OSBA

Cyber Resilience Act bremst Open Source

[17.08.2023] Das Europäische Datengesetz soll für höhere Sicherheitsstandards in der IT sorgen. Für Open-Source-Projekte entsteht damit große Rechtsunsicherheit, weil auch nicht-kommerzielle Mit-Akteure in Haftung genommen werden. Die Open Source Business Alliance nimmt Stellung.

Der Cyber Resilience Act (CRA) der europäischen Union will Hersteller, Vertreiber und Importeure von Produkten mit digitalen Komponenten zu höheren Sicherheitsstandards für ihre Produkte oder Dienstleistungen verpflichten. Nun beleuchtet die Open Source Business Alliance (OSB Alliance/OSBA) die Regulierungsinitiative mit Blick auf Open-Source-Software. Der Verband befürwortet ausdrücklich die Ziele des Cyber Resilience Act, die Qualität und Sicherheitsstandards von IT-Produkten zu erhöhen – dies entspreche auch dem Interesse der Mitgliedsunternehmen, die sichere Software vertreiben wollen und kommerzielle Software-Anbieter in der Verantwortung sehen. Allerdings würden unscharfe Formulierungen in den aktuellen CRA-Entwürfen eine Gefahr für das europäische Open-Source-Ökosystem und für die Innovations- und Wertschöpfungsfähigkeit des europäischen IT-Sektors darstellen. Die Bundesregierung müsse sich daher bei den anstehenden Trilogverhandlungen dafür einsetzen, dass das Open-Source-Ökosystem ausreichend geschützt werde.

Rechtsunsicherheit und Überregulierung

Der CRA scheint in erster Linie mit Blick auf die Entwicklungs- und Vertriebsmodelle proprietärer Software geschrieben zu sein, konstatiert die OSBA. Bei Open Source Software unterscheiden sich diese Modelle beträchtlich durch den offenen und kooperativen Ansatz und durch die mit den Lizenzen gewährten Freiheiten. Zwar strebe der CRA eine Ausnahme für Open Source Software an, die nicht für kommerzielle Aktivitäten eingesetzt werde – doch genau diese Abgrenzung sei schwierig. Das Open-Source-Ökosystem sei durch eine Verflechtung von ehrenamtlichen und kommerziellen Akteuren und Organisationen gekennzeichnet. So berge der CRA eine erhebliche Rechtsunsicherheit. Während kommerzielle Open-Source-Software-Anbieter aus Sicht der OSB Alliance ganz klar in den Anwendungsbereich des CRA fallen sollen, muss die Ausnahme für nicht-kommerzielle Open-Source-Hersteller noch verbessert werden.

Forderung an die Bundesregierung

Beim derzeitigen Stand des CRA bestehe die Gefahr, dass zu viele ehrenamtliche Open-Source-Initiativen, Projekte aus Forschung und Lehre oder Einzelpersonen mit in die Haftung genommen werden, die eigentlich nicht zur beabsichtigten Zielgruppe des CRA gehören. Aus Vorsicht würden sich möglicherweise Unternehmen und Initiativen vom europäischen Markt zurückziehen. Da zahllose digitale Produkte und Lösungen auf Open-Source-Komponenten aufbauen, sei von einem negativen Dominoeffekt für die gesamte Software-Branche auszugehen, befürchtet die OSBA.
Voraussichtlich ab September 2023 sollen die abschließenden Trilogverhandlungen zum CRA beginnen. Die Bundesregierung müsse sich dabei dafür einsetzen, dass im CRA das Open-Source-Ökosystem und damit wichtige Teile der IT-Wirtschaft und die digitale Souveränität Deutschlands geschützt werden. Hierfür sei ein Austausch mit Vertretern der Open-Source-Industrie unerlässlich, so die OSBA, die nach eigenem Bekunden jederzeit für einen Austausch sowie Beratungen zur Verfügung stehe.

(sib)

Komplette Stellungnahme der OSBA zum CRA

Stichwörter: Politik, Cyber-Sicherheit, IT-Sicherheit, OSBA