EU-Gesetzentwurf gefährdet Open Source

Mit dem Cyber Resilience Act will die EU-Kommission Hard- und Software sicherer machen und Haftungsfragen klären. Der Entwurf trifft aber auch Open-Source-Projekte und könnte gemeinnützige Organisationen haftbar machen. Die großen Software-Stiftungen schlagen jetzt Alarm und sehen die Zukunft der Softwareentwicklung in Gefahr.

Ein Aufschrei ging Mitte April durch die Open-Source-Community. Die Python Software Foundation, die Eclipse Foundation, die Linux Foundation und weitere erklärten gemeinsam: Einige Passagen im Entwurf der EU-Kommission für einen „Cyber Resilience Act“ (CRA) sind so unklar formuliert, dass nicht kommerzielle Open-Source-Organisationen künftig für Fehler in kommerzieller Software haftbar werden könnten, die ihre Komponenten nutzen.

Den Entwurf für den CRA hat die EU-Kommission bereits im Herbst 2022 veröffentlicht. Darin will sie alle, die Hard- und Softwareprodukte in Verkehr bringen, verpflichten, sich über den gesamten Lebenszyklus eines Produkts um die IT-Sicherheit zu kümmern, also Updates zu liefern und ein Schwachstellenmanagement einzuführen. Ein guter Ansatz und der richtige Weg, stellten Verbraucherschützer und auch die oben genannten Open-Source-Organisationen einhellig fest.

Für problematisch halten die Stiftungen aber die Definition von Inverkehrbringen im Entwurfstext. Die Formulierungen kann man so interpretieren, dass das Inverkehrbringen auch dann als kommerziell einzustufen ist, wenn kein Geld fließt. Dadurch könnten auch gemeinnützige Organisationen mit Haftungsrisiken konfrontiert werden, obwohl Dritte ihren frei verfügbaren Code in kommerzielle Produkte eingebaut haben. Die potenziellen Folgen wären drastisch: Die Python Software Foundation schloss nicht aus, Python und die Paketquelle PiPy dann in Europa nicht mehr anbieten zu können.

Um die Konsequenzen des EU-Entwurfs und politische Gegenmaßnahmen zu diskutieren, rief die Linux Foundation Europe im Rahmen der Cloudkonferenz KubeCon in Amsterdam eilig eine Podiumsdiskussion ins Leben. Dort war man sich einig, dass die Idee des Cyber Resilience Act gut sei, der Entwurf in der vorliegenden Form aber niemandem nütze.

Gabriele Columbro, General Manager der Linux Foundation Europe, gab zu, man habe noch nicht den richtigen Hebel gefunden, der Verwaltung in Brüssel das Konzept Open Source und die Bedeutung für die Wirtschaft zu vermitteln. Dort gebe es bis heute das Bild, es handle sich um Hobbyprojekte von Einzelpersonen. Dabei stecke Open Source in 70 Prozent aller digitalen Produkte und sei ein Wirtschaftsfaktor.

Frustriert zeigte sich auch Sachiko Muto, die CEO des Think-Tanks OpenForum Europe: Einerseits habe die EU-Kommission Open Source zur zentralen Säule für europäische Souveränität ernannt, andererseits unterliefen ihr beim Versuch zu regulieren solche Fehler, und Open-Source-Organisationen würden gar nicht gehört. Greg Kroah-Hartman, Fellow bei der Linux Foundation und rechte Hand von Linus Torvalds, sieht das gleiche Problem: Die Verantwortlichen wüssten nicht, mit wem sie sich zum Thema Open Source austauschen sollen. Er betonte, dass man Ausnahmen von der Haftung sauber definieren müsse. Sonst könnten Hersteller die Ausnahmen missbrauchen, um sich vor Verantwortung zu drücken. *(jam@ct.de)*

Um die Interessen von Open Source in Europa besser vertreten zu können, hat die in den USA ansässige Linux Foundation eine europäische Tochter gegründet.