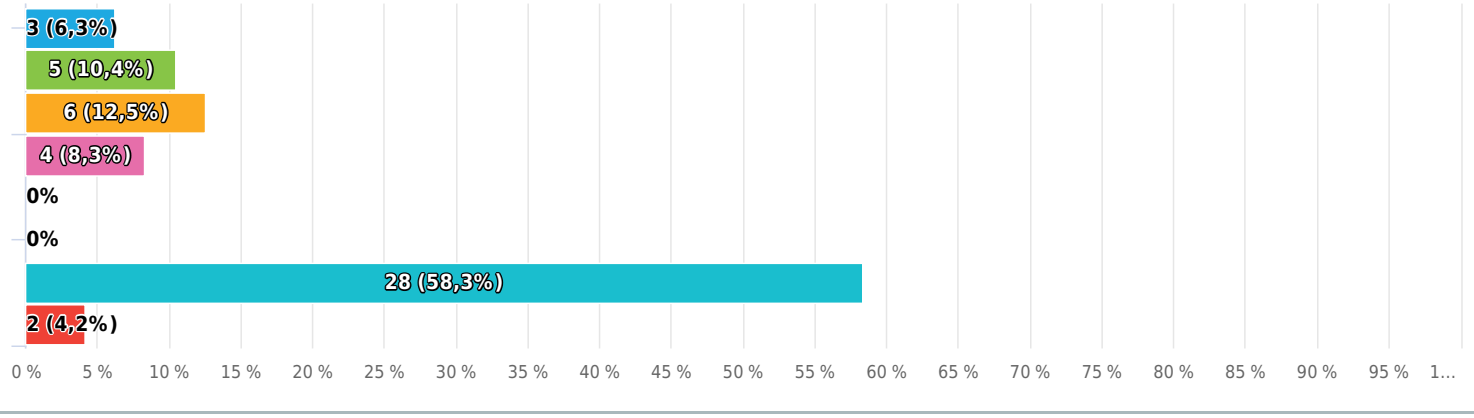
Antwort	Antworten	Verhältnis
Ja	7	19,4%
Nein	6	16,7%
Ist mir nicht bekannt	23	63,9%



20 Wie lange dauert es in der Regel, eine ausnutzbare Schwachstelle oberhalb eines CVE Scores von 7.0 (high) zu beheben?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

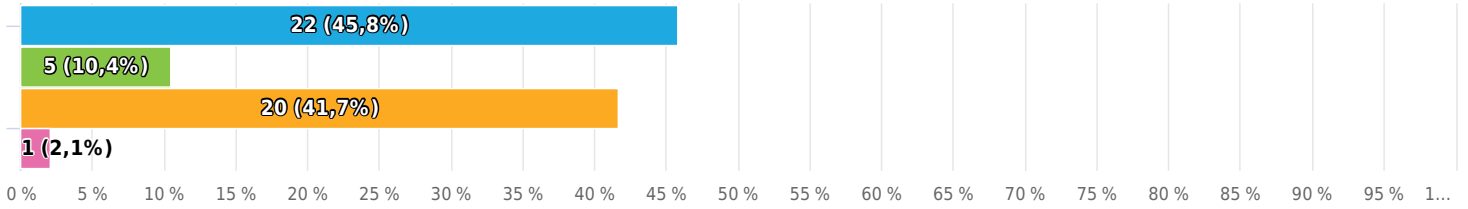
Antwort	Antworten	Verhältnis
Einen Tag	3	6,3%
< 3 Tage	5	10,4%
< 7 Tage	6	12,5%
< 14 Tage	4	8,3%
< 30 Tage	0	0,0%
> 30 Tage	0	0,0%
Ist mir nicht bekannt	28	58,3%
Andere (bitte geben Sie an)	2	4,2%



21 Werden Ihre Kunden/ Nutzer direkt über neue Schwachstellen informiert?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

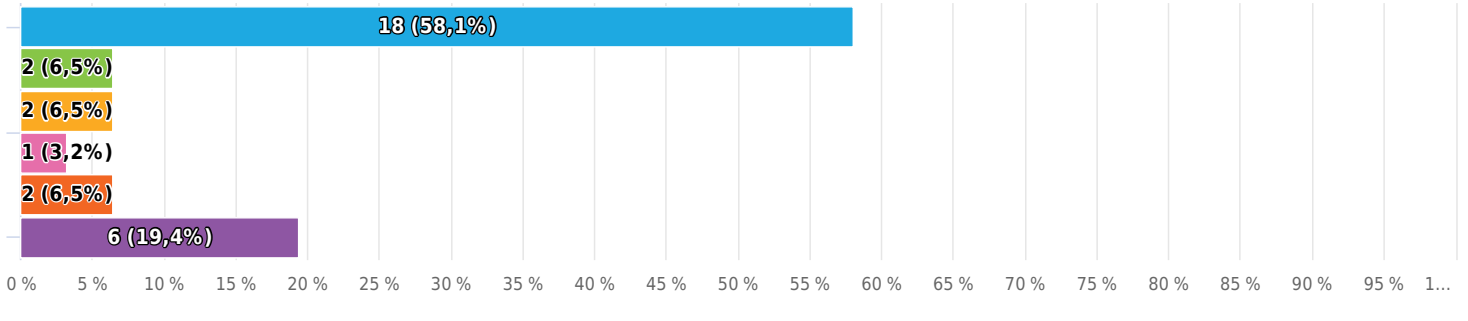
Antwort	Antworten	Verhältnis
Ja	22	45,8%
Nein	5	10,4%
Ist mir nicht bekannt	20	41,7%
Andere (bitte geben Sie an)	1	2,1%



22 Falls ja, über welchen Kommunikationskanal? (optional)

Einzelwahl , geantwortet 31 x, unbeantwortet 17 x

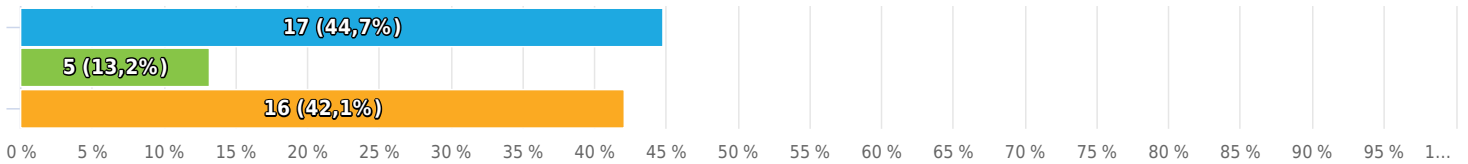
Antwort	Antworten	Verhältnis
Mail	18	58,1%
Telefon	2	6,5%
Die Software selbst (z. B. per Pop-Up)	2	6,5%
Messenger	1	3,2%
Vulnerability Exploitability eXchange (VEX)	2	6,5%
Andere (bitte geben Sie an)	6	19,4%



23 Falls ja, existiert für die Kommunikation der Schwachstelle ein geregelter Prozess? (optional)

Einzelwahl , geantwortet 38 x, unbeantwortet 10 x

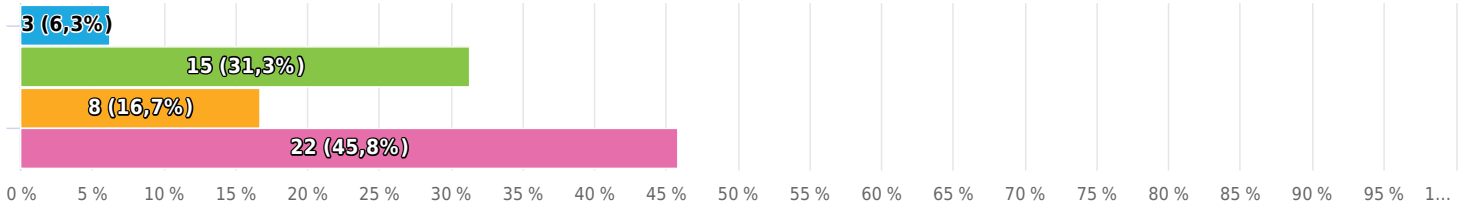
Antwort	Antworten	Verhältnis
Ja	17	44,7%
Nein	5	13,2%
Ist mir nicht bekannt	16	42,1%



24 Werden durch Ihr Unternehmen Zeitangaben bis zur erwarteten Behebung der Schwachstellen gegenüber den Nutzern/ Kunden angegeben?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

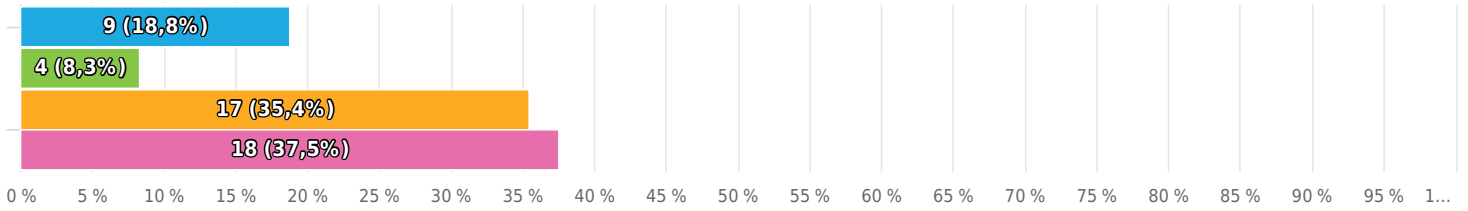
Antwort	Antworten	Verhältnis
Ja - genaue Angaben	3	6,3%
Ja - ungefähre Angaben	15	31,3%
Nein	8	16,7%
Ist mir nicht bekannt	22	45,8%



25 Sollte die Schwachstelle durch den Kunden/ Nutzer selbst behoben werden müssen. Wird eine detaillierte Anleitung/ Dokumentation mitgegeben.

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

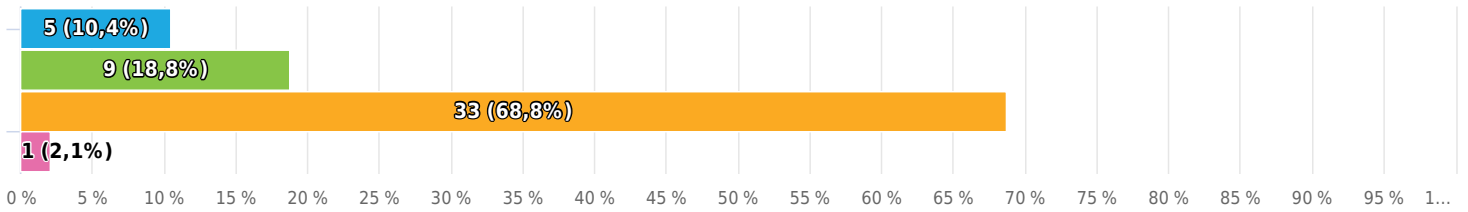
Antwort	Antworten	Verhältnis
Ja	9	18,8%
Nein	4	8,3%
Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	17	35,4%
Ist mir nicht bekannt	18	37,5%



26 Werden Schwachstellen in Ihrer Software nach Ihrer Behebung veröffentlicht? Z. B. in der NIST-NVD Database.

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

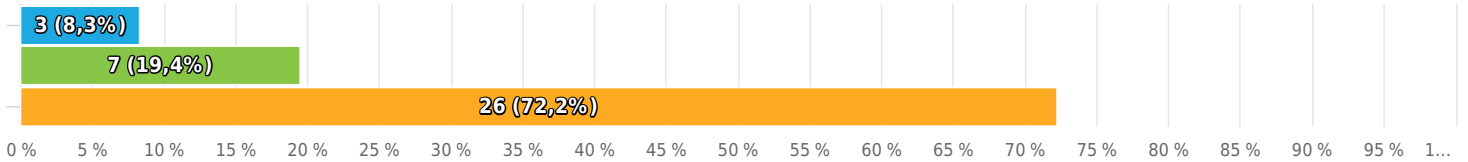
Antwort	Antworten	Verhältnis
Ja	5	10,4%
Nein	9	18,8%
Ist mir nicht bekannt	33	68,8%
Andere (bitte geben Sie an)	1	2,1%



27 Falls ja, existiert für die Veröffentlichung der Schwachstelle ein geregelter Prozess? (optional)

Einzelwahl , geantwortet 36 x, unbeantwortet 12 x

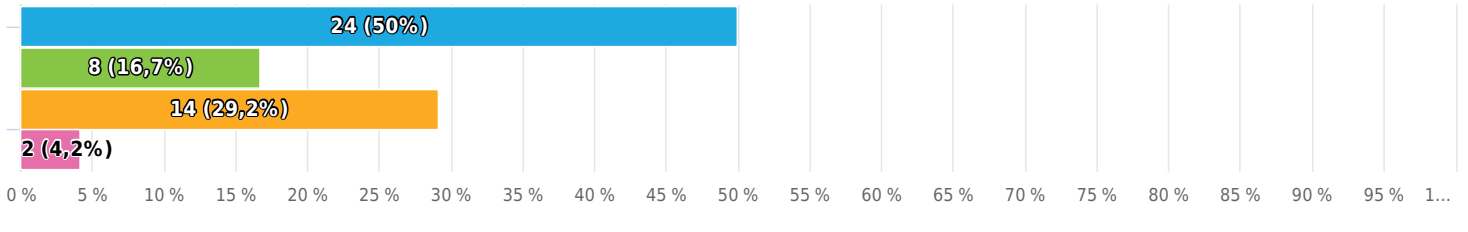
Antwort	Antworten	Verhältnis
Ja	3	8,3%
Nein	7	19,4%
Ist mir nicht bekannt	26	72,2%



28 Sollte eine Schwachstelle durch einen Dritten entdeckt werden. Ist eine Meldeadresse zur Meldung dieser entdeckten Schwachstellen an Ihr Unternehmen vorhanden? Z. B. per Responsible Disclosure.

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	24	50,0%
Nein	8	16,7%
Ist mir nicht bekannt	14	29,2%
Andere (bitte geben Sie an)	2	4,2%



29 Falls ein Meldeweg vorhanden ist: Wie können durch Dritte entdeckte Schwachstellen an Ihr Unternehmen kommuniziert werden? (optional)

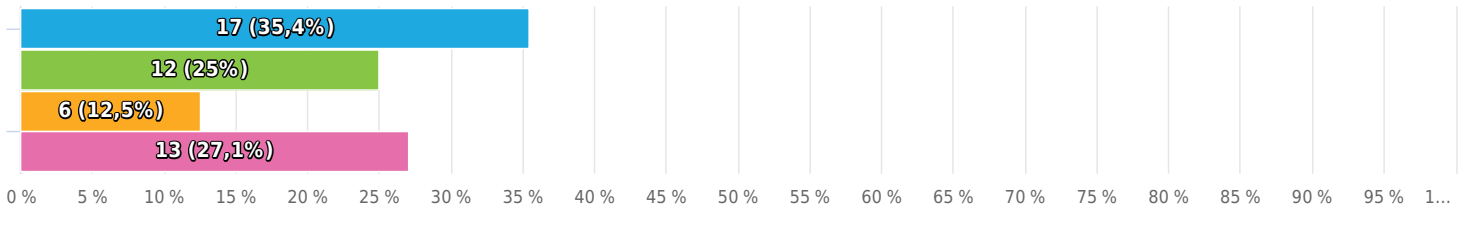
Text Frage , geantwortet 11 x, unbeantwortet 37 x

- E-Mail oder Issue post auf dem public GitHub repository.
- Gut dokumentierter prozess inklusive safe harbor erklärung. Hochladen von Berichten bei intigriti
- Jede Form vertraulicher Kommunikation wird akzeptiert
- Mail
- Mail an security@... oder über unser BugBounty-Programm
- Mailkontakt
- Nutzung des normalen Kontaktformulars
- security.txt
- Security.txt, E-Mail Kontakt
- Schlecht. Per anonymen Brief an den Hauptsitz wäre wahrscheinlich am besten. Ansonsten ist das eher schwer
- Verschlüsselte Email via security.txt direkt an das Operations Team

30 Wird die durch Ihr Unternehmen produzierte Software nach einem einheitlichen Schema versioniert? Z. B. Semantic Versioning 2.0.0

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

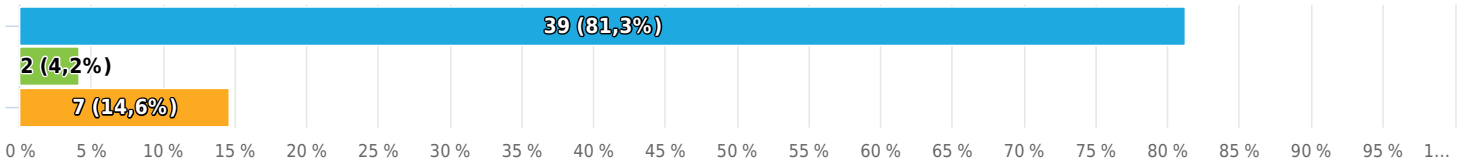
Antwort	Antworten	Verhältnis
Ja	17	35,4%
Ja, verschiedene Projekte nutzen jedoch unterschiedliche Arten der Versionierung	12	25,0%
Nein	6	12,5%
Ist mir nicht bekannt	13	27,1%



31 Existiert eine technische Dokumentation Ihrer Software?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

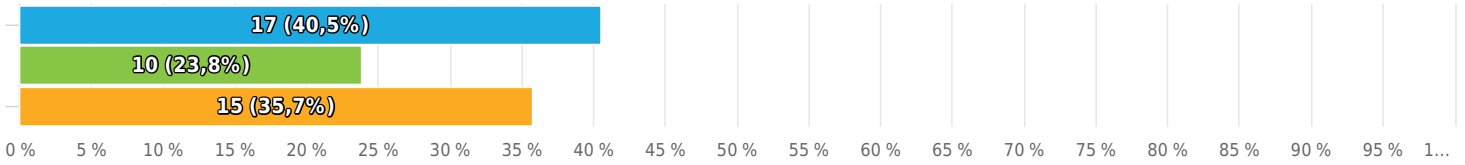
Antwort	Antworten	Verhältnis
Ja	39	81,3%
Nein	2	4,2%
Ist mir nicht bekannt	7	14,6%



32 Sollte der Kunde die Software selbst konfigurieren können oder müssen. Existiert eine dokumentierte und dem Kunden jederzeit verfügbare Anleitung zur sicheren Konfiguration der Software, die alle notwendigen Informationen zur sicheren Konfiguration enthält? (optional)

Einzelwahl , geantwortet 42 x, unbeantwortet 6 x

Antwort	Antworten	Verhältnis
Ja	17	40,5%
Nein	10	23,8%
Ist mir nicht bekannt	15	35,7%

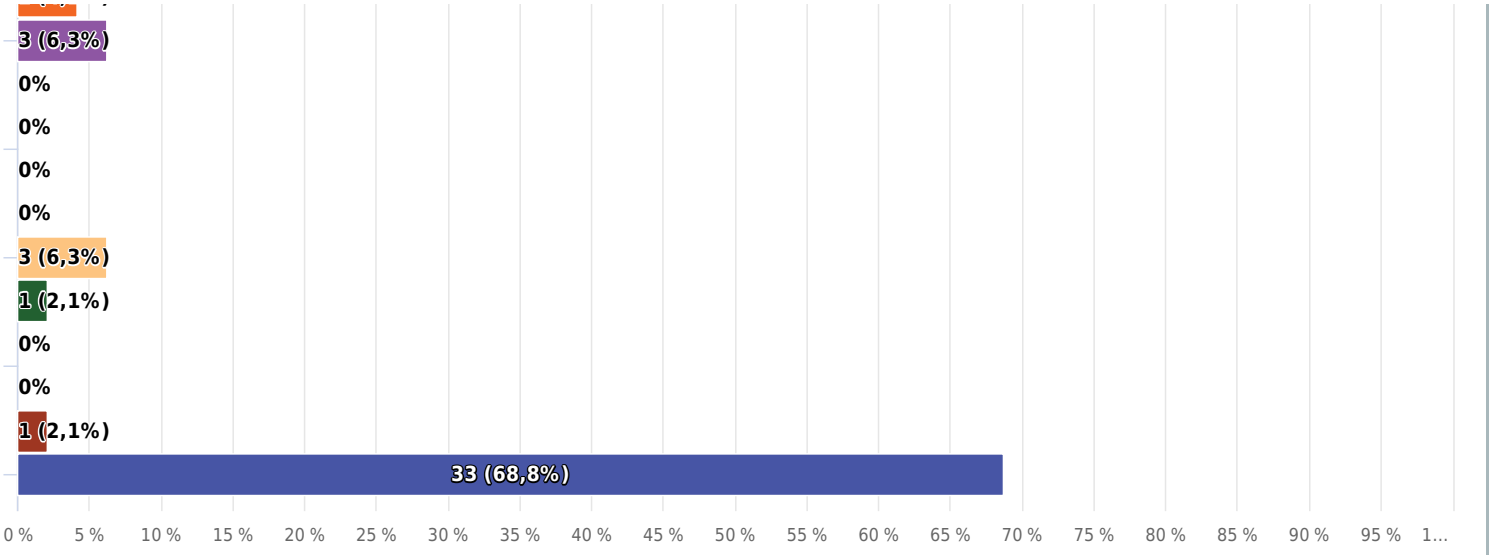


33 Gehört die von Ihnen entwickelte Software zu einer der hier genannten Produktkategorien/ Verwendungszwecken oder wird in diesen durch Ihr Unternehmen verbaut? Hinweis: Sollte Ihr Produkt zu einer der Kategorien gehören, fällt es in die Kategorie „Kritische Produkte“ und muss besondere Anforderungen im Rahmen des CRA erfüllen.

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
IAM - Systeme	0	0,0%
Internet-Browser	2	4,2%
Passwortmanager	1	2,1%
Software für die Suche, Entfernung und Quarantäne von Schadsoftware	0	0,0%
VPN	0	0,0%
Netzwerkmanagement, - Konfiguration oder -Monitoring	1	2,1%
SIEM	0	0,0%
Update- oder Patchmanager (inkl. Bootmanager)	0	0,0%
Systeme für die Anwendungskonfigurationsverwaltung	0	0,0%
Software für Fernzugriff und gemeinsame Datennutzung	0	0,0%
Software für die Mobilgeräteverwaltung	0	0,0%
Physische Netzschnittstellen	0	0,0%
Betriebssysteme für Server, Desktops und Mobilgeräte	0	0,0%
Betriebssysteme (andere)	1	2,1%
Firewalls, Angriffserkennungs- und/oder -präventionssysteme für den industriellen Einsatz	0	0,0%
Firewalls (andere)	0	0,0%
Router, Modems für die Internetanbindung und Switches für den industriellen Einsatz	0	0,0%
Router (andere)	0	0,0%
Allzweck-Mikroprozessoren	0	0,0%
Mikroprozessoren, die für die Integration in speicherprogrammierbare Steuerungen (PLC) und Sicherheitselemente bestimmt sind	0	0,0%
Mikroprozessoren (andere)	0	0,0%
Mikrocontroller	0	0,0%
Anwendungsspezifische integrierte Schaltungen (ASIC) und FPGAs im KRITIS Bereich	0	0,0%
Hypervisoren und Container-Runtime-Systeme, die eine virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen	0	0,0%

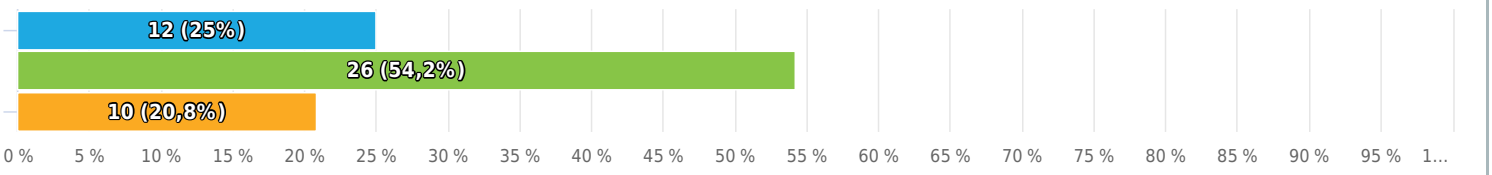
Public-Key-Infrastrukturen und Ausstellung digitaler Zertifikate	2	4,2%
Sicherheitselemente	3	6,3%
Hardware-Sicherheitsmodule (HSM)	0	0,0%
Sichere Kryptoprozessoren	0	0,0%
Chipkarten, Chipkartenleser und Token	0	0,0%
Industrielle Automatisierungs- und Steuerungssysteme (IACS) zur Verwendung durch KRITIS Einrichtungen	0	0,0%
Industrielle Automatisierungs- und Steuerungssysteme (IACS), nicht KRITIS	3	6,3%
Geräte für das industrielle Internet der Dinge (IIoT) im KRITIS Sektor	1	2,1%
Geräte für das industrielle Internet der Dinge (IIoT) (andere Sektoren)	0	0,0%
Sensor- und Aktuatorkomponenten von Robotern und Robotersteuerungen	0	0,0%
Intelligente Zähler	1	2,1%
Keine der genannten	33	68,8%



34 Handelt es sich bei der durch Sie vertriebenen Software um eine reine SaaS-Anwendung?

Einzelwahl , geantwortet 48 x, unbeantwortet 0 x

Antwort	Antworten	Verhältnis
Ja	12	25,0%
Nein	26	54,2%
Ist mir nicht bekannt	10	20,8%



35 Gibt es etwas, was sie im Rahmen der Befragung noch unbedingt erwähnen möchten? (optional)

Text Frage , geantwortet 8 x, unbeantwortet 40 x

- Bisher keinen Kontakt zu der Thematik gehabt...
- Bug bei Auswahl iam
- Die Fragen sind primär für Softwareentwickler gedacht. Ein Konzern hat aber wesentlich mehr Abteilungen die sich mit cra auseinandersetzen müssen.
- Ich bin als GF leider nicht so sehr in die Entwicklung involviert, denke aber, dass wir sichere Software bauen. Ich leite den Bogen an meine Entwickler weiter.
- Ich bin keine programmierende Person.UnserUnternehmen betreut Menschen in ihrer Lebensführung. Daten dieser zu schützen ist relevant.
- Ich bin selbst nicht an der Softwareentwicklung beteiligt, bin mir aber sicher, dass Vorgaben einghalten werden.

- Wir sind eine Agentur für Softwareentwicklung und liefern verschiedenste Softwareprojekte an Kunden. Viele der Projekte sind unterschiedlich, daher sind keine 100 % igen Angaben möglich. Sicherheit ist bei vielen unserer Kunden leider kein Thema, für das sie Geld ausgeben.
- Wir sind noch in einem frühen Stadium der Entwicklung. Einige der Punkte werden ggf. noch adressiert.

Anhang 2

Im Folgenden werden die genauen Ergebnisse der Befragung und die Antworten auf die Fragen aufgeführt. Aufgrund der Größe der Tabelle wird diese chronologisch gestückelt. Die Spalte Nr. dient jeweils zur Sortierung in umgekehrter chronologischer Reihenfolge der abgegebenen Antworten - Nr. 1 ist die letzte abgegebene und Nr. 48 die erste abgegebene Antwort.

Nr.	Datum	Zeit	Abgeschlossen in	Quelle	Frage: 1
1	2025-08-28	17:36:55	00:04:27	Direkter Link	Ja
2	2025-08-28	13:16:59	00:06:16	Direkter Link	Nein
3	2025-08-27	00:57:43	00:03:11	Direkter Link	Ja
4	2025-08-26	19:45:17	00:05:19	Direkter Link	Ja
5	2025-08-26	17:16:06	00:03:02	Direkter Link	Nein
6	2025-08-26	09:29:58	00:06:06	Direkter Link	Ja
7	2025-08-25	21:48:41	00:02:47	Direkter Link	Ja
8	2025-08-25	17:25:21	00:02:59	Direkter Link	Ja
9	2025-08-25	15:30:39	00:06:46	Direkter Link	Ja
10	2025-08-25	08:36:53	00:03:58	Direkter Link	Ja
11	2025-08-25	04:10:40	00:03:11	Direkter Link	Ja
12	2025-08-23	23:58:05	00:03:54	Direkter Link	Nein
13	2025-08-22	17:42:17	00:04:50	Direkter Link	Ja
14	2025-08-22	17:26:36	00:03:28	Direkter Link	Ja
15	2025-08-22	16:53:06	00:06:23	Direkter Link	Ja
16	2025-08-21	14:25:28	00:04:03	Direkter Link	Ja
17	2025-08-19	13:25:10	00:04:33	Direkter Link	Ja
18	2025-08-18	12:54:18	00:05:59	Direkter Link	Nein
19	2025-08-18	09:44:46	00:04:14	Direkter Link	Nein
20	2025-08-17	18:36:51	00:06:31	Direkter Link	Ja
21	2025-08-17	18:13:07	00:06:45	Direkter Link	Nein
22	2025-08-17	17:02:22	00:09:28	Direkter Link	Ja
23	2025-08-17	17:00:45	00:10:00	Direkter Link	Ja
24	2025-08-17	13:12:45	00:05:26	Direkter Link	Nein
25	2025-08-17	13:11:18	00:04:44	Direkter Link	Nein
26	2025-08-17	13:10:46	00:08:00	Direkter Link	Ja
27	2025-08-17	13:09:24	00:04:20	Direkter Link	Ja
28	2025-08-17	13:07:30	00:06:18	Direkter Link	Ja
29	2025-08-17	13:07:22	00:04:56	Direkter Link	Ja
30	2025-08-16	19:05:42	00:03:49	Direkter Link	Ja
31	2025-08-16	13:56:38	00:07:40	Direkter Link	Ja
32	2025-08-16	12:33:35	00:04:45	Direkter Link	Ja
33	2025-08-14	20:49:19	00:12:12	Direkter Link	Ja
34	2025-08-12	22:08:49	00:05:02	Direkter Link	Ja
35	2025-07-24	08:50:37	00:05:05	Direkter Link	Ja
36	2025-07-23	21:22:38	00:04:44	Direkter Link	Ja
37	2025-07-23	21:15:06	00:05:17	Direkter Link	Ja
38	2025-07-23	19:17:35	00:08:18	Direkter Link	Nein
39	2025-07-23	18:01:26	00:05:09	Direkter Link	Ja
40	2025-07-23	17:39:29	00:09:04	Direkter Link	Nein
41	2025-07-21	17:22:09	00:05:36	Direkter Link	Ja
42	2025-07-17	17:20:14	00:10:56	Direkter Link	Ja
43	2025-07-11	17:16:08	00:03:32	Direkter Link	Ja
44	2025-07-03	16:40:20	00:04:01	Direkter Link	Ja
45	2025-07-01	20:39:23	00:04:44	Direkter Link	Ja
46	2025-07-01	16:44:24	00:10:39	Direkter Link	Ja
47	2025-07-01	16:42:39	00:07:58	Direkter Link	Ja
48	2025-06-30	09:38:56	00:04:10	Direkter Link	Ja

Tabelle 9.1: *Rahmendaten und Antwort zur Kenntnis über den CRA*

Nr.	Frage: 2	Frage: 3	Frage: 4
1	Ja	Nein	35 - 45
2	Nein	Nein	55 - 65
3	Ja	Ja	35 - 45
4	Ja	Ja	<25
5	Nein	Ja	55 - 65
6	Ja	Nein	25 - 35
7	Ja	Ja	25 - 35
8	Ja	Ja	25 - 35
9	Ja	Ja	45 - 55
10	Ist mir nicht bekannt	Nein	<25
11	Nein	Ja	35 - 45
12	Nein	Ja	45 - 55
13	Ja	Nein	25 - 35
14	Ja	Ja	35 - 45
15	Nein	Nein	35 - 45
16	Nein	Ja	25 - 35
17	Nein	Ja	35 - 45
18	Ist mir nicht bekannt	Nein	55 - 65
19	Ist mir nicht bekannt	Nein	<25
20	Ist mir nicht bekannt	Ja	55 - 65
21	Ist mir nicht bekannt	Nein	35 - 45
22	Ja	Nein	55 - 65
23	Ja	Nein	25 - 35
24	Ist mir nicht bekannt	Nein	35 - 45
25	Nein	Nein	25 - 35
26	Ist mir nicht bekannt	Ja	
27	Nein	Ja	35 - 45
28	Ja	Ja	25 - 35
29	Ja	Ja	25 - 35
30	Ist mir nicht bekannt	Nein	<25
31	Ja	Ja	55 - 65
32	Nein	Nein	45 - 55
33	Ist mir nicht bekannt	Ja	45 - 55
34	Ja	Ja	35 - 45
35	Ja	Nein	
36	Nein	Ja	35 - 45
37	Ist mir nicht bekannt	Nein	25 - 35
38	Ist mir nicht bekannt	Nein	25 - 35
39	Nein	Ja	35 - 45
40	Nein	Nein	25 - 35
41	Ja	Ja	25 - 35
42	Ja	Ja	25 - 35
43	Nein	Nein	45 - 55
44	Ist mir nicht bekannt	Nein	25 - 35
45	Ja	Ja	<25
46	Ja	Nein	<25
47	Ja	Nein	25 - 35
48	Ja	Ja	25 - 35

Tabelle 9.2: *Antworten zur Personenkategorisierung der Umfrageteilnehmer (mit Softwareentwickler:in und Alter)*

Nr.	Frage: 5	Frage: 6	Frage 7: BSI-Grundschutz
1	Beratung & Dienstleistungen	Nein	Ja
2	Bildung & Forschung	Nein	Nein
3	Informationstechnologie	Nein	Nein
4	Beratung & Dienstleistungen	Nein	Nein
5	Medien & Kommunikation		Nein
6	Informationstechnologie	Ja	Ja
7	Informationstechnologie	Nein	Nein
8	Informationstechnologie	Nein	Nein
9	Informationstechnologie	Nein	Ja
10	Informationstechnologie	Nein	Nein
11	Gesundheitswesen	Ja	Ja
12	Öffentlicher Dienst	Ja	Ja
13	Beratung & Dienstleistungen	Nein	Ja
14	Finanzen & Versicherungen	Ja	Ja
15	Gesundheitswesen	Nein	Ja
16	Beratung & Dienstleistungen	Nein	Nein
17	Informationstechnologie	Nein	Nein
18	Beratung & Dienstleistungen	Nein	Nein
19	Ich arbeite noch nicht	Ist mir nicht bekannt	Nein
20	Informationstechnologie	Nein	Nein
21	Finanzen & Versicherungen	Nein	Nein
22	Informationstechnologie	Nein	Ja
23	Informationstechnologie	Nein	Ja
24	Gesundheitswesen	Ja	Nein
25	Glas	Ist mir nicht bekannt	Ja
26	Informationstechnologie	Nein	Nein
27	Informationstechnologie	Nein	Ja
28	Informationstechnologie	Nein	Nein
29	Industrie & Produktion	Nein	Ja
30	Beratung & Dienstleistungen	Nein	Nein
31	Medien & Kommunikation	Ja	Nein
32	Transport & Logistik	Ja	Nein
33	Informationstechnologie	Nein	Nein
34	Beratung & Dienstleistungen	Nein	Nein
35	Öffentlicher Dienst	Ist mir nicht bekannt	Ja
36	Verteidigung	Ja	Ja
37	Finanzen & Versicherungen	Ist mir nicht bekannt	Nein
38	Transport & Logistik	Ja	Nein
39	Informationstechnologie	Nein	Nein
40	Öffentlicher Dienst	Nein	Nein
41	Informationstechnologie	Ist mir nicht bekannt	Nein
42	Beratung & Dienstleistungen	Nein	Ja
43	Beratung & Dienstleistungen	Nein	Nein
44	Beratung & Dienstleistungen	Nein	Nein
45	Beratung & Dienstleistungen	Nein	Ja
46	Transport & Logistik	Ja	Ja
47	Beratung & Dienstleistungen	Nein	Ja
48	Informationstechnologie	Nein	

Tabelle 9.3: *Antworten zu Fragen bezüglich Branche, KRITIS und BSI-Grundschutz*

Nr.	Frage 7: NIS-2	Frage 7: PCI-DSS	Frage 7: HIPAA	Frage 7: TISAX
1	Ja	Nein	Nein	Nein
2	Nein	Nein	Nein	Nein
3	Nein	Nein	Nein	Nein
4	Nein	Nein	Nein	Nein
5	Nein	Nein	Nein	Nein
6	Nein	Nein	Nein	Nein
7	Nein	Nein	Nein	Nein
8	Nein	Nein	Nein	Nein
9	Ja	Nein	Nein	Ja
10	Nein	Nein	Nein	Nein
11	Nein	Nein	Nein	Nein
12	Nein	Nein	Nein	Nein
13	Nein	Nein	Nein	Nein
14	Nein	Ja	Ja	Nein
15	Nein	Nein	Nein	Nein
16	Nein	Nein	Nein	Nein
17	Nein	Nein	Nein	Nein
18	Nein	Nein	Nein	Nein
19	Nein	Nein	Nein	Nein
20	Nein	Nein	Nein	Nein
21	Nein	Nein	Nein	Nein
22	Ja	Nein	Nein	Nein
23	Nein	Nein	Nein	Nein
24	Nein	Nein	Nein	Nein
25	Nein	Nein	Nein	Ja
26	Nein	Nein	Nein	Nein
27	Nein	Nein	Nein	Nein
28	Nein	Nein	Nein	Nein
29	Nein	Nein	Nein	Nein
30	Nein	Nein	Nein	Ja
31	Nein	Nein	Nein	Nein
32	Ja	Nein	Nein	Nein
33	Nein	Nein	Nein	Nein
34	Nein	Nein	Nein	Nein
35	Nein	Nein	Nein	Nein
36	Nein	Nein	Nein	Nein
37	Nein	Nein	Nein	Nein
38	Nein	Nein	Nein	Nein
39	Nein	Nein	Nein	Nein
40	Nein	Nein	Nein	Nein
41	Nein	Nein	Nein	Nein
42	Ja	Nein	Nein	Nein
43	Nein	Nein	Nein	Nein
44	Nein	Nein	Nein	Nein
45	Ja	Nein	Nein	Nein
46	Ja	Nein	Nein	Nein
47	Ja	Nein	Nein	Nein
48	Nein	Nein	Nein	Nein

Tabelle 9.4: *Antworten zur Complianceanforderung: NIS-2, PCI-DSS, HIPAA, TISAX*

Nr.	Frage 7: C5	Frage 7: ISO 27001	Frage 7: NIST CSF	Frage 7: Keine bekannt
1	Ja	Ja	Nein	Nein
2	Nein	Nein	Nein	Nein
3	Nein	Ja	Nein	Nein
4	Nein	Nein	Nein	Ja
5	Nein	Nein	Nein	Ja
6	Nein	Ja	Nein	Nein
7	Nein	Nein	Nein	Ja
8	Nein	Ja	Nein	Nein
9	Nein	Ja	Nein	Nein
10	Nein	Ja	Nein	Nein
11	Nein	Nein	Nein	Nein
12	Nein	Nein	Nein	Ja
13	Nein	Ja	Nein	Nein
14	Nein	Ja	Nein	Nein
15	Nein	Nein	Nein	Nein
16	Nein	Nein	Nein	Ja
17	Nein	Ja	Nein	Nein
18	Nein	Ja	Nein	Nein
19	Nein	Nein	Nein	Ja
20	Nein	Ja	Nein	Nein
21	Nein	Nein	Nein	Ja
22	Nein	Nein	Nein	Nein
23	Nein	Ja	Nein	Nein
24	Nein	Nein	Nein	Nein
25	Nein	Ja	Nein	Nein
26	Nein	Nein	Nein	Ja
27	Nein	Ja	Nein	Nein
28	Nein	Nein	Nein	Ja
29	Nein	Ja	Nein	Nein
30	Nein	Ja	Nein	Nein
31	Nein	Nein	Nein	Ja
32	Nein	Ja	Nein	Nein
33	Nein	Nein	Nein	Nein
34	Nein	Nein	Nein	Nein
35	Nein	Ja	Nein	Nein
36	Nein	Ja	Ja	Nein
37	Nein	Ja	Nein	Nein
38	Nein	Ja	Nein	Nein
39	Nein	Nein	Nein	Ja
40	Nein	Nein	Nein	Ja
41	Nein	Nein	Nein	Nein
42	Nein	Ja	Nein	Nein
43	Nein	Nein	Nein	Nein
44	Nein	Nein	Nein	Nein
45	Nein	Ja	Ja	Nein
46	Nein	Ja	Nein	Nein
47	Nein	Ja	Nein	Nein

Tabelle 9.5: *Antworten zur Complianceanforderung: C5, ISO 27001, NIST CSF, keine bekannt*

Nr.	Frage 7: Keine Anforderungen	Frage 7: Keine Angabe	Frage 7: Andere
1	Nein	Nein	Nein
2	Ja	Ja	Nein
3	Nein	Nein	Nein
4	Nein	Nein	Nein
5	Nein	Nein	Nein
6	Nein	Nein	Nein
7	Nein	Nein	Nein
8	Nein	Nein	Nein
9	Nein	Nein	Nein
10	Nein	Nein	Nein
11	Nein	Nein	Nein
12	Nein	Nein	Nein
13	Nein	Nein	Nein
14	Nein	Nein	Nein
15	Nein	Nein	Nein
16	Nein	Nein	Nein
17	Nein	Nein	Nein
18	Nein	Nein	Nein
19	Ja	Nein	Nein
20	Nein	Nein	Nein
21	Nein	Nein	Nein
22	Nein	Nein	Nein
23	Nein	Nein	Nein
24	Nein	Ja	Nein
25	Nein	Nein	Nein
26	Nein	Nein	Nein
27	Nein	Nein	Nein
28	Nein	Nein	Nein
29	Nein	Nein	Nein
30	Nein	Nein	Nein
31	Nein	Nein	Nein
32	Nein	Nein	Nein
33	Ja	Nein	Nein
34	Ja	Nein	Nein
35	Nein	Nein	Nein
36	Nein	Nein	Nein
37	Nein	Nein	Nein
38	Nein	Nein	Nein
39	Nein	Nein	Nein

Tabelle 9.6: *Antworten zur Complianceanforderung: keine oder andere Anforderungen)(1/2)*

Nr.	Frage 7: Keine Anforderungen	Frage 7: Keine Angabe	Frage 7: Andere
40	Nein	Nein	Nein
41	Nein	Nein	Ich bin mir nicht sicher wie die heißen, aber wir müssen bei jedem Projekt der in Produktion geht mehrere Frameworks erfüllen.
42	Nein	Nein	Nein
43	Ja	Nein	Nein
44	Ja	Nein	Nein
45	Nein	Nein	Nein
46	Nein	Nein	Nein
47	Nein	Nein	Nein
48	Nein	Nein	Nein

Tabelle 9.7: *Antworten zur Complianceanforderung: keine oder andere Anforderungen)(2/2)*

Nr.	Frage: 8	Frage: 9	Frage: 10
1	Nein	Nein	3
2	Nein	Nein	0
3	Ja	Ja	3
4	Nein	Nein	1
5	Nein	Nein	-2
6	Ja	Ja	5
7	Ja	Ja	3
8	Nein	Ja	2
9	Ja	Ja	5
10	Ja	Ja	4
11	Nein	Ja	2
12	Nein	Nein	-2
13	Nein	Nein	4
14	Ja	Ja	4
15	Nein	Ja	3
16	Nein	Ja	1
17	Nein	Ja	2
18	Nein	Ja	-2
19	Nein	Ja	5
20	Ist mir nicht bekannt	Ja	5
21	Ja	Ja	4
22	Ja	Ja	2
23	Ja	Ja	5
24	Ja	Ja	5
25	Ja	Ja	3
26	Ja	Ja	5
27	Ja	Ja	3
28	Ja	Ja	5
29	Ja	Ja	2
30	Ja	Ja	3
31	Ja	Ja	3
32	Ja	Ja	3
33	Ja	Ja	4
34	Nein	Ja	-3
35	Ja	Ja	4
36	Ja	Ja	4
37	Ja	Nein	3
38	Ja	Nein	-5
39	Ja	Ja	5

Tabelle 9.8: *Antworten zu Fragen zur Priorisierung von Softwaresicherheit im Unternehmen (1/2)*

Nr.	Frage: 8	Frage: 9	Frage: 10
40	Ja	Ja	3
41	Ja	Ja	2
42	Ja	Ja	3
43	Ja	Ja	5
44	Ja	Ja	4
45	Ja	Ja	4
46	Ja	Ja	4
47	Ja	Ja	4
48	Ja	Ja	5

Tabelle 9.9: *Antworten zu Fragen zur Priorisierung von Softwaresicherheit im Unternehmen (2/2)*

Nr.	Frage 11: Konzeption/-Design	Frage 11: Entwicklung	Frage 11: Betrieb
1	Nein	Nein	Nein
2	Nein	Nein	Nein
3	Ja	Ja	Ja
4	Ja	Ja	Ja
5	Nein	Nein	Nein
6	Ja	Ja	Ja
7	Ja	Nein	Nein
8	Nein	Ja	Nein
9	Ja	Ja	Ja
10	Nein	Nein	Nein
11	Nein	Ja	Nein
12	Nein	Nein	Nein
13	Nein	Nein	Nein
14	Nein	Ja	Ja
15	Nein	Nein	Nein
16	Nein	Nein	Ja
17	Nein	Nein	Nein
18	Nein	Nein	Ja
19	Nein	Nein	Nein
20	Nein	Nein	Nein
21	Nein	Ja	Ja
22	Ja	Ja	Ja
23	Ja	Ja	Ja
24	Ja	Ja	Ja
25	Nein	Nein	Nein
26	Ja	Ja	Ja
27	Ja	Ja	Nein
28	Ja	Ja	Ja
29	Ja	Ja	Ja
30	Nein	Nein	Nein
31	Nein	Ja	Nein
32	Nein	Nein	Nein
33	Ja	Ja	Ja
34	Nein	Nein	Nein
35	Nein	Nein	Ja
36	Nein	Ja	Ja
37	Nein	Ja	Nein
38	Nein	Nein	Nein
39	Ja	Ja	Ja

Tabelle 9.10: *Antworten zu Fragen zur Integration von Sicherheitsmaßnahmen in Konzeption, Entwicklung und Betrieb der Software (1/2)*

Nr.	Frage 11: Konzeption/-Design	Frage 11: Entwicklung	Frage 11: Betrieb
40	Ja	Ja	Nein
41	Ja	Ja	Ja
42	Ja	Ja	Ja
43	Ja	Ja	Ja
44	Nein	Nein	Nein
45	Ja	Nein	Nein
46	Ja	Ja	Ja
47	Ja	Ja	Ja
48	Ja	Ja	Ja

Tabelle 9.11: *Antworten zu Fragen zur Integration von Sicherheitsmaßnahmen in Konzeption, Entwicklung und Betrieb der Software (2/2)*

Nr.	Frage 11: nach Bedarf	Frage 11: nicht integriert	Frage 11: Nicht bekannt
1	Ja	Nein	Nein
2	Ja	Nein	Nein
3	Nein	Nein	Nein
4	Nein	Nein	Nein
5	Ja	Nein	Nein
6	Ja	Nein	Nein
7	Nein	Nein	Nein
8	Nein	Nein	Nein
9	Nein	Nein	Nein
10	Ja	Nein	Nein
11	Nein	Nein	Nein
12	Nein	Nein	Ja
13	Ja	Nein	Nein
14	Nein	Nein	Nein
15	Nein	Nein	Ja
16	Nein	Nein	Nein
17	Ja	Ja	Nein
18	Nein	Nein	Nein
19	Nein	Ja	Nein
20	Nein	Ja	Nein
21	Nein	Nein	Nein
22	Nein	Nein	Nein
23	Nein	Nein	Nein
24	Nein	Nein	Nein
25	Ja	Nein	Nein
26	Nein	Nein	Nein
27	Nein	Nein	Nein
28	Nein	Nein	Nein
29	Nein	Nein	Nein
30	Nein	Nein	Ja
31	Nein	Nein	Nein
32	Nein	Nein	Ja
33	Nein	Nein	Nein
34	Nein	Nein	Ja
35	Nein	Nein	Nein
36	Nein	Nein	Nein
37	Nein	Nein	Nein
38	Nein	Nein	Ja
39	Nein	Nein	Nein

Tabelle 9.12: *Antworten zu Fragen zur Integration von Sicherheitsmaßnahmen in Softwareentwicklung (1/2)*

Nr.	Frage 11: nach Bedarf	Frage 11: nicht integriert	Frage 11: Nicht bekannt
40	Nein	Nein	Nein
41	Nein	Nein	Nein
42	Nein	Nein	Nein
43	Nein	Nein	Nein
44	Nein	Nein	Ja
45	Nein	Nein	Nein
46	Nein	Nein	Nein
47	Nein	Nein	Nein
48	Nein	Nein	Nein

Tabelle 9.13: *Antworten zu Fragen zur Integration von Sicherheitsmaßnahmen in Softwareentwicklung (2/2)*

Nr.	Frage: 12	Frage: 13	Frage: 14
1	Nein	Nein	Ja
2	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
3	Ja	Ja	Ja
4	Ja	Nein	Ja
5	Nein		Ist mir nicht bekannt
6	Ja	Ist mir nicht bekannt	Ist mir nicht bekannt
7	Ja	Ja	Ja
8	Nein	Nein	Ja
9	Ja	Ja	Ja
10	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
11	Nein		Ja
12	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
13	Ja	Nein	Ja
14	Nein		Ja
15	Nein		Ja
16	Nein	Nein	Ja
17	Nein		Nein
18	Nein	Ist mir nicht bekannt	Ja
19	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
20	Nein	Nein	Nein
21	Ist mir nicht bekannt	Ist mir nicht bekannt	Ja
22	Ist mir nicht bekannt	Ist mir nicht bekannt	Ja
23	Ja	Ja	Ja
24	Ja	Ist mir nicht bekannt	Ist mir nicht bekannt
25	Ja	Nein	Nein
26	Ja		Ja
27	Nein	Ist mir nicht bekannt	Ja
28	Ja	Ja	Nein
29	Ist mir nicht bekannt	Ist mir nicht bekannt	Ja
30	Ja	Ist mir nicht bekannt	Ist mir nicht bekannt
31	Ja	Ja	Ja
32	Ist mir nicht bekannt	Ja	Ja
33	Nein		Ja
34	Ist mir nicht bekannt	Ist mir nicht bekannt	Nein
35	Nein	Ist mir nicht bekannt	Ja
36	Ja	Ja	Ja
37	Ja	Ist mir nicht bekannt	Ja
38	Ist mir nicht bekannt		Ja
39	Nein		Nein

Tabelle 9.14: *Antworten zu Fragen zur Bedrohungsanalyse und Überprüfung von Software auf Schwachstellen (2/2)*

Nr.	Frage: 12	Frage: 13	Frage: 14
40	Ja	Ja	Nein
41	Ja	Ja	Ist mir nicht bekannt
42	Ist mir nicht bekannt	Ist mir nicht bekannt	Ja
43	Ja	Ist mir nicht bekannt	Ja
44	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
45	Ja	Ja	Ja
46	Ja	Ja	Ja
47	Ja	Ja	Ja
48	Nein	Nein	Ja

Tabelle 9.15: *Antworten zu Fragen zur Bedrohungsanalyse und Überprüfung von Software auf Schwachstellen (2/2)*

Nr.	Frage: 15	Frage: 16	Frage: 17
1	Ja, automatisiert		Nein
2			Ist mir nicht bekannt
3	Ja, automatisiert	Pentests (extern)	Ja
4	Ja, bei Produktabnahme	Code Reviews (4 Augen Prinzip)	Ist mir nicht bekannt
5			Ist mir nicht bekannt
6	Ist mir nicht bekannt		Ist mir nicht bekannt
7	Ja, manuell getriggert		Ja
8	Ja, manuell getriggert		Ist mir nicht bekannt
9	Ja, automatisiert		Ja
10	Ist mir nicht bekannt		Ist mir nicht bekannt
11	Ja, manuell getriggert		Ist mir nicht bekannt
12	Ist mir nicht bekannt		Ist mir nicht bekannt
13	Ja, bei Produktabnahme		Ist mir nicht bekannt
14	Ja, manuell getriggert		Ja
15	Ja, manuell getriggert	Schulungen durch die IT Abteilung	Ist mir nicht bekannt
16	Ja, bei Produktabnahme		Nein
17		Es wird sich auf das Know-How der Entwickler verlassen ...	Ist mir nicht bekannt
18	Nein	Patches	Ist mir nicht bekannt
19	Ist mir nicht bekannt		Ist mir nicht bekannt
20	Nein		Nein
21	Ja, automatisiert	Dependency updates mit renovate Trivy scan Sonarqube scans	Nein
22	Ja, manuell getriggert	4augenprinzip, immer Mal wieder pentest	Ist mir nicht bekannt
23	Ja, automatisiert		Ja
24	Ist mir nicht bekannt		Ja
25	Nein	Lol	Ist mir nicht bekannt
26	Ja, bei Produktabnahme		Ja
27	Ja, automatisiert		Ja
28	Nein		Ja
29	Ja, automatisiert		Ja
30	Ist mir nicht bekannt		Ist mir nicht bekannt
31	Ja, automatisiert		Ist mir nicht bekannt
32	Ja, automatisiert		Nein
33	Ja, bei Produktabnahme	SAST	Nein
34			Ist mir nicht bekannt
35	Ja, automatisiert		Ist mir nicht bekannt

Tabelle 9.16: *Antworten zu Fragen zur Regelmäßigkeit von Scans und zusätzliche Sicherheitsmaßnahmen (1/2)*

Nr.	Frage: 15	Frage: 16	Frage: 17
36	Ja, manuell getriggert	Kryptographische Mechanismen aus eigener Entwicklung	Ja
37	Ja, manuell getriggert		Ja
38			Ist mir nicht bekannt
39			Ja
40			Ja
41	Ist mir nicht bekannt	Regelmäßige Pen-tests	Ja
42	Ja, automatisiert		Ja
43	Ist mir nicht bekannt	Schulungen der Mitarbeiter	Ja
44	Ist mir nicht bekannt		Ist mir nicht bekannt
45	Ja, manuell getriggert	Pentests	Ja
46	Ja, automatisiert	Vorgaben für Frequent von SCA, CCA-scans. Verpflichtende jährliche pentests. Scan tools für produktive Infrastruktur via tools wie paloalto prisma cloud oder qualys.	Ja
47	Ja, automatisiert	Interne wie externe Audits	Ist mir nicht bekannt
48	Ja, automatisiert		Nein

Tabelle 9.17: *Antworten zu Fragen zur Regelmäßigkeit von Scans und zusätzliche Sicherheitsmaßnahmen (2/2)*

Nr.	Frage: 18	Frage: 19	Frage: 20
1	Nein	Nein	< 7 Tage
2	Ist mir nicht bekannt		Ist mir nicht bekannt
3	Ja	Ist mir nicht bekannt	< 3 Tage
4	Nein		< 14 Tage
5	Ist mir nicht bekannt		Ist mir nicht bekannt
6	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
7	Ja	Ist mir nicht bekannt	< 7 Tage
8	Ist mir nicht bekannt	Ist mir nicht bekannt	< 14 Tage
9	Ja	Ja	< 7 Tage
10	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
11	Ist mir nicht bekannt		Ist mir nicht bekannt
12	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
13	Nein	Nein	Ist mir nicht bekannt
14	Ist mir nicht bekannt	Ist mir nicht bekannt	< 7 Tage
15	Ist mir nicht bekannt		Ist mir nicht bekannt
16	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
17	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
18	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
19	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
20	Nein	Nein	Ist mir nicht bekannt
21	Nein	Nein	Einen Tag
22	Ja	Ja	Ist mir nicht bekannt
23	Ist mir nicht bekannt	Ist mir nicht bekannt	< 3 Tage
24	Ist mir nicht bekannt	Ist mir nicht bekannt	Einen Tag
25	Ist mir nicht bekannt	Ist mir nicht bekannt	They don't
26	Ist mir nicht bekannt	Ist mir nicht bekannt	< 3 Tage
27	Ja	Ja	< 14 Tage
28	Ist mir nicht bekannt	Ist mir nicht bekannt	< 7 Tage
29	Ja	Ja	Ist mir nicht bekannt
30	Ist mir nicht bekannt		Ist mir nicht bekannt
31	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
32	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
33	Nein		< 3 Tage
34	Ist mir nicht bekannt		Ist mir nicht bekannt
35	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
36	Ist mir nicht bekannt	Ist mir nicht bekannt	< 7 Tage
37	Ja	Nein	Ist mir nicht bekannt
38	Ist mir nicht bekannt		Ist mir nicht bekannt
39	Nein		Ist mir nicht bekannt

Tabelle 9.18: *Antworten zu Fragen zur SBOM-Erstellung und Behebung kritischer Schwachstellen (1/2)*

Nr.	Frage: 18	Frage: 19	Frage: 20
40	Nein		Ist mir nicht bekannt
41	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
42	Ja	Ja	Ist mir nicht bekannt
43	Ja	Ja	Ist mir nicht bekannt
44	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
45	Nein	Nein	Einen Tag
46	Nein	Nein	CVEs ab high dürfen nicht deployed werden ohne entsprechende Rechtfertigung (Build-breaker in Pipeline)
47	Ist mir nicht bekannt	Ist mir nicht bekannt	$<$ 3 Tage
48	Ja	Ja	$<$ 14 Tage

Tabelle 9.19: *Antworten zu Fragen zur SBOM-Erstellung und Behebung kritischer Schwachstellen (2/2)*

Nr.	Frage: 21	Frage: 22	Frage: 23
1	Nein	Werden nur bei besonders kritischer Schwachstelle informiert, wenn Gefahr für den Kunden besteht.	Ist mir nicht bekannt
2	Ist mir nicht bekannt		
3	Ja	Mail	Ja
4	Ja	Mail	Ja
5	Ist mir nicht bekannt		
6	Ist mir nicht bekannt		Ist mir nicht bekannt
7	Ja	Mail	Ja
8	Ist mir nicht bekannt	Mail	Ja
9	Ja	Mail	Ja
10	Ja	Mail	Ja
11	Ja	Mail	Ist mir nicht bekannt
12	Ist mir nicht bekannt		Ist mir nicht bekannt
13	Nein		Nein
14	Ja	Mail	Ja
15	Ist mir nicht bekannt		
16	Ist mir nicht bekannt		Ist mir nicht bekannt
17	Ist mir nicht bekannt	Mail	Ist mir nicht bekannt
18	Ist mir nicht bekannt	Mail	Ist mir nicht bekannt
19	Ja	Mail	Ist mir nicht bekannt
20	Ist mir nicht bekannt	Unbekannt	Ist mir nicht bekannt
21	Nein	Die Software selbst (z.B. per Pop-Up)	Nein
22	Ja	Mail	Ja
23	Ist mir nicht bekannt		Ist mir nicht bekannt
24	Ja		Ja
25	Nein	Nie	Nein
26	Ja	Telefon	
27	Ist mir nicht bekannt	Mail	Ist mir nicht bekannt
28	Ja	Mail	Nein
29	Ja	?	Ist mir nicht bekannt
30	Ist mir nicht bekannt		Ist mir nicht bekannt
31	Ist mir nicht bekannt		
32	Ist mir nicht bekannt		
33	Der Kunde scant selber	Messenger	Ja
34	Ist mir nicht bekannt		
35	Ja	Mail	Ist mir nicht bekannt

Tabelle 9.20: *Antworten zu Fragen zur Kundenkommunikation über Schwachstellen (1/2)*

Nr.	Frage: 21	Frage: 22	Frage: 23
36	Ja	Vulnerability Exploitability eXchange (VEX)	Ja
37	Ja	Die Software selbst (z.B. per Pop-Up)	Ja
38	Ist mir nicht bekannt		
39	Ja		
40	Ist mir nicht bekannt		
41	Ja	Mail	Ja
42	Ja	Abhängig von der vereinbarten Verantwortung per Mail durch uns oder durch die Software/Pipeline selbst	Ja
43	Ist mir nicht bekannt		Ist mir nicht bekannt
44	Ist mir nicht bekannt	Mail	Ist mir nicht bekannt
45	Ja	Mail	Ja
46	Ja	Status page des Services	Ja
47	Ja	Telefon	Ja
48	Nein	Vulnerability Exploitability eXchange (VEX)	Nein

Tabelle 9.21: *Antworten zu Fragen zur Kundenkommunikation über Schwachstellen (2/2)*

Nr.	Frage: 24	Frage: 25	Frage: 26
1	Nein	Nein	Nein
2	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist es nicht unsicher die Schwachstelle zu veröffentlichen?
3	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
4	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
5	Ist mir nicht bekannt	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
6	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
7	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
8	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
9	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ja
10	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
11	Ist mir nicht bekannt	Ja	Ist mir nicht bekannt
12	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
13	Nein	Nein	Nein
14	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
15	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
16	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
17	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
18	Ist mir nicht bekannt	Nein	Ist mir nicht bekannt
19	Ist mir nicht bekannt	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
20	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
21	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Nein
22	Ja - genaue Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt

Tabelle 9.22: *Antworten zu Fragen zu Angaben zu Zeitrahmen, Dokumentation und Veröffentlichung von Schwachstellen (1/2)*

Nr.	Frage: 24	Frage: 25	Frage: 26
23	Ist mir nicht bekannt	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
24	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
25	Nein	Ist mir nicht bekannt	Nein
26	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ja
27	Ja - ungefähre Angaben	Ja	Ja
28	Ja - genaue Angaben	Ja	Ja
29	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
30	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
31	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
32	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
33	Ist mir nicht bekannt	Ja	Nein
34	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
35	Nein	Ist mir nicht bekannt	Ist mir nicht bekannt
36	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ja
37	Ja - ungefähre Angaben	Nein	Ist mir nicht bekannt
38	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
39	Nein	Ja	Ist mir nicht bekannt
40	Nein	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Nein
41	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
42	Ja - ungefähre Angaben	Ja	Nein
43	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
44	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
45	Nein	Ja	Ist mir nicht bekannt
46	Ja - ungefähre Angaben	Schwachstellen werden nicht durch den Kunden/ Nutzer behoben	Ist mir nicht bekannt
47	Ja - genaue Angaben	Ja	Nein
48	Nein	Ja	Nein

Tabelle 9.23: *Antworten zu Fragen zu Angaben zu Zeitrahmen, Dokumentation und Veröffentlichung von Schwachstellen (2/2)*

Nr.	Frage: 27	Frage: 28	Frage: 29
1		Nein	
2		Kontaktformular auf der Website	Nutzung des normalen Kontaktformulars
3	Ja		
4	Ist mir nicht bekannt	Ja	
5		Nein	
6	Ist mir nicht bekannt	Ist mir nicht bekannt	
7	Ist mir nicht bekannt	Ja	
8	Ist mir nicht bekannt	Ja	
9	Ja	Ja	Mail an security@... oder über unser BugBounty-Programm
10	Ist mir nicht bekannt	Ja	
11	Ist mir nicht bekannt	Ist mir nicht bekannt	
12	Ist mir nicht bekannt	Ist mir nicht bekannt	
13	Nein	Nein	
14	Ist mir nicht bekannt	Ja	
15	Ist mir nicht bekannt	Nein	
16	Ist mir nicht bekannt	Ja	
17		Nein	
18	Ist mir nicht bekannt	Ist mir nicht bekannt	
19	Ist mir nicht bekannt	Ist mir nicht bekannt	
20	Ist mir nicht bekannt	Ist mir nicht bekannt	
21	Nein	Ja	Verschlüsselte Email via security.txt direkt an das Operations Team
22	Ist mir nicht bekannt	Ja	
23	Ist mir nicht bekannt	Ja	
24	Ist mir nicht bekannt	Ja	
25	Nein	Wir verklagen jeden	Schlecht. Per anonymen Brief an den Hauptsitz wäre wahrscheinlich am besten. Ansonsten eher schwer
26	Ja	Ja	
27	Ist mir nicht bekannt	Ja	Mail
28	Nein	Ja	
29	Ist mir nicht bekannt	Nein	

Tabelle 9.24: *Antworten zu Fragen zum Meldeprozess für durch Dritte entdeckte Schwachstellen (1/2)*

Nr.	Frage: 27	Frage: 28	Frage: 29
30	Ist mir nicht bekannt	Ist mir nicht bekannt	
31		Ist mir nicht bekannt	
32	Ist mir nicht bekannt	Ist mir nicht bekannt	
33		Ist mir nicht bekannt	
34		Ist mir nicht bekannt	
35	Ist mir nicht bekannt	Ja	Mailkontakt
36	Ja	Ja	
37	Ist mir nicht bekannt	Ja	
38		Ist mir nicht bekannt	
39		Nein	
40	Nein	Ja	E-Mail oder Issue post auf dem public GitHub repository
41	Ist mir nicht bekannt	Ja	
42	Ist mir nicht bekannt	Nein	
43	Ist mir nicht bekannt	Ist mir nicht bekannt	
44	Ist mir nicht bekannt	Ist mir nicht bekannt	
45		Ja	Security.txt, E-Mail Kontakt
46	Ja	Gut dokumentierter Prozess inklusive safe harbor Erklärung	Hochladen von Berichten bei Intigriti
47	Nein	Ja	Jede Form vertraulicher Kommunikation wird akzeptiert
48	Nein	Ja	security.txt

Tabelle 9.25: *Antworten zu Fragen zum Meldeprozess für durch Dritte entdeckte Schwachstellen (2/2)*

Nr.	Frage: 30	Frage: 31	Frage: 32
1	Ist mir nicht bekannt	Ist mir nicht bekannt	
2	Ist mir nicht bekannt	Ja	Ja
3	Ja	Ja	Nein
4	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	
5	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Nein
6	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Ist mir nicht bekannt
7	Ja	Ja	Ja
8	Ja	Ja	Nein
9	Ja	Ja	
10	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
11	Ja	Ja	Ja
12	Ja	Ja	Ja
13	Nein	Ja	Ist mir nicht bekannt
14	Ja	Ja	Ist mir nicht bekannt
15	Nein	Nein	Nein
16	Ja	Ja	Nein
17	Ja	Ja	Ja
18	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
19	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
20	Nein	Ja	Ist mir nicht bekannt
21	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Ist mir nicht bekannt
22	Ja	Ja	Nein
23	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	
24	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
25	Nein	Nein	Nein
26	Ja	Ja	Ja
27	Nein	Ja	Ja
28	Ja	Ja	Ja
29	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Ja

Tabelle 9.26: *Antworten zu Fragen zu Versionierung, Dokumentation und sichere Konfiguration der Software (1/2)*

30	Ist mir nicht bekannt	Ja	Ist mir nicht bekannt
31	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Ja
32	Ja	Ja	Ja
33	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Nein
34	Ist mir nicht bekannt	Ist mir nicht bekannt	
35	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Ja
36	Ja	Ja	Ja
37	Ist mir nicht bekannt	Ja	Ist mir nicht bekannt
38	Ist mir nicht bekannt	Ja	Ist mir nicht bekannt
39	Ja	Ja	Ja
40	Nein	Ja	Ja
41	Ist mir nicht bekannt	Ja	Ja
42	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Nein
43	Ist mir nicht bekannt	Ist mir nicht bekannt	Ist mir nicht bekannt
44	Ja	Ja	Ist mir nicht bekannt
45	Ist mir nicht bekannt	Ja	Ja
46	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	
47	Ja, verschiedene Projekte nutzen unterschiedliche Arten der Versionierung	Ja	Ist mir nicht bekannt
48	Ja	Ja	Nein

Tabelle 9.27: *Antworten zu Fragen zu Versionierung, Dokumentation und sichere Konfiguration der Software (2/2)*

Nr.	Frage: 33	Frage: 34	Frage: 35
1	Keine der genannten	Nein	
2	Keine der genannten	Ja	Ich bin als GF leider nicht so sehr in die Entwicklung involviert, denke aber, dass wir sichere Software bauen. Ich leite den Bogen an meine Entwickler weiter.
3	Passwortmanager	Ja	
4	Keine der genannten	Ja	Wir sind eine Agentur für Softwareentwicklung und liefern verschiedenste Softwareprojekte an Kunden. Viele der Projekte sind unterschiedlich, daher sind keine 100%igen Angaben möglich. Sicherheit ist bei vielen unserer Kunden leider kein Thema, für das sie Geld ausgeben.
5	Keine der genannten	Ja	
6	Sicherheitselemente	Nein	
7	Betriebssysteme (andere)	Nein	
8	Intelligente Zähler	Nein	
9	Keine der genannten	Ja	
10	Keine der genannten	Ist mir nicht bekannt	Ich bin selbst nicht an der Softwareentwicklung beteiligt, bin mir aber sicher, dass Vorgaben eingehalten werden.
11	Industrielle Automatisierungs- und Steuerungssysteme (IACS), nicht KRITIS	Nein	
12	Keine der genannten	Nein	Bisher keinen Kontakt zu der Thematik gehabt...
13	Keine der genannten	Ja	
14	Keine der genannten	Nein	
15	Internet-Browser	Ist mir nicht bekannt	Ich bin keine programmierende Person. Unser Unternehmen betreut Menschen in ihrer Lebensführung. Daten dieser zu schützen ist relevant.

Tabelle 9.28: *Antworten zu Fragen zu Produktkategorien, SaaS-Status und zusätzliche Anmerkungen (1/3)*

Nr.	Frage: 33	Frage: 34	Frage: 35
16	Keine der genannten	Nein	
17	Keine der genannten	Nein	
18	Keine der genannten	Nein	
19	Keine der genannten	Ist mir nicht bekannt	
20	Keine der genannten	Ja	Wir sind noch in einem frühen Stadium der Entwicklung. Einige der Punkte werden ggf. noch adressiert.
21	Keine der genannten	Ja	
22	Keine der genannten	Nein	Bug bei Auswahl iam
23	Keine der genannten	Ist mir nicht bekannt	
24	Keine der genannten	Ist mir nicht bekannt	
25	Keine der genannten	Nein	
26	Public-Key-Infrastrukturen und Ausstellung digitaler Zertifikate	Nein	
27	Keine der genannten	Nein	
28	Public-Key-Infrastrukturen und Ausstellung digitaler Zertifikate	Nein	
29	Industrielle Automatisierungs- und Steuerungssysteme (IACS), nicht KRITIS	Nein	
30	Keine der genannten	Ist mir nicht bekannt	
31	Keine der genannten	Ist mir nicht bekannt	
32	Keine der genannten	Ist mir nicht bekannt	Die Fragen sind primär für Softwareentwickler gedacht. Ein Konzern hat aber wesentlich mehr Abteilungen, die sich mit CRA auseinandersetzen müssen.
33	Keine der genannten	Nein	
34	Keine der genannten	Ist mir nicht bekannt	
35	Keine der genannten	Ja	
36	Netzwerkmanagement, -Konfiguration oder -Monitoring	Nein	
37	Keine der genannten	Ja	
38	Keine der genannten	Nein	
39	Keine der genannten	Ja	

Tabelle 9.29: *Antworten zu Fragen zu Produktkategorien, SaaS-Status und zusätzliche Anmerkungen (2/3)*

Nr.	Frage: 33	Frage: 34	Frage: 35
40	Industrielle Automatisierungs- und Steuerungssysteme (IACS), nicht KRITIS	Nein	
41	Keine der genannten	Ja	
42	Keine der genannten	Nein	
43	Keine der genannten	Nein	
44	Internet-Browser	Ist mir nicht bekannt	
45	Keine der genannten	Nein	
46	Geräte für das industrielle Internet der Dinge (IIoT) im KRITIS Sektor	Nein	
47	Sicherheitselemente	Nein	
48	Sicherheitselemente	Nein	

Tabelle 9.30: *Antworten zu Fragen zu Produktkategorien, SaaS-Status und zusätzliche Anmerkungen (3/3)*