STELLUNGNAHME

Berlin, 21. Februar 2023

## Deutsche Industrie- und Handelskammer

**DIHK-Stellungnahme Cyber Resilience Act (CRA)**

Je mehr Unternehmen digitalisiert und vernetzt sind, desto stärker hängt ihr Erfolg von funktionierenden Informations- und Kommunikationsinfrastrukturen und einer sicheren Datenverarbeitung und -speicherung ab. Für Unternehmen ist die Sicherheit ihrer Daten und Informationen deshalb eine der größten Herausforderungen bei der Digitalisierung. Deren volkswirtschaftliche Potenziale werden umfassend nur dann erschlossen, wenn Daten und Informationen sicher übertragen und verarbeitet werden. Dies erfolgt in der Regel auf Basis von softwarebasierten Produkten bzw. Produkten mit digitalen Elementen. Deren Cybersicherheit adressiert der CRA.

Das Bundesamt für Sicherheit in der Informationstechnik identifiziert in seinem aktuellen Lagebericht Schwachstellen in Produkten mit digitalen Elementen als eine der Hauptbedrohungen für Unternehmen. Viele dieser Produkte werden in kleinen, mittleren und großen Unternehmen eingesetzt und sind dort Produktionsfaktoren für die Herstellung ihrer eigenen Produkte und Dienstleistungen. Die DIHK setzt sich im Interesse aller Unternehmen dafür ein, dass Anbieter und Hersteller von Produkten mit digitalen Elementen von vornherein auf „Security by Design“ achten. Zusätzlich zu einem sicheren Zustand bei der Auslieferung der Produkte sollte über einen definierten Zeitraum eine sichere Nutzung durch Sicherheitsupdates gewährleistet werden. Insofern unterstützt die DIHK ausdrücklich die Intention des CRA, die Cybersicherheit von digitalen Produkten im Europäischen Binnenmarkt zu erhöhen. Der CRA kann sein Potenzial aber nur entfalten, wenn er Vorgaben macht, die nicht nur dem beabsichtigten Zweck dienen, sondern zugleich auch angemessen und praktikabel sind.

Der CRA stellt mit der Einführung von Konformitätsstandards für Produkte mit digitalen Elementen allerdings ein ambitioniertes und anspruchsvolles Unterfangen dar, dessen Umsetzung insbesondere für kleine und mittlere Hersteller mit merklichen Herausforderungen verbunden sein dürfte. Wir weisen ausdrücklich darauf hin, dass der vorgesehene sehr weite Anwendungsbereich – von smarten Alltagsgeräten im Internet of Things über Computer und mobile Geräte samt Betriebssystemen und Apps bis hin zu Komponenten, die in Netzwerken oder in industriellen Anlagen verbaut werden – sowie die Umsetzung von zusätzlichen Sicherheitsanforderungen und Meldepflichten über den Lebenszeitraum eines Produkts hinweg eine enorme Herausforderung für die Breite der gewerblichen Unternehmerschaft (vom Hersteller

**DIHK | Deutsche Industrie- und Handelskammer**
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Internet: www.dihk.de

über den Inverkehrbringer bis zum Händler) darstellt. Unternehmen müssen ihre internen Maßnahmen auf CRA-Konformität überprüfen beziehungsweise Prozesse neu etablieren und einen Mechanismus zum Umgang mit Schwachstellen implementieren. Dafür müssen sie sich an europäischen Normen orientieren, die allerdings zum großen Teil erst noch erarbeitet werden müssen. Unternehmen berichten auch sehr häufig, dass sie die dafür erforderlichen Fachkräfte nicht rekrutieren können. Dies trifft gleichermaßen auf den Aufbau von Organisationsstrukturen und Beschäftigten für die Marktüberwachung zu. Eine zeitliche Streckung der Übergangsfrist könnte dazu beitragen, die bereits bestehenden Fachkräfteengpässe zumindest nicht weiter zu verschärfen.

Durch die Umsetzung des CRA erwarten wir insgesamt steigende Herstellungskosten und damit höhere Preise für Produkte mit digitalen Elementen. Auf der anderen Seite erwarten wir einen Zugewinn an Sicherheit in Bezug auf die IT-Sicherheit von Produkten mit digitalen Elementen und dementsprechend eine Steigerung des allgemeinen Cybersicherheits-Niveaus. Denn viele Produkte werden in Unternehmen eingesetzt, deren Lieferketten-Sicherheit sich damit verbessern dürfte. Insofern gehen wir in Summe von einem positiven gesamtwirtschaftlichen Effekt durch die Umsetzung des CRA aus.

In den folgenden Bereichen sollte der Gesetzentwurf aus Sicht der DIHK nachgebessert werden:

**Ansatz einheitlicher Sicherheitsanforderungen konsequent verfolgen**

Die Europäische Kommission schlägt mit dem Cyber Resilience Act vor, bei allen Produkten, die miteinander oder mit dem Internet verbunden werden können, in den Phasen Design, Entwicklung und Produktion sowie während des Inverkehrbringens und der Nutzung risikoangemessene Cybersecurity-Maßnahmen zu etablieren. Der CRA stellt dabei – basierend auf den Prinzipien des New Legislative Framework (NLF) – Anforderungen an das Inverkehrbringen von Produkten und ergänzt diese um z. B. die Etablierung eines Schwachstellenamangements und Berichtspflichten in Bezug auf ausgenutzte Schwachstellen und Cybersicherheitsvorfälle über die Lebensdauer von Produkten mit digitalen Elementen hinweg.

Den Ansatz der risikobasierten Umsetzung auf Basis des New Legislative Frameworks greift auf etablierte Instrumente zurück. Dieser sog. horizontale Ansatz bildet nun einen einheitlichen Rahmen für sicherheitsrelevante Anforderungen an Produkte und ist nach Einschätzug der DIHK geeignet, die bisherigen sektoralen Richtlinien zu bereinigen und Cybersicherheit im gesamten Binnenmarkt zu stärken. Um Kohärenz tatsächlich sicherzustellen regen wir eine zeitnahe Evaluierung der einschlägigen Rechtsvorschriften an. Der CRA muss sich sehr nah am NLF orientieren, erforderlich Abweichungen sollten so gering wie möglich gehalten werden. Widersprüche zu Regelungen anderer Produktvorgaben zur IT-Sicherheit von Produkten, z. B. CE-Maschinenrichtlinie, geplante EU-KI-Richtlinie, müssen ausgeschlossen werden. Wir weisen aber auch darauf hin, dass das CE-Kennzeichen immer mehr Anforderungen abbilden soll – so

auch die Barrierefreiheit für viele digitale Güte oder Anforderungen aus dem Green Deal. Die Marktüberwachungsbehörden müssen in die Lage versetzt werden, all diese Anforderungen auch überprüfen zu können.

**Anwendungsbereich klar fassen**

Der von der EU-Kommission vorgeschlagene Anwendungsbereich bezieht sich auf alle "Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netzwerk beinhaltet". Damit soll sichergestellt werden, dass alle Produkte mit digitalen Elementen grundlegende Cybersicherheitsanforderungen erfüllen müssen. Aus Sicht der DIHK besteht Unklarheit darüber, welche Produkte unter den Anwendungsbereich fallen. Dies betrifft insbesondere Open Source Software und Cloud-Dienste.

**Open Source Software**

Im Fokus des CRA stehen Unternehmen und kommerzielle Produkte. In der Praxis sind Open Source Kompenenten Bestandteil zahlreicher kommerzieller Produkte. Die Intention des CRA, dass Innovationen, Forschung oder die wichtige, oft ehrenamtlich aktive Open Source Community nicht durch die Konformitätsanforderungen in Kreativität und Dynamik eingeschränkt, gehindert oder abgeschreckt werden sollen, unterstützt die DIHK.

Vor diesem Hintergrund sollte klarer gefasst werden, inwieweit Open Source Software im Zusammenhang mit dem Cyber Resilience Act behandelt wird, und wie die Anforderungen an die Verantwortlichkeit für Open Source Softwarekomponenten umgesetzt werden sollen, ohne Projeke durch bürokratischen Mehraufwand zu beeinträchtigen. Hier ist die richtige Balance gefragt. Unklarheiten ergeben sich etwa durch die Definition von „Geschäftstätigkeit“.

Die aktuelle Formulierung in Erwägungsgrund 10 zu Open Source “Im Zusammenhang mit Software ist eine Geschäftstätigkeit möglicherweise nicht nur dadurch gekennzeichnet, dass für ein Produkt ein Preis verlangt wird, sondern auch dadurch, dass für technische Unterstützungsleistungen ein Entgelt verlangt wird, dass eine Softwareplattform bereitgestellt wird, über die der Hersteller andere Dienste monetisiert, oder dass personenbezogene Daten zu anderen Zwecken als der alleinigen Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software verwendet werden.” kann bedeuten, dass nur "sehr reine" Open Source Produkte von den Regelungen des CRA ausgenommen werden. Selbst bei einer minimalen Geschäftstätigkeit würden mit dem Cyber Resilience Act Haftungsrisiken entstehen, die für Open Source Software außerhalb der EU nicht gelten, sodass diese Regelung dazu führen könnte, dass die Nutzung einzelner Open Source Software für die EU ausgeschlossen wird.

Die Definition der Geschäftstätigkeit sollte deutlich enger gefasst bzw. der oben zitierte Passus gestrichen werden, um den auch von der EU unterstützten Nutzen von Open Source nicht zu schmälern.

**Software as a Service**

Unklarheiten bestehen auch im Hinblick darauf, welche Art von Software unter die neuen Regelungen fallen soll. Erwägungsgrund 9 etwa schließt Dienstleistungen wie Software as a Service (SaaS) mit Ausnahme der Datenfernverarbeitung (remote data processing solutions) vom Anwendungsbereich aus. Hier sollte klarer definiert werden, dass Cloud-Dienste, die bereits als kritische Infrastrukturen betrachtet und ab einer bestimmten Größenordnung von der NIS2-Richtlinie erfasst werden, nicht unter den CRA fallen, da es sich hier nicht um Produkte im klassichen Sinne handelt.

**Eindeutige Definitionen erforderlich**

Der Cyber Resilience Act führt mehrere Begriffe und neue Definitionen ein. Allerdings gibt es für viele der Begriffe bereits gut etablierte internationale Definitionen, mit denen der CRA übereinstimmen sollte.

Der in der Verordnung verwendete zentrale Begriff „Produkte mit digitalen Elementen“ (Art. 3 Nr. 1 CRA) ist nicht identisch ist mit dem in § 327a Abs. 3 BGB. Der Begriff ist in der EU-Verordnung weiter gefasst als im deutschen Recht. Damit dies nicht zu Verunsicherungen bei den betroffenen Unternehmen führt, sollten die Begriffe vereinheitlicht werden.

Der Begriff „wesentliche Änderung“ (Art. 3 Nr. 31 CRA) führt zu Unsicherheiten in der Praxis. So könnte eine korrekte Anwendung des CRA beispielsweise bei Artikel 15, „…oder eine wesentliche Änderung an einem bereits in Verkehr gebrachten Produkt mit digitalen Elementen vornimmt“, ohne genaue Definition bzw. einer Vielzahl an erklärenden Beispielen zu Komplikationen führen (z. B. bei Händlern, die PCs usw. für Unternehmen zusammenstellen und die Betriebssysteme aufsetzen). sie dann in der Pflicht, das Konformitätsbewertungsverfahren und die dahinterstehende Haftung zu übernehmen, auch wenn sie Standardhard- und -software nutzen.

**Produktkategorien eindeutig an Kritikalität in der Anwendung ausrichten**

In ihrem Vorschlag unterscheidet die Europäische Kommission zwischen vier Arten von Produkten mit digitalen Elementen: [1]

[1]

**Nicht kritische Produkte mit digitalen Elementen (z. B. Festplatten, intelligente Lausprecher, Fotobearbeitung, Textverarbeitungssoftware und PC-Spiele),**

- kritische Produkte mit digitalen Elementen Klasse I (z. B. Browser, Software zum Entfernen von Schadsoftware, Passwort-Manager),
- kritische Produkte mit digitalen Elementen Klasse II (z. B. Betriebssysteme für Server, Desktops und Handys, Public-Key-Infrastrukturen, Firewalls für den industriellen Einsatz, Router, Sicherheitselemente, Chipkarten und Chipkartenleser),
- hochkritische Produkte mit digitalen Elementen (unter diese Kategorie fallen zunächst noch keine Produkte).

Nach Angaben der EU-Kommission sollen ca. 90 Prozent in die Gruppe der nicht kritischen Produkte fallen. Hersteller und Vertreiber von kritischen Produkten müssen strengere Anforderungen erfüllen, beispielsweise hinsichtlich der Konformitätsbewertung.

Die DIHK hält den Ansatz grundsätzlich für geeignet, die Regulierungstiefe von der Kritikalität eines Produktes abhängig zu machen. Allerdings ist anhand der im Anhang genannten Beispiele zum Teil nicht klar ersichtlich, warum Produkte in Klasse I und Klasse II eingestuft sein sollen. Es sollte klargestellt werden, welche Kriterien zur Einstufung der Produkte herangezogen werden. Zudem hängt die Kritikalität der Produkte auch davon ab, wo und unter welchen Bedingungen diese eingesetzt werden. Der Anwendungskontext sollte deshalb bei der Einstufung berücksichtigt werden.

Im CRA-Entwurf ist vorgesehen, dass die EU-Kommission mittels delegierter Rechtsakte die Listen der kritischen Produkte ergänzen und eine Liste der hochkritischen Produkte erstellen kann. Dies könnte bis zu 12 Monate dauern. Ob allen Wirtschaftsakteuren somit genügend Zeit bleibt sich mit ggf. veränderten Einstufungskriterien auseinanderzusetzen, darf zumindest angezweifelt werden. In den Definitions-Prozess sollten auf jeden Fall die potenziell betroffenen Unternehmen einbezogen werden.

**Voraussetzungen für Konformitätsbewertung zeitnah schaffen**

Produkte mit digitalen Elementen müssen dem Gesetzentwurf zufolge u. a. so konzipiert, entwickelt und hergestellt werden, dass sie ein angemessenes Cybersicherheitsniveau gewährleisten, ohne bekannte ausnutzbare Schwachstellen und in einer sicheren Standardkonfiguration, ausgeliefert werden.

**Konformitätsbewertungsverfahren**

Durch eine „Konformitätsbewertung“ wird überprüft, ob ein Produkt die Sicherheitsanforderungen und die Anforderungen zum Umgang mit Schwachstellen erfüllt. Für die sog. unkritischen Produkte können Hersteller die Konformität per Selbstbewertung anzeigen. Für kritische Produkte verlangt der CRA-Entwurf ein strengeres Nachweisprozedere, bei kritischen Produkten der Klasse II muss das Konformitätsbewertungsverfahren immer von einer dritten Partei durchgeführt werden. Eine Konformität mit den jeweiligen Sicherheitsanforderungen richtet sich nach der Risikoklasse und wird „vermutet“, wenn eine Übereinstimmung mit harmonisierten EU-Standards besteht. Die Kommission kann mittels Durchführungsrechtsakten EU-Cybersicherheitszertifizierungssysteme festlegen, die zum Nachweis der Konformität genutzt werden können. Die Konformität wird am Produkt mit dem „CE-Kennzeichen“ dokumentiert. Die Umsetzung wird von nationalen Marktüberwachungsbehörden überwacht.

Die betroffenen Unternehmen befürchten, dass weitere Bürokratie aufgebaut wird, die sie zusätzlich zu den bereits bestehenden gesetzlichen Anforderungen belasten wird. Der Mehraufwand ist deshalb auf das unbedingt erforderliche Maß zu beschränken. So legen die Unternehmen Wert darauf, dass das gesamte Verfahren digital und zu einem Großteil standardisiert ausgestaltet sein muss, um den bürokratischen Aufwand so gering wie möglich zu halten.

Der Rückgriff auf harmonisierte EU-Standards ist sinnvoll und dürfte es den Herstellern erleichtern, die Konformität ihrer Produkte nachzuweisen. Allerdings bestehen Zweifel, dass für die Vielzahl der Produktklassen bis zum Inkrafttreten des CRA entsprechende Standards zur Verfügung stehen. Ein Gleichlauf der Standardisierung und der Umsetzungserfordernisse der Unternehmen sollte sichergestellt werden. Es wird gewünscht, dass es eine kurze Frist für eine verbindliche Antwort der Stellen geben soll, die die Konformitätsbertung kritischer Produkte vornehmen.

Gerade im B2B-Bereich, insbesondere im Bereich der kritischen Infrastrukturen, gibt es viele Projekte mit einem hohen Individualanteil an Software, die mit Produktcharakter entwickelt werden. Wo ist hier in der Idee des Gesetzgebers die Grenze für Verpflichtungen zur Konformitätsbewertung durch Dritte? Oder ist tatsächlich intendiert, dass Anbieter jedes Produkt mit individueller Software einzeln zertifizieren sollen?

Es stellt sich außerdem die Frage, wie sich das CE-Kennzeichen zu dem freiwilligen BSI IT-Sicherheitskennzeichen aus dem IT-Sicherheitsgesetz 2.0 verhalten wird. Wäre das CE-Kennzeichen der pflichtmäßige „Basisschutz“ und das BSI-Kennzeichen geht noch einmal deutlich darüber hinaus, oder wäre das BSI-Kennzeichen nach inkrafttreten des CRA hinfällig? Ein BSI-Kennzeichen – falls überhaupt noch notwendig – sollte auf zusätzliche, besonders hohe Sicherheitsfeatures abzielen, mit denen Hersteller dann werben könnten.

**Software-Stückliste**

Hersteller müssen Komponenten und Schwachstellen des Produkts identifizieren und dokumentieren (über eine sog Software-Stückliste, Software Bill of Materials, SBOM).

Die Pflege einer Software-Stückliste beim Hersteller ist grundsätzlich sinnvoll und sollte als Stand der Technik anzusehen sein. Wobei einige Unternehmen dies anders sehen und deshalb SBOMs auf freiwilliger Basis vorschlagen. Allerdings beurteilen Unternehmen die Bereitstellung an Kunden oder gar Veröffentlichung kritisch. In komplexeren Produkten mit vielen Software-Komponenten könnten schnell viele Fehlalarme entstehen, da potentielle Schwachstellen anhand der genannten Komponenten gelistet würden, die in Wirklichkeit im Produkt aufgrund der Anwendung gar nicht relevant sein könnten.

Als sinnvoll erachten Unternehmen Standards für das Vorhalten von maschinenlesbaren Software-Stücklisten. Auch sollte darüber nachgedacht werden, wie die Unternehmen dabei unterstützt werden können, sich über Schwachstellen und Updates zu informieren, wenn diese in ihrem Verzeichnis der eingesetzten Software vorkommen.

**Umgang mit Schwachstellen bürokratiearm und praxistauglich gestalten**

Der CRA-Entwurf sieht vor, dass Hersteller Sicherheitslücken über den gesamten Produktlebenszyklus schließen müssen, maximal jedoch über fünf Jahre. Nutzer müssen über behobene Schwachstellen und über Cybersicherheitsvorfälle informiert werden. Gegebenenfalls muss ihnen mitgeteilt werden, welche Maßnahmen sie ergreifen können, um die Folgen eines Vorfalls zu begrenzen. Hersteller müssen darüber hinaus Cybersicherheitsvorfälle sowie jede aktiv ausgenutzte Schwachstelle innerhalb von 24 Stunden der europäischen Agentur für Cybersicherheit (ENISA) melden.

**Umgang mit Schwachstellen**

Die DIHK unterstützt ausdrücklich den Ansatz, Cybersicherheit über den Lebenszyklus eines Produktes hinweg zu betrachten. Eine Updatepflicht über 5 Jahre wird von vielen Unternehmen als ein angemessener Kompromiss angesehen. Es gibt aber auch Stimmen, die diesen Zeitraum als nicht ausreichend erachten. Am Ende kann sich ein Hersteller mit längeren Wartungszeiträumen vom Wettbewerb abheben bzw. sich dies nach Ablauf der 5 Jahre dann auch von den Nutzern bezahlen lassen. Für Komponenten, die in kritischen Wirtschaftsbereichen eingesetzt werden, könnten ggf. längerer Zeiträume sinnvoll sein. Hier stellt sich die Frage, nach welchen Kriterien dies entschieden würde und von wem. Es stellt sich auch die Frage, was passiert, wenn der Hersteller innerhalb von 5 Jahren nicht mehr am Markt ist.

In der Praxis erfolgt die Risikomeldung oft gemeinsam mit der Veröffentlichung des Patches zur Fehlerbehebung. Dies sollte so auch im CRA vorgesehen werden.

Grundlegende Voraussetzung für das Schließen von Schwachstellen ist jedoch, dass sie den Herstellern überhaupt bekannt sind. Die Begrifflichkeiten im CRA-Entwuf sollten dies klarer widerspiegeln. Der Begriff "bekannte ausnutzbare Schwachstellen" lässt viel Spielraum für Interpretationen. Ab wann kann davon ausgegangen werden, dass ein Hersteller von einer Schwachstelle weiß? Der Begriff „bekannte ausnutzbare Schwachstelle“ sollte durch die Formulierung durch „ausnutzbare Schwachstelle, die dem Hersteller bekannt ist“ ersetzt werden. Diese Klarstellung scheint uns auch erforderlich solange staatliche Stellen Schwachstellen kaufen und für geheimdienstliche Zwecke offenhalten statt unverzüglich auf deren Schließung hinzuwirken. Wir halten eine flankierende Regelung für erforderlich, die staatliche Sicherheitsbehörden dazu verpflichtet, ihre Informationen zu Schwachstellen mit den Herstellen der Produkte zu teilen, damit diese ihren Verpflichtungen aus dem CRA nachkommen können.

Auch besteht die Gefahr von Doppelaufwand. So normiert Artikel 15 die Fälle, in denen die Pflichten für Hersteller auch den Einführer und Händler betreffen. Dies ist in dem Fall, dass eine wesentliche Veränderung an dem Produkt vorgenommen wird, nachvollziehbar. In den Fällen, in denen das Produkt unverändert bleibt und lediglich unter anderem Namen bzw. anderer Marke veräußert wird, jedoch nicht. Dann müsste sichergestellt werden, dass der Verantwortliche erkennbar ist.

**Meldepflichten**

Der CRA-Entwurf sieht vor, dass Hersteller jeden Cybersicherheitsvorfall sowie jede aktiv ausgenutzte Schwachstelle binnen 24 Stunden der Agentur der Europäischen Union für Cybersicherheit (ENISA) melden, die ihr Produkt betreffen. Sie müssen auch die Nutzer über Cybersicherheitsvorfälle informieren und ihnen ggfs. mitteilen, welche Maßnahmen sie ergreifen können, um die Folgen eines Vorfalls zu begrenzen.

Insbesondere die kurzen Zeiträume für Meldungen an die ENISA hält die DIHK nicht für praktikabel. Sie würden viele Unternehmen überfordern. Die Pflichten sollten analog zur NIS 2-Richtlinie auf relevante Vorfälle bzw. Schwachstellen begrenzt werden.

Angemessene Fristen für Meldungen sollten sich am bestimmungsgemäßen Gebrauch orientieren. Für kritische Produkte, die beispielsweise bei kritischen Infrastrukturen eingesetzt werden, dürften die vorgeschlagenen Fristen nicht unangemessen sein. Andererseits erscheint für weniger kritische Produkte eine längere Frist akzeptabel und sinnvoll. Die meisten KMUs haben in der Regel nicht die Kapazitäten, Bereitschaftsdienste beispielsweise an Wochenenden einzusetzen, um Meldefristen einzuhalten. Die Entscheidung zu einer Meldung obliegt in der Praxis nur einem oder wenigen Experten in KMUs und ist somit an dessen Verfügbarkeit bzw.

Erreichbarkeit gebunden. Insofern wäre eine Frist von 72 Stunden eher praktikabel und angemessen.

Wir regen außerdem an, den Meldeaufwand für Unternehmen so niedrigschwellig wie möglich zu gestalten. Mehrfachmeldungen sollten vermieden werden. Unternehmen, die mit Schwachstellen und IT-Vorfällen zu tun haben, sollten nicht mehrere Meldewege bedienen müssen, wenn beispielsweise Komponenten betroffen sind, die unter den CRA und unter die NIS 2-Richtlinie fallen. Die Meldeinfrastrukturen aus der NIS 2-Richtlinie könnten entsprechend übernommen werden. Um Eindeutigkeit und direkte Bezüge herzustellen sind digitale Meldewege erforderlich. Dafür sollten digitale Plattformen zur Verfügung gestellt werden, in welcher nicht nur die abgegebenen Meldungen, sondern auch die für das Unternehmen relevanten Meldungen einsehbar sind (also eine „digitale Informations-Plattform“). Schon heute gibt es nach einem Vorfall nur selten eine Reaktion oder Unterstützung durch die zuständigen Behörden, hier sollten reziprok zu den Verpflichtungen für die Unternehmen entsprechende Angebote durch die Meldestellen etabliert werden.

**Pflichten für Händler und Einführer nicht überziehen**

Einführer dürfen Produkte mit digitalen Elementen nur dann in Verkehr bringen, wenn diese den Sicherheitsanforderungen und den Anforderungen zum Umgang mit Schwachstellen genügen. Dafür müssen sie prüfen, ob das Produkt des Herstellers ein Konformitätsbewertungsverfahren durchlaufen hat, eine technische Dokumentation vorliegt und ob das Produkt mit dem CE-Kennzeichen versehen ist. Auch Händler müssen sicherstellen, dass die Anforderungen des CRA erfüllt sind. Sie müssen u. a. prüfen, ob das Produkt mit dem CE-Kennzeichen versehen ist und die Informationen und Anleitungen des Herstellers zum Produkt zur Verfügung stehen. Bei Nichterfüllung müssen sie auf Korrekturmaßnahmen hinwirken oder das betroffene Produkt ggfs. vom Markt nehmen. Sie unterliegen ebenfalls Melde- und Informationspflichten gegenüber den Marktüberwachungsbehörden und den Kunden.

Die Verpflichtungen insbesondere für kleinere Händler werden von diesen als nicht praktikabel bewertet und sollte einer erneuten Betrachtung unter Beachtung des Angemessenheitsprinzips unterzogen werden. Nicht intendiert ist sicherlich, dass in der Lieferkette gerade (kleine) Händler diejenigen sind, die in Haftung genommen werden, wenn Zulieferer dies in ihren Lieferbedingungen ausschließen und das Risiko auf den Händler abgewälzt wird. Auch Vorgaben des CRA-Entwurfs, dass in einem Zeitraum von 5 Jahren Händler und Einführer Marktüberwachungsbehörden über die Einstellung der Betriebstätigkeit des Herstellers informieren müssen, werden von den Unternehmen als nicht praktikabel bezeichnet.

Ebenso ist der Anwendungsbereich in Artikel 17 ist zu weit gefasst. Nach der Formulierung müsste danach jeder nationale Verkäufer Name und Adresse von jedem Kunden 10 Jahre aufbewahren, dem er eine Ware mit digitalen Elementen verkauft hat. Das ist praktisch nicht durchführbar.

**Unterstützungsangebote für KMU erforderlich**

Um die Sicherheit im gesamten Binnenmarkt mittels Kennzeichnungs- und Meldepflichten zu stärken, werden einheitliche Standards vorgeschrieben, die sich primär an Produkten und Produktkategorien orientieren. Dieser Ansatz ist verständlich und sorgt für Homogenität.

Gleichzeitig heißt das, dass der CRA im Unterschied zu Gesetzesvorhaben wie dem Data Act und der NIS 2.0-Richtlinie keine Ausnahmeregelungen oder Abstufungen nach Sektoren oder Unternehmensgröße vorsieht. Um KMU und Start-Ups jedoch nicht überproportional zu belasten und gegenüber großen Wettbewerbern zu benachteiligen, sollte hier spätestens in der Umsetzung durch entsprechende staatliche Unterstützungs- und Beratungsangebote nachgesteuert werden, damit auch kleinere Unternehmen den Konformitätsanforderungen in geeigneter Zeit und Weise entsprechen können.

Dies ist explizit in Artikel 41 Abs. 8 vorgesehen. Allerdings sollte hier ein verbindlicheres Mandat formuliert werden: „Die Marktüberwachungsbehörden ~~können~~ geben den Wirtschaftsakteuren mit Unterstützung der Kommission Leitlinien und Ratschläge für die Durchführung dieser Verordnung ~~geben~~."

Wünschenswert wäre, dass auf die Erfahrungen bei der Umsetzung anderer umfassender CE-Kennzeichnungen zurückgegriffen wird und bspw. analog zu den Biozidprodukte-, Chemikalien- und REACH-Verordnungen ein CRA-Helpdesk auf nationaler Ebene oder bei der ENISA eingerichtet wird.

**Übergangszeiträume verlängern**

Der Kommissionsvorschlag sieht vor, dass der CRA bereits zwei Jahre nach seinem Inkrafttreten gelten soll.

Die DIHK hält die Übergangsfrist von 24 Monaten (12 Monate für Meldepflichten) für zu kurz, um die wesentlichen Anforderungen an alle Produkte mit digitalen Elementen umzusetzen. Daher sprechen wir uns für eine längere Übergangsfrist aus, zumindest für solche Produktkategorien, die als weniger kritisch erachtet werden.

Der sehr weite Anwendungsbereich des Cyber Resilience Act hat weitreichende Auswirkungen für viele Unternehmen. Diese müssen sektorübergreifend ihre internen Maßnahmen auf CRA-Konformität überprüfen bzw. sogar neu einrichten und einen Mechanismus zum Umgang mit Schwachstellen implementieren, der den Anforderungen aus Anhang I Abschnitt 2 entspricht. Neben den Kosten, anspruchsvollen Prozessanpassungen und dem Mangel an Fachkräften für die Umsetzung müssen Unternehmen auch die Komplexität von Lieferketten und die große Abhängigkeit von EU-externen Komponenten und Lösungen mitdenken. Auch für Produkte, die über längere Zeit entwickelt werden, würde sich größerer Anpassungsbedarf ergeben.

Gleichzeitig kann der CRA erst dann voll wirksam werden, wenn die im Gesetz genannten organisatorischen Rahmenbedingungen etwa in Bezug auf die Marktüberwachung und die harmonisierten Standards gegeben sind. Die Mitgliedstaaten müssen die Marktüberwachung organisieren. Dafür müssen neue Organisationsstrukturen festgelegt und neue Mitarbeitende eingestellt werden. Entscheidend für den Erfolg des CRA wird die rechtzeitige Verfügbarkeit von harmonisierten Standards sein. Fehlen diese, sind Engpässe bei der Verfügbarkeit zugelassener Produkte unumgänglich. Daher fordern wir die Europäische Kommission auf, frühzeitig entsprechende Normungsmandate zu erteilen, die die Normungsorganisationen im Schulterschluss mit der Wirtschaft zügig annehmen und umsetzen müssen. Auch die Prüfung, ob aktuelle Standards anwendbar werden könnten, wird erst nach dem Normungsauftrag möglich sein. Im Umkehrschluss würde das bedeuten, dass Hersteller zwingend eine notifizierende Stelle für die Konformitätsbewertung einbeziehen müssen. Die Konformitätsbewertungsstellen werden voraussichtlich nicht in der Lage sein, alle Klasse II-Produkte und die Produkte, für die es noch keine harmonisierten Standards gibt, in absehbarer Zukunft zu bewerten. Für all diese Prozesse sind viele Security-Experten erforderlich, die in absehbarer Zeit am Markt schlicht nicht verfügbar sein werden.

In diesem Zusammenhang stellt sich uns die Frage, ob es seitens der EU bereits Pläne für Abkommen über gegenseitige Anerkennung (sog. MRAs gemäß Erwägungsgrund 67) mit wichtigen Partnerländern und Märkten (bspw. USA, UK) gibt, durch die eine Anerkennung anderer Sicherheitsstandards ermöglicht und entsprechend die Nutzung und Einfuhr von EU-externen Soft- und Hardwareprodukten erleichtert wird?

Das weiteren stellt sich uns die Frage, wie mit Produkten umgegangen werden soll, die sich bereits im Portfolio eines Unternehmens befinden. Bis wann dürfen diese noch in den Verkehr gebracht werden?

Grundlage dieser Stellungnahme sind die der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs sowie die wirtschaftspolitischen/europapolitischen Positionen der DIHK. Sollten der DIHK noch weitere in dieser Stellungnahme noch nicht berücksichtigte relevante Äußerungen zugehen, wird die DIHK diese Stellungnahme entsprechend ergänzen.

**Ansprechpartner**

Dr. Katrin Sobania, sobania.katrin@dihk.de

Steffen von Eicke, voneicke.steffen@dihk.de

**Wer wir sind:**

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein.

Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zu gemeinsamen Positionen der Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Darüber hinaus koordiniert die DIHK das Netzwerk der 140 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 92 Ländern.

Sie ist im Register der Interessenvertreter der Europäischen Kommission registriert (Nr. 22400601191-42).