Vom Code zur Verantwortung: Einfluss des EU Cyber Resilience Act auf die Softwaretechnik

Peter Schoo
IT Sicherheit und Privacy Forschung, https://peterschoo.de, peter.schoo@posteo.de

Die F&E-Aktivitäten in der Informatik werden durch technologische Innovationen, Förderungsschwerpunkte als auch durch regulatorische Rahmenbedingungen geprägt. Neben derzeitigen Themen wie Künstlicher Intelligenz und Quantencomputing gewinnt insbesondere europäische Gesetzgebung an Bedeutung und beeinflussen unmittelbar Entwicklung und Betrieb digitaler Produkte.

Ein zentrales Beispiel hierfür ist der Cyber Resilience Act (CRA) der Europäischen Union. Die Verordnung etabliert verbindliche Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen und wirkt damit auch auf Softwaretechnik, Softwareentwicklung und Open-Source-Software-Ökosysteme. Durch die Einführung neuer Verantwortlichkeiten und Stakeholderrollen verändert der CRA zudem die Rahmenbedingungen für die Entwicklung, Bereitstellung und langfristige Pflege von Software.

Regulatorischer Hintergrund: Der CRA führt einen verbindlichen Rechtsrahmen für Produkte mit digitalen Elementen ein. Die Verordnung sieht vor, dass Hersteller während der gesamten Produktlebensdauer Anforderungen an Cybersicherheit erfüllen und nachweisen müssen. Bereits vor dem vollständigen Inkrafttreten der materiellen Anforderungen werden Verpflichtungen zur Meldung aktiv ausgenutzter Schwachstellen wirksam. Darüber hinaus enthält der CRA mehrere strukturelle Neuerungen:

- die Verknüpfung regulatorischer Anforderungen mit Konformitätsbewertungen und CE-Kennzeichnung,
- die Einführung einer risikobasierten Klassifizierung von Produkten,
- die Entwicklung harmonisierter europäischer Normen zur Konkretisierung der gesetzlichen Anforderungen sowie
- die Definition neuer Stakeholderrollen innerhalb des Softwareökosystems.

Durch neue Europäischen Normen entsteht eine enge Wechselwirkung zwischen Regulierung, Standardisierung und Softwareentwicklung.

Stewards als neue Stakeholder: Eine wesentliche Neuerung des CRA besteht in der Einführung der Rolle des Open-Source-Software Stewards (OSSS). Damit wird erstmals ein eigenständiger Stakeholder für Organisationen geschaffen, die zentrale Funktionen innerhalb von Open-Source-Software-Ökosystemen übernehmen.

Ein OSSS ist eine juristische Person, die Open-Source-Software (OSS) systematisch und dauerhaft unterstützt und deren Weiterentwicklung sowie Nutzbarkeit nachhaltig sicherstellt, ohne die betreffende Software selbst als kommerzielles Produkt auf dem Markt bereitzustellen. Die Rolle betrifft insbesondere solche Open-Source-Software-Projekte, die als Grundlage für Produkte oder Dienstleistungen Dritter dienen.

Typische Beispiele für Organisationen, die dieser Beschreibung entsprechen, sind die Apache Software Foundation und die Linux Foundation. Beide Organisationen stellen Governance-Strukturen, Entwicklungsinfrastrukturen, Sicherheitsprozesse sowie organisatorische Unterstützung für eine Vielzahl weit verbreiteter Open-Source-Software-Projekte bereit.

Regulatorischen Verantwortungszuweisung: Mit der Einführung der Rolle des OSSS verbindet der CRA bestimmte Verantwortlichkeiten hinsichtlich Sicherheits- und Compliance-Anforderungen. Gleichzeitig enthält die Verordnung keine ausdrücklichen Regelungen zur finanziellen oder organisatorischen Kompensation der hierdurch entstehenden Aufwände.

In der Literatur sowie in regulatorischen Begleitdokumenten wird daher diskutiert, inwieweit zusätzliche Unterstützungsmechanismen erforderlich sein könnten, um die langfristige Handlungsfähigkeit von OSSS sicherzustellen. Hierzu existieren verschiedene Leitlinien und Empfehlungen, die jedoch keine unmittelbare Rechtswirkung entfalten.

Vor diesem Hintergrund veröffentlichte die Gesellschaft für Informatik (GI) einen Policy Brief zur Anerkennung und Besserstellung von OSSS.[1] Darin werden Maßnahmen vorgeschlagen, die zur nachhaltigen Absicherung dieser Stakeholder beitragen sollen. Die Empfehlungen adressieren insbesondere Fragen der Finanzierung, institutionellen Anerkennung und regulatorischen Unterstützung.

Einordnung aus Sicht der Softwaretechnik: Aus einer systemischen Perspektive kann der CRA nicht ausschließlich als Sicherheitsvorschrift verstanden werden. Vielmehr lässt sich die Verordnung als Schritt zur Institutionalisierung von Softwareverantwortung interpretieren. Dabei werden Verantwortung, Haftung, Dokumentation und Sicherheitsnachweise über den gesamten Lebenszyklus digitaler Produkte hinweg regulatorisch verankert und nachhaltiger.

Diese Entwicklung betrifft auch die Erstellung und

[1] https://gi.de/meldung/gi-fordert-anerkennung-und-besserstellung-von-open-source-software-stewards

Pflege von OSS, die bislang häufig außerhalb formaler regulatorischer Strukturen erfolgte. Für die Softwaretechnik ergibt sich daraus eine Verschiebung des fachlichen Fokus: Neben der Entwicklung funktionaler Systeme gewinnen Aspekte der Sicherheit, Governance, Dokumentation und langfristigen Produktverantwortung an Bedeutung.

Eine zentrale Annahme dieser Analyse ist, dass die regulatorischen Anforderungen des CRA in industrielle Entwicklungsprozesse integriert werden. Da die normative Ausgestaltung (z. B. harmonisierte EU-Normen) noch nicht abgeschlossen ist, sind Umfang und Geschwindigkeit der Veränderungen derzeit nicht empirisch validierbar, d.h. es fehlen Langzeitdaten.

Gesellschaftliche Auswirkungen: Software erfährt eine veränderte Wahrnehmung und wird zunehmend als Bestandteil kritischer digitaler Infrastrukturen verstanden und nicht mehr ausschließlich als technisches Artefakt betrachtet. Daraus ergibt sich:

- Verantwortung für Cybersicherheit wird entlang digitaler Wertschöpfungs- und Lieferketten expliziter verteilt.
- Sicherheitsanforderungen werden stärker institutionell verankert.
- OSS-Projekte gewinnen an politischer und gesellschaftlicher Relevanz als Grundlage zahlreicher digitaler Produkte und Dienstleistungen.

Die regulatorische Sichtweise spiegelt damit den hohen Grad an gesellschaftlicher Abhängigkeit von digitalen Systemen.

Wirtschaft und digitale Wertschöpfung: Aus wirtschaftlicher Perspektive verschiebt sich Cybersicherheit von einer primär qualitätsbezogenen Eigenschaft hin zu einer regulatorisch überprüfbaren Anforderung, aus denen sich folgende Vorgaben ergeben:

- verbesserte Transparenz über Software-Lieferketten,
- Dokumentation von Softwarekomponenten und deren Herkunft,
- systematisches Risikomanagement,
- Nachweis regulatorischer Konformität sowie
- kontinuierliche Überwachung sicherheitsrelevanter Aspekte.

Darüber hinaus rückt die langfristige Finanzierung und Unterstützung von OSS stärker in den Fokus. Da ein erheblicher Teil digitaler Wertschöpfung auf frei verfügbarer Software basiert, werden unterschiedliche Formen der Kompensation und Unterstützung diskutiert, darunter direkte Finanzierung, Förderprogramme oder aktive Beiträge zur Weiterentwicklung von Projekten.

Von besonderer Bedeutung ist ferner die Rolle der Standardisierung. Die im Rahmen des CRA entstehenden Normen werden maßgeblich beeinflussen, welche Entwicklungsprozesse, Sicherheitsmaßnahmen und Konformitätsnachweise künftig als ausreichend gelten.

Technisch-methodische Konsequenzen: Auf technischer Ebene verstärkt der CRA bestehende Entwicklungen im Bereich sicherheitsorientierter Softwareentwicklung mit besonderem Schwerpunkten in:

- Security-by-Design und Secure-by-Default
- Threat Modelling und Security Engineering
- Schwachstellenbehandlung und kontinuierliche Sicherheitsüberwachung, sowie
- Lebenszyklus- und Konfigurationsmanagement.

Während traditionelle Softwareentwicklungsprozesse häufig auf funktionale Anforderungen fokussiert sind, erfordern regulatorische Rahmenbedingungen zunehmend den Nachweis sicherheitsbezogener Eigenschaften. Dokumentation, Rückverfolgbarkeit und Auditierbarkeit werden dadurch zu integralen Bestandteilen moderner Softwaretechnik.

Implikationen für Forschung und Lehre: Diese Entwicklungen erfordern, Cybersicherheit, Software-Lieferketten, Open-Source-Software-Governance und regulatorische Compliance stärker in F&E zu berücksichtigen. Diese Aspekte sollten bereits bei der Konzeption von Methoden, Werkzeugen und Softwarearchitekturen berücksichtigt werden und nicht erst nachgelagert in bestehende Entwicklungsprozesse einfließen.

Für die Forschung ergeben sich insbesondere Fragestellungen zur automatisierten Unterstützung von Compliance- und Sicherheitsprozessen, zur Risikobewertung und Nachweisführung sowie zu nachhaltigen Governance- und Finanzierungsmodellen für OSSS. Gleichzeitig sollten regulatorische Anforderungen stärker in Entwicklungswerkzeuge und Softwareentwicklungsprozesse integriert werden.

Auch die Ausbildung muss diese Entwicklung abbilden. Security Engineering, Software-Lieferketten, Vulnerability Management, Software Bills of Materials, Standardisierung und regulatorische Rahmenbedingungen sollten stärker Bestandteil der Softwaretechnik werden.

Damit steht die Informatik vor der Aufgabe, technische Innovation und regulatorische Anforderungen systematisch zusammenzuführen und Sicherheit, Nachweisbarkeit und langfristige Verantwortbarkeit nachhaltig und bereits bei der Gestaltung digitaler Systeme zu berücksichtigen.