Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Geschäftsstelle | c/o Freie Universität Berlin | Fabeckstraße 32 | 14195 Berlin

ZKI-Geschäftsstelle
c/o Freie Universität Berlin
Fabeckstraße 32
14195 Berlin

Tel.: 0049 30-2062262 0
Fax: 0049 30-2062262 98
geschaeftsstelle@zki.de

Ihr Ansprechpartner:
Torsten Prill
torsten.prill@zki.de

Autoren:
Karola Möhring, Johannes Nehlsen, Gernot Kirchner

14. März 2024

Position
des Vereins der „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI)“
zu den Auswirkungen des Vorschlags der EU-Kommission zum Cyber Resilience Act auf die Open-Source-Gemeinschaft

Abstract

Der wesentliche Unterschied von Open-Source-Software zu proprietärer Software besteht in der Offenlegung des Quellcodes (Open Source). Damit ist es möglich, die Rechts- und insbesondere Datenschutzkonformität der Software nachweisbar zu prüfen und zugleich eventuelle Schwachstellen bereits im Voraus zu erkennen. Eine Korrektur gefundener Schwachstellen kann durch eine Vielzahl von fachkundigen Personen erfolgen und nicht nur durch den ursprünglichen Hersteller.

Die Grundsätze der Verhältnismäßigkeit und der Praktikabilität müssen in den Anforderungen des Cyber Resilience Act (CRA) durch einfache, rechtssichere Regelungen, die die einzigartigen Eigenschaften von Open-Source-Software abbilden, gewahrt werden. Im CRA müssen das Bestreben und das Ziel der Open-Source-Gemeinschaft anerkannt werden, sichere Lösungen anzubieten, um die Cyberresilienz Europas deutlich zu erhöhen.

ZKI e.V. als Vereinigung von IT-Zentren

Der Verein „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (ZKI)“ als Vereinigung der IT-Zentren der Hochschulen, Universitäten und Forschungseinrichtungen in der Bundesrepublik Deutschland begrüßt, dass der Cyber Resilience Act einen Mehrwert für die Cybersicherheit schaffen soll, indem er Standards für vernetzte Produkte festschreibt, um die Widerstandsfähigkeit von Systemen gegen Cyberangriffe zu stärken.

Für die Mitglieder des ZKI ist neben kommerziellen Produkten Open-Source-Software ein wichtiger Bestandteil ihrer Digitalstrategie, insbesondere hinsichtlich Rechtskonformität, Flexibilität und Digitaler Souveränität. Sie sind daher unmittelbar von den Implikationen des CRA bezüglich der Entwicklung und Verwendung von Open-Source-Produkten betroffen.

Bankverbindung: DKB AG Berlin
Bankleitzahl: 120 300 00
Kontonummer: 2068120

IBAN: DE73 1203 0000 0002 0681 20
SWIFT BIC: BYLADEM1001

eingetragen im Vereinsregister
Berlin-Charlottenburg
Nr. 14209 Nz.

Vorstand:
Torsten Prill (Vorsitzender, Finanzvorstand)
Dr. Inga Scheler (stellv. Vorsitzende)
Prof. Dr. Gudrun Oevel (stellv. Vorsitzende)
Dr. Rainer Bockholt
Daniel Bündgens
Dr. Karl Molter

Produkte mit digitalen Elementen

Die EU-Kommission hat ihren Vorschlag zum Cyber Resilience Act im September 2022 veröffentlicht.[1] Der Ausschuss der Ständigen Vertreter der Regierungen der Mitgliedstaaten stimmte am 20. Dezember 2023 der geänderten Entwurfsfassung zum Cyber Resilience Act zu, welcher mit Abschluss der Trilog-Verhandlungen am 30. November 2023[2] zwischen dem Europäischen Parlament, der EU-Kommission und dem Rat der Europäischen Union ausgehandelt worden ist.[3] Gemäß diesem Vorschlag muss jeder Hersteller, bevor er Produkte mit digitalen Elementen[4] in Verkehr bringt, sicherstellen, dass die Produkte ohne bekannte Schwachstellen ausgeliefert werden. Eine technische Dokumentation und die Bewertung von Cybersecurity-Risiken müssen dabei ebenfalls vorhanden sein. Der Hersteller hat aber auch nach der Inverkehrbringung Melde- und gegebenenfalls Korrekturmaßnahmen-Pflichten zu erfüllen.

Bedeutung des Cyber Resilience Act für Hochschulen, Universitäten und Forschungseinrichtungen

An deutschen Hochschulen, Universitäten und Forschungseinrichtungen werden die Aktivitäten in der Digitalisierung auf Basis von Open-Source-Software stetig ausgebaut mit dem strategischen Ziel, die Digitale Souveränität zu stärken. Im Rahmen des Hochschul- und Universitätsbetriebes werden Softwarelösungen entwickelt. Diese organisieren die digitale Lehre, ermöglichen es, digitale Lehr- und Lernräume zu erstellen sowie Prüfungen abzuwickeln, und sind auf spezifische Bedürfnisse der Hochschulen und Universitäten zugeschnitten. Dabei werden unter anderem Open-Source-Plattformen und damit verbundene Communities geschaffen. Entwickler und Programmierer sind Teil einer wachsenden Open-Source-Gemeinschaft. Hochschulen, Universitäten und Forschungseinrichtungen können daher sowohl als Hersteller als auch als Nutzer digitaler Produkte von den Regelungen des CRA unmittelbar betroffen sein.

Vom Entwurf zum Cyber Resilience Act vom 30. November 2023 wird Open-Source-Software („free and open-source software“) nur erfasst, wenn sie auf dem Markt verfügbar gemacht und damit zum Vertrieb oder zur Nutzung im Rahmen einer kommerziellen Tätigkeit bereitgestellt, das heißt mit Gewinnerzielungsabsicht vertrieben (monetarisiert) wird (Erwägungsgrund 10c). Freie Open-Source-Software meint gemäß der nunmehr eingefügten Legaldefinition in Art. 3 Abs. 40a CRA-E Software, deren Quellcode offen zugänglich ist und die unter einer freien und quelloffenen Lizenz zur Verfügung gestellt wird, welche alle Rechte einräumt, um die Software frei zugänglich, nutzbar, veränderbar und weiterverteilbar zu machen. Vormals bestehende Unklarheiten, wie weit die Ausnahme für Open-Source-Software explizit reicht, wurden unter anderem im Erwägungsgrund 10c adressiert, so dass nunmehr klargestellt ist, dass Open-Source-Software, welche zur Integration durch andere Hersteller in ihre eigenen Produkte mit digitalen Elementen, nur dann unter den CRA fällt, wenn der ursprüngliche Hersteller der Open-Source-Software diese selbst monetarisiert und damit im Rahmen einer kommerziellen Tätigkeit bereitgestellt hat. Gleiches soll in der Regel auch für Open-Source-Software gelten, welche in ihrer Entwicklung von Unternehmen oder Softwareherstellern finanziell unterstützt worden sind, so dass die strengen Regelungen des CRA insofern keine Anwendung finden, sondern streng zwischen der Entwicklungs- und der Vertriebsebene unterschieden werden soll.

[1] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.
[2] https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/.
[3] https://data.consilium.europa.eu/doc/document/ST-17000-2023-INIT/EN/pdf.
[4] Gem. der Legaldefinition in Art. 3 Abs. 1 CRA-E soll als „Produkt mit digitalen Elementen“ jede Software oder Hardware, einschließlich zugehöriger Datenverarbeitungslösungen in der Cloud, gelten. Und auch Software- und Hardware-Komponenten, die separat in den Verkehr gebracht werden, sollen in den Anwendungsbereich des CRA fallen.

Abgrenzung zu „kommerzieller Open-Source-Software“ im Cyber Resilience Act gelöst

Die Open-Source-Gemeinschaft äußerte starke Bedenken hinsichtlich des Vorschlags der EU-Kommission in Bezug auf die Berücksichtigung der Besonderheiten von Open-Source-Software.[5] Besorgnis bestand, dass die Expertise der Open-Source-Gemeinschaft bei der bisherigen Ausarbeitung des CRA nicht ausreichend berücksichtigt worden ist. Es wurde gewarnt, dass das gesamte Open-Source-Ökosystem gefährdet werden könnte. Auf der Basis des Entwurfs der EU-Kommission wurde befürchtet, dass die Entwickler für Handlungen Dritter haften könnten. Der Entwurf versuchte zwar, dieses Problem zu umgehen, indem er kommerzielle Aktivitäten von nicht-kommerziellen Aktivitäten unterschied. Die Definition von „kommerziell“ war dagegen nicht klar genug und beließ einen zu großen Deutungsspielraum und keinen eindeutigen rechtlichen Geltungsbereich. Zugleich stellte der CRA-Entwurf zu hohe Anforderungen an diejenigen, die keine oder wenig Ressourcen haben, diese Anforderungen umzusetzen.

Entwicklungs- und Vertriebsmodelle proprietärer Software unterscheiden sich grundlegend von jenen für offene Software. Anstatt geschlossener Ökosysteme zeichnet sich Open-Source-Software durch den offenen und kooperativen Ansatz sowie durch standardbasierte anwenderfreundliche Softwarelizenzverträge aus. Ihre Hersteller, bei denen es sich teils um Freiwillige ohne kommerzielle Interessen handelt, haben damit keine direkte Kontrolle über die Weiterverarbeitung und das Inverkehrbringen ihrer Software durch Dritte und sollten hierfür auch nicht in die Haftung genommen werden können. Die Bedenken konnten im Trilog-Verfahren größtenteils durch die vor allem in den Erwägungsgründen nunmehr vorgesehenen Präzisierungen und der eindeutigen Differenzierung zwischen Entwicklungs- und Vertriebsebene ausgeräumt werden. Für öffentliche Hochschulen, Universitäten und Forschungseinrichtungen vor allem relevant und erfreulich ist, dass Open-Source-Software welche ausschließlich für den eigenen Gebrauch entwickelt worden ist, vom Anwendungsbereich des CRA nunmehr ausdrücklich ausgenommen werden soll. Letzteres soll zudem auch dann gelten, wenn die Open-Source-Software im Rahmen der Erbringung einer Dienstleistung beispielsweise von öffentlichen Hochschulen, Universitäten und Forschungseinrichtungen bereitgestellt wird, für welche lediglich eine Gebühr zur unmittelbaren Kostendeckung erhoben wird. Ein Anwendungsfall für diese Ausnahme könnten zukünftig die sogenannten EfA-Leistungen („Einer-für-Alle“) im Rahmen der OZG-Umsetzung darstellen.

Beteiligen sich Hochschulen, Universitäten und Forschungseinrichtungen dagegen systematisch und dauerhaft an der Weiterentwicklung von Open-Source-Software, welche dazu bestimmt ist, kommerziell eingesetzt zu werden, besteht auch zukünftig im Rahmen des CRA das Risiko, in der in den Trilog-Verhandlungen neu eingeführten Rolle des „Open-Source Software Stewards“ in Anspruch genommen zu werden, auch wenn die Einrichtungen selbst mit der Unterstützungsleistung keine Gewinnerzielungsabsicht verfolgen. Beispielsweise genannt werden in Erwägungsgrund 10d das Hosten und Verwalten von Plattformen für die Zusammenarbeit bei der Softwareentwicklung, das Hosten von Quellcode oder Software sowie das Verwalten von Open-Source-Software. Der Pflichtenkanon aus Art. 17a CRA-E ist gleichwohl aber reduzierter im Vergleich zu dem des Entwicklers.

Open Source als zentrales Element politischer Konzepte und Strategien

Die Bedeutung von Open Source als zentralem Element aktueller politischer Konzepte und Strategien – wie Open Innovation, Open Science oder Digitale Souveränität – steigt stetig, national wie international. In einer

[5] *Eclipse Foundation, Inc.*, https://newsroom.eclipse.org/news/announcements/open-letter-european-commission-cyber-resilience-act; *Open Source Business Alliance – Bundesverband für digitale Souveränität e.V.*, https://osb-alliance.de/pressemitteilungen/stellungnahme-zum-cyber-resilience-act; *Linux Foundation Europe*, https://linuxfoundation.eu/cyber-resilience-act; *Moodle*, https://moodle.com/de/news/ein-offenes-schreiben-an-eu-gesetzgeber-von-moodle-die-offene-source-plattform-die-mehr-als-70-von-europas-hochschul-bildungssystemen-betreibt/.

digitalen Wirtschaft und gleichfalls in der deutschen Hochschullandschaft spielt Open-Source-Software eine entscheidende Rolle. Der Stellenwert und die Relevanz von Open-Source-Software wurden bereits in der „Open Source Software Strategy 2020–2023“[6] der Europäischen Union beschrieben und im weiteren Kontext von Landesgesetzen[7] und Verordnungen[8] geregelt sowie im Koalitionsvertrag[9] und der Digitalstrategie[10] der Bundesregierung niedergelegt. Daher ist es unerlässlich, dass alle Rechtsvorschriften, die sich auf die Softwarebranche auswirken, die einzigartigen Bedürfnisse und Perspektiven von Open-Source-Software sowie die modernen Methoden zur Softwareentwicklung berücksichtigen.

Forderung und Einschätzung des ZKI e.V.

Wir begrüßen ausdrücklich, dass in den Trilog-Verhandlungen ein sensibler Umgang mit der Thematik gelungen ist und die im Unterschied zu proprietären Entwicklungs- und Vertriebssystemen bestehenden einzigartigen Eigenschaften und Besonderheiten des Open-Source-Ökosystems Berücksichtigung gefunden haben. Gleichwohl würde es auch zukünftig bei einem Inkrafttreten des CRA in der derzeit vorliegenden Form weiterhin der Rechtspraxis obliegen, die im CRA angelegten Ausnahmen für Open-Source-Software entwicklerfreundlich im Sinne der Open-Source-Gemeinschaft anzuwenden insbesondere da die Erwägungsgründe den Gesetzestext der Verordnung nicht ändern können und zudem nicht rechtsverbindlich sind.[11] Ein wesentlicher und wichtiger Schritt hin zur Stärkung der Cyber Resilience in der Europäischen Union unter gleichzeitiger Wahrung der Interessen der Open-Source-Gemeinschaft darf den Verhandlungsparteien des Trilog-Verfahrens aber ohne Zweifel bescheinigt werden.

Lizenzhinweis

Diese Veröffentlichung ist lizenziert unter einer Creative-Commons-Lizenz: Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0 DEED).

[6] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/open-source-software-strategy_en.

[7] Gesetz zur elektronischen Verwaltung für Schleswig-Holstein – § 7 EGovG; Thüringer Gesetz zur Förderung der elektronischen Verwaltung – § 4 ThürEGovG; Thüringer Vergabegesetz – § 4 Abs. 2 ThürVgG; Bayerisches Digitalgesetz – Art. 3.

[8] Beispielhaft**:** Verwaltungsvorschrift der Landesregierung Baden-Württemberg über die Vergabe öffentlicher Aufträge (VwV Beschaffung) vom 24. Juli 2018 – Az.: 64-0230.0/160.

[9] https://www.bundesregierung.de/resource/blob/974430/1990812/1f422c60505b6a88f8f3b3b5b8720bd4/2021-12-10-koav2021-data.pdf?download=1.

[10] https://digitalstrategie-deutschland.de/static/fcf23bbf9736d543d02b79ccad34b729/Digitalstrategie_Aktualisierung_25.04.2023.pdf.

[11] EuGH-Urteil vom 13. September 2018, Česká pojišťovna, C-287/17, EU:C:2018:707, Rn. 33.