

Berlin, 01.04.2026

Stellungnahme

zum

Referentenentwurf des Durchführungsgesetzes zur Cyberresilienz-Verordnung

Kontakt:

RA Karsten U. Bartels, LL.M.

HK2 RAe

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Stellvertretender Vorstandsvorsitzender

Leiter TeleTrust-AG "IT-Sicherheitsrecht"

bartels@hk2.eu

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Der Bundesverband IT-Sicherheit e.V. (TeleTrust) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breitgefächerte Mitgliedschaft und die Partnerorganisationen verkörpert TeleTrust den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrust bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrust ist Träger der "TeleTrust European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrust Information Security Professional" (T.I.S.P.) und "TeleTrust Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany" und "IT Security made in EU". TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Chausseestraße 17

10115 Berlin

Tel.: +49 30 4005 4310

<https://www.teletrust.de>

1. Einleitung

Der Cyber Resilience Act (CRA) etabliert erstmals einen unionsweit einheitlichen Rechtsrahmen für die Cybersicherheit von Produkten mit digitalen Elementen. Der CRA ist als EU-Verordnung unmittelbar in den Mitgliedstaaten anwendbar, ohne dass es eines nationalen Umsetzungsgesetzes bedarf. Der CRA verpflichtet die Mitgliedstaaten jedoch, flankierende Durchsetzungsmaßnahmen zu erlassen, insbesondere um die notwendige nationale Vollzugsarchitektur zu schaffen.

Die Mitgliedstaaten sind insbesondere verpflichtet, eine Marktüberwachungsbehörde und eine notifizierende Behörde zu benennen, Unterstützungsmaßnahmen für KMU zu ergreifen sowie den Sanktions- und Bußgeldrahmen festzulegen. Der Referentenentwurf enthält die rechtlich erforderlichen Regelungen hierzu, bleibt aber in zentralen Punkten zu inkonkret und recht praxisfern.

Besonders die unzureichende Ausstattung des BSI, die Ausgestaltung der Regelungen zur notifizierenden Behörde sowie die Unbestimmtheit der Unterstützungsleistungen des BSI sind Kritikpunkte, die einen erheblichen Nachbesserungsbedarf aufzeigen.

Die ersten Regelungen des CRA werden ab dem 11.06.2026 wirksam. Um ein Vertragsverletzungsverfahren zu vermeiden, einen sicheren Marktzugang für Unternehmen in Deutschland zu garantieren und Rechtssicherheit zu gewährleisten, muss das Durchführungsgesetz ebenfalls zum 11.06.2026 in Kraft treten. Der Referentenentwurf ist nun ein erster Schritt, um nationale Vorschriften nicht - wie bei der NIS-2- und CER-Richtlinie - erneut zu spät zu erlassen.

2. Hauptteil

a) Aufgabenbündelung beim BSI

Die Bündelung zentraler CRA-Aufgaben beim BSI (CSIRT, Marktüberwachung, Beschwerde- und Notifizierungsstelle) ist im Ansatz sinnvoll. Sie nutzt vorhandene Cybersicherheitskompetenz und verhindert eine zersplitterte Vollzugspraxis. Ihr Mehrwert besteht jedoch nur, wenn das BSI personell, technisch und organisatorisch in der Lage ist, diese Aufgaben tatsächlich im erforderlichen Umfang wahrzunehmen.

§ 65 BSIG-E: Marktüberwachung

Die Übertragung der Marktüberwachung auf das BSI ist grundsätzlich nachvollziehbar. Zwar fehlt bislang originäre Marktüberwachungserfahrung, jedoch bestehen einschlägige Vorerfahrungen im Bereich der IT-Sicherheitskennzeichen.

Der Entwurf beziffert den Vollzugaufwand zwar konkret, bleibt jedoch bei dessen Absicherung unzureichend. Angesichts der komplexen Aufgaben nach Art. 52-60 CRA ist es nicht ausreichend, den Mehrbedarf an Personal und Sachmitteln lediglich künftigen Haushaltsverfahren zu überlassen. Ohne verbindliche und langfristige Finanzierung droht die effektive Wahrnehmung der Marktüberwachung zu scheitern.

§ 66 BSIG-E: Notifizierung und Akkreditierung

Die Bestimmung des BSI als notifizierende Behörde ist im Grundsatz sachgerecht. Problematisch ist jedoch § 66 Abs. 3 BSIG-E, der eine Notifizierung von Konformitätsbewertungsstellen ohne Akkreditierung im „öffentlichen Interesse“ zulässt. In der vorliegenden Fassung ist diese Ausnahme zu weit. Wird bereits der bloße Mangel an notifizierten Stellen als öffentliches Interesse angesehen, droht die Regelung zu einem Instrument bloßer Kapazitäts- und Marktzugangssicherung zu werden. Dann rückt nicht mehr die belastbare Prüfung der fachlichen Eignung der Stellen in den Vordergrund, sondern die schnelle Beseitigung von Engpässen.

Damit wird die Qualität der Konformitätsbewertung insgesamt gefährdet. Werden unzureichend geprüfte Konformitätsbewertungsstellen notifiziert, steigt das Risiko, dass auch die vorgelagerte Prüfung von Produkten vor dem Marktzugang nicht das erforderliche Sicherheitsniveau erreicht. Die Ausnahme von der akkreditierungsbaasierten Notifizierung ist daher strikt zu begrenzen. Erforderlich sind enge tatbestandliche Voraussetzungen, klare Bewertungsmaßstäbe und eine belastbare personelle wie organisatorische Ausstattung des BSI.

Vorrangig muss jedoch sichergestellt werden, dass eine solche Ausweichregelung gar nicht erst benötigt wird. Dafür ist die DAkkS rechtzeitig so auszustatten, dass bis zum maßgeblichen Zeitpunkt des Art. 35 Abs. 2 CRA am 11. Dezember 2026 eine ausreichende Zahl von Konformitätsbewertungsstellen akkreditiert werden kann.

Die Auffangregelung darf kein regulatorisches Ventil für vorhersehbare Kapazitätsdefizite werden. Wer Engpässe bei der Akkreditierung durch erleichterte Notifizierung kompensiert, schwächt am Ende die Qualitätssicherung des CRA selbst.

b) § 67 Nr. 1 BSIG-E - Unterstützung der Wirtschaftsakteure

§ 67 BSIG-E bleibt massiv hinter dem tatsächlichen Unterstützungsbedarf der Unternehmen zurück. Zwar übernimmt der Entwurf formal die in Art. 33 CRA vorgesehenen Unterstützungsmaßnahmen, ihre konkrete Ausgestaltung bleibt jedoch weitgehend offen. Weder ist hinreichend klar, in welcher Form, mit welcher inhaltlichen Tiefe noch mit welchem praktischen Nutzen die vorgesehenen Schulungs- und Sensibilisierungsmaßnahmen erbracht werden sollen. Der Eindruck liegt nahe, dass hier vor allem unionsrechtliche Mindestvorgaben formal abgearbeitet werden, ohne ein belastbares und praxistaugliches Unterstützungskonzept zu schaffen.

Das wiegt umso schwerer, als der CRA für Hersteller und andere Wirtschaftsakteure erhebliche organisatorische, personelle und technische Umstellungen auslösen wird. Vor diesem Hintergrund ist der vorgesehene finanzielle Rahmen von 1,281 Mio. Euro ersichtlich zu knapp bemessen, insbesondere mit Blick auf den Unterstützungsbedarf kleiner und mittlerer Unternehmen. Ein Vergleich mit den Zahlen, die in der Begründung des Regierungsentwurfs zum NIS-2-Umsetzungsgesetz stehen, verdeutlicht die signifikant zu gering bemessene Finanzierung der Unterstützungsmaßnahmen: Während hierfür lediglich 1,281 Mio. Euro jährlich vorgesehen sind, werden für regelmäßige Schulungen in der Bundesverwaltung im NIS-2-Kontext rund 5,044 Mio. Euro jährlich veranschlagt. Für Schulungen in den betroffenen Unternehmen wird ein Erfüllungsaufwand der Wirtschaft von rund 165,24 Mio. Euro jährlich veranschlagt. Wenngleich die Zahlen nicht direkt auf den CRA-Kontext übertragbar sind, so ist dennoch festzustellen, dass mit dem geplanten Finanzierungsrahmen nur sehr begrenzte Schulungs- und Sensibilisierungsmaßnahmen möglich sind.

Darüber hinaus werden zwei in Art. 33 Abs. 1 CRA genannte Unterstützungstätigkeiten - die Einrichtung eines speziellen Kommunikationskanals für Kleinst- und Kleinunternehmen sowie die Unterstützung bei Prüf- und Konformitätsbewertungstätigkeiten - nicht explizit in § 67 BSIG-E aufgeführt. Damit ist unklar, ob und wie weit diese Tätigkeiten vom BSI übernommen werden. TeleTrusT fordert, diese Tätigkeiten in § 67 BSIG-E ebenfalls aufzunehmen und ausreichend Ressourcen hierfür zur Verfügung zu stellen.

Alternativ schlägt TeleTrusT vor, dass die Unterstützungsmaßnahmen nicht durch das BSI selbst vorgenommen werden, sondern durch externe, unabhängige Stellen. Das BSI ist als Marktüberwachungsbehörde die Stelle, die Sanktionen bei Verstößen gegen den CRA verhängt. Die Bündelung von Unterstützungsfunktion und Marktüberwachung beim BSI begründet die Sorge, dass Rollenklarheit, Akzeptanz und Wirksamkeit beider Aufgabenbereiche leiden könnten.

§ 67 BSIG-E bedarf daher einer deutlichen Schärfung: Erforderlich sind ein substantiell erweiterter finanzieller Rahmen sowie inhaltlich konkrete, niedrigschwellige und praxisnahe Unterstützungsangebote. Andernfalls ist die Vorschrift nicht tauglich, den betroffenen Unternehmen nennenswerten Mehrwert zu bieten.

c) § 67 Nr. 2 BSIG-E - Reallabor für Cyberresilienz

TeleTrusT begrüßt grundsätzlich die Einrichtung eines Reallabors für Cyberresilienz. Gerade für betroffene Wirtschaftsakteure, insbesondere kleine und mittlere Unternehmen, kann eine kontrollierte Prüfumgebung einen wertvollen Beitrag dazu leisten, regulatorische Anforderungen frühzeitig zu erfassen und praktische Umsetzungsfragen vor dem Inverkehrbringen eines Produkts zu klären.

In seiner derzeitigen Ausgestaltung besteht allerdings die Gefahr, dass das Reallabor zwar als innovationsfreundliches Unterstützungsinstrument angekündigt wird, sein tatsächlicher Mehrwert für die betroffenen Unternehmen jedoch marginal bleibt.

Der Entwurf lässt im Normtext wie auch der Begründung die konkrete Ausgestaltung dieses Instruments weitgehend offen. Insbesondere bleibt unklar, unter welchen Voraussetzungen die Nutzung „im öffentlichen Interesse“ liegen soll und nach welchen Kriterien Unternehmen Zugang zum Reallabor erhalten. Nach Art. 33 Abs. 2 CRA hat der Zugang zu den Reallaboren offen, fair und transparent zu erfolgen. In der Fassung des Referentenentwurfs finden sich keine Anhaltspunkte, dass dies auch so erfolgen wird. Hier bedarf es einer für KMU transparenten Nachschärfung.

Auch der konkrete praktische Mehrwert der Reallabors ist mehr als unklar. Der Leistungsumfang des Reallabors wird nicht beschrieben. Es ist nicht ersichtlich, ob dort lediglich allgemeine Testmöglichkeiten eröffnet werden oder ob Unternehmen tatsächlich verwertbare Unterstützung bei der Einhaltung der CRA-Anforderungen erhalten sollen.

In der Fassung des Referentenentwurfs droht das Reallabor mehr Symbolcharakter als wirksame Unterstützung zu sein.

d) § 69 BSIG-E - Sanktions- und Vollzugsrahmen

Ein einheitlicher und wirksamer Vollzug der Cyberresilienz-Verordnung ist aus Sicht von TeleTrusT grundsätzlich zu begrüßen. Die praktische Wirksamkeit der Verordnung wird maßgeblich davon abhängen, dass die Einhaltung ihrer Anforderungen konsequent überwacht und auf festgestellte Verstöße angemessen reagiert werden kann. Nur so lässt sich sicherstellen, dass Produkte mit digitalen Elementen tatsächlich den vorgesehenen Cybersicherheitsstandards genügen und das Vertrauen in den europäischen Binnenmarkt für sichere digitale Produkte gestärkt wird.

Hierbei gilt es jedoch zu beachten, dass aus Unternehmenssicht ein Bedarf an berechenbarem, verhältnismäßigem und fachlich konsistentem Vollzug besteht. Gerade in der Anfangsphase eines neuen und technisch anspruchsvollen Regulierungsregimes ist zu berücksichtigen, dass auf Seiten der betroffenen Unternehmen erhebliche Auslegungs- und Umsetzungsunsicherheiten bestehen werden.

Aus Sicht von TeleTrusT sollte der Fokus daher zunächst auf klarer Kommunikation, vorhersehbarer Aufsicht und nachvollziehbaren Maßstäben liegen. Sanktionen dürfen nicht an die Stelle einer praxistauglichen Orientierung treten.

Fazit:

Der Referentenentwurf greift die durch den CRA erforderlichen nationalen Regelungen zwar im Grundsatz auf, bleibt in seiner derzeitigen Fassung jedoch in zentralen Punkten hinter den praktischen und rechtlichen Anforderungen zurück. Die vorgesehene Aufgabenbündelung beim BSI ist nur dann tragfähig, wenn dessen personelle, technische und organisatorische Ausstattung verlässlich und dauerhaft abgesichert wird. Daran fehlt es bislang.

Besonders kritisch sind die zu weit gefasste Ausnahmeregelung für die Notifizierung von Konformitätsbewertungsstellen ohne Akkreditierung, die unzureichend konkretisierten Unterstützungsleistungen für Wirtschaftsakteure sowie die unklare Ausgestaltung des Reallabors für Cyberresilienz. In allen drei Bereichen besteht die Gefahr, dass der Entwurf formale Strukturen schafft, ohne deren praktische Wirksamkeit belastbar sicherzustellen.

TeleTrusT hält daher eine deutliche Nachschärfung des Entwurfs für erforderlich. Notwendig sind insbesondere eine verlässliche Finanzierung und Ausstattung des BSI und der DAkkS, enge und klare Voraussetzungen für Ausnahmen von der akkreditierungsbasierten Notifizierung, ein substantiell ausgebautes und praxisnahes Unterstützungskonzept für Unternehmen sowie transparente und nachvollziehbare Regelungen zum Reallabor.