CERTAINITY

universität innsbruck

Preparing for the European Cyber Resilience Act

Get your House in Order Before the New Legislation Hits

Title: European Cyber Resilience Act (CIS Compliance Summit 2023) | Author: Brunner, Sauerwein | Version, Date: 1.1, 19.09.2023 | Confidentiality Class: PUBLIC

Head of Security Engineering
Michael Brunner, PhD.

- Doktoratsstudium Informatik mit Fokus auf **Informationssicherheits- und Risikomanagement**
- Über 15 Jahre Berufserfahrung als IT-, Management-, und **Security-Consultant** sowie als **Software Engineer**
- Branchen-Know-How: Finanzdienstleister, Transportunternehmen, Energieversorger, Automobilhersteller und -zulieferer,
  - Zertifiziert als ISMS Manager und Auditor nach ISO 27001, SABSA Chartered Security Architect (SCF)

Kontaktdaten:

+43 664 9624028

michael.brunner@certainity.com

CERTAINITY

Vorstellung CERTAINITY

OFFENSIVE SECURITY

DEFENSIVE SECURITY

PROCESS CONSULTING

SECURITY ENGINEERING

CERTAINITY

Kontaktieren Sie unmittelbar unsere Experten bei einem Cyber Security Vorfall

cert@certainity.com +43 664 888 44 686

Assistenzprofessor für Security Engineering
DI Clemens Sauerwein, PhD.

- Doktoratsstudium Informatik mit Fokus auf Cyber Threat Intelligence Sharing
- Über 10 Jahre Berufserfahrung in Forschung und Lehre
- Forschungsschwerpunkte
  - Information Security
  - Information Systems
  - Security & Software Engineering Education
- Branchenfokus
  - Finanzdienstleister, Automobilhersteller und Zulieferer, KMUs in der Supply Chain

Kontaktdaten:
Clemens.Sauerwein@uibk.ac.at

universität innsbruck

Was Sie in den nächsten 30 Minuten erwartet

- Vorstellung des European Cyber Resilience Act
- High-Level Vorstellung der zukünftigen Anforderungen an Hersteller vernetzter Produkte mit digitalen Elementen

Studieneckdaten

- Zeitraum May – August 2023
- 42 Teilnehmer:Innen
- Großteil aus dem Bereich Informations-technologie und Kommunikation
- Ca. die Hälfte KMUs

- Umfrage-Ergebnisse der durchgeführten *European Cyber Resilience Act Preparedness* Studie
- Identifizierte Herausforderungen für betroffene Unternehmen

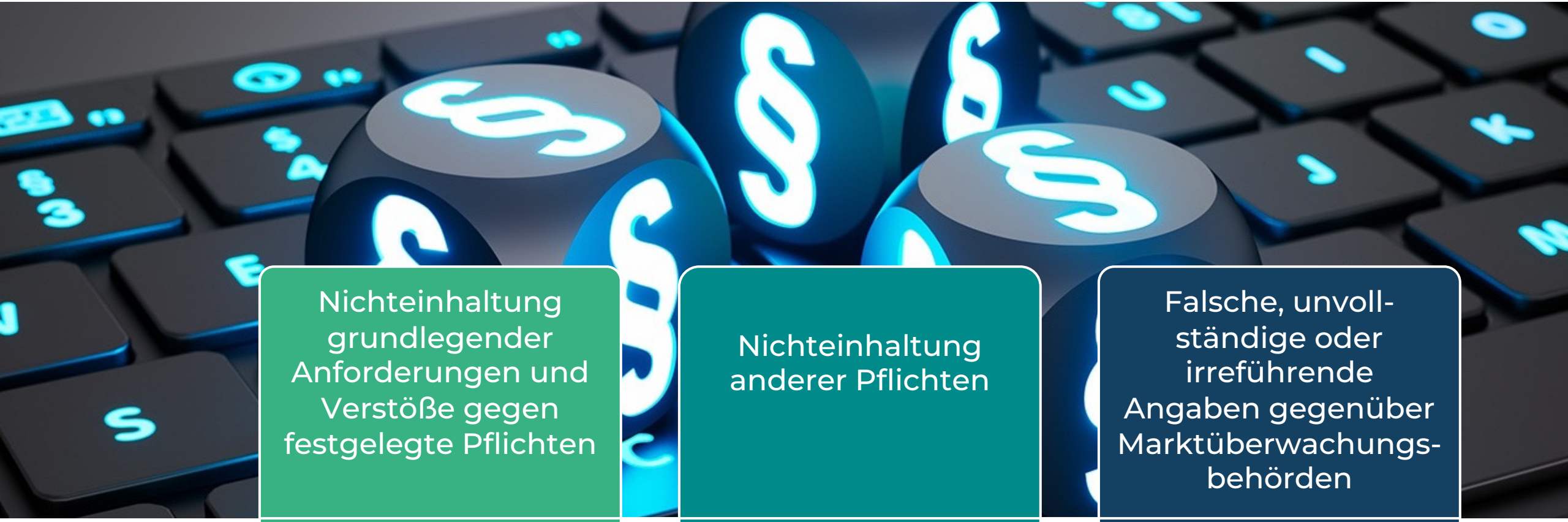
Der European Cyber Resilience Act

CERTAINITY

Der European Cyber Resilience Act – Big Picture

- Der European Cyber Resilience Act ist ein wesentlicher Bestandteil der EU Cyber Security Strategie
- Reglementiert breitenwirksam all jene Produkte und Branchen, die noch nicht durch gesonderte Vorgaben bedacht wurden – Insbesondere Softwareentwicklung im non-embedded Bereich

Strafen



Nichteinhaltung grundlegender Anforderungen und Verstöße gegen festgelegte Pflichten	Nichteinhaltung anderer Pflichten	Falsche, unvollständige oder irreführende Angaben gegenüber Marktüberwachungsbehörden
€ 15.000.000 2,5 % Umsatz (weltweit, Vorjahr)	€ 10.000.000 2 % Umsatz (weltweit, Vorjahr)	€ 5.000.000 1 % Umsatz (weltweit, Vorjahr)

CERTAINITY

Geltungsbereich in EU Legalese

Diese Verordnung gilt für Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische

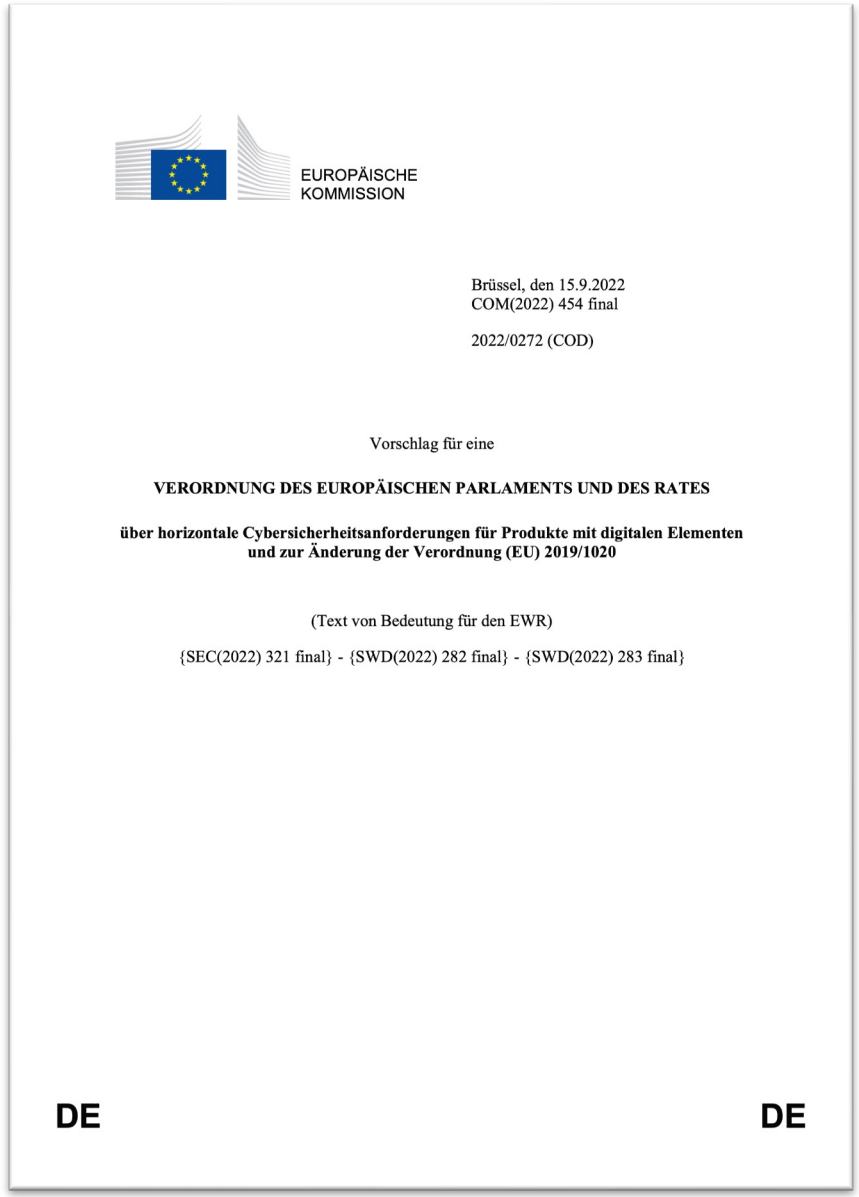
Software oder Hardware

und dessen Datenfernverarbeitungslösungen

Datenverbindung mit einem Gerät oder Netz

Ausnahmen: Services und Software-as-a-Service sowie Produkte, die in Bezug auf Cybersecurity bereits ausreichend reguliert sind (Automotive, Aeronautical, Medizinprodukte, et.)

erfüllen könnte.



EUROPÄISCHE KOMMISSION

Brüssel, den 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

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

(Text von Bedeutung für den EWR)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

DE **DE**

CERTAINITY

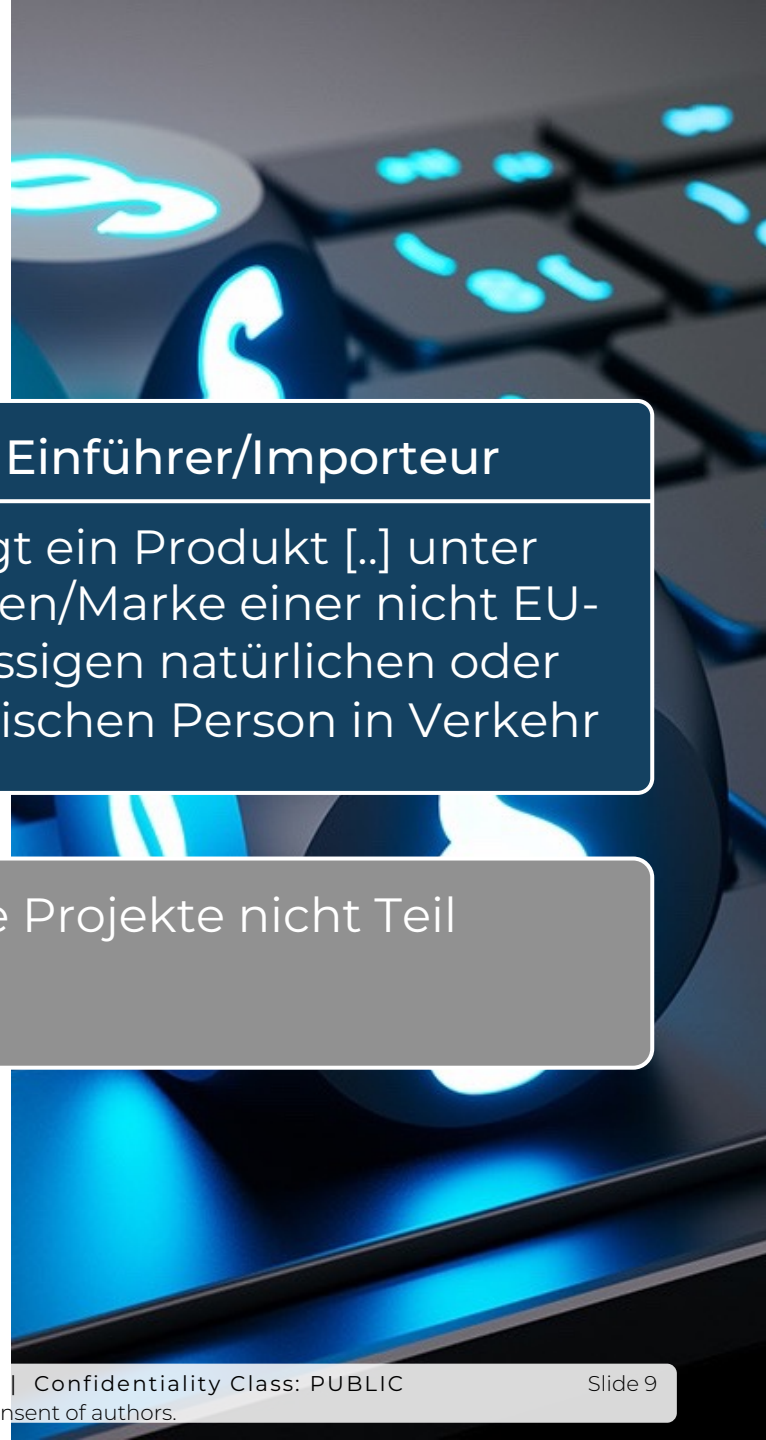
Ausnahmen: Produkte [..|, auf die Verordnungen (EU) 2017/745, 2017/746, 2019/2144 Anwendungen finden; Produkte [..] die nach Verordnung (EU) 2018/1139 zertifiziert sind, Produkte [..] die ausschließlich für Zwecke der nationalen Sicherheit und militärische Zwecke oder zur Verarbeitung von Verschlusssachen konzipiert sind; ...

Betroffene Unternehmen

Der CRA-E betrifft alle Akteure, die vernetzte Produkte mit digitalen Elementen in der EU in Verkehr bringen.

Hersteller	Händler	Einführer/Importeur
Entwickelt oder stellt Produkte [..] her bzw. lässt diese konzipieren, entwickeln oder herstellen	Stellt ein Produkt [..] ohne Änderung seiner Eigenschaften in der EU bereit	Bringt ein Produkt [..] unter Namen/Marke einer nicht EU-ansässigen natürlichen oder juristischen Person in Verkehr

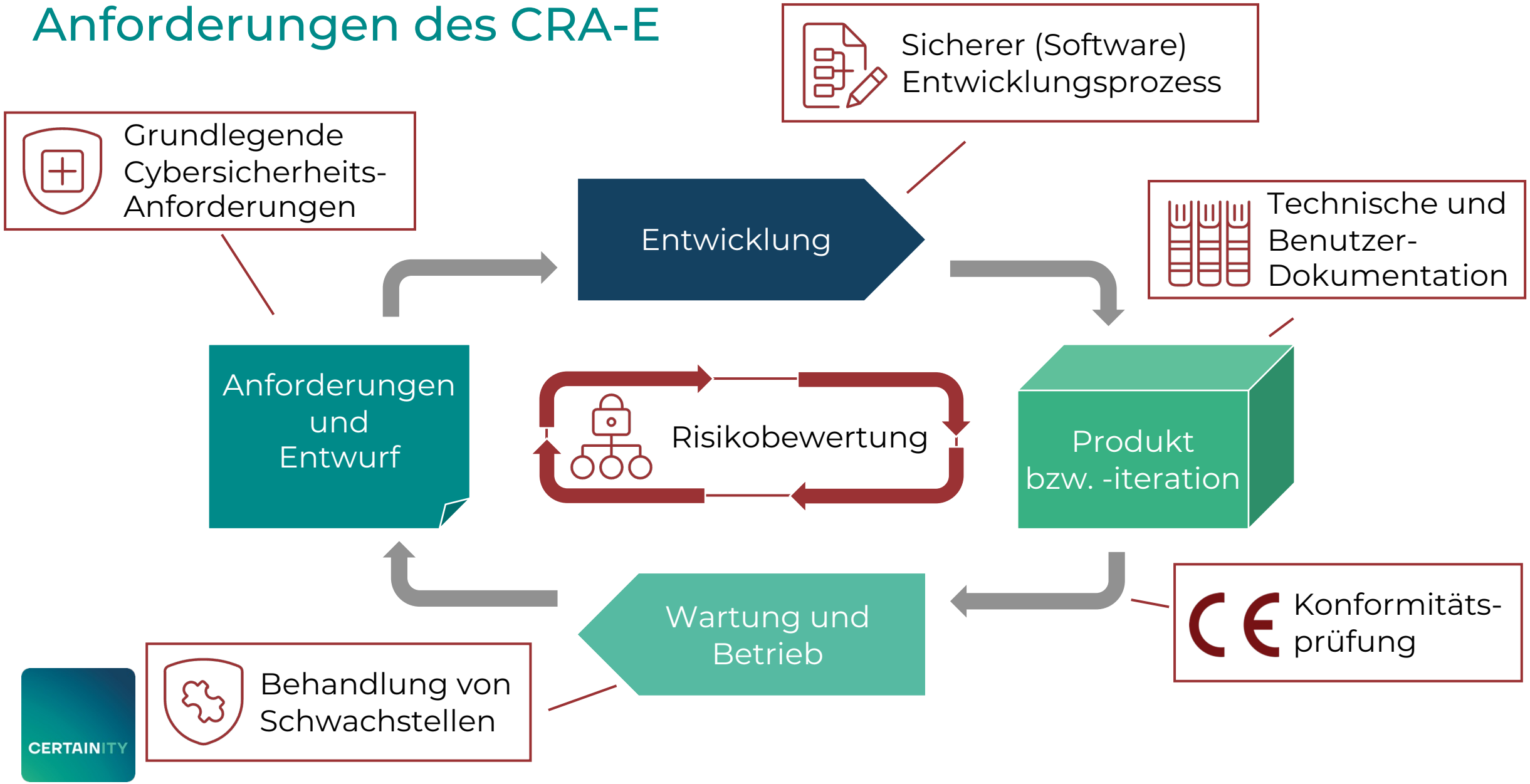
Open Source Projekte sind prinzipiell ausgenommen, solange diese Projekte nicht Teil kommerzieller Aktivitäten sind



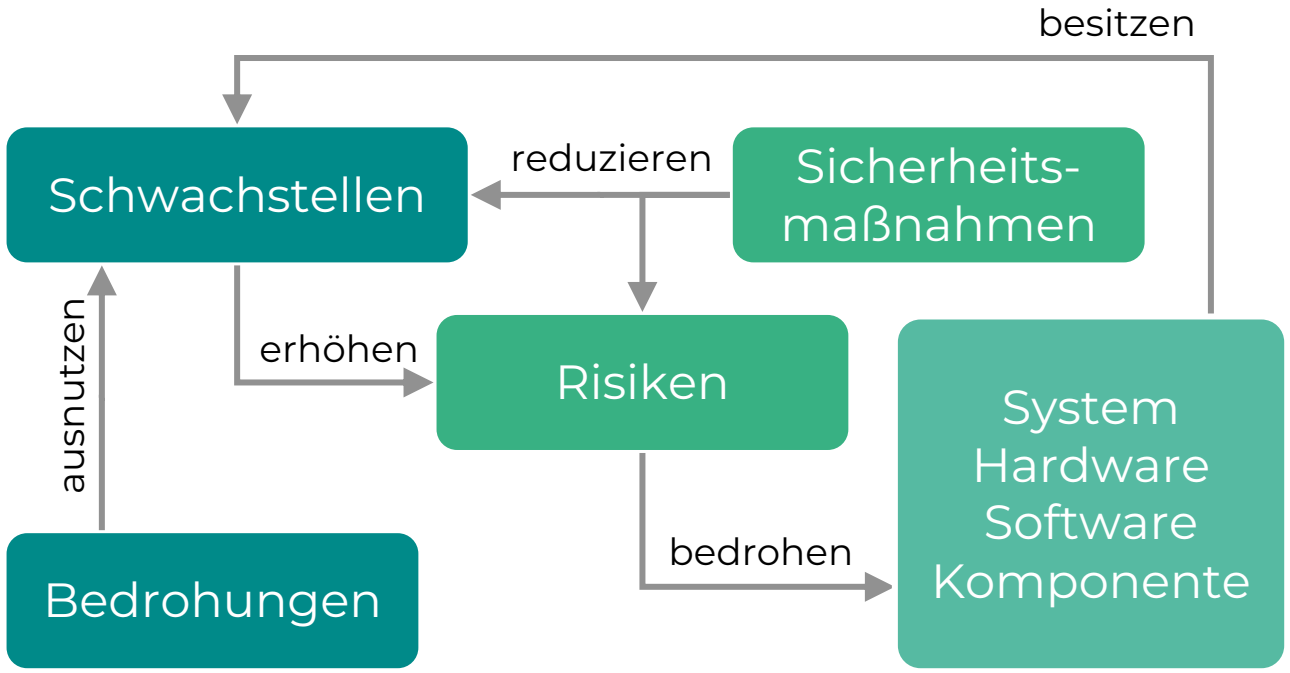
CERTAINITY

Ausschlaggebend ist die kommerzielle Verwertung, unabhängig davon ob Produkte kostenfrei bereitgestellt werden.

Anforderungen des CRA-E



Bewertung von Cybersicherheitsrisiken

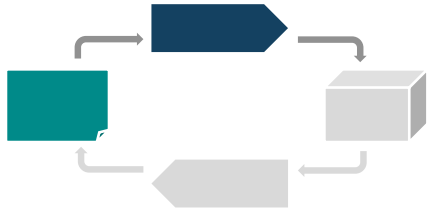


1. Neben einer intrinsischen Betrachtung sind zudem potentielle **Auswirkungen von Sicherheitsvorfällen auf Gesundheit und Sicherheit von Benutzern** zu betrachten!
2. Ebenso die eigenen **negativen Auswirkungen auf die Verfügbarkeit** der **von anderen Geräten** oder Netzen bereitgestellten Dienste

3. **Berücksichtigung von 3rd Party und Lieferketten Risiken**
   - Due Diligence bei Einbindung von 3rd Party Komponenten
   - Keine Beeinträchtigung der Sicherheitseigenschaften

CERTAINITY

Anforderungen an Produktentwicklung



Auf Basis der Bewertung der Cybersicherheitsrisiken müssen Produkte eine Reihe grundlegender Sicherheitsfeatures und Sicherheitseigenschaften umsetzen.

Schutz der Integrität von Befehlen, Programmen und Konfigurationen

Sichere Standard-Konfiguration

+ Reset-Feature

Modernste Verschlüsselung sensibler Daten (Vertraulichkeit)

during processing

at rest | in transit

Verfügbarkeit wesentlicher Funktionen gewährleisten

DoS Resilienz

Kontrollmechanismen zum Schutz vor unbefugtem Zugriff

Auth-Mgmt. | ID-Mgmt.

Minimierung der Angriffsfläche

+ ext. Schnittstellen

Minimierung negativer Auswirkungen auf andere Geräte/Services

Überwachung

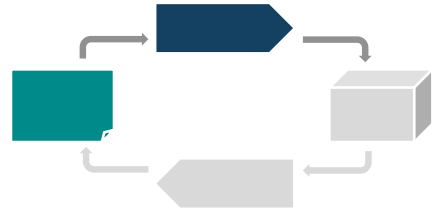
Aufzeichnung sicherheits-bezogener interner Vorgänge

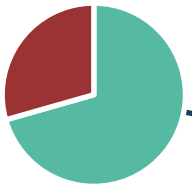
Sicherheitsaktualisierungen zur Behebung von Schwachstellen

User Benachrichtigung | auto. Updates

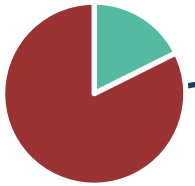
CERTAINITY

Anforderungen an Produktentwicklung





Sichere Standard-Konfiguration



+ Reset-Feature

Modernste Verschlüsselung sensibler Daten (Vertraulichkeit)

Schutz der Integrität von Befehlen, Programmen und Konfigurationen

during processing

at rest | in transit

Verfügbarkeit wesentlicher Funktionen gewährleisten

DoS Resilienz

Kontrollmechanismen zum Schutz vor unbefugtem Zugriff

Auth-Mgmt. | ID-Mgmt.

Minimierung der Angriffsfläche

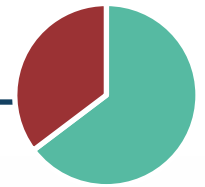
+ ext. Schnittstellen

Minimierung negativer Auswirkungen auf andere Geräte/Services

Überwachung

Aufzeichnung sicherheits-bezogener interner Vorgänge

Sicherheitsaktualisierungen zur Behebung von Schwachstellen



User Benachrichtigung

auto. Updates

Legende:

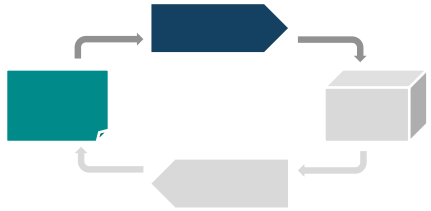
Umgesetzt

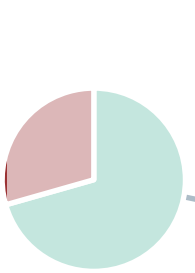
Nicht umgesetzt

CERTAINITY

universität innsbruck

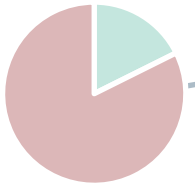
Anforderungen an Produktentwicklung





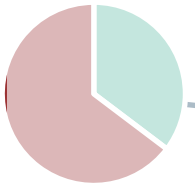
Sichere Standard-Konfiguration

+ Reset-Fea



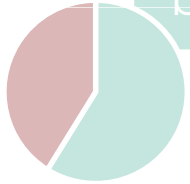
Kontrollme
Schutz vor ur

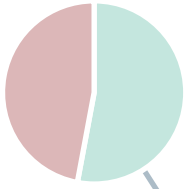
Auth-M



Überwachun

Aufzeichnung sicherheits-bezogener interner Vorgänge





Schutz der Integrität von Befehlen, Programmen und Konfigurationen

Modernste Verschlüsselung
sensibler Daten (Vertraulichkeit)

Verfügbarkeit wesentlicher
gewährleisten

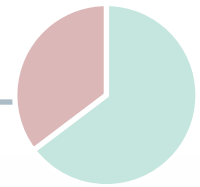
DoS Resilienz

ung negativer
gen auf andere
e/Services

zur
Behebung von Schwachstellen

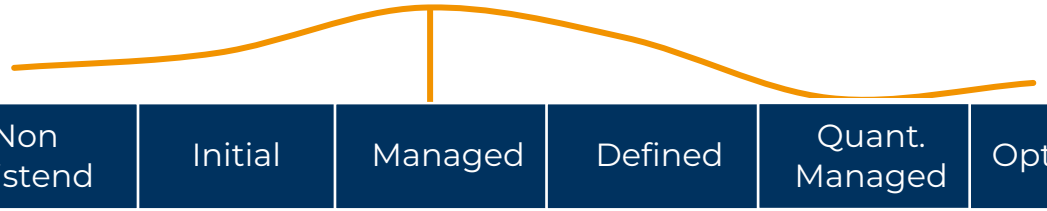
User Benachrichtigung

auto. Updates



Reifegrad Secure Software Development Lifecycle

- Threat Modeling wird von < 25% durchgeführt
- Security Guidelines werden in > 75% eingesetzt



Legende: Umgesetzt / Nicht umgesetzt

CERTAINITY

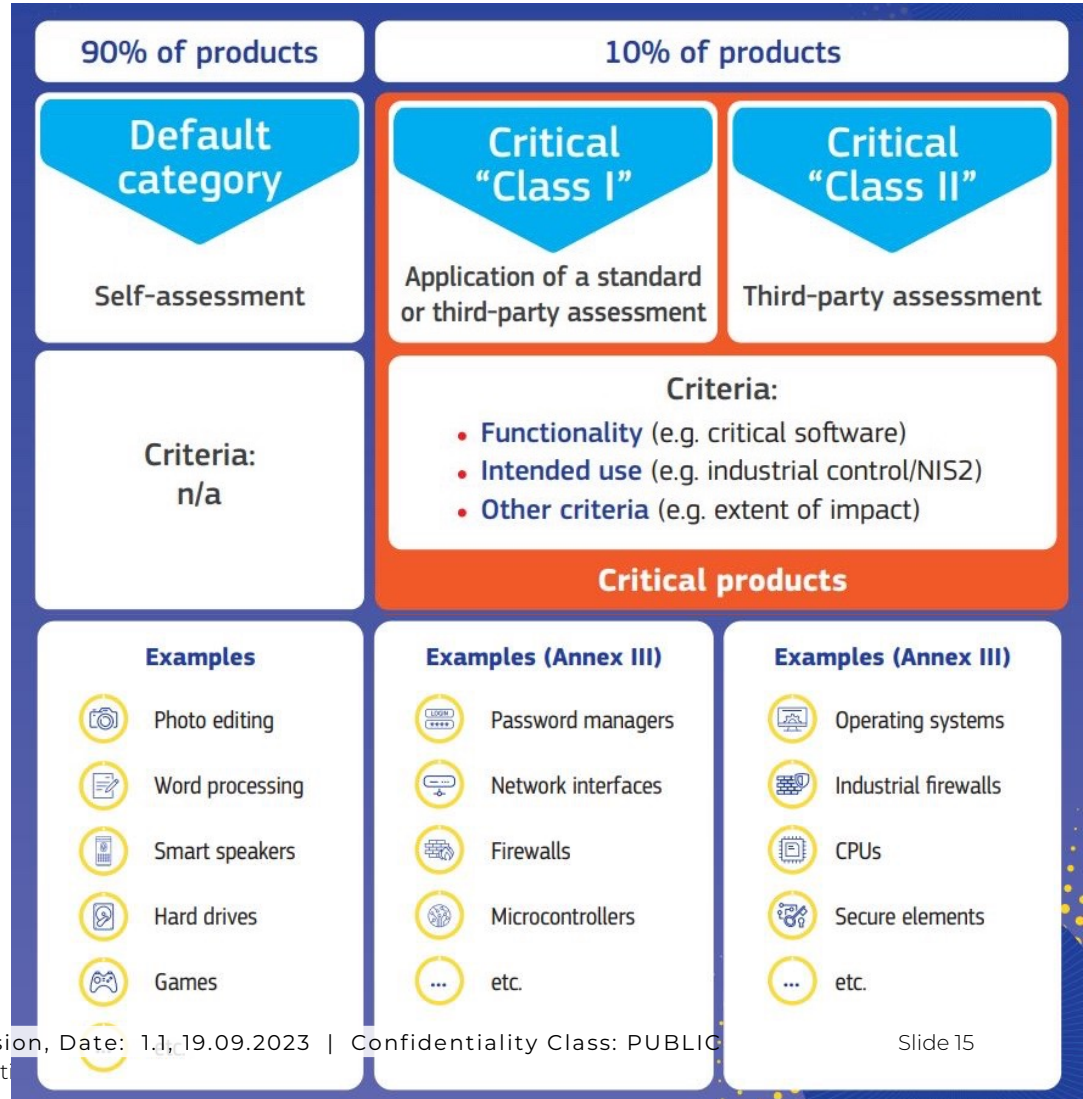
universität innsbruck

Konformitätsprüfung

Die Konformitätsprüfung erfolgt in unterschiedlicher Intensität entsprechend dreier Produkt-Kategorien.

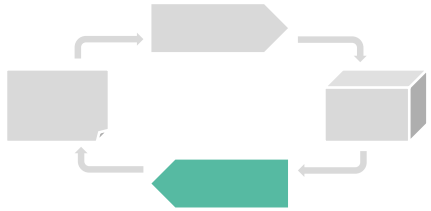
1. Allgemeine Produkte mit digitalen Elementen
   Self Assessment
2. Kritische Produkte mit digitalen Elementen (Class 1)
   Harmonisierte Normen
3. Hoch-kritische Produkte mit digitalen Elementen (Class 2)
   3rd Party Assessment

Die ENISA ist als Aufsichts- und Berichtsbehörde vorgesehen, Europäische Standardisierungs-Organisationen werden mit der Ausarbeitung harmonisierter Normen betraut.

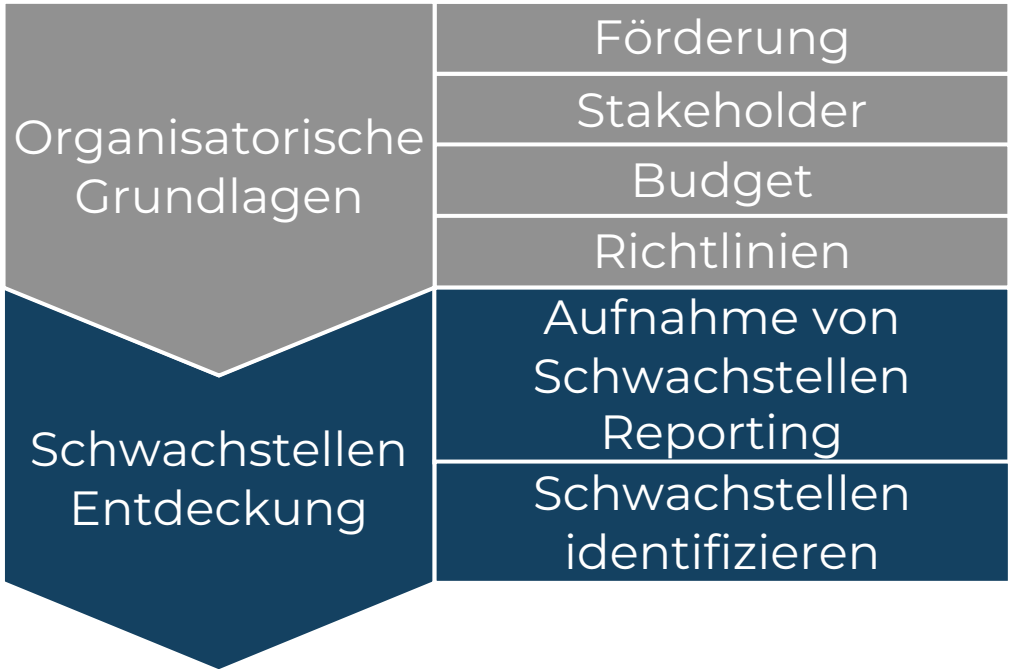


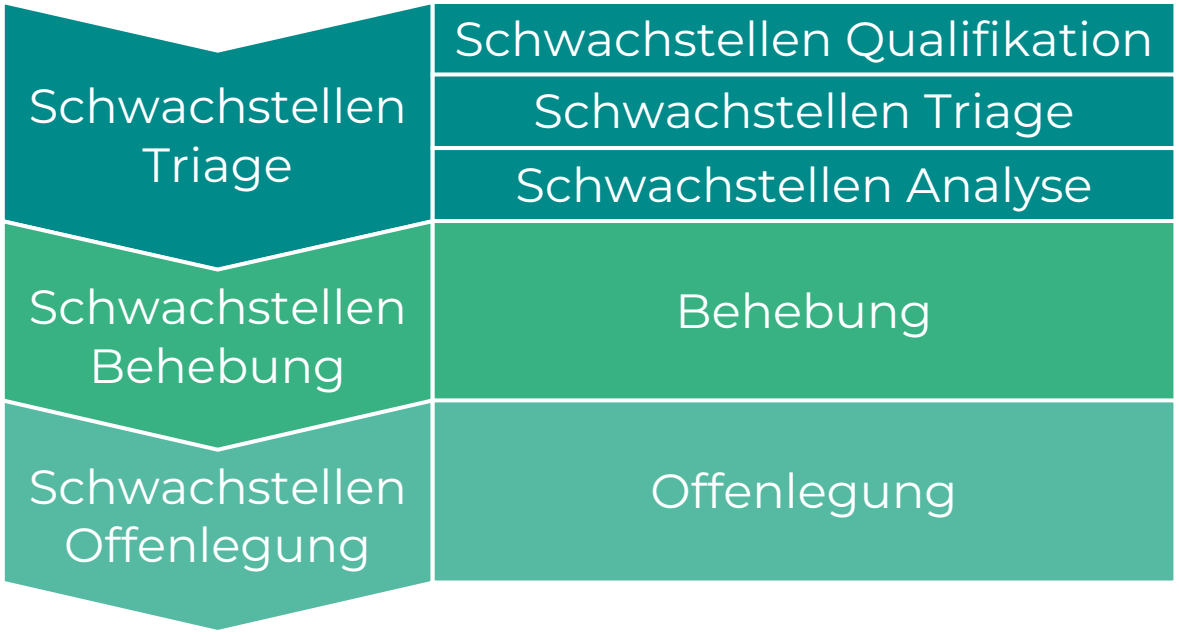
Bildquelle: European Commission, Cyber Resilience Fact Sheet, available at https://ec.europa.eu/newsroom/dae/redirection/document/89528 (accessed June 14th 2023)

Anforderungen an Schwachstellenmanagement



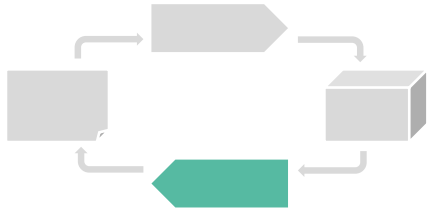
Schaffung der Voraussetzung für effizientes Schwachstellenmanagement durch Umsetzung eines Product Security Incident Response Teams (PSIRT)





CERTAINITY

Anforderungen an Schwachstellenmanagement



Organisatorische Grundlagen

Förderung

Stakeholder

Budget

Richtlinien

Aufnahme von

Schwachstell

Entdeckung

Schwachstellen Triage

Schwachstellen Qualifikation

Schwachstellen Triage

Schwachstellen Analyse

Schwachstellen

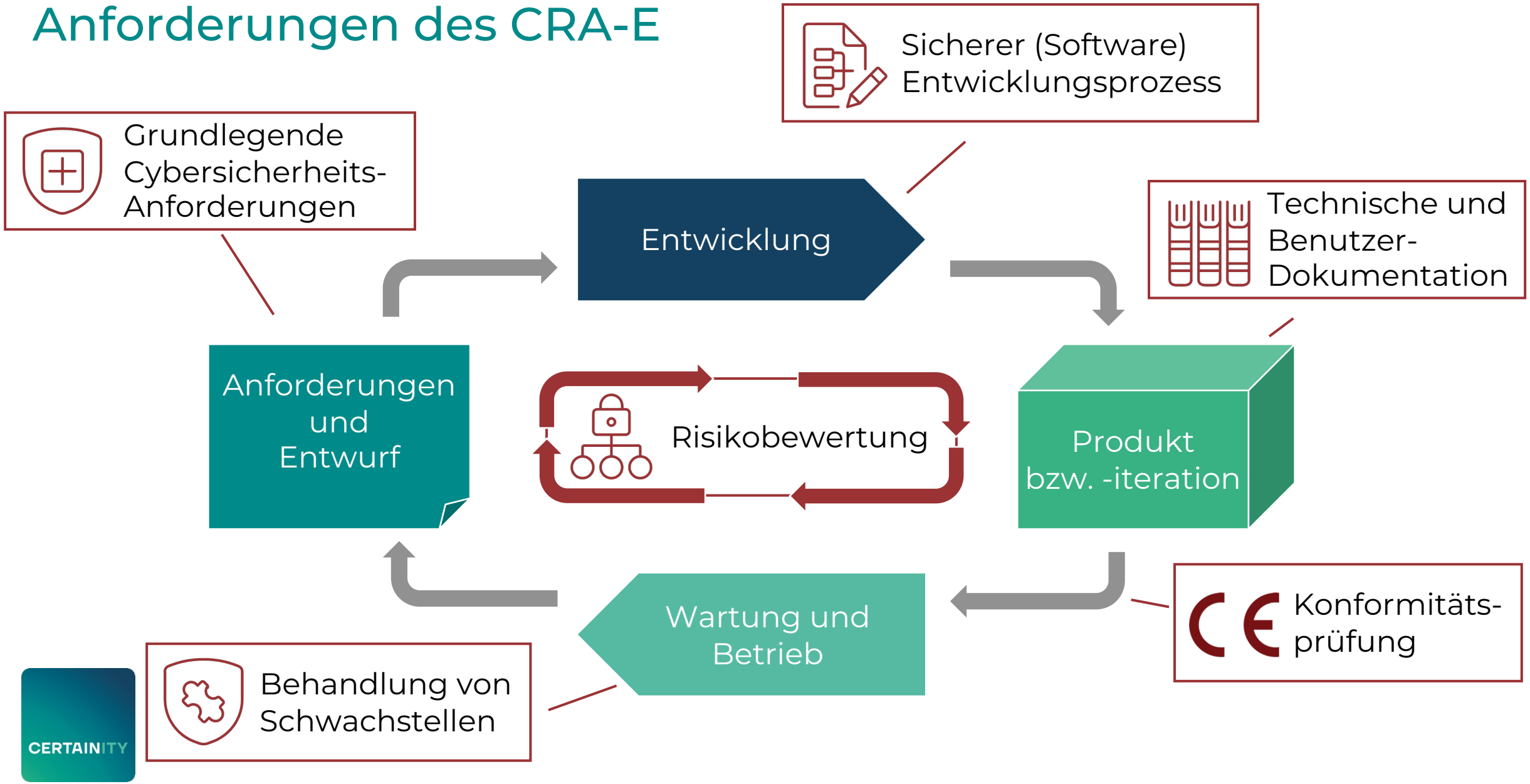
Behebung

Offenlegung

Reifegrad Vulnerability Management Process

- Schwachstellen können telefonisch per Mail und nur z.T. per Kundenportal gemeldet werden
- Security Updates werden überwiegend kostenlos bereit gestellt

Anforderungen des CRA-E



Herausforderungen bei der Umsetzung der Anforderungen

Conclusio

European Cyber Resilience Act (CRA-E) Compliance

Zielsetzung

Prüfung und Umsetzung der gesetzlichen Anforderungen des European Cyber Resilience Act für digitale vernetzte Produkte (Software und Hardware), deren Entwicklungsprozess und der Schwachstellenbehandlung

Fragestellung?

- Sind wir vom European Cyber Resilience Act direkt oder indirekt betroffen?
- Entspricht das Sicherheitsniveau unserer Produkte den gesetzlichen Bestimmungen?
- Sind wir im Stande, Schwachstellen gesetztes-konform zu behandeln?
- Wie können wir die Vorgaben fristgerecht umsetzen?

Vorgehensweise

Workshop zur Vorstellung des CRA-E und Scope-Bestimmung

- Analyse Produkt A
- Assessment Entwicklungsprozess
- Prüfung Behandlung von Schwachstellen

Bericht Status Quo

Roadmap CRA-E Compliance

Auswahl, Erstellung, Einführung, Verbesserung von ...

- Secure Development Practices (SSDLC)
- Product Security Incident Response Team (PSIRT)
- Cyber Risk Assessments
- SBOM
- u.v.m.

CRA-E Compliance

Nutzen

- Strategische Berücksichtigung der Auswirkungen des CRA-E auf Ihren Business Case und Ihr Geschäftsmodell
- Verfügbarkeit Ihrer Produkte am EU Markt absichern
- Vermeidung von Strafzahlungen

CERTAINITY

Warum CERTAINITY?

- ✓ Thought Leader für CRA-E Compliance
- ✓ Pragmatische Assessmentmethodik
- ✓ Ganzheitliche Umsetzungskompetenz

Ergebnisse

Erfüllungsgrad

Optimierungen

Policies und Vorlagen

Methoden und Tools

Prozesse

... für Cyberrisiko Bewertungen, sichere Produktentwicklung, Dokumentation sowie die Behandlung von Security Vorfällen und Schwachstellen

Etablierung erforderlicher technischer und organisatorischer Fähigkeiten

- Essentielle Security Anforderungen an Produkte
- Anforderungen an die Behandlung von Schwachstellen
- Dokumentation
- Assessment

Secure Software Development Lifecycle (SSDLC)

Fragestellung?

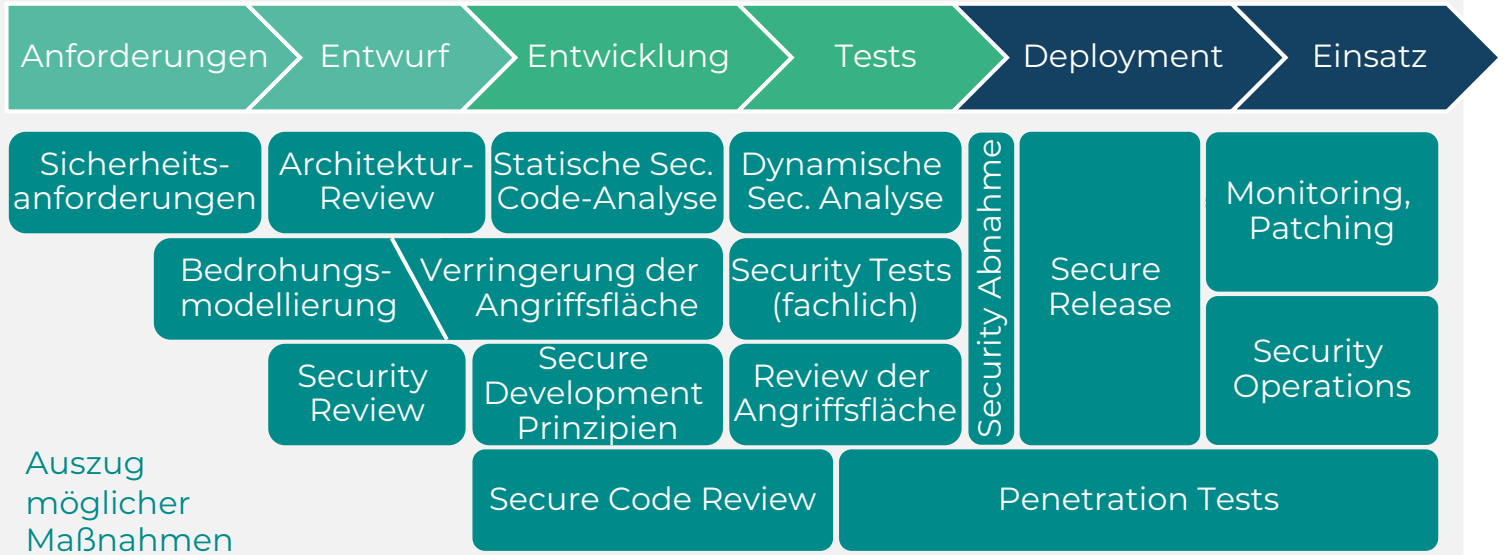
Wie können wir die Sicherheit unserer entwickelten Applikationen, Systeme und Produkte verbessern?

Zielsetzung

Steigerung der Produktsicherheit und Erreichung des erforderlichen Sicherheitsniveaus eigener Applikationen, Systeme und Services durch Einführung und Verbesserung von Praktiken zur sicheren Softwareentwicklung

Vorgehensweise

1. **Workshops** zur Awarenessbildung bei Entwicklern und dem Management, sowie zur Status-Quo Bestimmung
2. **Detailliertes Assessment** des aktuellen Entwicklungsprozesses und der entwickelten Produkte entlang anerkannter Branchen-Best-Practices und anzuwendender Normen
3. **Identifikation von Verbesserungspotenzialen** und **Entwicklung einer Roadmap** zur Umsetzung erforderlicher Maßnahmen
4. **Begleitung der Maßnahmenumsetzung**
5. **Entwicklung angepasster Trainings** und **Coaching** von Schlüsselpersonal



Ergebnisse

CERTAINITY

Warum CERTAINITY?

- ✓ Security Berater UND Entwickler
- ✓ Umfassendes Branchen Know-How und Methoden-Wissen

Nutzen

Bessere Marktposition

Kunden verlangen sichere Produkte und Services

Reduzierte Kosten

Frühzeitige Erkennung von Designfehlern und Security Schwachstellen

Gesteigerte Effizienz

Vermeidung von Security Bugs und deren Behebung

Threat Modeling und Assessment von Cyber Risiken in Produkten

Zielsetzung

Vermeidung kritischer Designfehler und Ermöglichung risikobasierte Entscheidungen während der Entwicklung zu treffen

Fragestellung?

- Wie können wir mögliche Schwachstellen und Angriffsvektoren schon in der Designphase der Entwicklung entdecken?
- Und die daraus resultierenden Sicherheits-Risiken bewerten?

Vorgehensweise

1. **Scoping Workshops** zur Festlegung des Untersuchungsgegenstandes und einzusetzender Modellierungstechniken und Methoden
2. **Unterstützung bei der Modellierung** des Untersuchungsgegenstandes
3. Durchführen der **Bedrohungsanalyse** und **Bewertung identifizierter Risiken**
4. **Empfehlung** umzusetzender Sicherheitsmaßnahmen

Methoden

UML	BPMN	SysML	CORAS	CVSS
C4	DFD	FMEA	HAZOP	OCTAVE
STRIDE	DREAD	Attack Trees	u.v.m.	

Methoden und Tools

Modellierungsprozesse

Bedrohungen und Risiken

Optimierung der internen Bedrohungsmodellierungsprozesse

Bericht mit Handlungsempfehlungen

Ergebnisse

CERTAINITY

Warum CERTAINITY?

- ✓ Umfassendes Know-How in der Bedrohungsmodellierung und Softwareentwicklung
- ✓ Ganzheitliche Unterstützung über alle Prozessschritte hinweg

Nutzen

- Vermeidung kritischer Designfehler
- Risikobasierte Entscheidungen während der Entwicklung
- Minimierung der Angriffsvektoren

Ihr direkter Draht zu CERTAINITY

Kontaktieren Sie unmittelbar unsere Experten bei einem Cyber Security Vorfall

cert@certainity.com

+43 664 888 44 686

Allgemeine Anfragen: sales@certainity.com oder direkt an

Mag. (FH) **Theresa Mosing**

Head of Sales

Tel: +43 664 9623932

Mail: theresa.mosing@certainity.com

Ulrich Fleck

CEO

Tel: +43 664 8223183

Mail: ulrich.fleck@certainity.com

CERTAINITY

CERTAINITY GmbH

reliable. trustworthy. bespoke.


Heiligenstädter Lände 27c | A – 1190 Wien
HG WIEN, FN 262176 D


office@certainity.com


https://certainity.com