Deutscher Bundestag **Drucksache 21/8884**

21. Wahlperiode 03.11.2026

Vorabfassung - wird durch die lektorierte Version ersetzt.

Kleine Anfrage

der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, Sebastian Maack, Tobias Ebenberger, Lars Haise, Edgar Naujok, Steffen Janich, Dr. Michael Kaufmann, Micha Fehre, Beatrix von Storch, Ronald Gläser, Peter Bohnhof, Thomas Ladzinski und der Fraktion der AfD

Umsetzung des Cyber Resilience Act – Meldepflichten, Prüfkompetenzen und Unterstützung für Unternehmen

Mit dem Cyber Resilience Act (CRA) hat die Europäische Union erstmals EU-weit verbindliche Mindestanforderungen für die Cybersicherheit von Produkten mit digitalen Elementen eingeführt. Die vollständige Anwendung der Verordnung ist erst für den 11. Dezember 2027 vorgesehen, einzelne Pflichten gelten jedoch bereits deutlich früher. Seit dem 11. September 2026 sind Hersteller verpflichtet, aktiv ausgenutzte Schwachstellen sowie schwerwiegende Sicherheitsvorfälle innerhalb von 24 Stunden gegenüber der zuständigen nationalen Behörde zu melden, diese Meldung innerhalb von 72 Stunden zu ergänzen und spätestens 14 Tage nach einer Abhilfemaßnahme (bei Schwachstellen) beziehungsweise einen Monat nach der Meldung (bei schwerwiegenden Vorfällen) einen Abschlussbericht vorzulegen (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act.html). In Deutschland wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale Meldestelle benannt.

Nach einer repräsentativen, im Frühjahr 2026 durchgeführten Befragung des Digitalverbands Bitkom unter 1 003 Unternehmen ab 10 Beschäftigten, veröffentlicht am 10. September 2026, also einen Tag vor Beginn der Meldepflicht, war zwar 67 Prozent der befragten Unternehmen der Cyber Resilience Act dem Namen nach bekannt, jedoch konnten nur 29 Prozent einschätzen, was das Gesetz konkret für das eigene Unternehmen bedeutet (www.bitkom.org/Presse/Presseinformation/Cyber-Resilience-Act-3-von-10-Unternehmen-vorbereitet). 38 Prozent hatten zwar davon gehört, konnten die Bedeutung für den eigenen Betrieb aber nicht einschätzen, 28 Prozent kannten den Cyber Resilience Act zum Zeitpunkt der Befragung überhaupt nicht (www.bitkom.org/Presse/Presseinformation/Cyber-Resilience-Act-3-von-10-Unternehmen-vorbereitet). Erschwerend kommt hinzu, dass die von der EU-Agentur für Cybersicherheit (ENISA) bereitgestellte zentrale Meldeplattform, über die auch das BSI die Meldungen deutscher Hersteller entgegennimmt, erst zum Stichtag des 11. September 2026 selbst in Betrieb genommen wurde. Selbst gut vorbereitete Unternehmen konnten sich damit im Vorfeld weder auf der Plattform registrieren noch die vorgeschriebenen Meldewege erproben.

Auch auf Seiten der zuständigen Behörde zeigen sich erhebliche Anlaufschwierigkeiten. Bereits seit dem 11. Juni 2026 gilt nach Artikel 71 des Cyber Resilience Act der rechtliche Rahmen für die Notifizierung von Konformitätsbewertungsstellen gemäß Kapitel IV der Verordnung (https://cyber-resilience-act.de/c

ra/kapitel-4/). Nach Artikel 35 Absatz 2 des Cyber Resilience Act müssen die Mitgliedstaaten bis zum 11. Dezember 2026 dafür sorgen, dass eine ausreichende Zahl notifizierter Stellen zur Verfügung steht, die Konformitätsbewertungen durchführen können, um Engpässe und Hindernisse mit Blick auf den Marktzugang zu verhindern (https://cyber-resilience-act.de/cra/kapitel-4/). Die auf deutscher Seite dafür notwendige Prüfkompetenz wurde jedoch erst mehr als drei Monate nach Beginn des Notifizierungsrahmens geschaffen. Am 24. September 2026, und damit weniger als elf Wochen vor Ablauf der Frist aus Artikel 35 Absatz 2, haben das BSI und die Deutsche Akkreditierungsstelle (DAkkS) eine aktualisierte Verwaltungsvereinbarung unterzeichnet, mit der weitere Geltungsbereiche für die Benennung des BSI als Befugnis erteilende Behörde geschaffen sowie die Bereitstellung von Fachbegutachtern des BSI für Akkreditierungsverfahren der DAkkS im Bereich der Informationssicherheit geregelt werden (www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/2026/CRA-Konformitaet_BSI_DAkkS_260925.html). Aus der Praxis, unter anderem von Branchenverbänden des Mittelstands, wird zudem Kritik laut, dass insbesondere kleine und mittlere Unternehmen (KMU) bei der Umsetzung der umfangreichen neuen Anforderungen nur unzureichend unterstützt würden, während größere Unternehmen über eigene Rechts- und Compliance-Abteilungen verfügen (www.itsa365.de/de-de/news-knowledge/2026/09/cyber-resilience-act-enisa-playbook-fuer-hersteller).

Nach Auffassung der Fragesteller zeigt sich damit ein wiederkehrendes Muster europäischer und nationaler Digitalgesetzgebung, nach dem bereits nach der Datenschutz-Grundverordnung und der NIS-2-Richtlinie erneut weitreichende Meldepflichten mit engen Fristen in Kraft gesetzt werden, ohne dass die für den Vollzug zuständigen Behörden und insbesondere der deutsche Mittelstand ausreichend Zeit und Unterstützung erhalten, sich auf die neuen Anforderungen vorzubereiten. Dies gefährdet nicht nur die digitale Souveränität, sondern auch die Wettbewerbsfähigkeit des deutschen Mittelstands.

Vor diesem Hintergrund besteht ein erhebliches parlamentarisches Informationsbedürfnis darüber, über welche personellen und technischen Kapazitäten das BSI für die Umsetzung der neuen Meldepflichten tatsächlich verfügt und welche konkrete Unterstützung die Bundesregierung kleinen und mittleren Unternehmen bei der Erfüllung der Anforderungen des Cyber Resilience Act zukommen lässt.

Wir fragen die Bundesregierung:

1. Wie viele Meldungen nach Artikel 14 des Cyber Resilience Act sind beim BSI seit dem 11. September 2026 bis zum aktuellen Zeitpunkt eingegangen (aufgeschlüsselt nach Frühwarnmeldungen, Aktualisierungen und Abschlussberichten sowie, soweit bekannt, nach der Größe der meldenden Hersteller in Kleinst-, kleine, mittlere und große Unternehmen)?
2. Wie viele dieser Meldungen betrafen aktiv ausgenutzte Schwachstellen und wie viele schwerwiegende Sicherheitsvorfälle im Sinne des Cyber Resilience Act?
3. In wie vielen Fällen hat das BSI seit dem 11. September 2026 Erkenntnisse aus Meldungen nach Artikel 14 des Cyber Resilience Act an Strafverfolgungsbehörden weitergegeben oder auf deren Grundlage Warnungen an betroffene Nutzer oder Unternehmen herausgegeben, und wie viele Ermittlungsverfahren wurden nach Kenntnis der Bundesregierung daraufhin eingeleitet?

Vorabfassung - wird durch die lektorierte Version ersetzt.

4. Über wie viele Vollzeitäquivalente verfügt das BSI aktuell für die Bearbeitung und Auswertung der nach dem Cyber Resilience Act eingehenden Meldungen?
5. Wie viele dieser Stellen waren zum 11. September 2026 tatsächlich besetzt und wie viele befanden sich zu diesem Zeitpunkt noch im Besetzungsverfahren?
6. Innerhalb welcher durchschnittlichen Zeitspanne wurden die seit dem 11. September 2026 eingegangenen Meldungen durch das BSI bearbeitet?
7. Welche technischen Systeme und Schnittstellen nutzt das BSI zur Entgegennahme und Weiterverarbeitung der über die europäische Meldeplattform der ENISA eingehenden Meldungen?
8. Zu welchem Zeitpunkt waren diese technischen Systeme und Schnittstellen des BSI vollständig einsatzbereit?
9. Welche Geltungsbereiche und Produktkategorien umfasst die am 24. September 2026 zwischen dem BSI und der Deutschen Akkreditierungsstelle (DAkkS) unterzeichnete Verwaltungsvereinbarung konkret?
10. Wie viele Fachbegutachter stellt das BSI der DAkkS auf Grundlage dieser Vereinbarung für Akkreditierungsverfahren im Bereich der Informationssicherheit zur Verfügung?
11. Wie viele Konformitätsbewertungsstellen sind seit Unterzeichnung der Vereinbarung durch die DAkkS im Bereich des Cyber Resilience Act akkreditiert worden?
12. Wie viele Anträge auf Akkreditierung als Konformitätsbewertungsstelle im Bereich des Cyber Resilience Act liegen der DAkkS aktuell zur Bearbeitung vor und wie viele davon werden nach Einschätzung der Bundesregierung bis zum 11. Dezember 2026 abgeschlossen sein können?
13. Mit welcher durchschnittlichen Bearbeitungsdauer rechnet die Bundesregierung für ein vollständiges Akkreditierungsverfahren einer Konformitätsbewertungsstelle nach dem Cyber Resilience Act?
14. Für welche Produktkategorien nach dem Cyber Resilience Act wird ab dem 11. Dezember 2027 eine Konformitätsbewertung durch eine unabhängige Stelle erforderlich sein?
15. Wie viele Konformitätsbewertungsstellen müssen nach Einschätzung der Bundesregierung bis zum 11. Dezember 2027 akkreditiert sein, damit Hersteller entsprechender Produkte fristgerecht eine Bewertung erhalten können?
16. Welche konkreten Informations- und Unterstützungsangebote stellt die Bundesregierung kleinen und mittleren Unternehmen zur Erfüllung der Meldepflichten nach dem Cyber Resilience Act zur Verfügung?
17. Welche finanziellen Mittel hat die Bundesregierung im Jahr 2026 für die Unterstützung kleiner und mittlerer Unternehmen bei der Umsetzung des Cyber Resilience Act bereitgestellt?
18. Wie viele Anfragen kleiner und mittlerer Unternehmen zur Umsetzung des Cyber Resilience Act sind beim BSI seit dem 11. September 2026 eingegangen und innerhalb welcher durchschnittlichen Zeitspanne wurden diese Anfragen durch das BSI beantwortet?
19. Welche Erkenntnisse liegen der Bundesregierung zu den Ergebnissen der Bitkom-Umfrage vom 10. September 2026 vor, wonach nur 29 Prozent der befragten Unternehmen einschätzen konnten, was der Cyber Resilience Act konkret für das eigene Unternehmen bedeutet?

Vorabfassung - wird durch die lektorierte Version ersetzt.

20. Wann wurde die Bundesregierung durch die ENISA über den Zeitpunkt der Inbetriebnahme der zentralen Meldeplattform informiert?

21. Wie viele nach dem Cyber Resilience Act notifizierte Konformitätsbewertungsstellen sind der Bundesregierung zum aktuellen Zeitpunkt EU-weit und in Deutschland bekannt?

22. Inwieweit wird die Bundesregierung die Frist aus Artikel 35 Absatz 2 des Cyber Resilience Act, wonach bis zum 11. Dezember 2026 eine ausreichende Zahl notifizierter Konformitätsbewertungsstellen zur Verfügung stehen muss, nach heutigem Kenntnisstand einhalten können und welche Maßnahmen ergreift sie andernfalls?

Berlin, den 2. November 2026

Dr. Alice Weidel, Tino Chrupalla und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333