T.I.S.P./T.P.S.S.E. Community Meeting 2026

Berlin, 10. - 11.11.2026

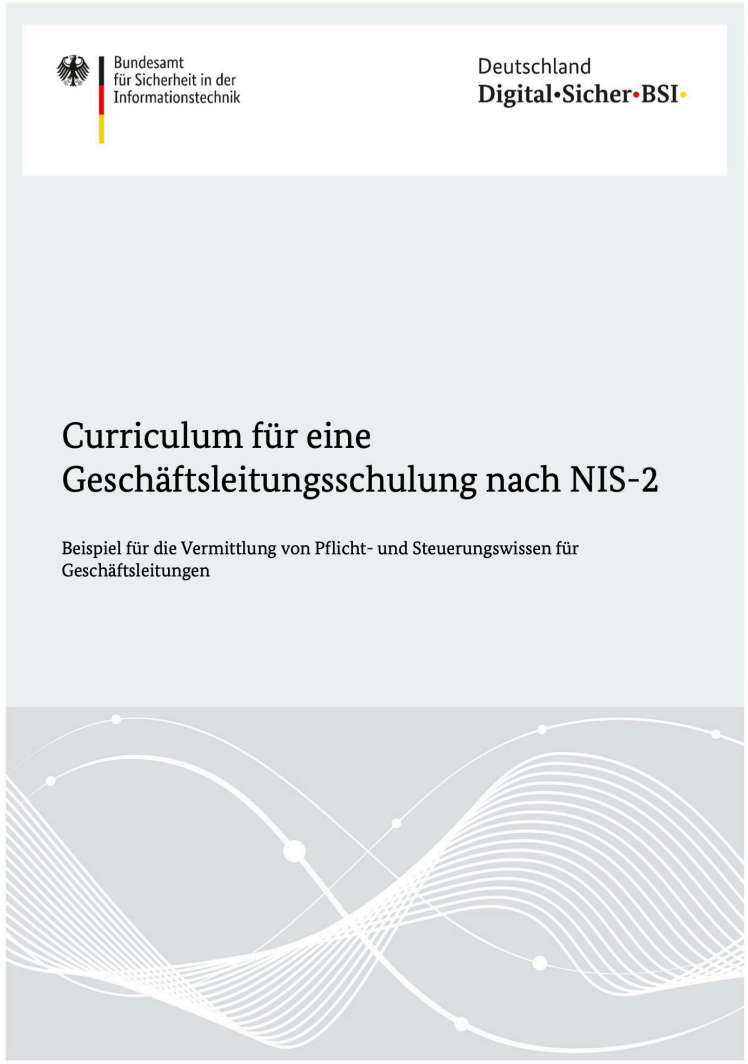
Update zum IT-Sicherheitsrecht

RA Karsten U. Bartels LL.M.
HK2 Rechtsanwälte
Vorstand TeleTrusT, Leiter AG IT-Sicherheitsrecht

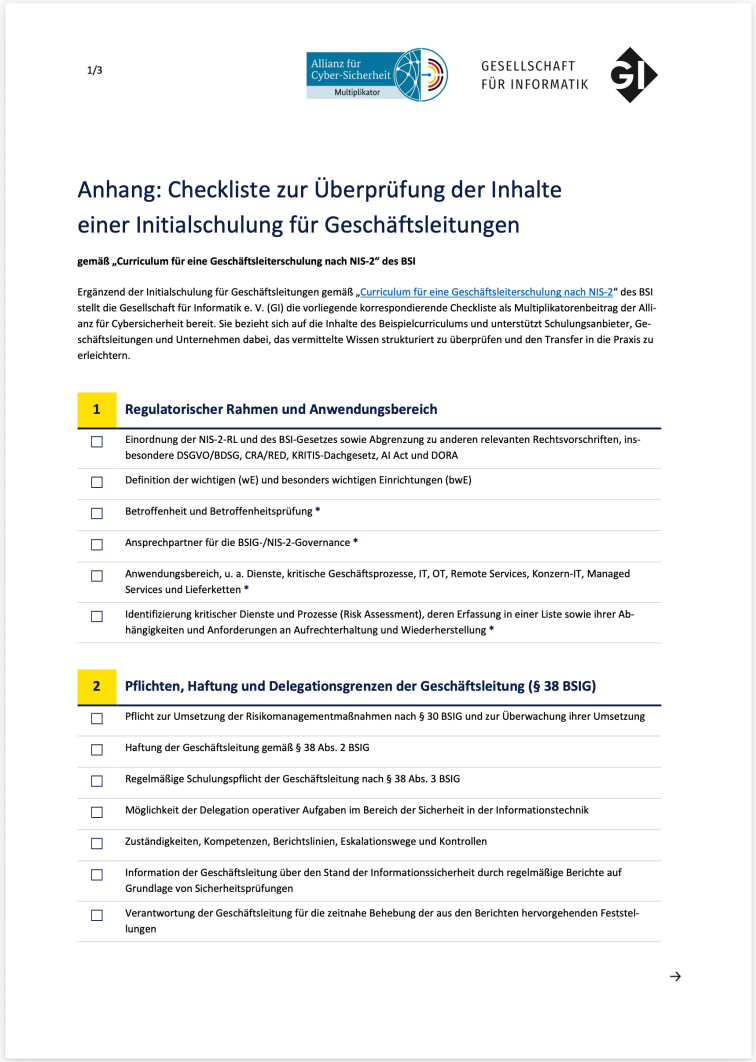
HK2



BSIG



www.bsi.bund.de



1/3

Allianz für Cyber-Sicherheit
Multiplikator

GESELLSCHAFT
FÜR INFORMATIK

Anhang: Checkliste zur Überprüfung der Inhalte einer Initialschulung für Geschäftsleitungen

gemäß „Curriculum für eine Geschäftsleiterschulung nach NIS-2" des BSI

Ergänzend der Initialschulung für Geschäftsleitungen gemäß „Curriculum für eine Geschäftsleiterschulung nach NIS-2" des BSI stellt die Gesellschaft für Informatik e. V. (GI) die vorliegende korrespondierende Checkliste als Multiplikatorenbeitrag der Allianz für Cybersicherheit bereit. Sie bezieht sich auf die Inhalte des Beispielcurriculums und unterstützt Schulungsanbieter, Geschäftsleitungen und Unternehmen dabei, das vermittelte Wissen strukturiert zu überprüfen und den Transfer in die Praxis zu erleichtern.

1 Regulatorischer Rahmen und Anwendungsbereich

- ☐ Einordnung der NIS-2-RL und des BSI-Gesetzes sowie Abgrenzung zu anderen relevanten Rechtsvorschriften, insbesondere DSGVO/BDSG, CRA/RED, KRITIS-Dachgesetz, AI Act und DORA
- ☐ Definition der wichtigen (wE) und besonders wichtigen Einrichtungen (bwE)
- ☐ Betroffenheit und Betroffenheitsprüfung *
- ☐ Ansprechpartner für die BSIG-/NIS-2-Governance *
- ☐ Anwendungsbereich, u. a. Dienste, kritische Geschäftsprozesse, IT, OT, Remote Services, Konzern-IT, Managed Services und Lieferketten *
- ☐ Identifizierung kritischer Dienste und Prozesse (Risk Assessment), deren Erfassung in einer Liste sowie ihrer Abhängigkeiten und Anforderungen an Aufrechterhaltung und Wiederherstellung *

2 Pflichten, Haftung und Delegationsgrenzen der Geschäftsleitung (§ 38 BSIG)

- ☐ Pflicht zur Umsetzung der Risikomanagementmaßnahmen nach § 30 BSIG und zur Überwachung ihrer Umsetzung
- ☐ Haftung der Geschäftsleitung gemäß § 38 Abs. 2 BSIG
- ☐ Regelmäßige Schulungspflicht der Geschäftsleitung nach § 38 Abs. 3 BSIG
- ☐ Möglichkeit der Delegation operativer Aufgaben im Bereich der Sicherheit in der Informationstechnik
- ☐ Zuständigkeiten, Kompetenzen, Berichtslinien, Eskalationswege und Kontrollen
- ☐ Information der Geschäftsleitung über den Stand der Informationssicherheit durch regelmäßige Berichte auf Grundlage von Sicherheitsprüfungen
- ☐ Verantwortung der Geschäftsleitung für die zeitnahe Behebung der aus den Berichten hervorgehenden Feststellungen

→

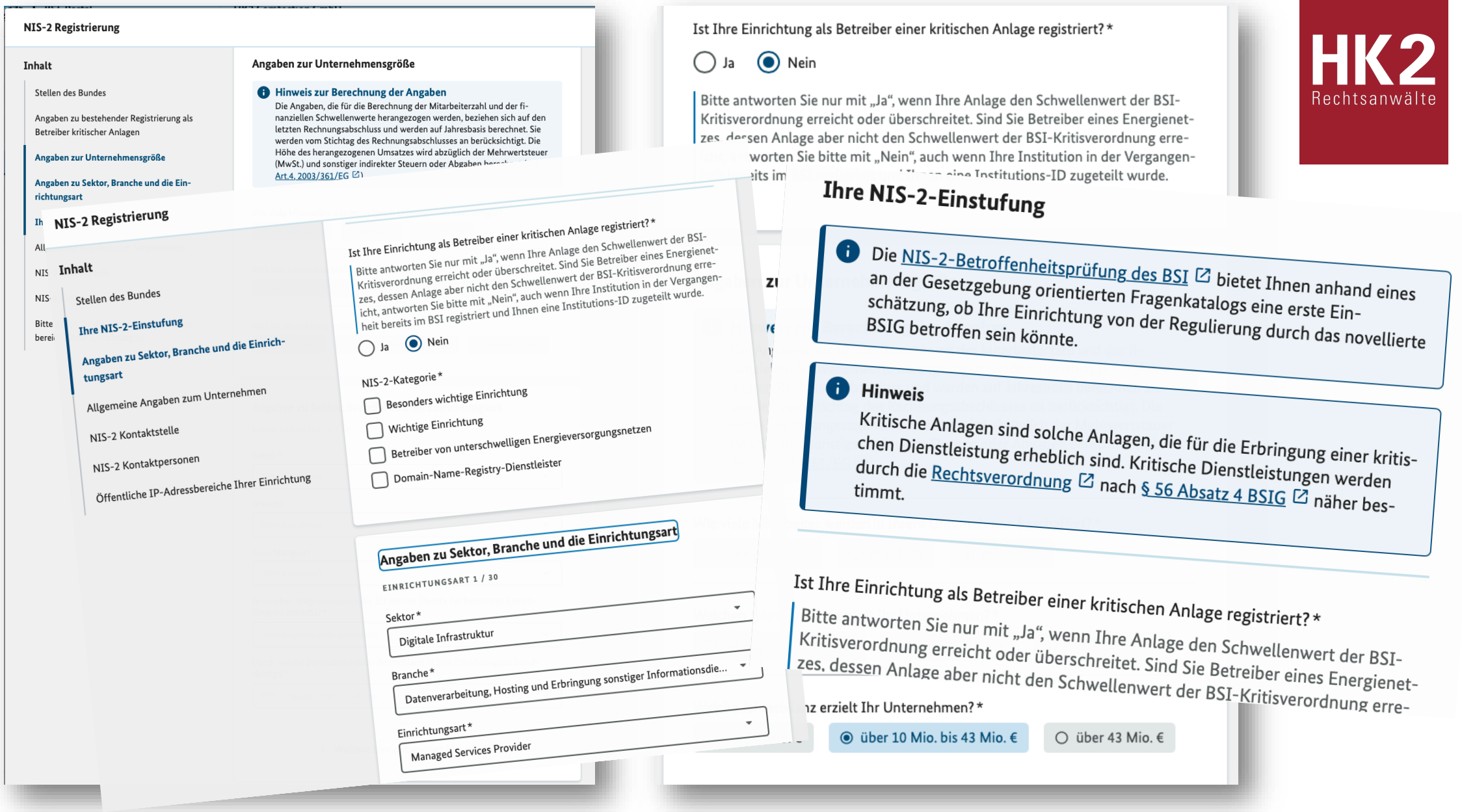
www.allianz-fuer-cybersicherheit.de

HK2
Rechtsanwälte

HK2
Rechtsanwälte



https://portal.bsi.bund.de/



HK2
Rechtsanwälte

HK2 Rechtsanwälte

Technische und organisatorische Maßnahme, § 30 Abs. 2 BSIG

1. **Konzepte** in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
2. Bewältigung von **Sicherheitsvorfällen**
3. **Aufrechterhaltung** des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
4. Sicherheit der **Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern
5. **Sicherheitsmaßnahmen** bei **Erwerb**, **Entwicklung** und **Wartung** von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich **Management und Offenlegung von Schwachstellen**

Umsetzung?

HK2

Der Cyber Resilience Act



HK2 Rechtsanwälte

EU - Cybersicherheitsstrategie





Physische Sicherheit	IT-Sicherheit		
CER-Richtlinie	NIS-2-Richtlinie	Cyber Resilience Act (CRA)	Digital Operational Resilience Act (DORA)
KRITIS-Dachgesetz	BSIG	Unmittelbare Geltung	

HK2 Rechtsanwälte

CRA

- Ziel der EU: Schutz von Verbrauchern und Unternehmen vor Cyberrisiken
- Produktbezogen
- Macht den Zugang zum EU-Markt von der Einhaltung bestimmter Anforderungen abhängig



HK2 Rechtsanwälte

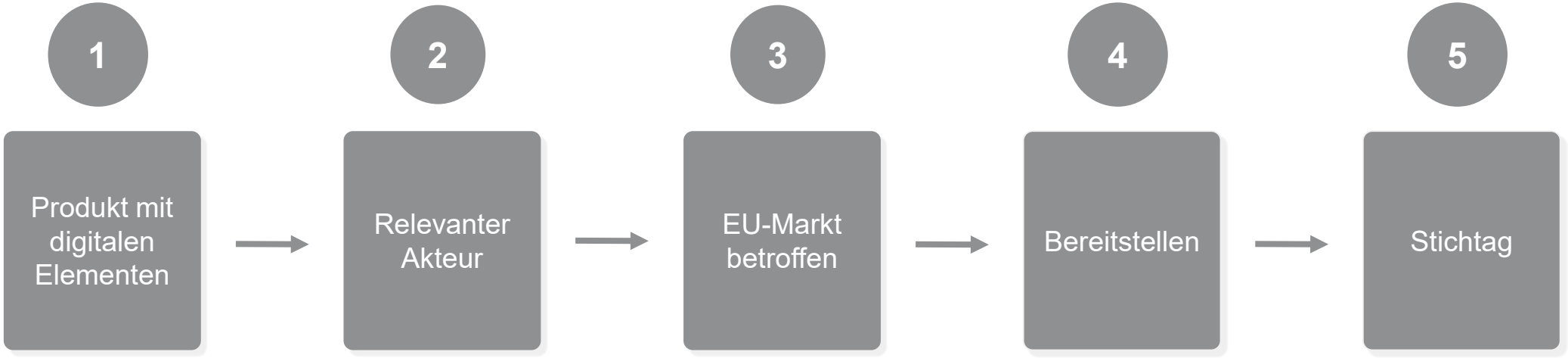
Pflichten aus dem Cyber Resilience Act

1. Grundlegende Cybersicherheitsanforderungen
2. Cybersicherheits-Risikobewertung
3. Security-by-design
4. Dokumentation der Cybersicherheits-Risikobewertung
5. Sorgfalt bei Drittkomponenten
6. Dokumentation von Cybersicherheitsaspekten
7. Schwachstellenmanagement
8. Festlegung des Unterstützungszeitraums
9. Koordinierte Offenlegung von Schwachstellen
10. Update-Verfügbarkeit
11. Technische Dokumentation
12. Konformitätsbewertung
13. **EU-Konformitätserklärung**
14. **CE-Kennzeichnung**
15. Aufbewahrungspflichten
16. CRA-Konformität bei Serienherstellung
17. Produkt- und Herstellerkennzeichnung
18. Benennung einer zentralen Anlaufstelle
19. Nutzerinformationen und Anleitungen
20. Information über das Ende des Unterstützungszeitraums
21. Korrekturmaßnahmen
22. Rückruf
23. Rücknahme
24. Auskunfts- und Kooperationspflichten
25. Meldung aktiv ausgenutzter Schwachstellen
26. Meldung schwerwiegender Sicherheitsvorfälle
27. Nutzerinformationen zu Sicherheitsvorfällen
28. Nachverfolgbarkeit der Wirtschaftskette

HK2 Rechtsanwälte

Schritte der CRA-Anwendbarkeitsprüfung

Art. 2 CRA: *Diese Verordnung gilt für* ***auf dem Markt bereitgestellte Produkte mit digitalen Elementen****, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine* ***direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt****.*



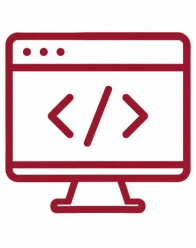
HK2 Rechtsanwälte

Produkte mit digitalen Elementen, Art. 3 Nr. 1 CRA

*„Produkt mit digitalen Elementen“ [bezeichnet] ein **Software-** oder **Hardwareprodukt** und dessen **Datenfernverarbeitungslösungen**, einschließlich Software- oder Hardware**komponenten**, die getrennt in den Verkehr gebracht werden*



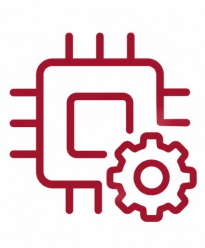
1. Hardware



2. Software



3. Komponenten



4. Datenfernverarbeitung

HK2 Rechtsanwälte

Hardware-Produkte - Beispiele



Laptop



Smartphone



Smartwatch



WLAN-Router



Smart-TV



Industrielle 3D-Drucker



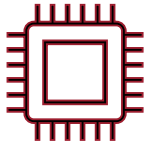
Werkzeugmaschinen mit Fernzugang



Intelligente Sensorik



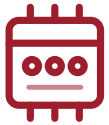
Vernetzte Laborgeräte



Motherboards und Mikrocontroller



Netzwerkdrucker



Industrie-Controller

1. Hardware | **2. Software** | **3. Komponenten** | **4. Datenfernverarbeitung**

Software-Produkte - Beispiele

Reine SaaS fällt nicht unter den CRA



Betriebssysteme



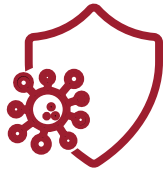
Apps



Browser und Web-Apps



Unternehmens-software



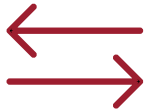
Antivirus-Software



VPN-Clients und -Server



Videospiele

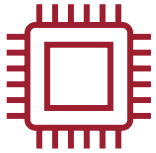


API-Clients

1. Hardware | **2. Software** | 3. Komponenten | 4. Datenfernverarbeitung

HK2 Rechtsanwälte

Komponenten-Beispiele



Mikrocontroller



Speichermodul



Sensoren



GPS-Module



Lademodul



Software-Libraries und SDKs



Treiber



Updates

1. Hardware | 2. Software | **3. Komponenten** | 4. Datenfernverarbeitung

HK2 Rechtsanwälte

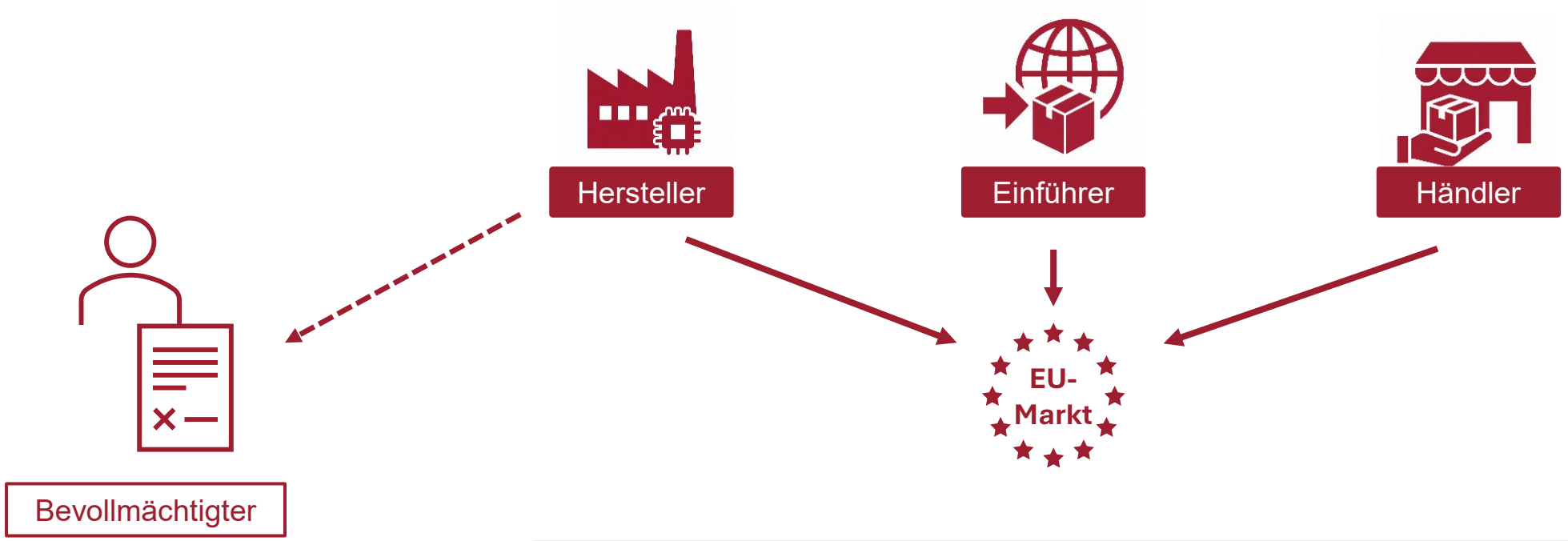
Datenfernverarbeitungslösung, Art. 3 Nr. 2 CRA

1. Entfernt stattfindende Datenverarbeitung
2. ohne die das Produkt mindestens eine seiner Funktionen nicht erfüllen könnte **und**
3. vom Hersteller oder unter seiner Verantwortung konzipiert wurde.

HK2 Rechtsanwälte

Adressierte Akteure

Wesentliche Veränderungen = Herstellerfiktion!



Ein Sitz in der EU ist nicht erforderlich

HK2
Rechtsanwälte

Artikel 13

Pflichten der Hersteller

(1) Wenn sie ein Produkt mit digitalen Elementen in den Verkehr bringen, gewährleisten die Hersteller, dass dieses Produkt gemäß den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I konzipiert, entwickelt und hergestellt worden ist.

(2) Für die Zwecke der Erfüllung von Absatz 1 führen die Hersteller eine Bewertung der Cybersicherheitsrisiken durch, die ein Produkt mit digitalen Elementen birgt, und berücksichtigen das Ergebnis dieser Bewertung in der Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase des Produkts mit digitalen Elementen, um die Cybersicherheitsrisiken zu minimieren, Sicherheitsvorfälle zu verhindern und die Auswirkungen solcher Sicherheitsvorfälle, auch in Bezug auf die Gesundheit und Sicherheit der Nutzer, so gering wie möglich zu halten.

(3) Die Bewertung des Cybersicherheitsrisikos wird während eines gemäß Absatz 8 festzulegenden Unterstützungszeitraums dokumentiert und gegebenenfalls aktualisiert. Diese Bewertung des Cybersicherheitsrisikos umfasst mindestens eine Analyse der Cybersicherheitsrisiken auf der Grundlage der Zweckbestimmung und der vernünftigerweise vorhersehbaren Verwendung des Produkts mit digitalen Elementen, wie der Betriebsumgebung oder der zu schützenden Anlagen, wobei die voraussichtliche Nutzungsdauer des Produkts berücksichtigt wird. In der Bewertung des Cybersicherheitsrisikos wird angegeben, ob und gegebenenfalls in welcher Weise die Sicherheitsanforderungen gemäß Anhang I Teil I Nummer 2 auf das einschlägige Produkt mit digitalen Elementen anwendbar sind und wie diese Anforderungen auf der Grundlage der Bewertung des Cybersicherheitsrisikos umgesetzt werden. Ferner ist anzugeben, wie der Hersteller Anhang I Teil I Nummer 1 anzuwenden hat und welche Anforderungen an die Behandlung von Schwachstellen in Anhang I Teil II festgelegt sind.

ANHANG I

GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN

Teil I Cybersicherheitsanforderungen 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) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

a) ohne bekannte ausnutzbare

b) mit einer sicheren Standardk
dem gewerblichen Nutzer i
vereinbart wurde, und die M

c) sicherstellen, dass Schwachst
durch automatische Sicher
Zeitrahmens installiert werde
bei dem die Nutzer über v

Teil II Anforderungen an die Behandlung von Schwachstellen

Die Hersteller von Produkten mit digitalen Elementen müssen

(1) Schwachstellen und Komponenten der Produkte mit digitalen Elementen ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen;

ABl. L vom 20.11.2024 DE

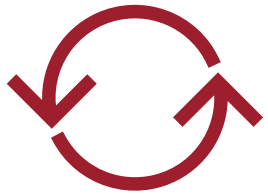
(2) im Hinblick auf die Risiken im Zusammenhang mit den Produkten mit digitalen Elementen unverzüglich Schwachstellen behandeln und beheben, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen; soweit technisch machbar, müssen neue Sicherheitsaktualisierungen getrennt von den Funktionsaktualisierungen bereitgestellt werden;

HK2 Rechtsanwälte

Sicherheitsaktualisierungen

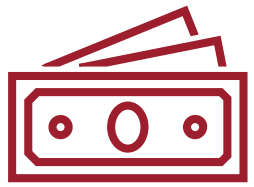
Kostenlos

- Sicherheitsupdates während des Supportzeitraums
- Bereitstellung der Sicherheitsupdates für 10 Jahre

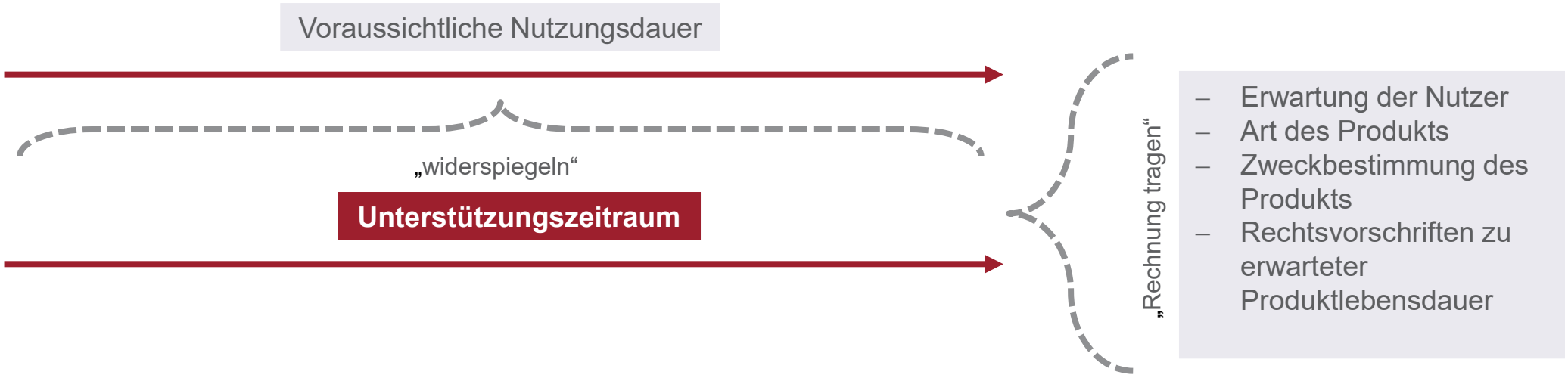


Vergütungsfähig

- Funktionsupdates
- Sicherheitsupdates
  - Im B2B-Bereich (nach Vereinbarung)
  - Nach Ende des Unterstützungszeitraums



Festlegung des Unterstützungszeitraums nach Art. 13 Abs.8 UAbs. 1-3 CRA



→ Einhaltung der Anforderungen an die Behandlung von Schwachstellen nach Anhang I Teil II CRA

HK2 Rechtsanwälte

Wann ist eine Schwachstelle bekannt und ausnutzbar?

Bekannt

- European Vulnerability Database (EUVD) der ENISA = Europäische Schwachstellendatenbank
  ErwGr. 66 CRA → Art. 12. Abs. 2 NIS-2-RL
- CSIRTs/ CERTs
- Fachmitteilungen/ -medien

Ausnutzbar

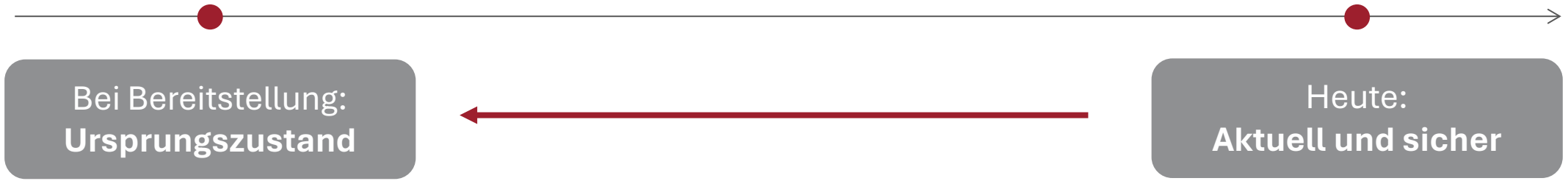
Common Vulnerability Scoring System (CVSS):

- Exploitability Metrics
- Exploit Maturaty

HK2 Rechtsanwälte

Möglichkeit eines „Factory Reset“

- Das Produkt muss bei Bereitstellung eine sichere Standardkonfiguration haben (**security by default**)
- Es soll die **Möglichkeit** geben, das Produkt jederzeit **zurückzusetzen**, Anhang I Tl. 1 Abs. 2 lit. b CRA.



HK2
Rechtsanwälte

Produktklassen

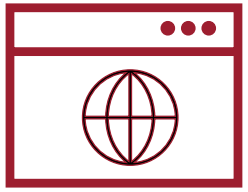


HK2 Rechtsanwälte

Wichtige Produkte – Klasse I



Identitätsmanagement/
privilegierte Zugänge



Browser (eigenständig / eingebettet)



Passwort-Manager

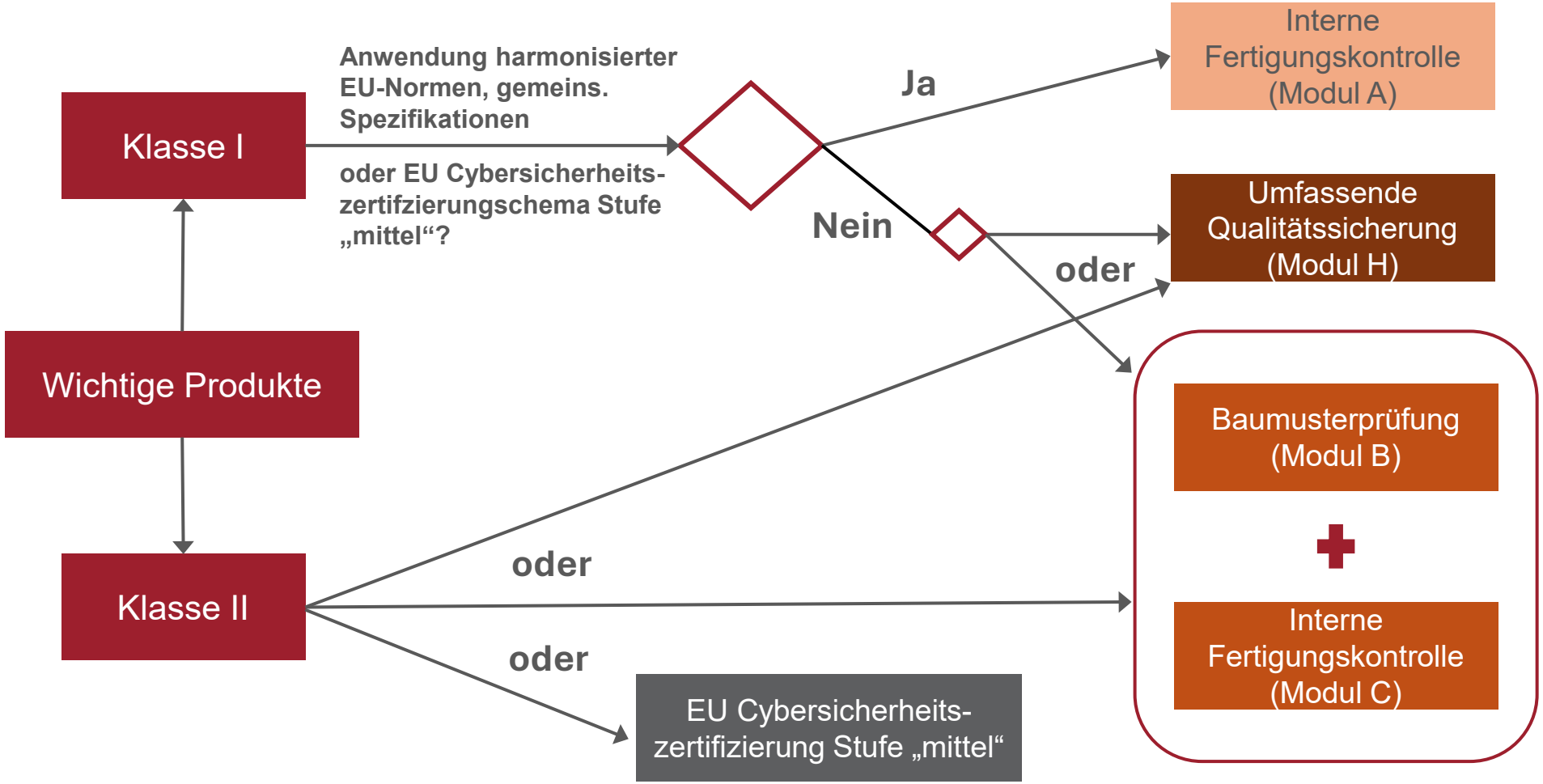


VPN-Produkte

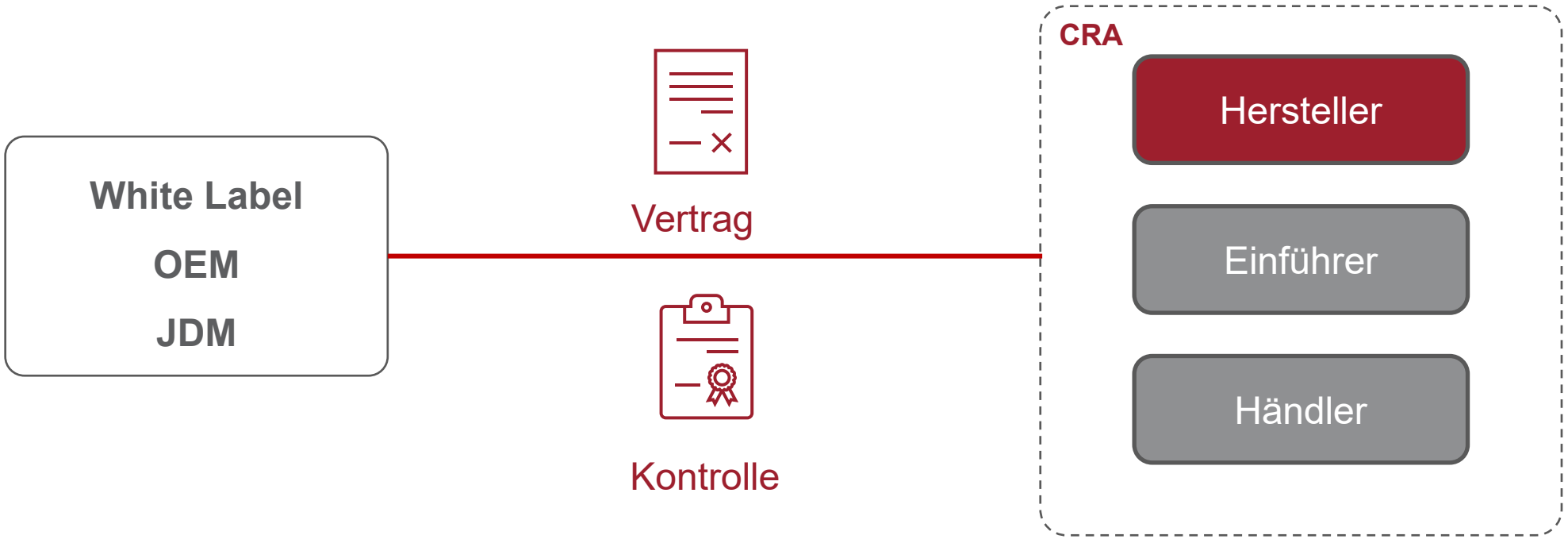


Router, Modems und Switches

Das richtige Konformitätsbewertungsverfahren bei wichtigen Produkten

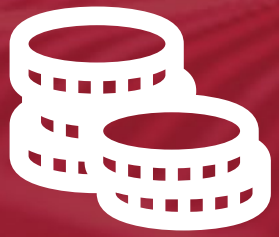


Supplier Management bei Akteuren, auch außerhalb des Anwendungsbereichs des CRA



HK2

Produkthaftungsgesetz



HK2 Rechtsanwälte

Produkthaftungsrichtlinie 2.0: Worum geht es?

Modernisierung der Herstellerhaftung für fehlerhafte Produkte

- Neue Richtlinie in Kraft seit 9.12.2024
- Gilt für Produkte, die ab dem **9.12.2026** in Verkehr gebracht werden.
- Stand: VÖ im Bundesgesetzblatt vom 27.10.2026.



Bundesgesetzblatt

Teil I

PDF-Anzeige

2026 **Ausgegeben zu Bonn am 27. Oktober 2026** **Nr. 321**

Gesetz zur Modernisierung des Produkthaftungsrechts und zur Änderung weiterer Vorschriften*

Vom 22. Oktober 2026

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz – ProdHaftG)

Inhaltsübersicht

Teil 1

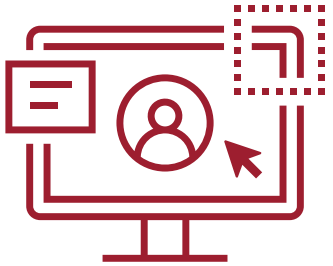
Haftung des Herstellers

§ 1 Haftung
§ 2 Produkt
§ 3 Hersteller

HK2 Rechtsanwälte

Software als Produkt

- **Eigenschaften**:
  - Eigenständig (stand-alone)
  - Integriert (Komponente)
  - Verbundene Dienste (als Komponente)
  - Art der Bereitstellung/ Nutzung irrelevant
- **Ausnahme:**
  - Free and Open-Source Software
- **Beispiele**:
  - Betriebssysteme, Firmware, Computerprogramme, Anwendungen, **SaaS** oder KI-Systeme



Produktfehler (Art. 7 ProdHaftRL)

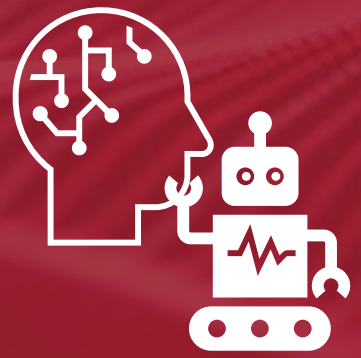
- *Neu:* Nichteinhaltung gesetzlicher Sicherheitsvorgaben an Produktsicherheit!

- Mitsamt „sicherheitsrelevanter Cybersicherheitsanforderungen“
  - **Cyber Resilience Act** (**CRA**)
  - Einheitliche Sicherheitsanforderungen für breites Spektrum an Produkten mit digitalen Elementen



HK2

KI + KIVO



HK2

KI-gestützte Cyberangriffe sind das neue Normal.

KI fungiert als Akteur der Cyberangriffe.

HK2

Wirkung von KI im IT-Sicherheitsrecht

1. KI-Einsatz *für* IT-Sicherheit wird zunehmend zur Maßnahme gemäß dem **Stand der Technik**.

2. Wenn IT-sicherheitsrelevante Fehlerminimierung bei IT-Produkten durch einen verfügbaren KI-Einsatz möglich und ihrerseits sicher ist, wird sie grds. nach den IT-Sicherheitsgesetzen als **angemessene und zumutbare Maßnahme** einzusetzen sein.

3. KI wird zum **Compliance-Faktor**.

HK2

Was prägt das Jahr 2027?

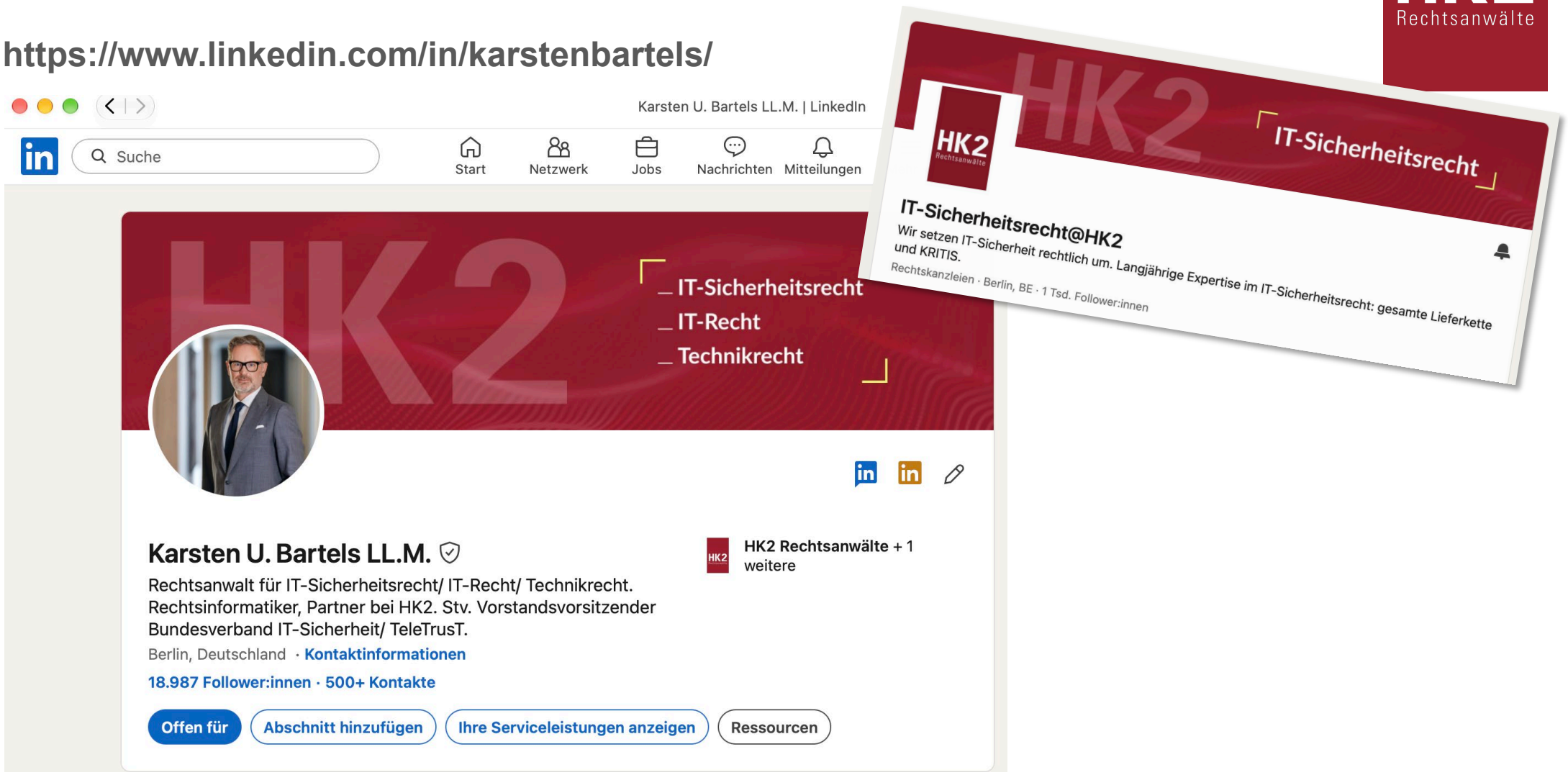
Produktsicherheit

Lieferkette

KI

HK2
Rechtsanwälte

https://www.linkedin.com/in/karstenbartels/



HK2
Rechtsanwälte

Kontakt



linkedin.com/in/karstenbartels

www.hk2.eu

www.comtection.de