Ausschuss für Digitales
20. Wahlperiode

Deutscher Bundestag

Anlagenkonvolut zum Protokoll der 37. Sitzung am 10. Mai 2023

Tagesordnungspunkt 5 Anlage

Bundesministerium
des Innern
und für Heimat

Bundesministerium des Innern und für Heimat, 11014 Berlin

-per elektronischer Post-

Vorsitzende des
Ausschusses für Digitales
Frau Tabea Rößner, MdB

RD Michael Popp
Referatsleiter PK I 2

Alt-Moabit 140
10557 Berlin

Postanschrift
11014 Berlin

Tel +49 30 18 681-[redacted]

Fax +49 30 18 681-[redacted]

[redacted]@bmi.bund.de
www.bmi.bund.de

Bericht zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 – Cyber Resilience Act

Az: KabParl-12003/4#2
Berlin, 5. Juni 2023

Sehr geehrte Frau Vorsitzende,

anliegend übersende ich Ihnen den oben erwähnten Bericht und bitte, diesen an die Mitglieder Ihres Ausschusses weiterzuleiten.

Mit freundlichen Grüßen
im Auftrag

[redacted]

Michael Popp

Anlage
-1- Bericht

Bundesministerium
des Innern
und für Heimat

Bericht der Bundesregierung zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 – Cyber Resilience Act

Bundesministerium
des Innern
und für Heimat

Der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (Cyber Resilience Act – CRA) wurde am 15. September 2022 von der EU-Kommission (KOM) veröffentlicht. Am 21. September 2022 wurde der CRA der Horizontalen Arbeitsgruppe zu Fragen der Cybersicherheit und Cyber-Außenpolitik (HWPCI) durch die KOM präsentiert. Der vorliegende Verordnungsvorschlag soll sicherstellen, dass digitale Produkte – wie drahtlose und drahtgebundene Hardware sowie Software – für die Nutzer in der gesamten EU sicherer in Bezug auf Cybersicherheit werden. Zum einen müssen Hersteller mehr Verantwortung übernehmen, da sie verpflichtet werden, Unterstützung und Softwareaktualisierungen bereitzustellen, um festgestellte Schwachstellen zu beheben. Zum anderen sollen die Verbraucher über die Cybersicherheit der Produkte, die sie kaufen und verwenden, ausreichend informiert werden. Der Geltungsbereich des CRA soll sich im Rahmen des New Legislative Framework (NLF) erstrecken und stellt Bezüge zur Verordnung (EU) 2019/881 (Cybersecurity Act - CSA) her. Über grundlegende Anforderungen werden wesentliche Cybersicherheitsanforderungen an die Produkte im europäischen Binnenmarkt eingeführt. Produkte sollen nach Inkrafttreten des CRA nur noch auf dem Markt bereitgestellt werden dürfen, wenn sie auch die Anforderungen des CRA erfüllen.
Es wird eine Marktaufsicht für die Kontrolle der Einhaltung der vom CRA aufgestellten Cybersicherheitsanforderungen bei den betroffenen Produkten eingeführt. Derzeitig wird der CRA in der Ratsarbeitsgruppe HWPCI unter SWE Vorsitz diskutiert und verhandelt. Es zeichnet sich ab, dass unter SWE Ratspräsidentschaft keine allgemeine Ausrichtung des Rates erzielt werden wird. Daher wird die ESP Ratspräsidentschaft den Verhandlungsstand aufgreifen und die Diskussionen ab dem 1. Juli 2023 fortsetzen.

Nach Ansicht der Bundesregierung ist der Verordnungsvorschlag zum Ziel der Einführung von verbindlichen Cybersicherheitsanforderungen für den gesamten EU-Binnenmarkt zu begrüßen. Die BReg bringt sich aktiv in die Verhandlungen zum Cyber Resilience Act ein.
Im Rahmen der Diskussionen unter den Mitgliedstaaten werden unter anderem die Aspekte hinsichtlich der Anforderungen für den Lebenszeitraum besprochen. Der Entwurf der KOM sieht eine Begrenzung auf fünf Jahre vor. Dies greift in manchen Anwendungsfällen jedoch zu kurz. Die BReg befürwortet daher eine Streichung der Begrenzung der Geltungsdauer auf fünf Jahre. Der Unterstützungszeitraum für die Produkte sollte sich daher an einem angemessenen und zu erwartenden Produktlebenszyklus orientieren, welcher vom Hersteller klar kommuniziert wird und sich an objektiven Erfahrungswerten und durchschnittlicher Einsatzdauer bemisst.

Diskussionen finden auch hinsichtlich des Anwendungsbereiches statt. Hierbei sind unter anderem Konkretisierungen hinsichtlich des Einbezugs von Open-Source-Lösungen und Definitionen für Ausnahmen im Sinne der nationalen Sicherheit wesentliche Diskussionspunkte. Dazu zählen auch eine sichere Beschreibung und Abgrenzung, wie mit sogenannten Dual-Use-Produkten umzugehen ist. Nach Ansicht der Bundesregierung sollte hier ein angemessenes Verhältnis zwischen den Interessen der nationalen Sicherheit und dem Anwendungsbereich hergestellt werden, sodass genügende Rechtssicherheit geschaffen werden kann. Hingegen sollte eine allzu breit gefasste Ausnahme letztendlich nicht dazu führen, dass ein Großteil von Produkten außerhalb des Anwendungsbereichs fällt.