CERTAINITY

Der European Cyber Resilience Act

Secure Product Development Backlog Item?

Head of Security Engineering

Michael Brunner, PhD.

- Doktoratsstudium Informatik mit Fokus auf **Informationssicherheits- und Risikomanagement**
- Mehr als 15 Jahre Berufserfahrung als IT-, Management-, und **Security-Consultant** sowie als **Software Engineer**
- Branchen-Know-How: Finanzdienstleister, Transportunternehmen, Energieversorger, Automobilhersteller und -zulieferer

michael.brunner@certainity.com | +43 664 9624028 | Profile

CERTAINITY

© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

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

© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

CERTAINITY Support für CRA-E Compliance

European Cyber Resilience Act

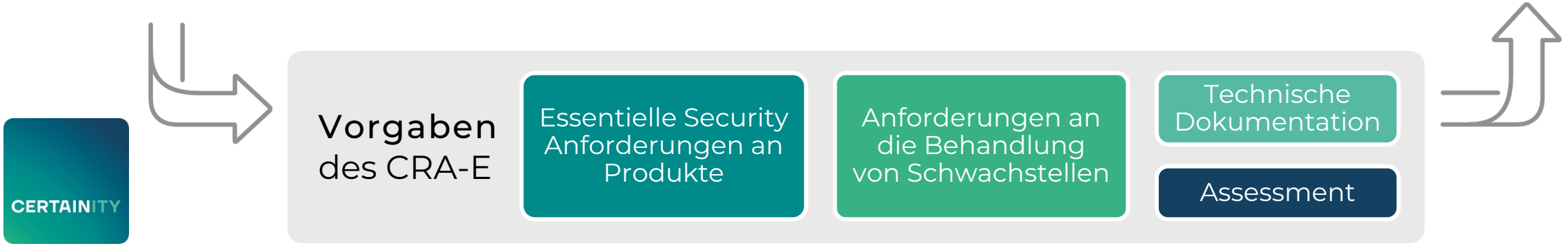
Strebt Verbesserung der Cybersicherheits-lage für Produkte mit digitalen Elementen an:

> *„Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardware-komponenten, die getrennt in Verkehr gebracht werden sollen.“*

Mit einer Inkraftsetzung ist spätestens 2024 zu rechnen, Umsetzung innerhalb von 2 Jahren verpflichtend

- **Initialer Workshop** zur Vorstellung der CRA-E Vorgaben inkl. Scope-Bestimmung und High-Level Assessment des Umsetzungsgrades
- **Detailliertes Assessment** zur Umsetzung von CRA-E Vorgaben und Empfehlungen für
  - einzelne oder mehrere Produkte
  - Produkt- und Softwareentwicklungsprozesse
  - Schwachstellenmanagement für Produkte

Zielsetzung: Bewertung der CRA-E Compliance



© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

CERTAINITY Support für CRA-E Compliance – Fortsetzung

Bedrohungsmodellierung und Bewertung von Cyberrisken für Produktentwicklung

- Auswahl geeigneter Modellierungstechniken
- Ausarbeitung individuell anwendbarer Schwachstellen- und Bedrohungskatalogen
- Toolauswahl und -einführung
- Schulungen und Trainings

Zielsetzung: Erhöhung der Dokumentations-qualität sowie Umsetzung geforderter Vorgaben für Dokumentation und Produkt Assessment

Etablierung eines Product Security Incident Response Teams (PSRIT)

- Erhebung und Analyse des Status Quo (organisatorisch, technisch, personell)
- Entwicklung/Optimierung Prozessmodell
- Einführungsunterstützung und Prozess-begleitung zur kontinuierlichen Verbesserung

Zielsetzung: Schaffung geforderter Capabilities, um Schwachstellen in Produkten effizient zu managen und Reporting Vorgaben zu erfüllen

Sichere Software- und Produktentwicklung

- Workshops zur Awarenessbildung und Standort-Bestimmung
- Entwicklung einer Roadmap zur SSDLC Einführung
- Tool-Auswahl und Einführung für Security Testing, SBOM, u.v.m.
- Begleitung der Maßnahmenumsetzung und Trainings

Zielsetzung: Umsetzung geforderter Sicherheits-anforderungen und des benötigten Sicherheits-niveaus, Reduktion von Haftungsrisiken

CERTAINITY

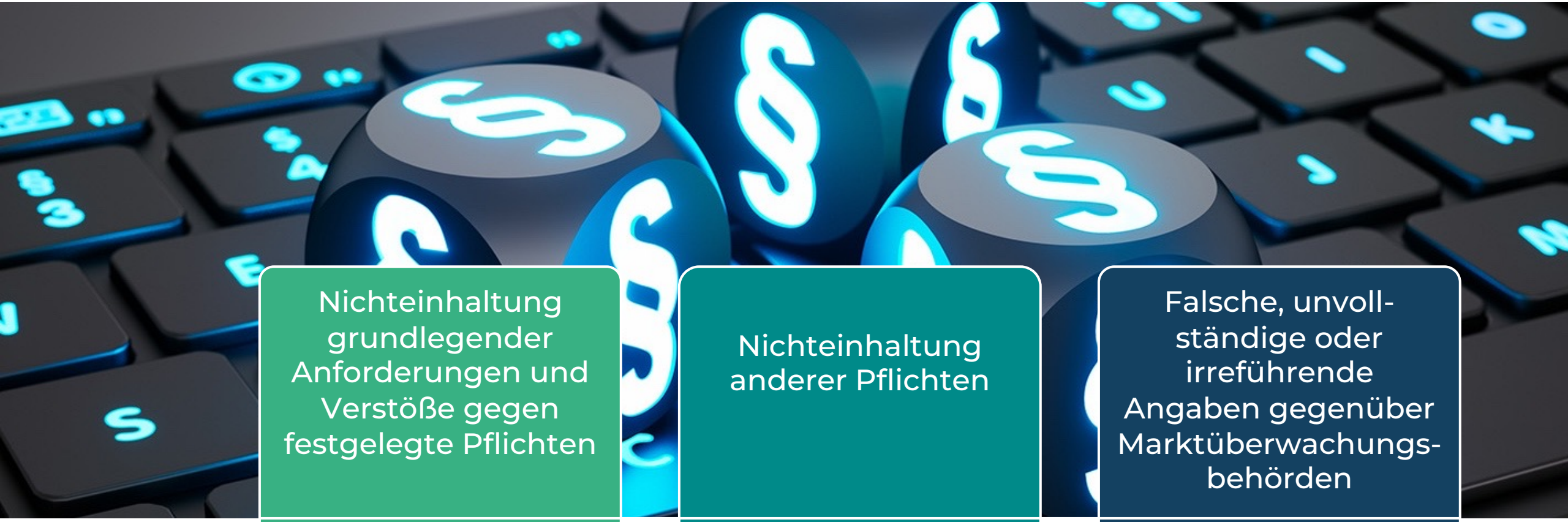
© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

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

© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

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

© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

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

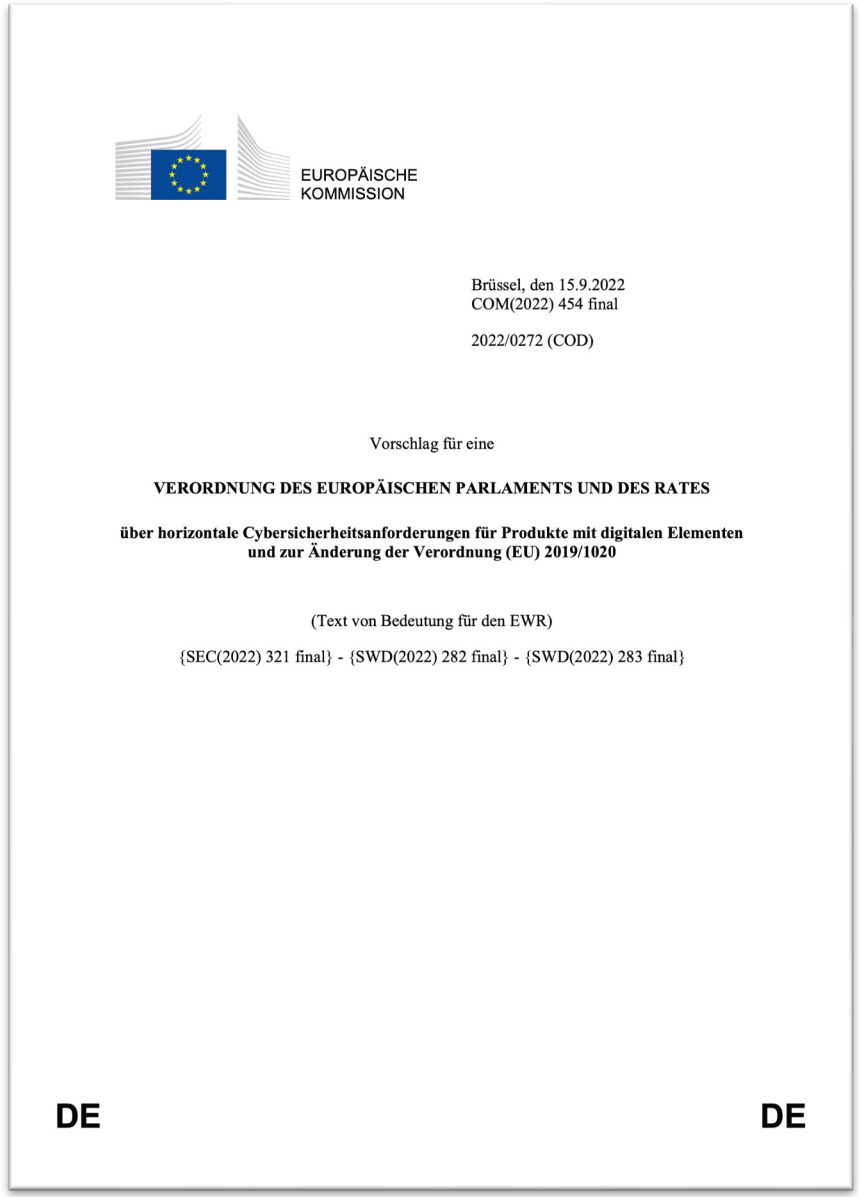
Software oder Hardware

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; ...

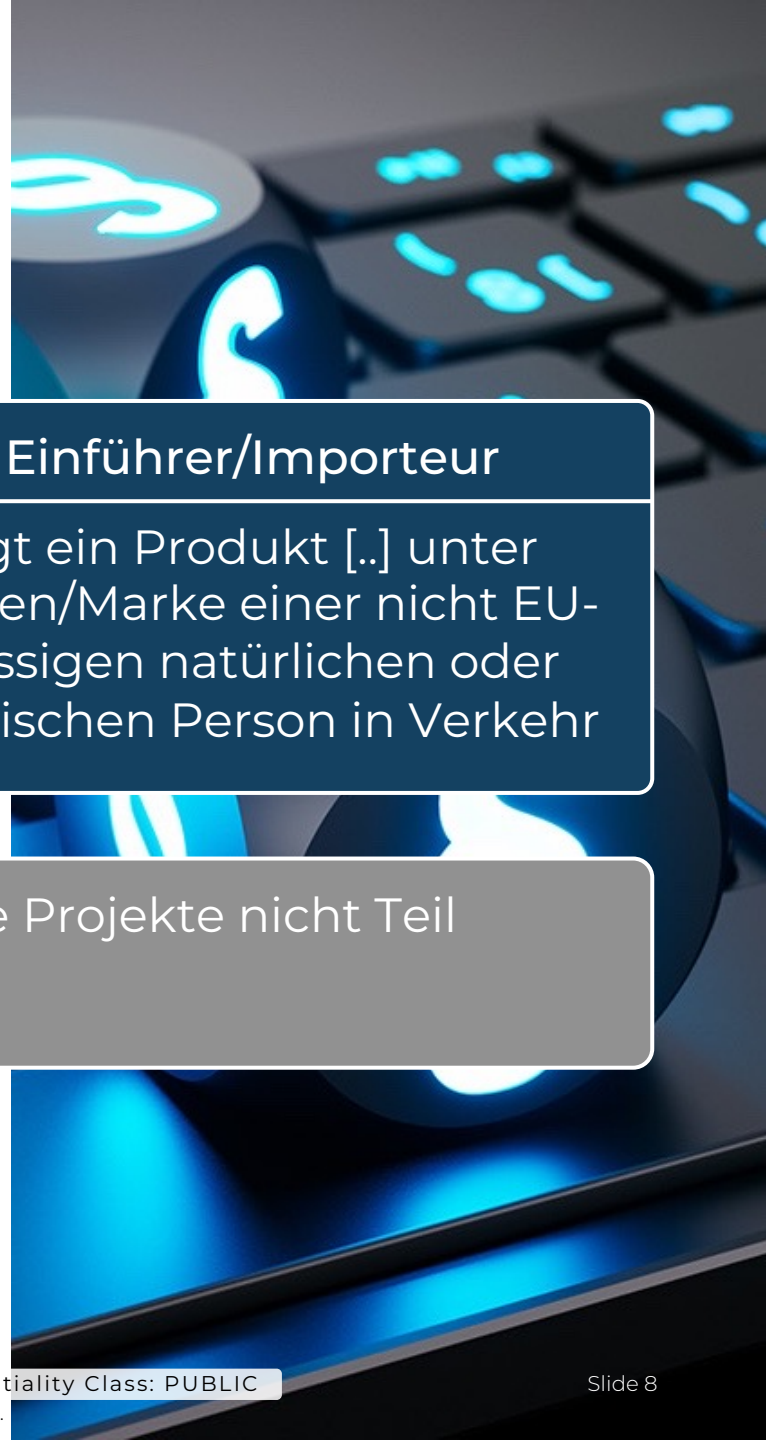
© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

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

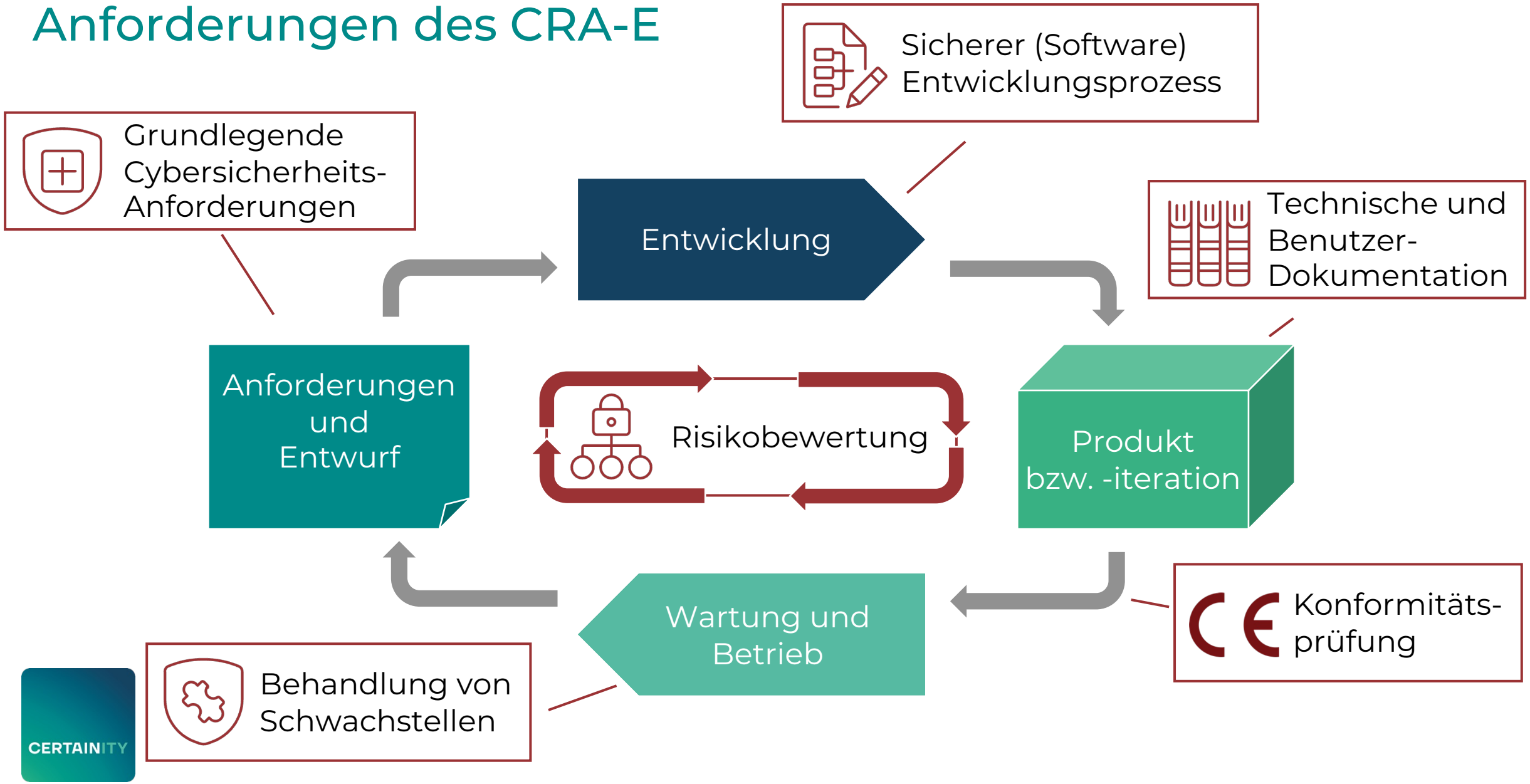


CERTAINITY

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

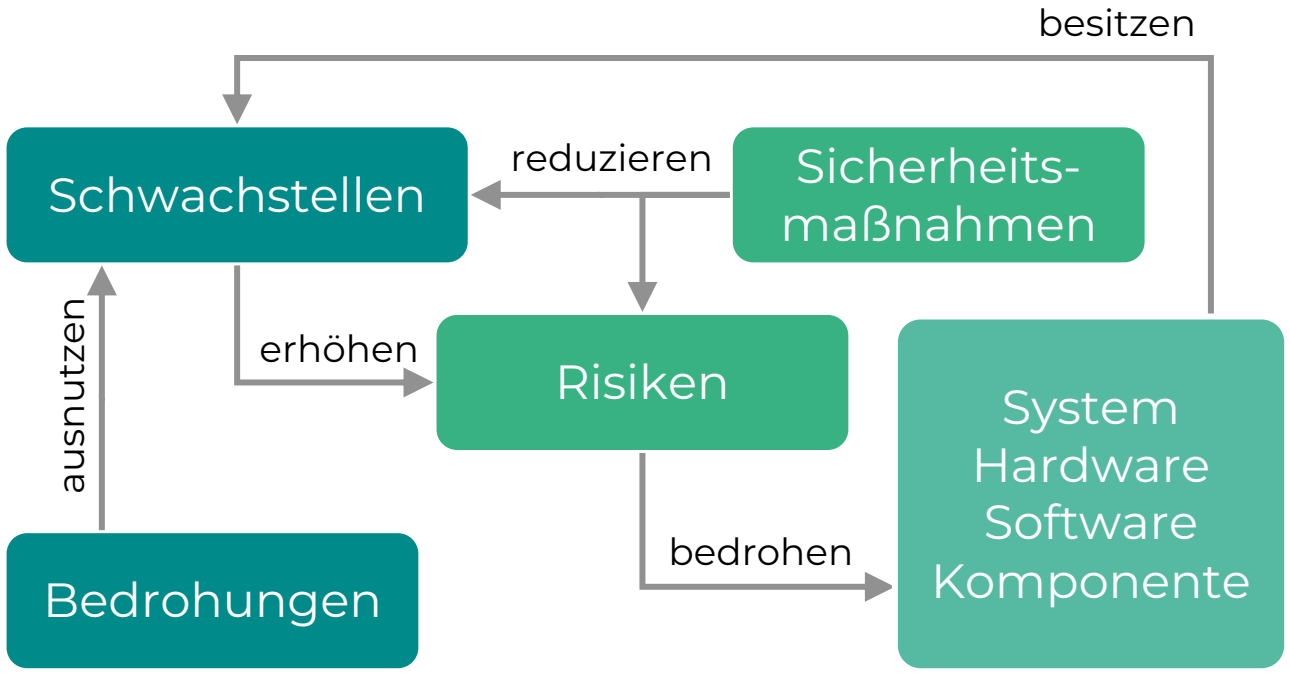
© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

Anforderungen des CRA-E



© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

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

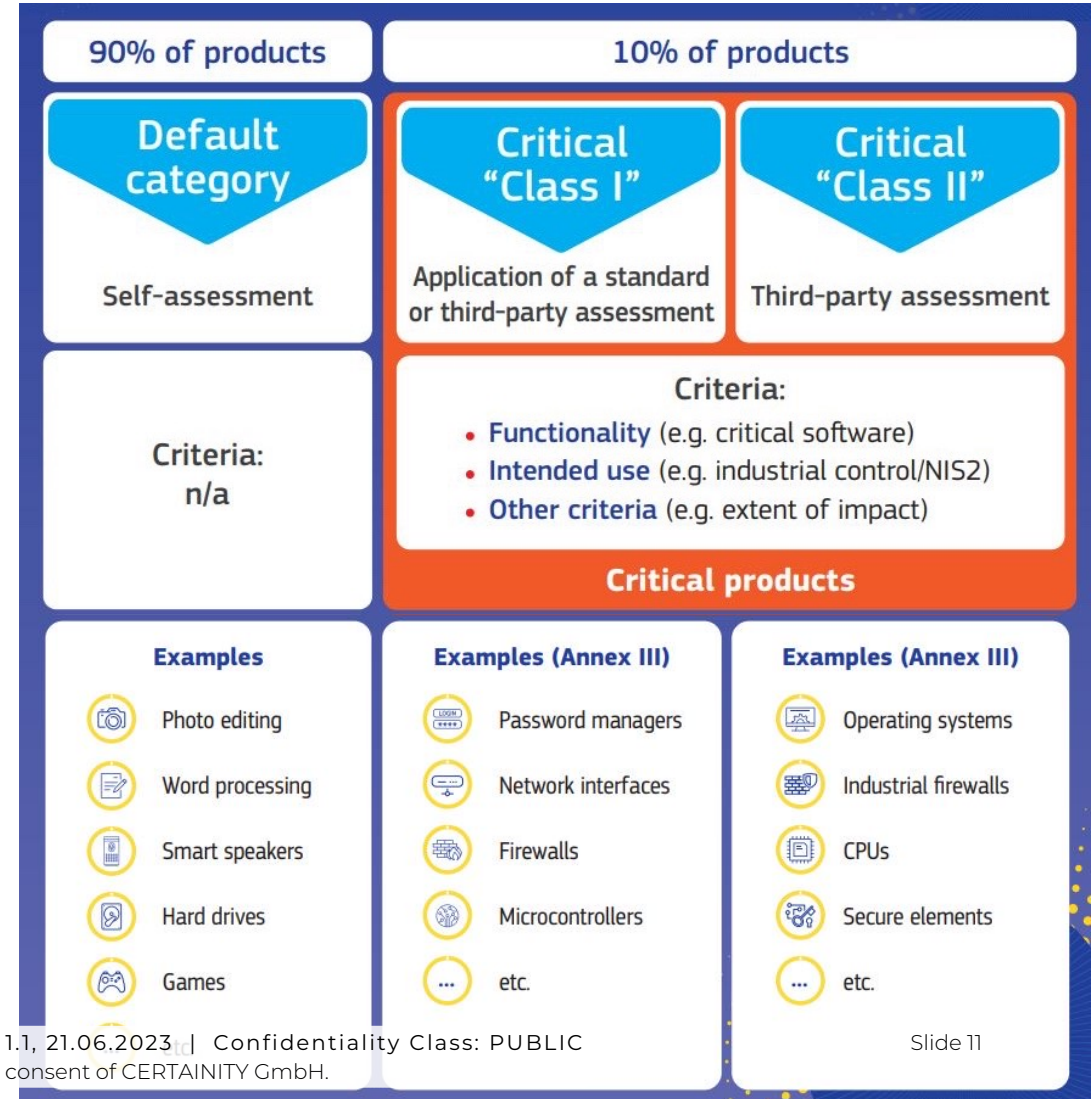
© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

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

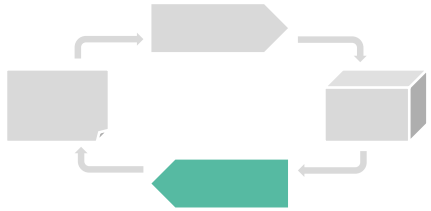
Die ENISA ist als Aufsichts- und Berichtsbehörde vorgesehen, Europäische Standardisierungs-Organisationen werden mit der Ausarbeitung harmonisierter Normen betraut.



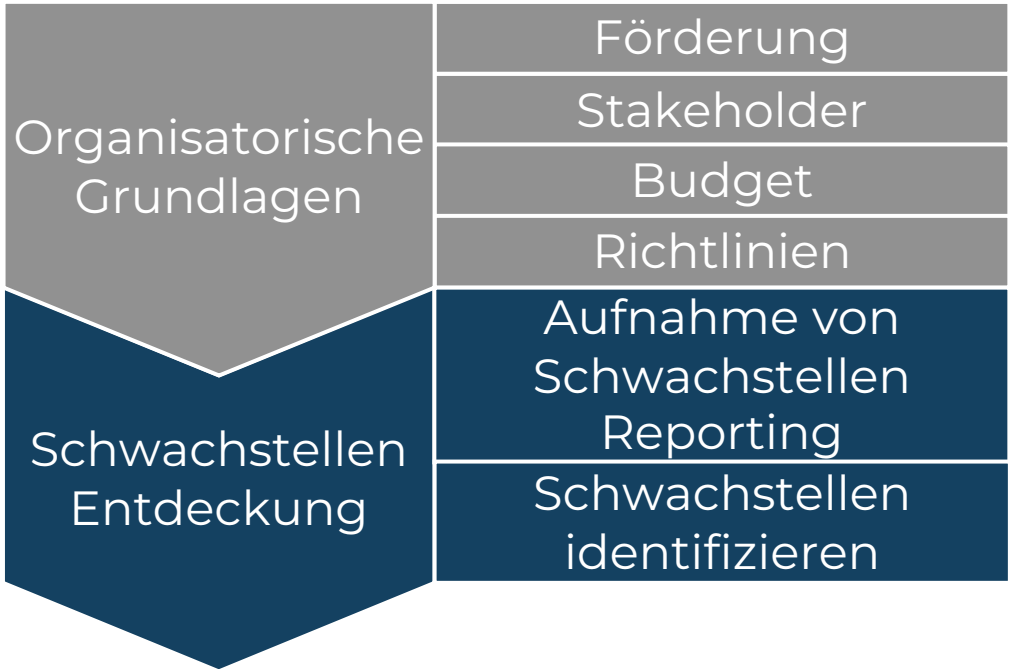
Bildquelle: European Commission, Cyber Resilience Fact Sheet, available at https://ec.europa.eu/newsroom/dae/redirection/document/89528 (accessed June 14th 2023)

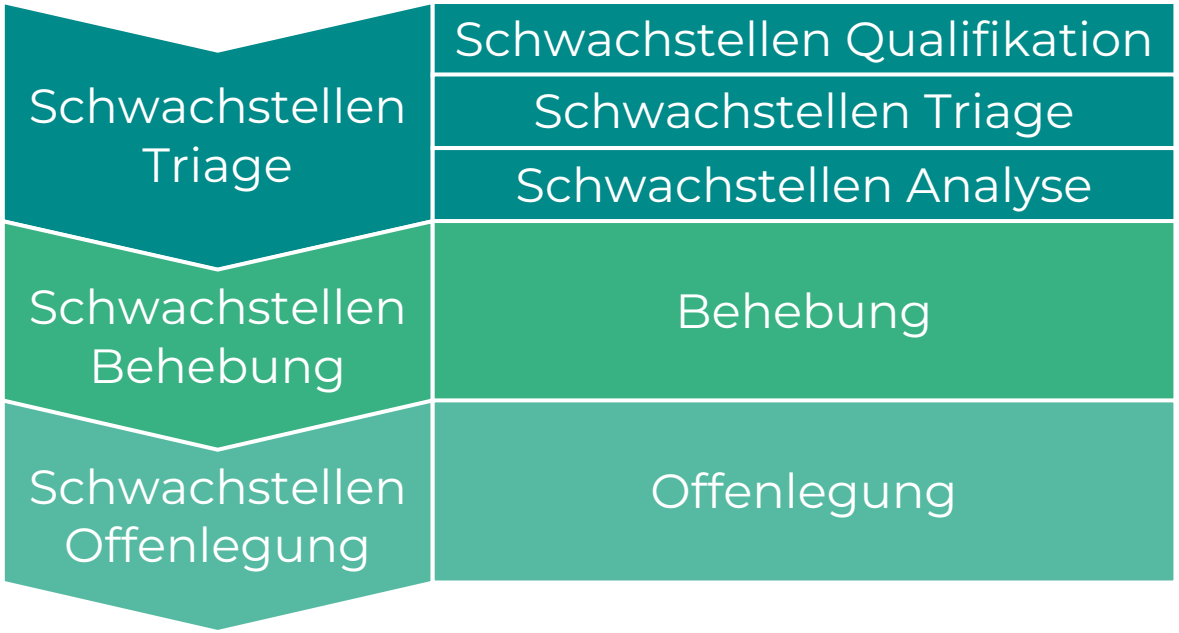
© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

Anforderungen an Schwachstellenmanagement



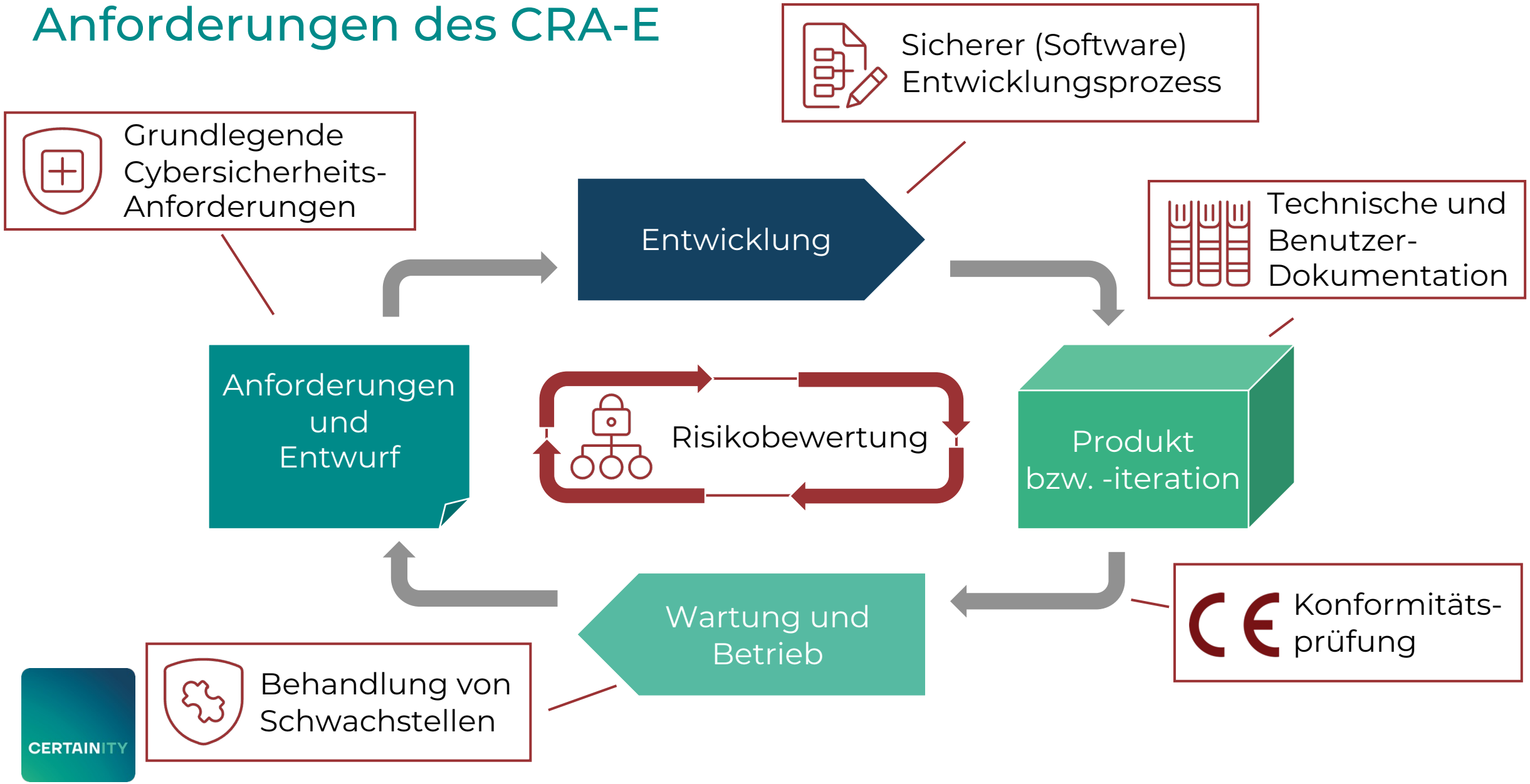
Schaffung der Voraussetzung für effizientes Schwachstellenmanagement durch Umsetzung eines Product Security Incident Response Teams (PSIRT)



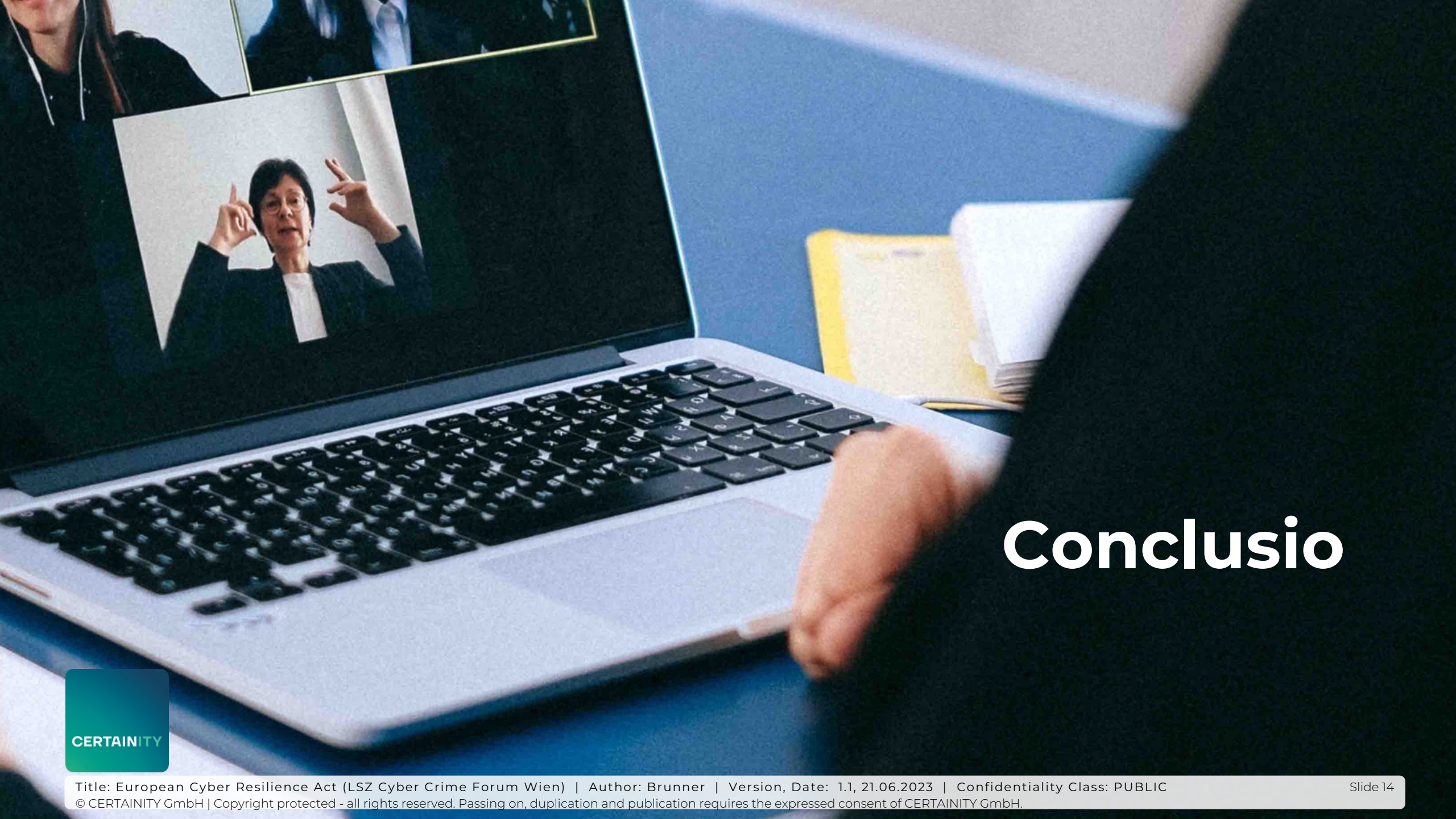


© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

Anforderungen des CRA-E



© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.



Conclusio

© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

CERTAINITY Umfrage *European Cyber Resilience Act Preparedness von Unternehmen*

In Zusammenarbeit mit der Universität Innsbruck führt CERTAINITY eine Online-Umfrage durch, um zu untersuchen, wie gut Unternehmen auf die Einführung des European Cyber Resilience Act vorbereitet sind.

Wir bitten Sie, sich 10 bis 15 Minuten Zeit nehmen, um Ihre Expertise einzubringen und unser Vorhaben zu unterstützen. Wir stellen Fragen zu Ihrem Unternehmen, dem aktuellen Status Ihrer Prozesse für sichere Produktentwicklung und für die Verwaltung von Schwachstellen, sowie zu Ihren aktuellen Dokumentationspraktiken.

VIELEN DANK!

https://umfrage.uibk.ac.at/limesurvey/allgemein/index.php/561482?lang=de

© CERTAINITY GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

Ihr direkter Draht zu uns

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 GmbH | Copyright protected - all rights reserved. Passing on, duplication and publication requires the expressed consent of CERTAINITY GmbH.

CERTAINITY

CERTAINITY GmbH

reliable. trustworthy. bespoke.

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

office@certainity.com
https://certainity.com

ALL RIGHTS TO THIS PRESENTATION ARE RESERVED. THE WORK INCLUDING ITS PARTS IS PROTECTED BY COPYRIGHT. THE INFORMATION CONTAINED HEREIN IS CONFIDENTIAL. THE ELABORATION AND ITS CONTENTS MAY NOT BE USED, TRANSLATED, DISTRIBUTED, REPRODUCED OR PROCESSED IN ELECTRONIC SYSTEMS WITHOUT THE EXPRESS CONSENT OF CERTAINITY GMBH AND THE CLIENT. IN PARTICULAR, DISCLOSURE TO ANY THIRD PARTY IS NOT PERMITTED.