OSBA

Cyber Resilience Act und Open Source

[09.04.2026] Open Source ist Grundlage der meisten Softwareprodukte und daher zentral für die IT-Sicherheit. Dies muss auch in der Umsetzung des Cyber Resilience Act berücksichtigt werden, fordert die OSBA. Open Source braucht eine passende Regulierung mit Unterstützung der Wirtschaft und klaren Verfahren.

Der Cyber Resilience Act (CRA) ist die erste europäische Verordnung, die ein Mindestniveau an Cyber-Sicherheit für vernetzte Produkte auf dem EU-Markt festlegt. Seit Dezember 2024 gilt: Alle Produkte, die in der EU verkauft werden und digitale Elemente enthalten, müssen die grundlegenden Anforderungen des Cyber Resilience Act erfüllen. Das betrifft sowohl günstige Verbraucherprodukte als auch Unternehmenssoftware und komplexe industrielle Systeme.

Die Verordnung gilt in allen Mitgliedstaaten der Europäischen Union und wird schrittweise umgesetzt. Ab Dezember 2027 müssen alle Anforderungen des CRA bei neuen Produkten eingehalten werden. In Deutschland läuft derzeit die organisatorische Vorbereitung, also der Aufbau von Aufsichtsstrukturen und die Vorbereitung der Wirtschaft auf die Anforderungen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) übernimmt die Rolle der marktüberwachenden Behörde für Deutschland und trägt außerdem Verantwortung für die EU-weite einheitliche Umsetzung des CRA. Zudem liegt der Gesetzentwurf zur Durchführung der Cyberresilienz-Verordnung derzeit als Referentenentwurf vor und ist offen zur Kommentierung.

96 Prozent der Softwareprodukte mit Open-Source-Komponenten

Nun hat die Open Source Business Alliance (OSBA) eine Stellungnahme zum deutschen Durchführungsgesetz des Cyber Resilience Act vorgelegt und darin die Rolle des Open-Source-Ansatzes genauer skizziert. Rund 96 Prozent aller Softwareprodukte enthalten nach Angaben der OSBA Open-Source-Komponenten. Open Source ist damit ein unverzichtbarer Treiber der IT-Industrie und der gesamten Wirtschaft. Die Sicherheit von Open-Source-Lösungen für die Funktionsfähigkeit von Unternehmen und der Verwaltung ist also zentral.

Vor diesem Hintergrund fordert die OSBA, dass bei der Unterstützung der betroffenen Wirtschaftsakteure durch das BSI Hersteller von Open-Source-Produkten und Open Source Software Stewards gesondert berücksichtigt werden, da sie besondere Anforderungen zu erfüllen haben. Ziel des CRA-Durchführungsgesetzes muss es sein, die europäischen Cybersicherheitsvorgaben so umzusetzen, dass sie ein hohes Sicherheitsniveau gewährleisten und gleichzeitig Innovation sowie wirtschaftliche Leistungsfähigkeit stärken.

Die Open-Source-Linie des CRA konsequent umsetzen

Der OSBA-Vorstandsvorsitzende Peter Ganten ordnet den aktuellen Referentenentwurf zur CRA-Durchführung hinsichtlich der Berücksichtigung von Open Source Software ein: „Open Source bietet durch Transparenz und unabhängige Überprüfbarkeit beste Voraussetzungen für ein hohes Sicherheitsniveau.

Die EU erkennt im CRA Open Source daher als sicherheitsrelevanten Bestandteil digitaler Infrastruktur an und berücksichtigt die Besonderheiten offener Entwicklungsmodelle. Diese Differenzierung muss nun auch konsequent in der nationalen Umsetzung fortgeführt werden. Denn das Open-Source-Ökosystem unterscheidet sich strukturell von der Entwicklung proprietärer Software: Es ist geprägt von einem Zusammenspiel aus kommerziellen Anbietern, öffentlichen Institutionen und ehrenamtlichen Entwicklerinnen und Entwicklern. Das CRA-Durchführungsgesetz muss diese Besonderheiten berücksichtigen, um wirksam und zugleich praktikabel zu sein."

Die Verbandsmitglieder der OSBA befassen sich bereits seit 2024 in einer eigenen Arbeitsgruppe intensiv mit dem CRA, den Anforderungen für unterschiedliche Software-Anbieter und Akteure, mit der Standardisierung in europäischen Standardisierungsgremien sowie mit der entsprechenden Technischen Richtlinie TR-03183 des BSI zur Umsetzung des CRA.

(sib)

• Gesetzentwurf zur Durchführung der Verordnung (EU) 2024/2847 (Cyberresilienz-Verordnung)
• Stellungnahme der Open Source Business Alliance zum Referentenentwurf für ein Durchführungsgesetz zur Cyberresilienz-Verordnung

Stichwörter: Digitale Souveränität, Cyber Resilience Act, IT-Sicherheit, Open Source, OSBA