Cyber Resilience Act - Ende der Geduld des Regulators

CRA enfaltet Wirkung auf nicht regulierte Akteure

Holger Friedrich
Dr. Waldemar Grudzien
Leon Kuhlmann

Februar 2023
Blogpost

Key Facts

- Europäische Harmonisierung der Sicherheitsanforderungen für „Produkte mit digitalen Elementen“ (Hard- und Software) ist zu begrüßen
- Primärziel der Verordnung ist die Verpflichtung der Hersteller sich während des vollständigen Lebenszyklus eines Produkts „ernsthaft“ um die Sicherheit zu kümmern
- Ziel der CRA-Verordnung ist die Erhöhung der Produktsicherheit, die Durchsetzung bedarf Anpassungen an Marktrealitäten sowie geostrategisch veränderter Rahmenbedingungen
- Inverkehrbringer und Händler werden zum Teil mit erheblichen Pflichten zur Sicherheit belegt
- Anforderungen werden kleinere und mittlere Wirtschaftsakteure überfordern, Reaktionen im Markt derzeit nicht abschätzbar
- Unternehmen und Unternehmensverbände sollten Lobbyarbeit intensivieren, um Verordnung nicht nur für große Akteure umsetzbar zu gestalten
- Im Wirkgefüge stellt CRA-Verordnung das Pendant zum Lieferkettengesetz am Anfang der Lieferkette dar, mit marktbereinigender Wirkung

Einleitung

Die EU intensiviert und vervollständigt schrittweise ihre Digitalgesetzgebung. Mit dem Cyber Resilience Act (CRA) in der Entwurfsversion vom 16. September 2022 wird die Europäische Datenstrategie, welche auf den vier Säulen Datenschutz, Grundrechte, Sicherheit und Cybersicherheit beruht, in der vierten Säule gestärkt. Die Grundsätze der Produkthaftung werden auf Hardware- und Softwareprodukte, im Sprachgebrauch der CRA „Produkte mit digitalen Elementen“ ausgeweitet.

Mit der CRA stimuliert die EU die Optimierung von zwei wesentlichen Herausforderungen im europäischen Wirtschaftsgefüge: Ein strukturell geringes Maß an Cybersicherheit sowie das unzureichende Verständnis sowie der mangelnde Informationszugang von Nutzern zu Cybersicherheit.

Mit dem Ziel der Unterstützung des Europäischen Binnenmarkts wurden zwei übergeordnete Ziele festgelegt:

1) Die Schaffung von Bedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen, um Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr zu bringen, ergänzend dass Hersteller für den vollständigen Lebenszyklus eines Produkts für die Sicherheit in Verantwortung genommen werden, und

2) die Schaffung von Bedingungen, die es Nutzern ermöglicht, bei Auswahl und Verwendung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen.

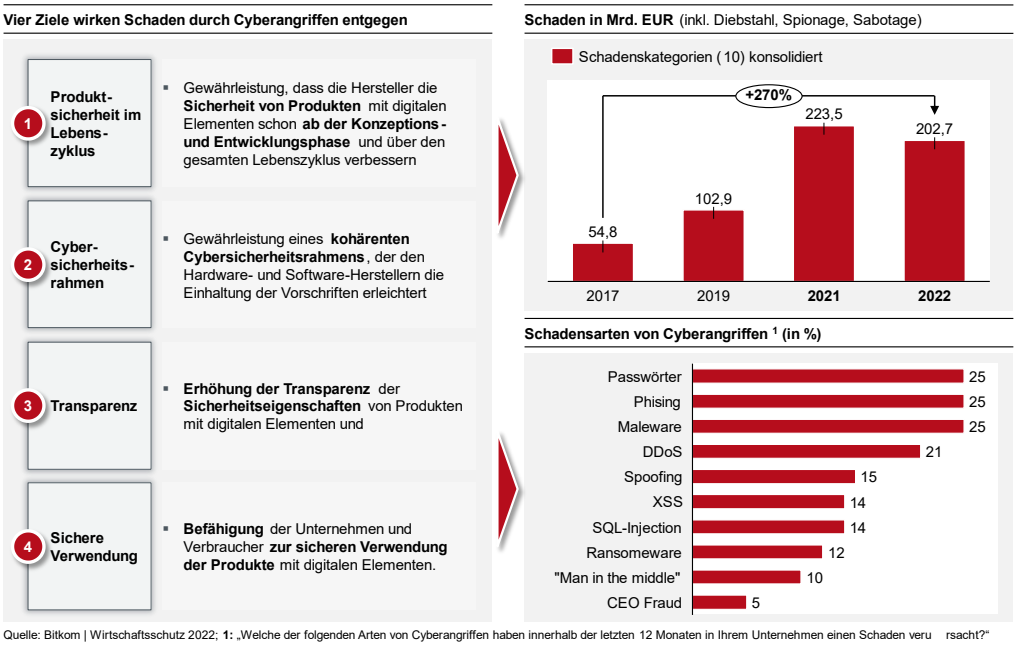


Abbildung 1: Deutsche Wirtschaft in der Breite von Angriffen betroffen und rechnet mit verstärkten Cyberangriffen

Hierzu wurden untergeordnet vier spezifische Ziele festgelegt:

i. Gewährleistung, dass Hersteller die Sicherheit von Produkten mit digitalen Elementen ab der Konzeptions- und Entwicklungsphase und über den gesamten Lebenszyklus verbessern,

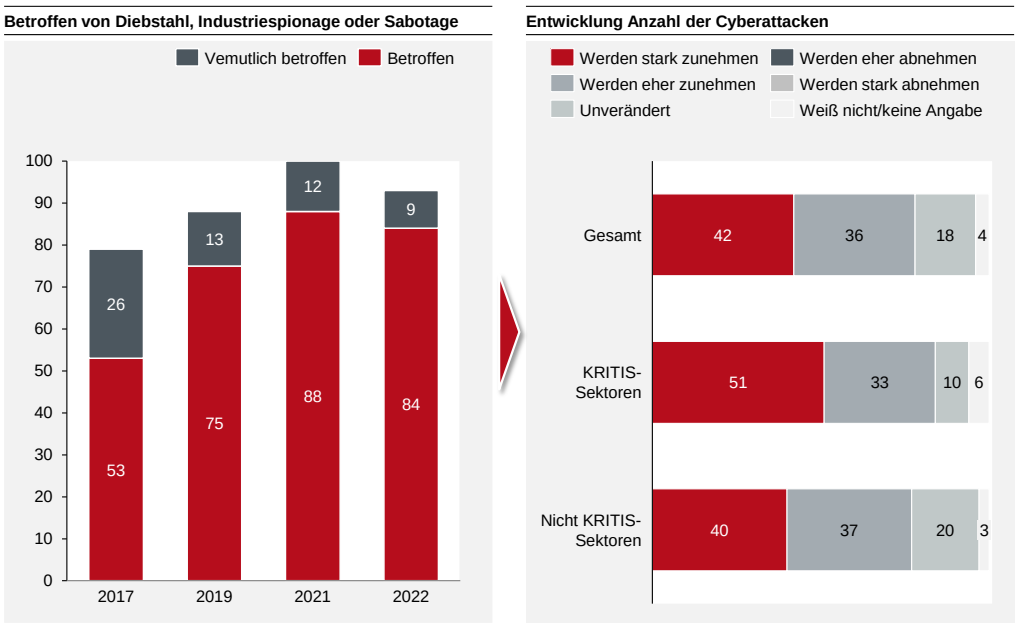
ii. Gewährleistung eines kohärenten Cybersicherheitsrahmens, der den Hardware- und Software-Herstellern die Einhaltung von Vorschriften erleichtert,

iii. Erhöhung der Transparenz von Sicherheitseigenschaften für Produkte mit digitalen Elementen und

iv. Befähigung der Unternehmen und Verbraucher zur sicheren Verwendung der Produkte mit digitalen Elementen

In Abbildung 1 sind die vier oben genannten spezifischen Ziele illustrativ gegen die Schäden und Schadensarten aus erfolgreichen Cybersicherheitsangriffen in der zeitlichen Entwicklung seit 2017 aufgetragen.

Primärziel der CRA ist somit eine Hersteller-Verpflichtung für „Produkte mit digitalen Elementen“ während des vollständigen Lebenszyklus eines Produkts Sicherheit „ernsthaft“ (Erwägungsgrund 2) sicherzustellen. Ergänzend werden Einführer (Inverkehrbringer) und Händler mit Pflichten zur Sicherheit belegt. Dass das Streben nach Erreichung der Ziele der CRA notwendig ist zeigt Abbildung 2, die den Bedarf an Schutzmaßnahmen in Erwartung „stark und eher zunehmender Cyberattacken“ anzeigt. Dabei ist das hohe Adaptationsniveau der KRITIS-Sektoren mit 84% auffalend und positiv zu bewerten.



1: Basis: Alle befragten Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

Abbildung 2: CRA-Ziele sollen Schäden durch Cyberangriffe (Diebstahl, Sionage, Sabotage, ...) entgegenwirken

Technische Analyse

Die Regelungsinhalte des Cyber Resilience Act (CRA) sind in Abbildung 3 dargestellt. Im Folgenden werden die Kapitel der CRA im Detail, oder bei bereits bekannten Sachverhalten kursorisch besprochen. Im Detail analysiert werden Artikel, die ergänzende Aufwände erfordern, wie beispielsweise Sicherheitsanforderungen an Wirtschaftsakteure, ergänzender Verwaltungsaufwand zu bestehenden Regulierungen und Weiteres. Dieses Vorgehen ist dem Umstand geschuldet, dass Regelungsumfänge, wie die europäische Konformitätsregelung (CE-Zeichen) der Kapitel 3 und 4 hinlänglich geübte Praxis in der Wirtschaft darstellen.

Cyber Security Act Com (2022) 454 - Regelungsinhalte

Kapitel	Titel	Artikel
1 Kapitel I	Allgemeine Bestimmungen	Artikel 1 bis Artikel 9
2 Kapitel II	Pflichten der Wirtschaftsakteure	Artikel 10 bis Artikel 17
3 Kapitel III	Konformität des Produkts mit digitalen Elementen	Artikel 18 bis Artikel 24
4 Kapitel IV	Notifizierung von Konformitätsbewertungsstellen	Artikel 25 bis Artikel 40
5 Kapitel V	Marktüberwachung und Durchsetzung	Artikel 41 bis Artikel 49
6 Kapitel VI	Übertragene Befugnisse und Ausschussverfahren	Artikel 50 bis Artikel 51
7 Kapitel VII	Vertraulichkeit und Sanktionen	Artikel 52 bis Artikel 53
8 Kapitel VIII	Übergangs- und Schlussbestimmungen	Artikel 54 bis Artikel 57

Quelle: CORE

Abbildung 3: Regelungsinhalte des Cyber Security Act COM(2022) 454, Version vom 16.09.2022

Artikel 1 legt den „Gegenstand“ der CRA für Produkte mit digitalen Elementen in vier Anforderungsgruppen an Cybersicherheit fest:

a) Vorschriften für das Inverkehrbringen
b) Anforderungen an die Konzeption, Entwicklung und Herstellung
c) grundlegende Anforderungen an die Behandlung von Schwachstellen
d) Vorschriften für Marktüberwachung und Durchsetzung der Anforderungen.

Artikel 2 „Anwendungsbereich“ legt fest welche Produkte in den Ordnungsrahmen der CRA fallen und welche nicht: zur ersteren Gruppe fallen Produkte mit digitalen Elementen, deren „bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“. Praktisch bedeutet dies, dass alle Produkte mit einer Netzwerkschnittstelle eingeschlossen sind.

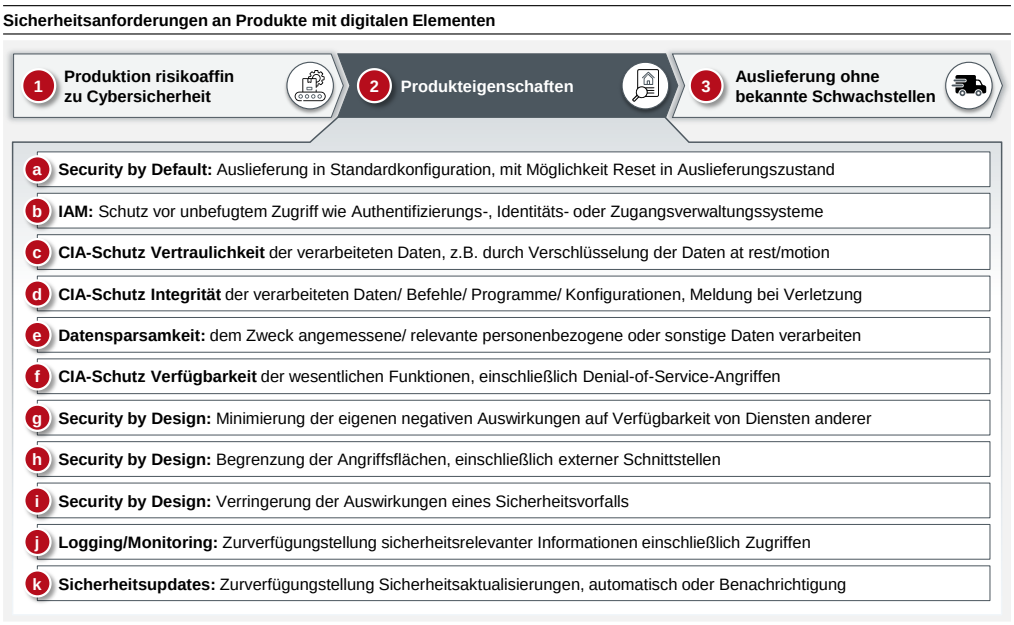
Nicht unter die CRA fallen Produkte, auf die andere Rechtsakte der Union Anwendung finden: Medizinprodukte, In-Vitro-Diagnostika, Kraftfahrzeuge und Produkte für die zivile Luftfahrt. Nach

Absatz 4 kann die Anwendung der Verordnung auf Produkte mit digitalen Elementen, die unter andere Rechtsvorschriften der EU mit gleichgerichteter Risikoaffinität fallen und dasselbe Schutzniveau erreichen, eingeschränkt oder gar ausgeschlossen werden. Nach Absatz 5 gilt die Verordnung nicht für Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit oder für militärische Zwecke entwickelt wurden, und auch nicht für Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind. Hier behalten sich die Mitgliedstaaten das Recht auf ihre nationale Sicherheit vor – ein deutlicher Hinweis zur Lösung der Privacy Shield Herausforderungen im Rahmen der ersten Novellierung der DSGVO.

Artikel 4 „Freier Verkehr" Absatz 3 bietet ein neues Geschäftsmodell für den Abmahnmissbrauch: Software die dieser Verordnung nicht entspricht (für Testzwecke, nur für einen begrenzten Zeitraum verfügbar), muss über eine „sichtbare Kennzeichnung" verfügen, „dass sie dieser Verordnung nicht entspricht".

Artikel 5 öffnet das zu erfüllende Tableau der „Anforderungen an Produkte mit digitalen Elementen". Diese dürfen nur dann im Markt bereitgestellt werden, wenn sie gemäß Nr. 1 den grundlegenden Anforderungen in Anhang I Abschnitt 1 (Sicherheitseigenschaften, siehe Abbildung 4) genügen und unter der Bedingung, dass sie ordnungsgemäß installiert, gewartet und bestimmungsgemäß oder unter vernünftigerweise vorhersehbaren Umständen verwendet sowie gegebenenfalls aktualisiert werden.

Der zweite Teil von Artikel 5 Nr. 1 – „ordnungsgemäß installiert, gewartet und bestimmungsgemäß oder unter vernünftigerweise vorhersehbaren Umständen verwendet sowie gegebenenfalls aktualisiert werden" – zielt auf Anhang II (Informationen und Anweisungen für die Nutzer, siehe Abbildung 5 rechte Seite)).

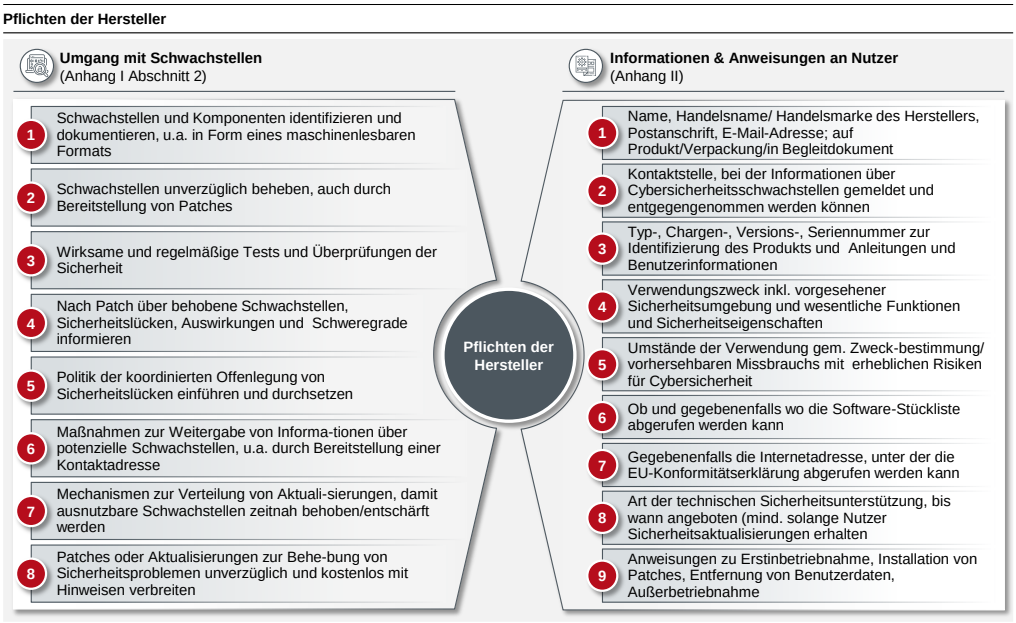


Quelle: CORE

Abbildung 4: Sicherheitseigenschaften von Produkten mit digitalen Elementen (Anhang I Abschnitt 1)

Die in den elf Buchstaben „a“ bis „k“ zusammengestellten Sicherheitseigenschaften für Entwurf, Entwicklung und Herstellung bilden das Who-is-Who der IT-Produktsicherheit sowie des Datenschutzes und werden seit Jahren durch Politik und Verbraucherschützer gefordert: CIA-Schutz, Security by Design und by Default, IAM, Datensparsamkeit, Logging/Monitoring und Patching. Dies ist unter Betrachtung des Anhang III ein anspruchsvolles Paket. Den aus der Nutzung erwachsenen Risiken müssen angemessene Maßnahmen zur Gewährleistung der Cybersicherheit gegenübergestellt werden.

Gemäß Anhang I Abschnitt 1 Absatz 2 müssen Produkte mit digitalen Elementen ohne bekannte ausnutzbare Schwachstellen ausgeliefert werden. Für nicht bekannte Schwachstellen stellt Anhang I Abschnitt 2 acht Forderungen zum Umgang mit diesen auf (Abbildung 5 linke Seite) auf. Zur weiteren Hilfe müssen die Hersteller den Nutzern Informationen und Anweisungen zu Produkten mit digitalen Elementen (Anhang II) zur Verfügung stellen (Abbildung 5 rechte Seite).



Quelle: CORE

Abbildung 5: Umgang mit Schwachstellen bei Produkten mit digitalen Elementen sowie Informationen und Anweisungen für die Nutzer von Produkten mit digitalen Elementen

Artikel 6 gilt für „Kritische Produkte mit digitalen Elementen“. Diese sind in Anhang III mit ihren Kernfunktionen, unterteilt in zwei Klassen I und II und damit zwei Cybersicherheitsrisikoklassen, gelistet. Absatz 2 gibt der EU Kommission das Recht Änderungen an der Liste vorzunehmen; hierzu bestimmt sie die Höhe des Cybersicherheitsrisikos eines potenziellen Kandidaten für die Liste anhand verschiedener Kriterien:

- Cybersicherheitsfunktion und mindestens eins der Merkmale
  - i) erhöhte Privilegien/Verwaltung von Privilegien;
  - ii) direkte oder privilegierter Zugang zu Netz- oder Rechenressourcen;
  - iii) Zugangskontrolle zu Daten/operativer Technik;

iv) Funktion mit entscheidender Bedeutung für Vertrauen/insbesondere Sicherheitsfunktion (Netzsteuerung, Endpunktsicherheit, Schutz des Netzes)

- unterliegt der NIS-2-Richtlinie
- unterliegt der DSGVO
- Beeinträchtigung einer Vielzahl von Personen (Mengenkriterium betroffener Personen aus Datenschutz)
- Verluste, Störungen, erhebliche Bedenken in der Vergangenheit

Gemäß Absatz 4 unterliegen kritische Produkte den Konformitätsbewertungsverfahren nach Artikel 24 Absätze 2 (Klasse I) und 3 (Klasse II). Kritische Produkte der Klasse I können eine Konformitätsvermutung nach Artikel 18 für sich beanspruchen. Diese ist den kritischen Produkten der Klasse II verwehrt und sie müssen sofort ein EU-Baumusterprüfverfahren oder eine Konformitätsbewertung durchlaufen.

Eine Frage stellt sich zu Klasse I Nr. 13 „Remote access/sharing software“: SaaS[1]-Angebote fallen gemäß Erwägungsgrund 9 nicht in den Ordnungsrahmen der CRA, sondern der NIS-2-Richtlinie. Doch sind SaaS-Angebote über die genannte Nr. 13 durch die CRA adressiert. Hier sollte die EU KOM eine eindeutige Klärung herbeiführen. Open Source Software wird eindeutig ausgeschlossen durch Erwägungsgrund 10: Freie und quelloffene Software, die außerhalb einer Geschäftstätigkeit entwickelt und bereitgestellt wird sowie Software zu Testzwecken (Erwägungsgrund 21) fallen ebenso nicht unter die CRA.

Im letzten Absatz 5 behält sich die EU KOM vor, Kategorien für hochkritische Produkte mit digitalen Elementen festzulegen. Hersteller müssten für diese Produkte die Cybersicherheits-zertifizierung im Rahmen eines europäischen Systems gemäß Cyber Security Act erlangen. Die Artikel 7 bis 9 befassen sich mit dem Zusammenwirken des Cyber Resilience Act mit Regulierungen für andere Produktkategorien: allgemeine Produktsicherheit für Produkte, die nicht der CRA unterliegen (Artikel 7), Hochrisiko-KI-Systeme, die durch die KI-Verordnung reguliert sind (Artikel 8) und Maschinenprodukte im Anwendungsbereich der Verordnung für Maschinenprodukte (Artikel 9).

Kapitel II „Pflichten der Wirtschaftsakteure“ mit den Artikeln 10 bis 17 stellt den zentralen Anforderungskatalog der Verordnung dar. Aus Artikel 10 (Pflichten der Hersteller), Artikel 13 (Pflichten der Einführer) und Artikel 14 (Pflichten der Händler) ergeben sich insgesamt 23 kombinierte Pflichten für diese drei Wirtschaftsakteure (siehe Abbildung 6 und Abbildung 7). Dabei ist zu beachten, dass Einführer und Händler nicht nur überprüfen müssen, ob die Hersteller ihren Pflichten nachgekommen sind, sondern in einigen Fällen auch selbst aktive Prüfungshandlungen durchzuführen haben, um Anforderungen gerecht zu werden.

[1] Software-as-a-Service

Anforderungen des CRA-Gesetzes an Hersteller, Einführer und Händler X Umsetzung △ Check ob umgesetzt ☐ Hoher Aufwand

No.	Hersteller (Artikel 10)	Einführer (Artikel 13)	Händler (Artikel 14)	Anforderungen an Hersteller, Einführer und Händler	Hersteller	Einführer	Händler
1	(1)	(1)	(2)	1 Anhang I Abschnitt 1	X	△	△
2	(2)	…	…	2 Bewertung von Cybersicherheitsrisiken (Planung bis Wartung)	X	…	…
3	(3)	…	…	3 Aufnahme von 2 in Dokumentation	X	…	…
4	(4)	…	…	4 Sicherstellung von 1 bei bezogenen Komponenten Dritter	X	…	…
5	(5)	…	…	5 Dokumentation der Cybersicherheitsaspekte[1]	X	…	…
6	(6)	…	…	6 Schwachstellenbehandlung in der Lebensdauer (max. 5 Jahre)	X	…	…
7	(7)	(2) a) b)	…	7 Techn. Dokumentation (Art. 23) + Konformitätserklärung (Art. 24)	X	△	…
8	(8)	…	…	8 Aufbewahrung Dokumentation für 10 Jahre[2]	X	…	…
9	(9)	…	…	9 Gewährleistung der Sicherheit auch bei Serienproduktion	X	…	…
10	(10)	(2) c) + (5)	(2) b)	10 Beifügung Informationen und Anleitung aus Anhang II	X	△	△
11	(11)	…	(2) b)	11 Information über EU-Konformitätserklärung	X	…	△
12	(12)	(6)	(4)	12 Korrekturmaßnahmen zur Wiederherstellung der Konformität	X	X	X
13	(13)	(8)	(5)	13 Unterlagenübermittlung an Marktüberwachungsbehörde[3]	X	X	X

Quelle: CORE | 1: inkl. Schwachstellen, Aktualisierung der Dokumentation bei Bedarf | 2: gemäß der EU-Konformitätserklärung | 3: zum Nachweis der Konformität

Abbildung 6: Kombinierte Pflichten der Wirtschaftsakteure Hersteller, Einführer und Händler – Aufzählung 1 bis 13

An einigen Beispielen werden die aktiven Prüfungshandlungen von Einführer und Händler erläutert:

- Abbildung 6, Nummer 1:
  - Artikel 10 Absatz 1: Hersteller müssen gewährleisten, dass das Produkt gemäß den grundlegenden Anforderungen in Anhang I Abschnitt 1 konzipiert, entwickelt und hergestellt worden ist.
  - Artikel 13 Absatz 1: Einführer müssen prüfen ob die Produkte den grundlegenden Anforderungen in Anhang I Abschnitt 1 genügen und bei denen die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I Abschnitt 2 genügen
  - Artikel 14 Absatz 2: Händler haben bei dieser Aufgabe geringere Pflichten

- Was bedeutet der Prüfauftrag an die Einführer? Ist damit ein Soll-Soll-Check gemeint, d.h. die Überprüfung der Papiere der Hersteller, oder ist damit ein Soll-Ist-Check gemeint, d.h. ein aktives Nachprüfen, ob das was der Hersteller in der Dokumentation behauptet, auch tatsächlich zutrifft. Im zweiten Fall muss die Frage erlaubt sein, welche Einführer dieses vermögen und wieviele Einführer im Markt verbleiben werden.

- Abbildung 6, Nummer 12:
  - Artikel 10 Absatz 12: Hersteller müssen bei Diskonformität unverzüglich die erforderlichen Korrekturmaßnahmen zur Wiederherstellung der Konformität oder um gegebenenfalls das Produkt vom Markt zu nehmen oder zurückzurufen
  - Artikel 13 Absatz 6: Einführer müssen die erforderlichen Korrekturmaßnahmen unverzüglich „ergreifen“

- Artikel 14 Absatz 4: Händler „sorgen“ dafür, dass die erforderlichen Korrekturmaßnahmen unverzüglich „ergriffen werden“

- Was bedeuten die Aufträge für Einführer und Händler? Hat ein Einführer eigenständig Korrekturmaßnahmen zu ergreifen, wie bspw. einen Rückruf oder die Information von Nutzern bei identifizierten Schwachstellen? Wieviele Einführer können dies realistisch leisten? Auch Händler haben dafür zu sorgen, dass angemessene Maßnahmen ergriffen werden. Im Zweifel bedeutet diese Vorgabe eine Dreifachprüfung jedes Produktes mit digitalen Elementen, da sich Einführer und Händler nicht auf die Angaben der Hersteller verlassen dürfen, sondern selbst jedes Produkt im Lichte der Angaben der Hersteller zu kontrollieren haben

Anforderungen des CRA-Gesetzes an Hersteller, Einführer und Händler — X Umsetzung △ Check ob umgesetzt ☐ Hoher Aufwand

No.	Hersteller (Artikel 10)	Einführer (Artikel 13)	Händler (Artikel 14)	Anforderungen an Hersteller, Einführer und Händler	Hersteller	Einführer	Händler
14	(14)	(9)	(6)	14 Information an Marktüberwachungsbehörde bei Einstellung Betrieb	X	X	X
15	(15)	…	…	15 EU-KOM kann Elemente der Software-Stückliste festlegen	…	…	…
16	…	(3)	…	16 Inform. an Marktüberwachungsbehörde bei Cybersicherheitsrisiken	…	X	…
17	…	(4)	(2) b)	17 Kontaktdaten des Einführers	…	X	△
18	…	(5)	…	18 Anhang II in einer leichten Sprache für Nutzer	…	X	…
19	…	(6) Teil 1	(4) Teil 1	19 Nicht-Erfüllung Anhang I führt zu Korrekturmaßnahmen (Rückruf)	…	X	X
20	…	(6) Teil 2	(4) Teil 2	20 Information an Hersteller und Marktüberwachungsbehörde[1]	…	X	X
21	…	(7)	…	21 Vorhalten der Dokumentation und der EU-Konformitätserklärung	…	X	…
22	…	(8)	(5)	22 Bereitstellung aller Informationen an Marktüberwachungsbehörde2	…	X	X
23	…	…	(1)	23 Beachtung des Cyber Resilience Act mit „gebührender Sorgfalt“	…	…	X

Quelle: CORE | 1: Information an Hersteller zu Schwachstellen und an Marktüberwachungsbehörde zu Cybersicherheitsrisiken und Korrekturmaßnahmen | 2: sollte dies so verlangt werden

Abbildung 7: Kombinierte Pflichten der Wirtschaftsakteure Hersteller, Einführer und Händler – Aufzählung 14 bis 23

- Abbildung 7, Nummer 20
  - Artikel 13 Absatz 6 (Teil 2) / Artikel 14 Absatz 4 (Teil 2): Bei Feststellung einer Schwachstelle in dem Produkt mit digitalen Elementen informieren die Einführer / Händler den Hersteller unverzüglich über diese Schwachstelle. Wenn das Produkt mit digitalen Elementen ein erhebliches Cybersicherheits-risiko birgt, unterrichten die Einführer / Händler zudem unverzüglich die Marktüberwachungsbehörden der Mitgliedstaaten, in denen sie das Produkt mit digitalen Elementen auf dem Markt bereitgestellt haben, und machen dabei genaue Angaben insbesondere über die Nichtkonformität und ergriffene Korrekturmaßnahmen.

- Und auch im dritten Beispiel muss gefragt werden, welche Einführer und welche Händler Schwachstellen sowie erhebliche Cybersicherheitsrisiken feststellen können; ergänzend einen Regelprozess zur Meldung an die Marktüberwachungsbehörden aufbauen und

als Linienprozess betreiben als auch eigene Korrekturmaßnahmen bis hin zum Rückruf ergreifen können.

Artikel 10 Absatz 10 bietet einen Angriffspunkt für die Abmahnindustrie, wenn ein Hersteller nicht alle Anforderungen aus Anhang II erfüllt.

Neu für die Hersteller sind die in **Artikel 11** formulierten Meldepflichten. Diese sind beispielhaft der Finanzindustrie wohl bekannt, jedoch neu und damit eine mehrdimensionale Herausforderung für die Mehrzahl der Hersteller von Produkten mit digitalen Elementen. In Abbildung 8 sind die Meldepflichten ikonisch zusammengestellt.

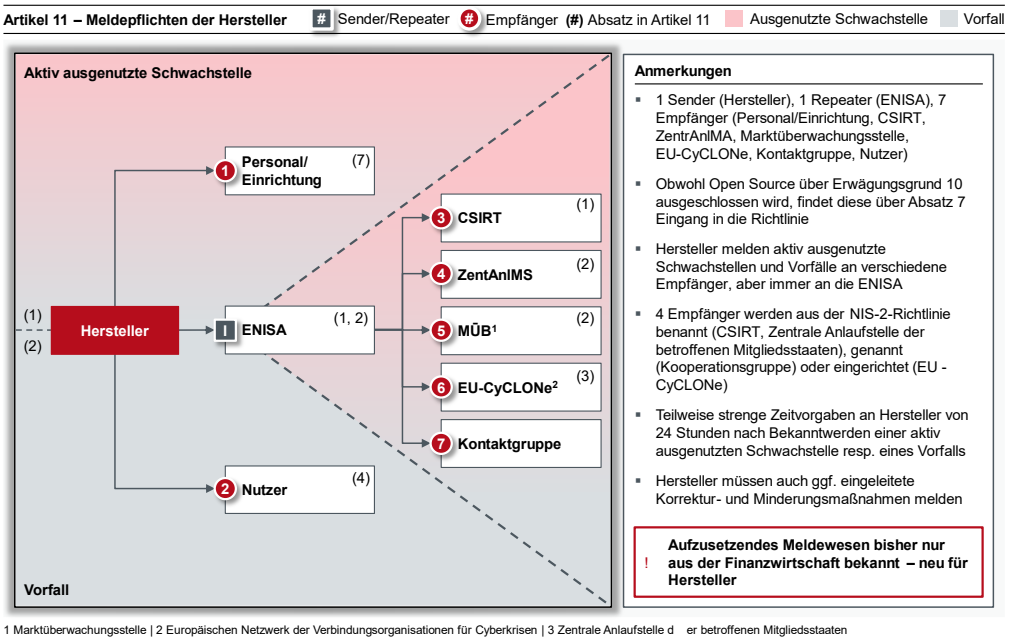


Abbildung 8: Meldepflichten der Hersteller aus Artikel 11

Unter anderem müssen Hersteller innerhalb von 24 Stunden bekannt gewordene aktiv ausgenutzte Schwachstellen (Absatz 1) resp. Vorfälle (Absatz 2) an die ENISA melden. Die ENISA meldet an die CSIRTs[2] der betroffenen Mitgliedstaaten weiter. Sind die Informationen aus (1) und (2) von Bedeutung für das Management massiver Cybersicherheitsvorfälle und -krisen auf operativer Ebene, müssen Hersteller dies aus Absatz 3 an EU-CyCLONe melden. In Absatz 4 schließlich spielen auch die End-Nutzer eine Rolle: Hersteller müssen diese über Maßnahmen informieren, die sie zur Abhilfe ergreifen können. Die ENISA muss alle zwei Jahre der Kooperationsgruppe einen technischen Bericht über Trends der Cybersicherheitsrisiken vorlegen (Absatz 6). Absatz 7 birgt eine interessante Wendung: Obwohl Open Source über Erwägungsgrund 10 ausgeschlossen wird, findet es hier Eingang in die Richtlinie, denn „sobald der Hersteller eine Schwachstelle in einer in das Produkt mit digitalen Elementen integrierten

[2] Computer Security Incident Response Team

Komponente, einschließlich einer Open-Source-Komponente, feststellt, meldet er die Schwachstelle der Person oder Einrichtung, die diese Komponente wartet."

Was bedeutet diese Anforderung genau? Eine „Open Source Komponente", die in das Produkt integriert ist, kann doch nur ein Software-Artefakt sein. Damit würde auch Open Source Software, ob vom Hersteller direkt oder als Zulieferung zu seinem Produkt, betroffen sein. Und um über eine Schwachstelle in einer Komponente Meldung erstatten zu können, muss der Hersteller die gesamte verwendete Open Source Software überprüfen.

In Kapitel II definiert **Artikel 17** „Identifizierung der Wirtschaftsakteure" Anfrage-Situationen. Hersteller, Einführer und Händler haben auf Anfrage der Marktüberwachungsbehörde Informationen zu den Bezugsquellen als auch zu den Empfängern der Produkte zur Verfügung zu stellen, und hierüber 10 Jahre lang auskunftsfähig zu bleiben. Sinn der Regelung ist die detailgenaue Darstellung einer Strukturanalyse aller Komponenten und Produkte vom Hersteller und seinen Bezugsquellen bis hin zu den Händlern und – nach Möglichkeit – all ihrer Empfänger über einen Zeitraum von 10 Jahren hinweg. Zwar klingt dieser Zeitraum für die üblichen Lebenszyklen von Angriffsmustern lang gewählt; bedenkt man jedoch die teils verbreitete Legacy in vielen Infrastrukturen, so sind die 10 Jahre gut gewählt, um ausnutzbare Schwachstellen und Vorfälle zu verwalten.

Kapitel III „Konformität des Produktes mit digitalen Elementen" besteht aus den Artikeln 18 bis 24 und sollte mit dem letzten Artikel beginnen, denn **Artikel 24** legt die Mechanik zur Feststellung der Konformität fest. Stellt der Hersteller fest, dass es sich bei seinem Produkt um ein Produkt mit digitalen Elementen gemäß Artikel 2 handelt, muss er eine Konformitätsbewertung durchführen. Hierzu stehen drei Verfahren zur Verfügung:

a) Internes Kontrollverfahren (gemäß Anhang VI Modul A) oder
b) EU-Baumusterprüfverfahren (gemäß Anhang VI Modul B) oder
c) Konformitätsbewertung (gemäß Anhang VI Modul H)

Handelt es sich beim Produkt um ein kritisches Produkt gemäß Artikel 6, dürfen nur zwei Verfahren b) oder c) verwendet werden. Dies gilt bei einem Produkt nach Anhang III Klasse I mit und bei einem Produkt nach Anhang III Klasse II ohne Konformitätsvermutung gemäß **Artikel 18**. Bei dieser Konformitätsvermutung wird eine Konformität mit den grundlegenden Anforderungen in Anhang I vermutet, wenn das Produkt und die vom Hersteller festgelegten Verfahren mit harmonisierten Normen der Europäischen Union oder Teilen davon übereinstimmen, soweit diese Anforderungen von den betreffenden Normen oder Teilen davon abgedeckt sind. Eine Konformität wird ebenfalls vermutet bei Übereinstimmung mit gemeinsamen Spezifikationen gemäß **Artikel 19** und bei einer EU-Konformitätserklärung oder einem Cybersicherheitszertifikat gemäß Cybersicherheitsrichtlinie.

Die vom Hersteller selbst ausgestellte EU-Konformitätserklärung (Muster in Anhang IV) besagt, dass die grundlegenden Anforderungen in Anhang I erfüllt sind. Für diesen Nachweis muss das Konformitätsbewertungsverfahren gemäß Artikel 24 durchlaufen werden. Alle drei Verfahren (Anhang VI Modul A, Modul B oder Modul H) der Konformitätsbewertung verlangen eine technische Dokumentation gemäß **Artikel 23**. Diese Dokumentation hat es in sich, denn sie verlangt „zumindest" die Angaben aus Anhang V. Unter anderem sind dies

- Absatz 2c): vollständige Informationen und Spezifikationen zur Produktion und zum Monitoring des Produkts und die Validierung dieser Prozesse
- Absatz 3: eine Bewertung der Cybersicherheitsrisiken, gegen die das Produkt gemäß Artikel 10 entworfen, entwickelt, hergestellt, geliefert und gewartet wird
- Absatz 5: Testberichte zur Überprüfung der Konformität des Produkts und der Verfahren zur Behandlung von Schwachstellen mit den geltenden grundlegenden Anforderungen in Anhang I
- Absatz 7: gegebenenfalls die Software-Stückliste gemäß der Definition in Artikel 3 Nummer 37 auf begründeten Antrag einer Marktüberwachungsbehörde, sofern dies erforderlich ist, damit diese Behörde die Einhaltung der grundlegenden Anforderungen gemäß Anhang I überprüfen kann

Die technische Dokumentation muss während der Produktlebensdauer, aber mindestens 5 Jahre aktualisiert werden. Auch hier die Frage welche Hersteller diesen bürokratischen Aufwand realistisch leisten können?

Kapitel IV „Notifizierung von Konformitätsbewertungsstellen“ mit den **Artikeln 25 bis 40** befasst sich mit den Anforderungen an die Notifizierungsstellen, sowohl den notifizierenden Behörden als auch den notifizierenden Stellen.

Kapitel V „Marktüberwachung und Durchsetzung“ (Artikel 41 bis 49) weist noch einige interessante Aspekte auf: So beschreibt **Artikel 43** nationale Verfahren für Produkte mit digitalen Elementen, die ein erhebliches Cybersicherheitsrisiko bergen, um diese Produkte letztendlich vom Markt zu nehmen. **Artikel 45** beschreibt das gleiche Verfahren auf EU-Ebene. D.h. dass sowohl ein Mitgliedstaat wie auch die EU bei Gefahr im Verzug Produkte vom Markt nehmen dürfen. **Artikel 44** stellt mit dem „Schutzklauselverfahren der Union“ ein Bindeglied zwischen beiden Verfahren dar, denn es bietet einem Mitgliedstaat und der Kommission die Möglichkeit, in einem anderen Mitgliedstaat zu Produkten bei Gefahr im Verzug einzuschreiten. Selbst wenn ein Produkt konform mit der CRA ist, kann es bei Auftreten eines erheblichen Cybersicherheitsrisikos gemäß **Artikel 46** aus dem Markt entfernt werden. Im letzten Artikel von Kapitel V werden so genannte „Koordinierte Kontrollen (Sweeps)“ eingeführt, wonach die Marktüberwachungsbehörden beschließen können, zur Prüfung der Einhaltung der CRA oder zur Feststellung von Verstößen gegen die CRA, gleichzeitige koordinierte Kontrollen („Sweeps“) durchzuführen. Hier bleibt die tatsächliche Anwendung der CRA in etwa drei Jahren abzuwarten. Eine Zusammenarbeit von mehreren Marktüberwachungsbehörden ist im Finanzsektor bekannt, hierbei arbeiten BaFin und Bundesbank bei Prüfungen der technisch-organisatorischen Ausstattung eines Aufsichtsobjektes erfolgreich zusammen, bei „bedeutenden“ Instituten wird diese Kopplung durch die EZB ergänzt. Inwieweit solche europäisch koordinierten Prüfungs- und Überwachungshandlungen bei Produkten mit digitalen Elementen zum Einsatz kommen, muss sich in Zukunft zeigen.

Bei den Sanktionen gemäß **Artikel 53** nimmt die CRA sowohl bei der Höhe der Bußgeder als auch der Art der Verstöße Anleihen bei der DSGVO. Während es bei der DSGVO zwei Bußgeldrahmen gibt, kennt die CRA sogar drei:

- Nichteinhaltung der grundlegenden Anforderungen in Anhang I oder Verstößen gegen die in den Artikeln 10 (Pflichten der Hersteller) und 11 (Meldepflichten der Hersteller)

festgelegten Pfichten: Geldbuße von bis zu 15 Mio Euro oder bis zu 2,5% des gesamten weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist

- Verstöße gegen andere Pflichten: Geldbuße von bis zu 10 Mio Euro oder bis zu 2% des gesamten weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist
- Falsche, unvollständige oder irreführende Angaben gegenüber notifizierten Stellen und Marktüberwachungsbehörden auf deren Auskunftsverlangen: Geldbuße von bis zu 5 Mio Euro oder bis zu 1% des gesamten weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist

Wenn es sich nicht um einen Fehler im Entwurf handelt, dann bietet der dritte Geldbußerahmen mit der Nennung der notifizierenden „Stellen“ (und nicht notifiziernede „Behörde“) eine Tür zur Denunziation für böswillige Stellen. Auch hier muss die Praxis abgewartet werden; denn ein Prüfungsunternehmen wird bei unsauberem Verhalten den Herstellern gegenüber zeitnah Reaktionen im Markt realisieren.

Nur Unternehmen können mit einer Geldbuße belegt werden. Allerdings erlässt gemäß Artikel 53 Absatz 8 jeder Mitgliedstaat Vorschriften darüber, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können. Der Erfahrung mit anderen Rechtsakten folgend wird das in Deutschland negativ entschieden. Im letzten Absatz 10 von Artikel 53 wird ausgeführt, dass je nach Umständen des Einzelfalls Geldbußen zusätzlich zu anderen Korrekturmaßnahmen oder einschränkenden Maßnahmen, die Marktüberwachungsbehörden für denselben Verstoß auferlegen, verhängt werden können.
Zu guter Letzt noch Inkrafttreten und Geltungsbeginn (**Artikel 57**): dieser startet 2 Jahre nach Inkrafttreten der CRA, nur die Meldepflichten der Hersteller (Artikel 11) beginnen bereits ein Jahr nach Inkrafttreten. Wohlwollend betrachtet kann dieses Vorziehen der Meldepflichten als Lernphase für die Hersteller zum Umgang mit der CRA ausgelegt werden.

Empfehlungen

Unsere in Abbildung 9 zusammengefassten und im Nachgang vertieften Empfehlungen gelten den vier in der Verordnung hauptsächlich adressierten Wirtschaftsakteuren, den Unternehmensverbänden, den nationalen wie europäischen Aufsichten, den nicht unmittelbar betroffenen Wirtschaftsakteuren wie der Finanzindustrie sowie der deutschen und europäischen Politik.

1) Hersteller, Einführer und Händler sollten unserer Auffassung nach über ihre Unternehmensverbände national als auch auf europäischer Ebene auf Verbesserungen der Verordnung hinarbeiten. Diese Verbesserungen betreffen die technisch-organisatorischen Anforderungen. Die technischen Anforderungen aus Anhang I werden tendenziell nur von größeren und großen Akteuren bewältigt werden können. Auch den verwaltungstechnischen Mehraufwand im Meldewesen sowie den Informationspflichten in Anhang II und Anhang V werden viele Hersteller nicht angemessen umsetzen können. Hinzu kommen diverse oben beschriebene Aufbewahrungs- und Informationspflichten auf Anfrage verschiedender Behörden.

2) Zudem sollten die Adressaten eine zumindest zeitlich beschränkte Größenbeschränkung für Hersteller, Einführer und Händler nach dem Vorbild des Lieferkettengesetzes in die Diskussion mit Regulatorik und Politik einbringen. Andernfalls wird mit der Anwendung der Verordnung ein Großteil der Wirtschaftsakteure non-konform zur Verordnung agieren – mit entsprechenden Sanktionsrisiken.

3) Des Weiteren müssen sich die Markt-Akteure zeitnah auf die Verordnung vorbereiten und mit der Umsetzung der Anforderungen beginnen. Der Weg kann hier nur skizziert werden: Gap-Analyse zur Verordnung, Maßnahmenplanung, Migrationsplan, Umsetzung, Überprüfung auf Konformität. Noch ist mit wohl mindestens 3 Jahren bis zur Anwendung der CRA genug Zeit für alle Beteiligten vorhanden.

4) Auch die nationalen und europäischen Aufsichten sollten unserer Auffassung nach die Verordnung wie oben beschrieben abmildern. Ziel sollte eine umsetzbare Sicherheitsstrategie sein, keinesfalls ein Regelwerk, das nur von großen Akteuren gelebt werden könnte. Denn entweder wird die Aufsicht zumindest die ersten Jahre bei mittleren und kleinen Akteuren zurückhaltend agieren – Hinweis auf Größenlimite wie im Lieferkettengesetz fehlen bisher – oder das Ausscheiden vieler und vornehmlich europäischer, da kleiner Anbieter aus dem Markt wird zu akzeptieren sein. Ein Umstand, den die europäischen Politik diskutieren sollte.

5) Auch die nicht unmittelbar betroffenen Wirtschaftsakteure wie zum Beispiel die Finanzindustrie sollten die Entwicklung dieser Verordnung verfolgen und ggf. frühzeitig in die Gesetzesentwicklung eingreifen. Denn aus der heutigen Prüfungspraxis von Kreditinstituten und Versicherungsunternehmen lässt sich eine mögliche „Weiterentwicklung“ der Aufsichtspraxis für Finanzunternehmen wie folgt ableiten:

Quelle: CORE | 1: als Vertreterin der nicht unmittelbar Betroffenen Wirtschaftsakteure

Abbildung 9: Empfehlungen an mittelbar und unmittelbar Betroffene der Verordnung zur Stärkung des Standortes Europa

In der CRA gibt es Artikel für die Pflichten der Akteure Hersteller (Artikel 10), Einführer (Artikel 13) und Händler (Artikel 14). Es gibt aber keinen Artikel „Pflichten der Nutzer“. Auch Finanzunternehmen sind am Ende nur Nutzer von Produkten mit digitalen Elementen, d.h. Hardware und Software. Daher folgende Ableitung: Heute muss eine Bank im Outsourcing so eng steuern und überwachen, als ob sie weiterhin in eigener Verantwortung Systeme betreiben würde. Das gilt auch dann, wenn die Outsourcingunternehmen selbst über alle wichtigen Sicherheitszertifizierungen und Betriebszertifizierungen verfügen. Die Finanzaufsicht besteht auf eigene Prüfungshandlungen der Aufsichtsobjekte. Analog müssen Hersteller von Produkten mit digitalen Elementen viele neuen Anforderungen aus der Verordnung erfüllen. Was passiert, wenn Finanzunternehmen diese Produkte einsetzen? Dürfen sie sich auf die CRA-Zulassung verlassen oder müssen sie eigene Prüfungshandlungen vornehmen? Überträgt man die heutige Situation in der Finanzaufsicht auf die Zukunft mit der CRA, müssen die Finanzunternehmen auch diese Produktgattung selbst überprüfen: ein kaum kalkulierbarer Mehraufwand. Es wäre die Fortschreibung der heutigen Aufsichtssituation zum Beispiel aus Sonderprüfungen der technisch-organisatorischen Ausstattung. Eine statthafte Frage der Aufsicht an Finanzunternehmen würde lauten: „Haben Sie selbst die Bewertung der Cybersicherheitsrisiken des Herstellers geprüft?“ Diese Pflicht zu eigenen Prüfungshandlungen trotz Konformität mit der CRA würde sich nicht nur auf Hersteller beschränken, sondern auch die Handlungen der Einführer und Händler umfassen. Dieser möglichen Aufweitung der Aufsichtspraxis sollten Finanzunternehmen präventiv vorbeugen, da andernfalls der Regulierungsaufwand unkalkulierbar steigt.

Die deutsche und europäische Politik sollte unter Berücksichtigung geopolitischer Veränderungen auf das industriepolitische Tableau zwischen den USA und China reagieren. Dies bedeutet, die Verordnung unter wirtschaftlichen und politischen Folgen für den europäischen Wirtschaftsraum revisionieren. Trägt diese Rigorosität in der Anwendung der Verordnung, d.h. ohne Größenschranken für regulierte Unternehmen und mit hohen Anforderungen von Anfang an für alle Unternehmen gleichgewichtig dazu bei, europäische Unternehmen am Markt zu stärken? Ein zweiter möglicher Effekt der Verordnung könnte die weitere Reduzierung der Anzahl von Herstellern, Einführern und Händlern sein, da in diesem „survival of the fittest“ nur größere, global agierende Marktteilnehmer entsprechen können. Will die Politik tatsächlich die in diesem Bereich eher auf mittlere und kleine Strukturen bauende europäische Wirtschaft weiter einschränken? Oder sollte die Verordnung nicht gezielt an europäische industriepolitische Realitäten angepasst werden? Dem Grundsatz folgend, dass gleiche Rechte und Pflichten für alle Unternehmen gelten, doch angepasst an europäische Anforderungen.

Die Kommission geht davon aus, „etwaige Befolgungskosten für die Unternehmen durch die Vorteile aufzuwiegen, die ein höheres Sicherheitsniveau der Produkte mit digitalen Elementen und letztlich ein höheres Vertrauen der Nutzer in diese Produkte mit sich bringen.“ Doch werden größere Marktteilnehmer den Anforderungen leichter entsprechen können. Leider sind die wenigsten größeren Marktteilnehmer in Europa ansässig.

Fazit

Die Inhalte der CRA wurden von Politik und Verbraucherschutz seit Jahrzehnten gefordert und immer wieder aufgeschoben. Was bisher auf Good Will Basis versucht und nicht erreicht wurde, findet sich nun im Entwurfstext wieder. Obwohl das Ziel der Verordnung nicht anzuzweifeln ist,

sollte der Wag dahin eingehend mit mittelbar und unmittelbar Betroffenen erörtert werden. Das Ziel der europäisch harmonisierten Produktsicherheit sollte nicht um den Preis der Schädigung der zukünftig wichtiger werdenden Industrien Software und Hardware erreicht werden.

Anforderungen wie die Bewertung der Cybersicherheitsrisiken, Meldung von aktiv ausgenutzten Schwachstellen an die ENISA, europäische Schwachstellendatenbank, Information der Nutzer über Vorfälle und ggf. über Korrekturmaßnahmen, Dokumentation der Produkte (auch Software-Stücklisten), gleichzeitige koordinierte Kontrollen (Sweeps) sind zu begrüßen, sollten jedoch kleinere Hersteller, Einführer und Händler nicht überfordern.

Die Hauptadressaten müssen bereits heute, ca. 3 Jahre vor Anwendung der CRA mit den Vorbereitungen zur Umsetzung ihrer jeweiligen Pflichten beginnen. Auch hier sollte die Politik prüfen, ob Pflichten für Einführer und Händler zu Überforderungen führen. Die an sich richtige Verordnung würde wirkungslos, wenn die Adressaten eine Umsetzung nicht sicherstellen können und aus dem Markt ausscheiden.

Auch Wirtschaftsakteure wie die Finanzindustrie müssen den Entwurf prüfen und sich bei Bedarf in den politischen Dialog einschalten. Die heutige Aufsichtspraxis mit geforderten internen Prüfungshandlungen im Outsourcing lässt vermuten, dass der Regulator aus einer Risikoabwägung die Prüfung der Anwendung der CRA einfordert.

Insofern sollten Unternehmen direkt und über ihre nationalen wie europäischen Verbände Lobbyarbeit leisten. Diskutierbare Optimierungen können Unternehmensgrößenlimite wie im Lieferkettengesetz, zeitliche Streckung der umzusetzenden Maßnahmen wie in der DORA mit den zeitlich verteilten Regulatory Technical Standards (RTS) und generell das vertiefte Nachdenken über aktualisierte Informations- und Berichtspflichten sein. Mit dem vorliegenden Entwurf ist nicht auszuschließen, dass die CRA als „Pendant“ des Lieferkettengesetzes wirkt und die kleinen und mittleren Unternehmen durch zu hohe Anforderungen aus dem Markt drängt – es verblieben nur mehr die großen Unternehmen als Regelungsobjekte für die CRA, so wie es derzeit nur große Marktteilnehmer für das Lieferkettengesetz sind.

Soweit muss es nicht kommen. Es ist genug Zeit vorhanden. Wenn ein Optimierungsprozess einsetzt, ist der Entwurf der CRA bereits jetzt ein großer Wurf.

Holger Friedrich ist Managing Partner der CORE SE. Er ist langjährig erfolgreicher Experte für die Transformation komplexer IT-Systeme. Seine langjährige Erfahrung für internationale Klienten in regulierten Industrien macht ihn zum gefragten Ansprechpartner für Investoren, Aufsichtsgremien und das Senior-Management.

Mail: holger.friedrich@core.se

Dr. Waldemar Grudzien ist Expert Partner der CORE SE. Er ist ausgewiesener Spezialist für Regulations- und Compliance-Aspekte im Einsatz unternehmeskritischer Infrastrukturen. Durch die Vielzahl von Publikationen, Mandaten sowie erfolgreichen Projekten ist er und seine Teams gefragter Ansprechpartner für Anwender hoch regulierter IT-Systeme.

Mail: waldemar.grudzien@core.se

Leon Kuhlmann ist Transformation Director bei CORE. Mit seinem „International Business“ Hintergrund und Erfahrung im agilen und klassischen Projektmanagement sowie Kenntnissen in IT-Sicherheit, Prozessmanagement und Compliance begleitet er Klienten bei der Umsetzung komplexer IT-Transformationen. Sein Fokus reicht von der Strategieentwicklung bis zum „Go-Live“.

Mail: leon.kuhlmann@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se