

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Jeanne Dillschneider, Dr. Konstantin von Notz, Rebecca Lenhard, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 21/6672 –**

IT-Sicherheit für vom Cyber Resilience Act ausgenommene sicherheits- und verteidigungsrelevante Produkte

Vorbemerkung der Fragesteller

IT-Sicherheitslücken kennen keine nationalen Grenzen; ein ungepatchtes System in Frankfurt gefährdet ebenso Infrastruktur in Singapur oder São Paulo und umgekehrt. Aus diesen Interdependenzen ergibt sich die Verantwortung, ein möglichst einheitlich hohes Niveau an Vorgaben für die IT-Sicherheit herzustellen. Die Verantwortung für den Schutz integrier digitaler Infrastrukturen lässt sich direkt aus unserer Verfassung ableiten. Doch dieser Verantwortung wird die Bundesregierung bis heute nicht gerecht.

Die Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act (CRA)) ist am 10. Dezember 2024 in Kraft getreten und ab dem 11. Dezember 2027 vollständig anwendbar. Sie verpflichtet Hersteller, Importeure und den Vertrieb eines breiten Produktspektrums (von Smartphones und vernetztem Spielzeug über Firewalls bis hin zu mobilen Apps und Buchhaltungssoftware) erstmals verbindlich, Cybersicherheit über den gesamten Produktlebenszyklus (Cybersecurity by Design) zu gewährleisten. Damit schließt sie eine seit Jahren beklagte Regelungslücke im europäischen Binnenmarkt (siehe CRA-Verordnung (EU) 2019/1020 (COM (2022) 454 final).

Produkte, die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder geändert wurden, sowie Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind, fallen jedoch nach Artikel 2 Absatz 7 CRA nicht in den Anwendungsbereich der Verordnung.

Der europäische Gesetzgeber hat diese Ausnahmen mit der Erwartung verknüpft, dass die Mitgliedstaaten für die betroffenen Produkte eigenständig ein gleichwertiges oder höheres Schutzniveau sicherstellen (siehe CRA-Verordnung (2024/2847), Erwägungsgrund 26). Weitreichende Ausnahmetatbestände bergen ein erhebliches systemisches Risiko, Produkte bewusst als sicherheitsrelevant zu klassifizieren, um der regulatorischen Pflicht zur Transparenz, zu Schwachstellenmeldungen und zu Sicherheitsupdates zu entgehen. Dies würde das erklärte Ziel des CRA, den europäischen Binnenmarkt sicherer zu gestalten,

ten, nicht nur untergraben, sondern auch die IT-Sicherheit insgesamt schwächen.

Gerade im sicherheits- und verteidigungsrelevanten Bereich sind Angriffe jedoch besonders folgenreich. Umso zentraler ist die unverzügliche Umsetzung der Verpflichtungen zur Schaffung mindestens äquivalenter Voraussetzungen für IT-Produkte, die unter die Ausnahmeregelung des Artikel 2 Absatz 7 CRA fallen.

Bislang ist nicht erkennbar, wie die Bundesregierung dieser Verpflichtung nachkommen will. Die Anforderung, für die ausgenommenen Produkte CRA-äquivalente Cybersicherheitsstandards zu gewährleisten, erfordert eine eigenständige nationale Regelung, die weder der CRA selbst noch das nationale Durchführungsgesetz leisten kann. Weder die Klassifizierung betroffener Produktgruppen noch die vorgesehenen Konformitätsbewertungsverfahren wurden bislang öffentlich kommuniziert. Auch zu der Frage, wie Hersteller betroffener Produkte zur Einhaltung CRA-äquivalenter Anforderungen verpflichtet werden sollen, hat sich die Bundesregierung bisher nicht positioniert.

1. Hat die Bundesregierung eine Klassifizierung für Produkte nach Artikel 2 Absatz 7 CRA, die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder geändert wurden, und für Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind, vorgenommen, differenziert nach wichtigen Produkten Klasse I, wichtigen Produkten Klasse II sowie kritischen Produkten mit digitalen Elementen, wenn ja, welche Produktgruppen fallen in jede der drei Kategorien, welche Konformitätsbewertungsverfahren sind für jede der drei Kategorien vorgesehen, entsprechend Artikel 32 CRA, und wenn nein, wie stellt die Bundesregierung das gleiche oder ein höheres Schutzniveau wie das im CRA spezifizierte sicher, vor dem Hintergrund, dass die Maßnahmen des CRA zwischen diesen drei Produktkategorien differenzieren?
2. Welche konkreten Maßnahmen hat die Bundesregierung bereits unternommen bzw. sind in Planung, um dieser Aufforderung nachzukommen?
3. Inwiefern verpflichtet die Bundesregierung Hersteller betreffender Produkte, die Integrität von freien und quelloffenen Softwarekomponenten, die sie in ihre Produkte integrieren, sicherzustellen und insbesondere festgestellte Schwachstellen darin zu behandeln und beheben, entsprechend Artikel 13 (5) und (6) CRA?
4. Inwiefern verpflichtet die Bundesregierung Hersteller betreffender Produkte, Sicherheitsupdates während der erwarteten Produktlebensdauer, mindestens jedoch für fünf Jahre bereitzustellen, entsprechend Artikel 13 (8) CRA?
5. Wie wird sichergestellt, dass die betreffenden Produkte die Cybersicherheitsanforderungen nach Anhang I Teil I CRA erfüllen oder übertreffen, entsprechend Artikel 13 (1) CRA?
6. Inwiefern verpflichtet die Bundesregierung Hersteller betreffender Produkte
 - a) zur Gewährleistung eines angesichts der Risiken angemessenen Cybersicherheitsniveaus entsprechend Annex I Teil I (1) CRA,
 - b) zur Bereitstellung von Produkten ohne bekannte ausnutzbare Schwachstellen entsprechend Annex I Teil I (2) a) CRA,

- c) zur Konzeption, Entwicklung und Herstellung ihrer Produkte in einer Weise, die sicherstellt, dass sie – auch bei externen Schnittstellen – möglichst geringe Angriffsflächen bieten und die Auswirkungen eines Sicherheitsvorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden, entsprechend Annex I Teil I (2) j) und k) CRA?
7. Wie wird sichergestellt, dass die betreffenden Produkte die Anforderungen an die Behandlung von Schwachstellen nach Anhang I Teil II CRA erfüllen oder übertreffen, entsprechend Artikel 13 (8) CRA?
8. Inwiefern verpflichtet die Bundesregierung Hersteller betreffender Produkte
- a) zur Erstellung einer Software-Stückliste, etwa in Form einer Software Bill of Materials (SBOM), entsprechend Annex I Teil II (1) CRA,
 - b) zur Behandlung und Behebung von Schwachstellen entsprechend Annex I Teil II (2) CRA,
 - c) zur Bereitstellung von Informationen über bekannte Schwachstellen und ihre Ausnutzbarkeit und Behebung von Schwachstellen entsprechend Annex I Teil II (4) CRA,
 - d) zur Aufstellung und Umsetzung einer Strategie für die koordinierte Offenlegung von Schwachstellen, einschließlich einer Adresse für die Meldung von Schwachstellen entsprechend Annex I Teil II (5 und 6) CRA?

Die Fragen 1 bis 8 werden gemeinsam beantwortet.

Eine Klassifizierung im Sinne der Fragestellung wurde nicht vorgenommen.

Gemäß der Verschlusssachenanweisung Bund dürfen für informationssicherheitsrelevante Anwendungsbereiche ausschließlich durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) für den jeweiligen Anwendungsfall zugelassene Produkte verwendet werden.

Aufgrund individueller Anforderungen werden im jeweiligen Beschaffungsvorgang gegebenenfalls Leistungen des Herstellers für den Einzelfall vertragsrechtlich festgelegt, die u. a. Vorgaben

- zur Sicherstellung der Integrität von freien und quelloffenen Software-Komponenten,
 - zu Sicherheitsupdates,
 - zur Meldung und Behandlung von Schwachstellen,
 - zu einer Software Bill of Materials (SBOM) oder
 - weitere Sicherheitsanforderungen
- enthalten können.

9. Wie viele anonyme und nichtanonyme Schwachstellenmeldungen hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) seit 2020 erhalten (bitte nach Jahren und anonymer und nichtanonymer Meldung aufschlüsseln)?

Seit 2020 wurde valide Schwachstellenmeldungen im Rahmen des CVD-Prozesses im nachfolgenden Umfang bearbeitet:

2020: 15 Meldungen,

2021: 87 Meldungen,

2022: 134 Meldungen,

2023: 459 Meldungen,

2024: 136 Meldungen,

2025: 111 Meldungen.

Eine Unterscheidung von anonymen und nicht-anonymen Schwachstellenmeldungen ist nicht möglich, da die Verifizierung der gegebenenfalls angegebenen Namen nicht möglich ist. Es ist dem BSI bekannt, dass Meldungen auch unter Verwendung von Synonymen abgegeben werden.

Vorabfassung - wird durch die lektorierte Version ersetzt.