CYBERRESILIENZGESETZ

Vorschlag COM(2022) 454 vom 15. September 2022 für eine **Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen** und zur Änderung der Verordnung (EU) 2019/1020.

cep**Analyse** Nr. 1/2023

KURZFASSUNG [zur Langfassung]

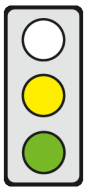
Hintergrund | Ziel | Betroffene

Hintergrund: Soft- und Hardwareprodukte sind in den vergangenen Jahren immer häufiger von Cyberattacken betroffen gewesen. Ein wesentlicher Grund hierfür ist ein geringes Maß an Cybersicherheit dieser Produkte. Allein 2021 entstanden weltweit Schäden in Höhe von 5,5 Billionen Euro. Die Kommission schlägt daher ein Cyberresilienzgesetz (Cyber Resilience Act, CRA) vor.

Ziel: Die Kommission will einheitliche Cybersicherheitsvorschriften für Hersteller, Importeure und Händler von Produkten mit digitalen Elementen (PmdE) etablieren. Hersteller von PmdE sollen die Cybersicherheit ihrer Produkte bereits in der Konzeptions- und Entwicklungsphase verbessern. Ferner soll die Transparenz über die Sicherheitseigenschaften von PmdE gestärkt werden.

Betroffene: Hersteller, Importeure und Händler von PmdE, Nutzer von PmdE, Konformitätsbewertungsstellen

Kurzbewertung



Pro

- Das Cyberresilienzgesetz leistet einen bedeutenden Beitrag zur Stärkung der Cybersicherheit in der EU. Mehrere Defizite auf den Märkten für Produkte mit digitalen Elementen werden zielgerichtet adressiert.
- Einheitliche Cybersicherheitsanforderungen beugen Fehlanreizen bei Herstellern, Einführern und Händlern von PmdE entgegen. Diese müssen nun einen größeren Teil der Kosten tragen, die mit unsicheren PmdE einhergehen. Eine Abwälzung auf Kunden und Dritte wird erschwert.
- Käufer von PmdE können aufgrund der Transparenzvorgaben die Sicherheitseigenschaften von PmdE besser einordnen und vergleichen.
- Die Festlegung eines Zeitraums für die Behebung von Schwachstellen stärkt das Vertrauen der Nutzer von PmdE in die Produktqualität.

Contra

- Die bereits von der Kommission vorgenommene Einstufung von Produkten in die Klassen 1 und 2 für kritische Produkte ist undurchsichtig und nicht schlüssig. PmdE in den beiden Klassen können nicht per se als kritisch angesehen werden.
- Die Einstufung von PmdE nach ihrer Kritikalität kann nicht als rein technische und von politischen Erwägungen befreite Entscheidung angesehen werden. Die Übertragung von Befugnissen an die Kommission zum Erlass delegierter Rechtsakte zur Einstufung ist daher zumindest zweifelhaft.
- Der vorgesehene Geltungsbeginn – 2 Jahre nach Inkrafttreten des CRA – ist zu ambitioniert.

Allgemeine Einschätzung [Langfassung C.1.1]

Kommissionsvorschlag: Es wird ein Rechtsrahmen für die Entwicklung und das Inverkehrbringen von cybersicheren Produkten mit digitalen Elementen (PmdE) in der EU geschaffen.

cep-Bewertung: Hersteller von PmdE bringen regelmäßig Produkte auf den Markt, die nicht cybersicher sind. Käufer von PmdE haben gleichzeitig Schwierigkeiten, sichere Produkte nachzufragen. Dies ist auf verschiedene Defizite der Märkte für PmdE zurückzuführen, etwa Fehlanreizen auf Seiten der Hersteller und mangelnde Informationen auf Seiten der Käufer. Der CRA leistet einen spürbaren und bedeutenden Beitrag zur Behebung dieser Marktdefizite.

Autoren: Dr. Anastasia Kotovskaia, LL.M. und Philipp Eckhardt | kotovskaia@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-0 | www.cep.eu

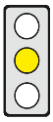
Einheitliche Cybersicherheitsanforderungen [Langfassung C.1.2]

Kommissionsvorschlag: Hersteller, Einführer und Händler von PmdE müssen grundlegende Cybersicherheitsanforderungen erfüllen. Sie müssen die Cybersicherheit bereits in der Konzeption, Entwicklung und Herstellung eines Produkts hinreichend berücksichtigen.

cep-Bewertung: Einheitliche Cybersicherheitsanforderungen beugen Fehlanreizen auf Seiten der Hersteller, Einführer und Händler von PmdE entgegen. Sie müssen künftig verstärkt in die Cybersicherheit ihrer Produkte investieren, was die Kosten, die Kunden und Dritte bisher häufig aufgrund unsicherer PmdE tragen müssen, reduziert. Zudem werden Wettbewerbsnachteile für jene Wirtschaftsakteure, die proaktiv sichere Produkte bereitstellen verringert und ein Trittbrettfahrerverhalten auf Seiten der Käufer von PmdE, wird erschwert.

Anwendungsbereich [Langfassung C.1.4]

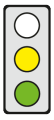
Kommissionsvorschlag: Der CRA gilt für Produkte mit digitalen Elementen (PmdE). Das sind insbesondere verbindungsfähige Software- bzw. Hardwareprodukte. PmdE werden in vier Gruppen unterteilt: (1) Nicht-kritische PmdE, u.a. Festplatten und PC-Spiele, (2) Kritische PmdE (Klasse I), u.a. Browser und Passwort-Manager, (3) Kritische PmdE (Klasse II), u.a. Betriebssysteme für Server, Router und Chipkarten, sowie (4) noch nicht näher spezifizierte hochkritische PmdE.



cep-Bewertung: Die Festlegung eines sehr breiten Geltungsbereichs ist sachgerecht. Denn Schwachstellen können in vielen, auch vermeintlich unkritischen PmdE auftreten. Jedoch ist die bereits vorgenommene Einstufung von Produkten in die Klassen 1 und 2 für kritische Produkte undurchsichtig. Zudem ist die Einstufung nicht schlüssig. Denn vielfach sind die PmdE in den beiden Klassen nicht per se und immer als kritisch anzusehen. Ihre Kritikalität hängt vielmehr davon ab, von wem, unter welchen Bedingungen und wo sie eingesetzt werden.

Schwachstellenmanagement [Langfassung C.1.6]

Kommissionsvorschlag: Hersteller von PmdE müssen für eine Behebung von Schwachstellen sorgen; dies gilt, je nachdem, welcher Zeitraum kürzer ist, für die voraussichtliche Lebensdauer des Produkts oder fünf Jahre ab dem Zeitpunkt des Inverkehrbringens des Produkts.



cep-Bewertung: Die Festlegung eines Zeitraums, in dem Hersteller für eine Behebung von Schwachstellen sorgen müssen, erhöht das Vertrauen der Nutzer von PmdE in die Produktqualität. Jedoch ist die Kohärenz mit anderen EU-Rechtsakten bei der Dauer der Pflicht zur Schwachstellenbehebung noch nicht gegeben, insbesondere gegenüber dem Vorschlag für eine Richtlinie zur Haftung für fehlerhafte Produkte und den neuen Ökodesignvorgaben für Smartphones, Tablets und Mobiltelefonen.

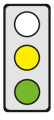
Transparenzvorgaben [Langfassung C.1.8]

Kommissionsvorschlag: Hersteller von PmdE müssen Produktnutzern Informationen bereitstellen, etwa darüber, unter welchen Umständen bei Nutzung des PmdE Cybersicherheitsrisiken eintreten können, wie lange Sicherheitsupdates bereitgestellt werden und an wen im Unternehmen Informationen über Schwachstellen gemeldet werden können.

cep-Bewertung: Die Transparenzvorgaben ermöglichen es Verbrauchern und Unternehmen, die Sicherheitseigenschaften von PmdE besser einordnen und vergleichen zu können. Dies erleichtert es ihnen, eine fundierte Entscheidung über den Erwerb eines PmdE fällen zu können. Sie tragen daher zum Abbau von durch Informationsasymmetrien bedingtem Marktversagen bei.

Meldepflichten [Langfassung C.1.9]

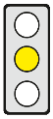
Kommissionsvorschlag: Hersteller von PmdE müssen jeden Cybersicherheitsvorfall sowie jede aktiv ausgenutzte Schwachstelle binnen 24 Stunden der Agentur der Europäischen Union für Cybersicherheit (ENISA) melden.



cep-Bewertung: Hersteller von PmdE wollen Cybersicherheitsvorfälle oder Schwachstellen oft nicht freiwillig melden, da Reputationsrisiken drohen. Solche Meldungen haben jedoch häufig einen hohen volkswirtschaftlichen Nutzen, da frühzeitiger Schritte zur Risikominderung getroffen werden können. Meldepflichten sind daher sachgerecht. Jedoch ist die Pflicht zur Notifizierung jedweder ausnutzbaren Schwachstelle bzw. jedwedes Sicherheitsvorfalls überschießend. Analog zur NIS 2-Richtlinie sollte auf deren Signifikanz abgestellt werden.

Einstufung von PmdE nach ihrer Kritikalität [Langfassung C.2.3]

Kommissionsvorschlag: Die Kommission kann mittels delegierter Rechtsakte die Listen der kritischen PmdE um neue Kategorien kritischer Produkte ergänzen bzw. Kategorien aus diesen Listen entfernen. Zudem kann sie so eine Liste mit Kategorien von hochkritischen PmdE erstellen. Die Entscheidung trifft sie auf Basis mehrerer Kriterien, etwa, ob die PmdE von Betreibern kritischer Infrastrukturen genutzt wird.



cep-Bewertung: Bei der Bestimmung der Listen der (hoch)kritischen PmdE mittels delegierter Rechtsakte durch die Kommission mangelt es an einer transparenten Begründung ihrer Entscheidungen. Ferner ist nicht festgelegt, zu welchem Grad die Kriterien erfüllt sein müssen. Bezüglich der Befugnisübertragung an die Kommission besteht die Gefahr, dass die Einstufung von PmdE durch politische Erwägungen beeinflusst werden könnte.