Diskussionspapier

Marktorientierte Förderstrukturen für das Open Source Software Ökosystem

Analyse gegenwärtiger Situation von Open Source Software und Vorschlag zur Finanzierung professioneller Entwicklungsstrukturen und hinreichender Cybersicherheitsmassnahmen

Autoren: Dr. sc. ETH David M. Sommer, Florian Kubiak, Dr. Raphael M. Reischuk

Executive Summary

Digitale Infrastrukturen bilden heute eine zentrale Grundlage für Verwaltung, Wirtschaft und Gesellschaft. Mit der zunehmenden Nutzung von Software- und Cloud-Technologien treten strukturelle Sicherheitsfragen stärker in den Vordergrund, insbesondere im Hinblick auf die Vertraulichkeit schützenswerter Daten sowie die Verfügbarkeit, Integrität und Resilienz der zugrunde liegenden Infrastrukturen. Wie in jüngster Zeit wiederholt erkennbar wurde, weisen die in der Schweiz und der Europäischen Union eingesetzten Software- und Cloud-Technologien strukturelle Sicherheitsdefizite auf. Diese verdichten sich – angesichts wachsender Infrastruktur-Komplexität, zunehmender Abhängigkeiten in den Lieferketten und neuer regulatorischer Anforderungen – zu einem strategischen Risiko für Europa.

Das vorliegende Diskussionspapier untersucht strategische Handlungsoptionen zur Minderung dieser Defizite durch die Förderung von Alternativen auf Basis offener Software und offener digitaler Kommunikationsprotokolle. Ziel ist es, die grundlegenden Anforderungen an innovative, sicherheitsrobuste und nachhaltig kontrollierbare Lösungen herauszuarbeiten und daraus strategische, regulatorische und infrastrukturelle Rahmenbedingungen für deren Umsetzung zu entwickeln.

Das Diskussionspapier analysiert zudem die Marktanforderungen an offene Software-Komponenten und -Unternehmen, die unter dem Sammelbegriff Open Source Software (OSS) geführt werden. Kennzeichnend für OSS ist der frei zugängliche Quellcode, der eine Nutzung, Weiterentwicklung und Weiterverbreitung durch eine breite Akteurslandschaft ermöglicht. Aufbauend darauf präsentiert der Bericht eine strukturierte Übersicht bestehender Projekte und Initiativen zur langfristigen Finanzierung und Stärkung von OSS-Ökosystemen durch Unternehmen, Privatpersonen und staatliche Institutionen.

Die Ergebnisse der Analyse verdeutlichen eine **signifikante Diskrepanz zwischen der hohen Relevanz und Nutzung von Open Source Software** einerseits und dem **Umfang der hierfür verfügbaren finanziellen und organisatorischen Ressourcen** andererseits. Diese Unterfinanzierung gefährdet die Innovationsfähigkeit, die Professionalisierung der Entwicklungsprozesse und die Einhaltung angemessener Cybersicherheitsstandards. Daher ergibt sich dringlich, bestehende und neue Finanzierungsoptionen für Open Source Software auszuloten und umzusetzen.

Als Lösungsansatz werden koordinierte Förderstrukturen vorgeschlagen, die das bestehende OSS-Ökosystem gezielt stärken und weiterentwickeln. Wesentliche Bestandteile dieser Förderstrukturen sind klar definierte Rollen öffentlicher Institutionen und philanthropischer Stiftungen sowie Mechanismen zur systematischen Gewährleistung der Cybersicherheit, der langfristigen Anpassungsfähigkeit und der strategischen Weiterentwicklungsfähigkeit der geförderten Technologien.

—

Das vorliegende Diskussionspapier wurde ermöglicht von der Stiftung Mercator (Fokus Unterstützung von Responsible Tech) und vom Nationalen Testinstitut für Cybersicherheit NTC (Fokus Sicherheitsprüfung von Software und Infrastruktur). Die Autoren danken Christian Folini und Vlad-Stefan Harbuz herzlich für ihr kritisches Gegenlesen des Manuskripts und die wertvollen Anregungen, die zur Verbesserung dieses Textes beigetragen haben.

Inhaltsverzeichnis

1 Einführung

Die europäische IT-Infrastruktur basiert in weiten Teilen auf Plattformen und Diensten weniger marktführender Anbieter. Da diese Anbieter überwiegend ausserhalb Europas ansässig sind, entstehen Abhängigkeiten, die die europäische Entscheidungs- und Handlungsfähigkeit auf technologischer und politischer Ebene beeinträchtigen können. Wiederkehrende Sicherheitsvorfälle unterstreichen zudem, dass etablierte Technologien nicht in allen Fällen den Anforderungen an ein angemessenes Cybersicherheitsniveau genügen. Während in der Vergangenheit aufgrund der vergleichsweise niedrigen Bedrohungslage die Risiken eines Outsourcings insgesamt als akzeptabel galten, befeuern die neueren internationalen Entwicklungen die Diskussion um eine dedizierte europäische IT-Infrastruktur.

So wird der Wunsch nach verfügbaren Alternativen lauter. Gemäss einer Bitkom-Umfrage vom Dezember 2024[1] wünschen sich 92 % der deutschen Unternehmen mehr Unabhängigkeit von den USA, 96 % sind für mehr digitale Souveränität und 86 % wünschen sich einen europäischen Hyperscaler. Gemäss eines Reports des NTC vom Dezember 2024[2] halten 95 % die gegenwärtigen Abhängigkeiten für gefährlich und 90 % wünschen sich einen schweizerischen oder europäischen Hyperscaler. Der Draghi-Rapport zur EU-Wettbewerbsfähigkeit vom September 2024[3] mahnt, dass Europa 80 % der digitalen Technologie importiert und schlägt gezielte Wirtschaftsförderung vor.

Eine zukunftsfähige Alternative zu geschlossener Software und internationalen Abhängigkeiten ist der Einsatz und die gezielte Förderung von Open Source Software (OSS), welche bereits heute einen fundamentalen Bestandteil der modernen Softwarelandschaft darstellt. So ist OSS in 97 % der von Blackduck gescannten Software[4] enthalten. Dies sind häufig zentrale Bausteine, die in ihrem Meer an Ausgestaltungsformen meist nur von wenigen einzelnen Software-Entwicklern getragen werden und aufgrund des Fokus auf maximale Funktionalität oft Massnahmen der Cybersicherheit vernachlässigen. Das NTC hat zusammen mit dem Schweizer Bundesamt für Cybersicherheit (BACS) gezeigt, dass gezielte Prüfungen die Sicherheit von OSS stärken und die Cyberresilienz der Schweiz erhöhen können[5]. Eine nachhaltige Pflege der zentralen Bausteine wird zunehmend zur Notwendigkeit, um eine resiliente Infrastruktur bereitzustellen und die diskutierten Risiken abzufangen.

Angesichts der wachsenden Relevanz von Open Source Software für Alternativen in der europäischen Soft- und Hardwarelandschaft untersucht dieses Diskussionspapier Optionen, marktkompatible OSS-Ökosysteme gezielt zu fördern. Ein besonderer Fokus liegt auf den Schwerpunkten Verfügbarkeit, Vertraulichkeit und Integrität von IT-Lösungen. Durch ein gezieltes Einbeziehen der Anforderungen des Marktes in die Entwicklung und Förderung von Open Source Software kann Europa die damit einhergehenden Herausforderungen angehen, Betriebskosten senken und eine innovative Anpassung an wechselnde Bedürfnisse gewährleisten. Eine klare Strategie zur Schliessung der Versorgungslücke zwischen offenen Infrastrukturen und lukrativen Endkunden-Produkten ist erforderlich, mit einem Fokus auf nachhaltige Finanzierung und professionellen Entwicklungsstrukturen.

Motivation der beteiligten Akteure. Die Stiftung Mercator Schweiz unterstützt mit diesem Diskussionspapier die Evaluation eines wesentlichen

[1] https://www.bitkom.org/Presse/Presseinformation/Tech-Unternehmen-fordern-Unabhaengigkeit-USA
[2] https://www.ntc.swiss/hubfs/20241216-kurzbericht-systemabhaengigkeiten-ntc-de.pdf
[3] https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en
[4] https://www.blackduck.com/content/dam/black-duck/en-us/reports/rep-ossra.pdf
[5] https://www.ntc.swiss/aktuelles/2025-reports-oss-bacs

Aspekts der digitalen Reife der Schweiz und Europas und zielt darauf ab, einen Beitrag zur Etablierung verantwortungsvoller Technologie zu leisten. Ergänzend dazu konzentriert sich das NTC verstärkt auf die allgemeine Sicherheit von unzureichend geprüften digitalen Lösungen, inklusive Open Source Software. Das NTC engagiert sich, um sicherzustellen, dass Technologien sicher sind, indem es die Integration von Cybersicherheit als feste Entwicklungs- und Testschritte propagiert, und notwendige Tests auch selbst durchführt.

Geografische Perspektive. Dieses Diskussionspapier ist primär aus schweizerischer Sicht verfasst und richtet sich an Schweizer Akteure aus Politik, Wirtschaft und Zivilgesellschaft. Viele der beschriebenen Herausforderungen sind jedoch europäischer oder globaler Natur — OSS-Ökosysteme kennen keine Landesgrenzen, und Massnahmen entfalten ihre Wirkung oft nur im Verbund mit europäischen Partnern. Dieses Diskussionspapier unterscheidet diese Ebenen nicht systematisch, was als Einschränkung zu verstehen ist. Eine weiterführende Ausarbeitung sollte explizit klären, welche Massnahmen auf nationaler Ebene umsetzbar sind, welche europäischer Koordination bedürfen und welche nur im internationalen Rahmen Wirkung erzielen können.

2 Derzeitige Herausforderungen

Die Mehrzahl der Unternehmen und staatlichen Institutionen setzen für ihre Betriebsprozesse auf Software-Lösungen, die entweder direkt oder indirekt von den grossen, aussereuropäischen Tech-Unternehmen abhängen. Diese Abhängigkeiten führen zu konkreten Herausforderungen in der Praxis: Risikoanalysen[6] warnen vor Datenkontrollverlust, eingeschränkter Datenhoheit und schwer bewertbaren Sicherheits- und Compliance-Risiken, da der Software-Stack vieler Anbieter häufig eine Black Box bleibt. Die internen Massnahmen der Anbieter sind häufig intransparent[7] und grundsätzlich schwer zu kontrollieren. Die Nichtverfügbarkeit von essenziellen Dienstleistungen, wie es beispielsweise Nicolas Guillou, Richter am Internationalen Strafgerichtshof, widerfahren[8] ist, entwickelt sich ebenfalls zu einem Kernrisiko.

Darüber hinaus können monopolistische Anbieter die Preise durch fehlende Software-Alternativen beliebig erhöhen und SaaS-Dienste ohne Vorwarnung einstellen. Die Betreiber von Infrastruktur und Software haben volle Kontrolle über den Datenfluss und könnten sensible Daten abfliessen lassen, z.B. via US CLOUD-Act[9]. Geopolitische Veränderungen werden unter Umständen schneller erfolgen, als Alternativen geschaffen werden können. Bei Datenmigration hin zu neuen Systemen besteht die Gefahr, dass bestehende Daten nicht vollständig extrahiert werden können. Proprietäre Datenformate und Schnittstellen verstärken diesen Vendor-Lock-In-Effekt zusätzlich und erschweren einen Anbieterwechsel erheblich.

Diese Herausforderungen sind zentral und entstehen unter anderem dadurch, dass Europa keinen ausreichend grossen Anteil an der eingesetzten Hardware- sowie Software-Infrastruktur selbst stellt und dass es keine starke Governance über diese zentralen Teile des Technologiestacks ausübt.

2.1 Marktbedürfnisse

Die Ursachen für die zuvor diskutierten Herausforderungen resultieren unter anderem aus den Anforderungen des privatwirtschaftlichen Marktes

[6] https://www.bcg.com/publications/2025/sovereign-clouds-reshaping-national-data-security

[7] https://www.sciencedirect.com/science/article/abs/pii/S0167404823005321

[8] https://www.lemonde.fr/en/international/article/2025/11/19/nicolas-guillou-french-icc-judge-sanctioned-by-the-us-you-are-effectively-blacklisted-by-much-of-the-world-s-banking-system_6747628_4.html

[9] https://dnip.ch/2025/02/27/die-cloud-als-spielball-der-winde/

und der öffentlichen Beschaffung an Software-Technologie und Infrastruktur. Unternehmen und staatliche Organe stellen folgende grundsätzliche Anforderungen mit unterschiedlicher Relevanz je nach Branche und Bereich:

Kosten: Fokus auf kosteneffiziente Lösungen, einschliesslich Produkt-Einführung und Datenmigration, Betrieb, Anpassung und Abschaltung.

Verfügbarkeit: Ausreichend Verfügbarkeit von Software und Dienstleistungen, sodass Geschäftsprozesse nur minimal beeinträchtigt werden.

Funktionsumfang: Einfachheit der Integration in die bestehende IT-Struktur mit erforderlichen Zugriffsfunktionen und Skalierbarkeit sowie Adaptivität an neue Bedürfnisse.

Support-Optionen: Vertraglich garantierte, langfristige Unterstützung bei Betrieb, Migration und Nutzung.

Unterhalt und Weiterentwicklung: Sicherstellung der kontinuierlichen Produktpflege und Anpassung.

Datensouveränität: Kontrolle sensibler Daten und Geschäftsgeheimnisse gemäss Datenschutz.

Zertifizierungen: Anforderungen an Anbieter wie bspw. ISO/IEC 27001 für Informationssicherheit.

Exit-Strategie: Berücksichtigung von Wechselmöglichkeiten zur Vermeidung von Vendor-Lock-In.

Cybersicherheit: Erfüllung moderner Sicherheitsanforderungen, regelmässig geprüft und verbessert.

Nur wenige Anbieter erfüllen obige Anforderungen vollständig. Etablierte Grossanbieter wie Microsoft oder Google decken zwar weite Teile davon ab – insbesondere Funktionsumfang, Support und Verfügbarkeit – weisen jedoch bei Datensouveränität, Exit-Strategie und nachvollziehbarer Cybersicherheit erhebliche Lücken auf. Europäische und auf Open Source basierende Alternativen erfüllen zwar häufig die Anforderungen an Offenheit und Datenkontrolle, scheitern jedoch oft an fehlenden Supportstrukturen, Zertifizierungen oder unzureichendem Funktionsumfang für den Enterprise-Einsatz. Entsprechend setzen sich Alternativen kaum durch. Verstärkt wird dies durch Netzwerkeffekte: Je weiter verbreitet eine Software ist, desto attraktiver wird sie für weitere Nutzer — nicht wegen ihrer technischen Qualität, sondern wegen der geteilten Infrastruktur und des gemeinsamen Wissensstands. So können Unternehmen bei neuen Mitarbeitenden Kenntnisse verbreiteter Software wie Microsoft Office schlicht voraussetzen, was Einarbeitungsaufwand und Schulungskosten senkt. Auch die einfache Zusammenarbeit mit Kunden und Partnern, die dieselben Werkzeuge einsetzen, stärkt diesen Effekt. Für Alternativen ist es entsprechend schwierig, trotz technischer oder souveränitätsbezogener Vorteile Fuss zu fassen.

Besonders das Argument der Kosten ist nur vordergründig offensichtlich: Als Beispiel investieren die USA und China systematisch in ihre IT-Industrie und generieren für ihre Unternehmen damit einen erheblichen Wettbewerbsvorteil gegenüber Anbietern, die sich rein aus dem Markt finanzieren müssen.

2.2 Herausforderungen im Corporate-Markt

Durch fehlende Investitionsbereitschaft und Mut zur Innovation herrscht ein Mangel an passenden Software-Alternativen auf dem Corporate-Markt: Softwareerstellung ist vergleichsweise kostenintensiv, aber die Grenzkosten des Hostings der Software sind minimal. Oft gibt es selbst in grossen Märkten nur wenige Anbieter. Kleine Unternehmen können gegen etablierte Produkte kaum konkurrieren und müssen sich auf Nischen spezialisieren. Die finanzkräftigere Konkurrenz kauft zudem Mitbewerber oft schon im Entstehungsstadium auf. Verfügbare Support- und Vertriebsnetz-

werke, wie die von Microsoft, bieten einen grossen Wettbewerbsvorteil, während selbst Giganten wie Apple im Corporate-Markt zögern oder gänzlich fehlen. Zudem bevorzugen Entscheidungsträger etablierte Produkte, um persönliche Karriere-Risiken zu minimieren. Diese Marktdynamiken machen es unwahrscheinlich, dass tragfähige Alternativen allein durch private Initiative entstehen. Ohne gezielte politische Unterstützung – etwa durch öffentliche Beschaffungsentscheide, Anschubfinanzierung oder regulatorische Rahmenbedingungen – werden die bestehenden Konzentrationskräfte kaum zu durchbrechen sein. Dies gilt auch für die Schweiz, die bislang noch wenig eigene Akzente in diesem Bereich gesetzt hat.

3 Mögliche Alternative: Open Source Software

Der Begriff Open Source Software (OSS) umfasst unterschiedliche Kontexte und Lizenzformen. In diesem Diskussionspapier wird bewusst diese unscharf gehaltene Definition verwendet, in welche die folgenden Punkte eingeschlossen sind:

Zugänglichkeit: Quellcode ist frei verfügbar für Einsicht, Nutzung und Veränderung.

Zusammenarbeit: Entwickler und Nutzer arbeiten zusammen, mit Rückfluss der Ergebnisse ins Projekt für alle.

Transparenz: Software ist transparent und verständlich für Nutzer und Programmierer, nutzt offene Protokolle für hohe Interoperabilität.

Anpassbarkeit: Software kann angepasst und weiterentwickelt werden, auch bei inaktiven Projekten; Forking (das erlaubte Kopieren und getrennte Weiterentwickeln) ist dabei zentral.

Lizenzierung: Lizenzen gewährleisten freie Nutzung und Modifikation von Open Source Software, wobei diese Garantien für die Kommerzialisierung teilweise abgeschwächt werden.

Die Gemeinschaftlichkeit von OSS-Projekten steht häufig im Gegensatz zur Profit- und Ausschlusslogik kommerzieller Projekte, was für OSS oft zu Wettbewerbsnachteilen führt. Stattdessen ist OSS-Projekten der kollaborative Geist gemein: Durch offenen Zugang zum Quellcode werden Entwicklungen geteilt. Die Open Source Definitionen der Vereinten Nationen[10] und der Open Source Initiative[11] fördern Transparenz, wobei die starken Forderungen die Verbreitung der Lizenz einschränken können. Der Fokus auf Gemeinschaft kollidiert zudem mit kommerziellen Profitinteressen, was zu Finanzierungsengpässen von OSS führt. Dennoch sind laut Black Duck Security-Reports[12] OSS-Komponenten in 97 % der gescannten Software enthalten und 70–90 % und es sind im Mittel 70 % – häufig sogar mehr als 90 % – der Software-Komponenten in Anwendungen OSS.

3.1 Zielgebiete und Vorteile von OSS-Projekten

Der Paradigmenwechsel und kollaborative Ansatz von Open Source Software verbessert häufig die Softwarequalität und ermöglicht bessere Integration. OSS-Komponenten können unabhängig betrieben werden und verringern Vendor-Lock-In-Risiken. Ihre Verfügbarkeit fördert Innovation und schnelles Erstellen von Infrastruktur. OSS lohnt sich wirtschaftlich bei gemeinsamen Bedarf, nicht aber bei Nischenfunktionalität, wo wenige Käufer Interesse haben. Trotz anfänglicher Kosten sind langfristige Einsparungen möglich: Eine Studie von Harvard und der Linux-Foundation[13] stellt fest, dass

[10] https://unite.un.org/en/news/sixteen-organizations-endorse-un-open-source-principles
[11] https://opensource.org/osd
[12] https://www.blackduck.com/content/dam/black-duck/en-us/reports/rep-ossra.pdf
[13] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4693148

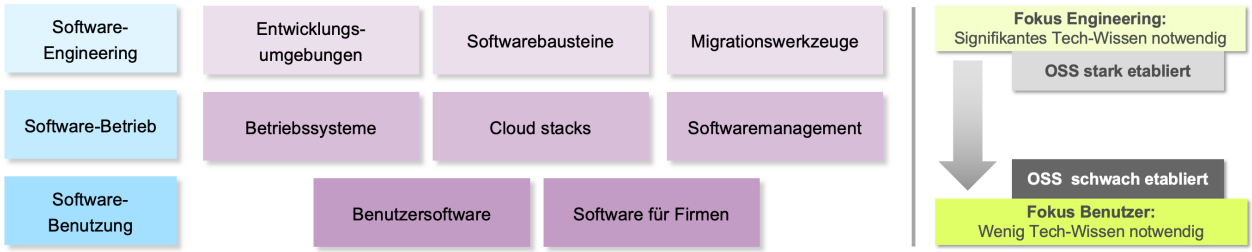

Abbildung 1: Stark vereinfachte Übersicht verschiedener Software-Typen zur Illustration der verschieden entwickelten OSS Einsatzgebieten. Grundsätzlich gilt: je näher beim Software-Programmierer, desto besser funktioniert die OSS-Landschaft.

Unternehmen das 3.5-fache mehr als derzeit für Software ausgeben müssten, wenn es keine OSS gäbe. Sie schätzt den Wert der OSS-Nachfrageseite optimistisch[14] auf $8.8 Billionen. Darüber hinaus werden 96 % des Wertes auf der Nachfrageseite von nur 5 % der OSS-Entwickler geschaffen.

3.2 Herausforderung: OSS und Marktdefizite

Es besteht eine nennenswerte Diskrepanz zwischen der starken Verbreitung von OSS im Software-Engineering-Bereich und der schwachen Verbreitung im Endnutzerbereich, wie in Abbildung 1 illustriert. Im Bereich für technikaffine Anwender gibt es qualitativ hochwertige OSS wie Entwicklungswerkzeuge und Bibliotheken. Die Bereiche der benutzernahen Software und Unternehmenslösungen, etwa CRMs und ERPs, hingegen sind in der Open Source-Welt weniger ausgearbeitet. Finanzielle Interessen stimulieren Bereiche wie Betriebssysteme und Cloud-Management mit Hyperscalern. Während die Infrastrukturkerne offen sind, behalten grosse Anbieter die darauf aufbauenden, gewinnbringenden Dienste – etwa KI-Plattformen, Auto-Scaling oder verwaltete Datenbanken – bewusst proprietär.

Diese höherwertigen Komponenten sind es, die Kunden binden und Umsatz generieren; sie werden daher nicht als OSS veröffentlicht.

Aktuell zeigen sich folgende Defizite von OSS gegenüber kommerzieller Closed Source Software:

Wettbewerbsnachteil: OSS ist oft kostenfrei verfügbar und generiert keine direkten kommerziellen Erträge. Zudem wird OSS teils unter Verletzung von Lizenzbedingungen kommerziell genutzt.

Fehlende Monetarisierung: Die Finanzierungsmöglichkeiten von Entwicklungs- und Verkaufsaktivitäten sind begrenzt, z.B. im Open Core[15] Modell.

Fehlende Professionalisierung: Qualitätssicherung, Verkauf, Alignierung mit weiteren Akteuren und Sicherheitsinfrastruktur fehlen häufig.

Fehlende Enterprise-Features: Aus Hobby-Projekten entstandene Lösungen folgen oft einer Ein-Benutzer-Perspektive und bieten keine modernen IT-Integrationen wie Benutzerverwaltung oder Auditfunktionen.

Schlechte Benutzbarkeit: OSS ist oft nicht intuitiv nutzbar und es fehlt an Komfortfunktionen.

Fehlende Synergieeffekte: Etablierte kommerzielle Software bietet umfassende Plattformunterstützung, Community-getragene OSS-Produkte häufig nicht.

[14] https://openpath.quest/2024/questioning-the-value-of-open-source-software/
[15] https://fcl.dev/

Fehlender Support: Supportverträge und zuverlässige Hilfe sind aufgrund fehlender juristischer Strukturen und fehlender Experten schwer zu gestalten.

Geringe Ausfallsicherheit: Kleine Teams oder Einpersonenprojekte sind anfällig für Personalausfälle.

Developer/Maintainer-Burnout: Hohes Engagement in kleinen Teams ohne finanzielle Kompensation führt schneller zu Überlastung.

Lobbyismus gegen OSS: Unternehmen vermeiden Konkurrenz durch Unterbindung offener Alternativen.

KI-generierte Angriffsfläche: OSS-Projekte sind zunehmend mit automatisiert erstellten Vulnerability-Reports und Pull-Requests durch KI-Systeme konfrontiert. Da die Qualität dieser Eingaben oft schwer einzuschätzen ist, entsteht ein erheblicher Mehraufwand bei Triage und Review — eine Belastung, die kleine Maintainer-Teams schnell überfordert. Daniel Stenberg, Hauptentwickler von curl, hat dieses Problem öffentlich beschrieben und dokumentiert[16].

Open Source Software wird häufig erst von Unternehmen finanziert, sobald sie ausreichend gross und relevant ist, was im Bereich von Projekten wie dem Linux-Kernel zwar der Fall ist, jedoch bei viel genutzten OSS-Bilbiotheken und -Software häufig nicht. OSS lohnt sich hingegen, um Software-Verbreitung zu fördern. Folglich ist es eine zentrale Herausforderung, die Finanzierungslücke bis zur hinreichenden Relevanz zu überbrücken. Bei Firmen und öffentlicher Beschaffung ist weniger das Modell (offen vs. geschlossen) entscheidend, sondern eher die vertraglich gesicherten Supportleistungen, die bei OSS oft unzureichend bis nicht-existent sind.

Microsoft wird in verschiedenen Communities regelmässig kritisch diskutiert, kann jedoch im Hinblick auf seine Marktpositionierung als Orientierungspunkt dienen. Im Corporate-Markt ist das Unternehmen besonders erfolgreich, da es seine Software mit einem breiten Angebot an Dienstleistungen und Supportleistungen kombiniert, die für viele Unternehmen einen entscheidenden Faktor darstellen.

Es wird geschätzt, dass der Grossteil der Open Source Software[17] von nur etwa 3'000 bis 5'000 Entwicklern[18] entwickelt wird, verglichen mit 23.7 Millionen Entwicklern weltweit[19]. Diese Entwickler sind gemäss Einschätzung der Autoren hochqualifiziert, d.h. diese hohe Leistung von durchschnittlichen Software-Entwicklern zu erwarten ist unrealistisch. Die Schätzung macht trotzdem deutlich, dass sich mit genügend politischem Willen erhebliche Fortschritte erzielen lassen. Da der Grossteil des OSS-Fundaments von einer so kleinen Gruppe getragen wird, würde bereits eine gezielte Aufstockung um einige Hundert zusätzliche, hochqualifizierte Entwicklerinnen und Entwickler einen überproportional grossen Effekt erzielen. Gemessen an der Gesamtzahl der weltweit tätigen Softwareentwickler ist dies ein volkswirtschaftlich bescheidener Aufwand — mit potenziell grosser Hebelwirkung.

3.3 Ziele der Lizenzmodelle

Softwarelizenzen regulieren die Nutzung von Code sowie Ausführbarkeit und Änderung von und an Programmen. In der Open Source Community existieren Modelle wie Copyleft, das Änderungen unter derselben Lizenz bindet, und Free Use, das freie Modifikation erlaubt. Grundsätzlich sollten Lizenzen die Entwickler- und Nutzerinteressen respektieren und bestehende Geschäftsmodelle schützen.

[16] https://daniel.haxx.se/blog/2024/01/02/the-i-in-llm-stands-for-intelligence/
[17] https://opensourcefundingsurvey2024.com/
[18] https://openpath.quest/2024/funding-the-five-thousand/
[19] https://www.statista.com/statistics/627312/worldwide-developer-population/

In der Open Source Welt existieren zudem Lizenzmodelle, die Copyleft und Free Use aufgrund kommerzieller Bedürfnisse einschränken: **Open Core**[15]-Methodiken offerieren Basisversionen kostenlos und erheben Gebühren für erweiterte Funktionen. Ansätze wie **Fair Code**[20] schränken kommerzielle Nutzung ein, während **Fair Source**[21] die Veröffentlichung verzögert. **Fair Core**[15] folgt der Open Core Mentalität mit einer Lizenz, die die Verwendung und Verfügbarkeit des offenen Core etwas einschränkt. **Post-Open Source**[22] verlangt Gebühren für kommerzielle Unternehmen.

Eine Überprüfung der Lizenzpraktiken ist notwendig[23], um die kommerzielle Nutzbarkeit im Einklang mit rechtlichen Definitionen zu verbessern und Open Source Software finanziell nachhaltiger zu gestalten.

4 Finanzierung von OSS

Die Finanzierung der OSS-Landschaft folgt keinem simplen Prinzip. Verschiedene private, staatliche und gewerbliche Akteure vertreten ihre Partikularinteressen, indem sie nach eigenen Möglichkeiten beitragen. Dies stellt kein nachhaltiges, marktorientiertes Konzept[24] dar.

In diesem Kapitel werden zuerst die Optionen zur Finanzierung ausgeführt und danach wird auf konkrete, bereits existierende Finanzierungsschemata ausgehend von Privatpersonen, Stiftungen, Unternehmen und staatlichen Akteuren eingegangen.

4.1 Finanzierungsoptionen

Nachfolgend werden wichtige Optionen zur Finanzierung von OSS-Projekten aufgeführt. Es wird dabei grundsätzlich zwischen Anschubfinanzierung und kontinuierlicher Pflege unterschieden. Europäische Investitionen sind zurückhaltender bei ersterer, weil sie aus Einzelprojektsicht riskant sind.

Eigeninitiative/Eigenkapital: Entwickler starten Projekte aus Eigeninteresse, oft ohne weiterzuwachsen.

Investments bei Produktrelevanz: Firmen investieren in OSS-Produkte ihrer Lieferkette, jedoch minimal und primär für ihre Kerninteressen, oft in Form von Programmierer-Arbeitsstunden, selten finanziell.

Geschäftsmodell-Unterstützung: Unternehmen geben eigenentwickelte Werkzeuge und Produkte aus kommerziellen Gründen frei, siehe Commoditisierung von Komplementen[25].

Venture Capital: Finanzierung von Entwicklung mit dem Hauptziel, monetären Gewinn zu erwirtschaften. Im konservativen europäischen Markt selten, trotz Potenzials für hohen Gewinn[26].

Crowdfunding: Finanzierung durch die Community für Projekte oder spezifische Features (Bounty-Program).

Staatliche Innovationsprogramme: Förderung durch Programme wie Sovereign Tech Fund[27] oder Horizont Europa[28].

Verteilungsorganisationen: Spenden werden gesammelt und an Entwickler verteilt.

[20] https://faircode.io/

[21] https://fair.io

[22] https://www.theregister.com/2023/12/27/bruce_perens_post_open/

[23] Für eine ausführliche Begründung siehe https://dirkriehle.com/2024/07/11/a-plea-for-an-open-source-cloud-copyleft-license/

[24] https://openpath.quest/2024/the-open-source-sustainability-crisis/

[25] https://gwern.net/complement

[26] https://www.toptal.com/management-consultants/venture-capital-consultants/open-source-software-investable-business-model-or-not

[27] https://www.sovereign.tech/de

[28] https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/horizon-europe_en

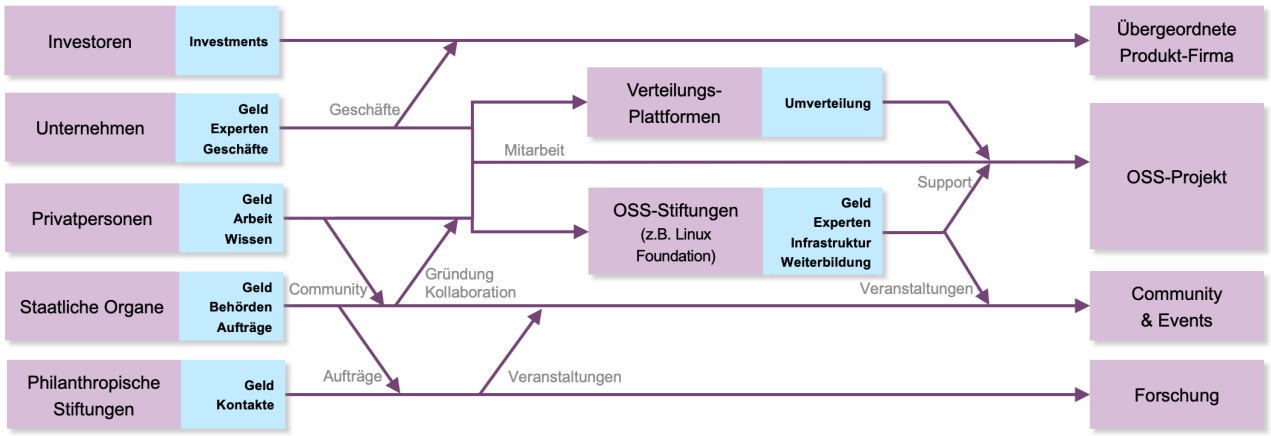

Abbildung 2: Illustration des Flusses der verfügbaren Mittel durch die OSS-Landschaft. Finanzielle Mittel fliessen über jeden Pfeil.

SaaS-Versionen: Cloud-basierter Betrieb der Software und Verdienst durch den Verkauf von Zugängen zur Software.

Business-Version/Lizenz: Basisversion kostenfrei, professionelle Version kostenpflichtig, oft Open Core[15] genannt, siehe Abschnitt 3.3.

Paid Support/Service: Einnahmen werden erzielt durch erbrachte Dienstleistungen rund um OSS-Produkte

Strategische Partnerschaften: Kooperation zum Erreichen gemeinsamer Ziele inklusive Sponsoring.

Staatliche Beschaffung: Inklusion von (OSS) als Auswahlkriterium bei Ausschreibungen, wie z.B. im relativ jungen Schweizer EMBAG[29], zur Erhöhung der Nachfrage und damit Bereitstellung von Geldern für Entwicklung. Erwähnenswert ist hier besonders das Prinzip öffentliche Gelder, öffentliche Software[30], welches die Öffnung von öffentlich finanzierter Software verlangt.

Stiftungen und Vereine: Unterstützung durch Organisationen (Bsp: Linux Foundation[31], Apache Software Foundation[32], OWASP[33], Eclipse Foundation[34]).

Externe Unterstützer: Vielfältige Einzelzuwendungen wie Spenden oder geleistete Arbeit.

Für die Akzeptanz von monetären Abgaben der Teilnehmer im Ökosystem entscheidend sind das eingegangene Risiko sowie der Return-on-Invest (ROI), die Freiwilligkeit der Mittelabgabe durch die Nutzer und die Mitbestimmungsmöglichkeiten der Nutzer und Entwickler.

4.2 Realisierte Finanzierungsschemata

Im Folgenden werden die in Abb. 2 skizzierten Beiträge an OSS näher betrachtet.

[29] Siehe *Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben*, https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/open_source_software/hilfsmittel_oss.html

[30] https://publiccode.eu

[31] https://www.linuxfoundation.org

[32] https://apache.org

[33] https://owasp.org

[34] https://www.eclipse.org/org/foundation/

4.2.1 Stiftungen als Finanzierer

Stiftungen sind entweder fachlich orientiert (z.B. Linux Foundation[35]), die ihre Mittel direkt an Projekte oder in Fachpersonal investieren, oder philanthropisch, weniger technisch mit Fokus auf finanzielle Unterstützung, Grundlagenarbeit und Events. Das Sicherheitsbewusstsein in der OSS-Welt stieg seit Heartbleed[36] (2014), was zur Gründung der heutigen OS Security Foundation[37] führte, die jährlich $30 Mil. in OSS-Sicherheit investiert und Meetings mit grossen Stakeholdern veranstaltet. Diese Initiative gehört zur Linux Foundation.

4.2.2 Privatpersonen als Finanzierer und Verteilungsplattformen

Privatpersonen fördern OSS durch eigene Projekte, ehrenamtliche Community-Arbeit, Code-Reviews und Wissensaustausch in Internet-Foren (z.B. Stack-Overflow[38]). Projekte können gezielt unterstützt werden, doch unbekannte, wichtige Projekte bleiben oft unbeachtet. Es existieren Plattformen, die Spenden direkt an Projekte verteilen und deren Verwendung offenlegen.

Folgende Plattformen bilden für Privatpersonen und Stiftungen eine Auswahl:

GitHub Sponsors: Verteilt Gelder automatisch an Software-Abhängigkeiten, was mehreren Projekten zugute kommt.[39]

OpenCollective: Vereinfacht Organisationsprozesse, beherbergt Open Source Projekte, ohne Geldverteilung kann aber Spenden für Projekte empfangen und verwalten.[40]

Tidelift: Analysiert und finanziert Software-Lieferketten (ist profit-orientiert, erworben von Sonar).[41]

thanks.dev: Unterstützt die finanzielle Verteilung an die eigene Software-Abhängigkeitskette.[42]

Liberapay: Ermöglicht Spenden an Projekte und private Entwickler.[43]

Wie Gelder fair und effizient verteilt werden können ist komplex und ohne konkrete Lösung. Demokratische Prinzipien und zielgerichtete Verteilung können unter Berücksichtigung von Komplexität, Nutzungshäufigkeit und Sicherheitsrisiken temporäre Lösungen stellen. Organisationen wie The Open Source Endowment[44] beschäftigen sich damit. Ansätze wie Built With[45], bindep[46] und Ecosystem Dashboards[47] verwenden Metriken für Komplexität und Verbreitung. Ebenso existieren Contributor Tiers[48] und funding.json[49]. Ein EU-Bericht[50]

[35] https://www.linuxfoundation.org
[36] https://en.wikipedia.org/wiki/Heartbleed
[37] https://openssf.org/
[38] https://stackoverflow.com/questions
[39] https://github.com/sponsors
[40] https://opencollective.com/
[41] https://tidelift.com/
[42] https://thanks.dev/
[43] https://liberapay.com/
[44] https://endowment.dev
[45] https://builtwith.com
[46] https://codeberg.org/vladh/bindep
[47] https://blog.ecosyste.ms/2025/09/25/ecosystem-dashboards.html
[48] https://typescript-eslint.io/maintenance/contributor-tiers/
[49] https://www.fundingjson.org
[50] https://interoperable-europe.ec.europa.eu/sites/default/files/news/2022-04/Development%20of%20a%20Funding%20Mechanism%20for%20Sustaining%20Open%20Source%20Software%20for%20European%20Public%20Services.pdf

empfiehlt klare Aufgabenverteilung und wechselnde Experten.

4.2.3 Unternehmen als Finanzierer

Neben der ehrenamtlichen Arbeit der Entwickler sind Investitionen von grossen Unternehmen relevant. Sie investieren durch eigene Projekte, finanzielle Mittel oder bezahlte Arbeitsstunden. Laut einer Studie der Linux Foundation und Harvard Business School[17] entfallen 86 % des gesamten Unternehmensengagements in OSS auf bezahlte Arbeitsstunden — also Mitarbeitende, die von Unternehmen angestellt werden und einen Teil ihrer Arbeitszeit in OSS-Projekte investieren. Dies entspricht etwa $7.7 Mrd. pro Jahr. Direkte finanzielle Zuwendungen an Projekte machen hingegen nur einen kleinen Teil aus. Dennoch fliesst wenig in die Software-Sicherheit, und die ursprünglichen Entwickler sowie Vermarktungsaspekte werden kaum berücksichtigt. Wesentliche Beiträge von Unternehmen an die OSS-Welt sind eigene Projekte wie Kubernetes, React oder KI-Modelle (LLMs), die der Öffentlichkeit zur Verfügung gestellt werden.

Für Unternehmen existieren Stiftungen und Initiativen wie der Open Source Pledge[51]: Firmen verpflichten sich freiwillig, $2'000 pro Jahr und Entwickler an genutzte Open Source Software zu spenden, was in 2025 etwa $3.5 Mio. einbrachte.

4.2.4 Staatliche Projekte als Finanzierer

Staatliche Projekte für Autonomie und OSS gibt es auf nationaler, internationaler, EU- und UN-Ebene. Die UN bietet einen Leitfaden[52] für offene Software.

Die EU fördert Cybersicherheit, -Souveränität und wirtschaftliche Konkurrenzfähigkeit. Sie erstellt Studien zum Einfluss quelloffener Technologien[53] und zur Entwicklung einer Finanzierung kritischer Software[54]. Das Gaia-X[55]-Projekt legt die Basis für eine europäische Cloud. Subventionen werden durch Horizont Europa[28] und EIC Pathfinder bereitgestellt.

Es gibt gesellschaftliche Forderungen, diese Bemühungen zu verstärken. Bedeutende Initiativen sind die EuroStack-Bewegung[56] und die Forderung des Open Forum Europe, den deutschen Sovereign Tech-Fund[27] auf Europa-Ebene [57]auszuweiten. National ist er erfolgreich in der Finanzierung von IT-Projekten, ebenso wie das Sprin-D-Projekt[58] zur Gründung innovativer Startups.

Weitere bemerkenswerte Projekte und Bemühungen auf nationaler Ebene im Software-Bereich sind

[51] https://opensourcepledge.com/
[52] https://unite.un.org/en/news/osi-first-endorse-united-nations-open-source-principles
[53] https://op.europa.eu/en/publication-detail/-/publication/29effe73-2c2c-11ec-bd8e-01aa75ed71a1/language-en
[54] https://interoperable-europe.ec.europa.eu/sites/default/files/news/2022-04/Development%20of%20a%20Funding%20Mechanism%20for%20Sustaining%20Open%20Source%20Software%20for%20European%20Public%20Services.pdf
[55] https://gaia-x.eu/
[56] https://eurostack.eu/the-letter/
[57] https://eu-stf.openforumeurope.org/
[58] https://www.sprind.org/
[59] https://www.opendesk.eu/
[60] https://www.zendis.de/
[61] https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/standarddienste/bueroautomation/poc-boss.html
[62] https://netzwerksds.ch/
[63] https://www.numerique.gouv.fr/numerique-etat/dinum/
[64] https://www.etalab.gouv.fr
[65] https://matrix.org/

OpenDesk[59]/ZenDiS[60]/BOSS[61]/Netzwerk SDS[62] und die DINUM-Projekte[63] Etalab[64], das Chatprotokolls Matrix[65] und der darauf basierenden Regierungschat Tchap[66], der leider als Beispiel für die Notwendigkeit von Security-Reviews[67] dient.

Projekte wie der Deutschland-Stack[68] und das französische *logiciels libres et communs numériques*[69] sind eng fokussiert. Trotz ihrer monetären Wirkung haben sie eine strukturelle Schwäche: Die Förderung ist an einen vorab definierten Katalog genehmigter Software gebunden. Neue oder innovative Projekte müssen aufwändige Aufnahmeprozesse durchlaufen, bevor sie überhaupt förderfähig werden — ein erheblicher Nachteil gegenüber der schnellen Innovationsdynamik des freien Marktes. Hinzu kommt, dass staatliche Stellen häufig keinen vollständigen Überblick darüber haben, welche OSS-Komponenten tatsächlich in ihren Systemen eingesetzt werden. Ohne dieses Wissen ist eine gezielte Förderung kaum möglich. Ein systematisches Monitoring der genutzten Software – etwa in Form eines Software Bill of Materials (SBOM) – wäre eine Grundvoraussetzung für eine wirkungsvolle und marktnahe Förderung.

Insbesondere in sicherheitskritischen Bereichen geht die Tendenz zum Einsatz von offenen Alternativen: So wechselte das österreichische Bundesheer von MS365 zuletzt auf eine offene Alternative[70] und in der Schweiz scheint es bei der Armee eine vergleichbare Einstellung[71] zu geben.

Immer wieder werden interne Daten trotz höherer Geheimhaltungsanforderungen von Regierungen auf nicht-europäischen Servern gespeichert[72]. Daraus entstehen Initiativen wie die niederländische *Rijkscloud*[73] für nationale Cloud-Plattformen.

Der EuroStack empfiehlt der Europäischen Kommission einen Policy-Fokus zur Förderung europäischer IT-Firmen von Hardware bis Daten-Management.

4.3 Startkapital wird benötigt

Es folgen die wichtigsten Befunde. Das Problem überlasteter Maintainer[74] ist seit längerem bekannt: 73 % der OSS-Entwickler[75] haben in ihrer Karriere bereits ein Burn-Out erlitten und zahlreiche Initiativen versuchen, dem entgegenzuwirken. Viele engagierte Projekte entwickeln Unterstützungsmodelle, während Unternehmen neue Funktionen bereitstellen und Programmier-Frameworks veröffentlichen, um technologische Entwicklungen und Marktstandards mitzugestalten und sich damit Marktvorteile zu sichern. Stiftungen wie die Linux Foundation sowie staatliche Akteure fördern zunehmend Sicherheitsmassnahmen und suchen nach nachhaltigen Finanzierungs- und Governance-Modellen — nicht zuletzt als Reaktion auf den Heartbleed-Bug[36] .

Parallel dazu wächst das Interesse von Staaten an autonomen und resilienten Cloud- und Regierungsinfrastrukturen. Entsprechende Projekte werden geschaffen, sind jedoch unterrepräsentiert und unterfinanziert.

Als erstes Fazit lässt sich festhalten: Es gilt, die Lücke zu schliessen zwischen der Server-

[66] https://tchap.numerique.gouv.fr/
[67] https://securityaffairs.com/84219/breaking-news/hacker-broke-tchap.html
[68] https://deutschland-stack.gov.de/
[69] https://code.gouv.fr/fr/plan-action-logiciels-libres-et-communs-numeriques/
[70] https://www.derstandard.de/consent/tcf/story/3000000288311/microsoft-wird-ausgemustert-bundesheer-wechselt-zu-libreoffice
[71] https://www.republik.ch/2025/10/31/der-armeechef-stemmt-sich-gegen-microsoft
[72] https://www.bankinfosecurity.com/eu-commission-microsoft-appeal-edps-office-365-decision-a-25327
[73] https://digitalpolicyalert.org/change/13766-establishment-of-government-cloud-system-rijkscloud
[74] https://mirandaheath.website/report-on-burnout-in-open-source-software/
[75] https://www.jetbrains.com/lp/devecosystem-2023/

Infrastruktur, wo bereits viel auf Open Source Infrastruktur basiert, und den Endkunden-Produkten, wo das Geld verdient wird. Um die OSS-Landschaft aus Nutzungsgebühren zu fördern, muss zu Beginn Startkapital beschafft und ein nachhaltiges Finanzabflussmodel entwickelt werden.

5 Relevanz der Cybersicherheit

Unzureichende Investitionen in die Cybersicherheit führen zu wirtschaftlichen Verlusten in Milliardenhöhe[76] und zunehmenden Ransomware-Angriffen[77] auf die IT-Landschaft. Cyber-Versicherungen mindern selten das Gesamtrisiko, sondern verteilen lediglich die Kosten. Trotz der hohen Rentabilität von Investitionen in die Cybersicherheit zeigt sich, dass Entwickler oft mehr in funktionale Features als in Sicherheit investieren. Nur durch sichere Systeme mit klarem Konzept können jedoch Resilienz und Schutz der Daten gewährleistet werden. In der Privatwirtschaft wird oft zu wenig in Sicherheitsmassnahmen investiert, da diese als reine Kosten betrachtet werden. Da Cybersicherheit in gemeinsam genutzter Infrastruktur den Charakter eines öffentlichen Gutes hat – alle Nutzer profitieren, aber kaum jemand hat einen individuellen Anreiz, allein zu investieren – legt dies koordinierte Ansätze nahe, die über rein marktwirtschaftliche Mechanismen hinausgehen.

Viele wichtige OSS-Projekte werden von Privatpersonen ohne ausreichende Sicherheitskenntnisse entwickelt. Eine strategische Professionalisierung der Prozesse durch Reviews, Tests und Updates ist notwendig, um die Sicherheit dieser Software zu gewährleisten. Code-Audits und DevSecOps-Tools sind essenziell, um Risiken wie die Log4Shell-Schwachstelle[78] in der weitverbreiteten Java-Bibliothek Log4j zu minimieren, die Ende 2021 Millionen von Systemen weltweit gefährdete und den dringenden Handlungsbedarf bei der Sicherheit von OSS-Abhängigkeiten exemplarisch aufzeigte. Eine Studie aus Dänemark[79] aus dem Jahr 2025 zeigt: Die Open Source Security Foundation (Teil der Linux Foundation) und die Sovereign Tech Agency in Deutschland sowie EU-Initiativen[80] arbeiten als eine der wenigen an der Finanzierung von Sicherheitslösungen, doch die staatsnahe Bürokratie bremst benötigte flexible Marktanpassungen aus.

Die Dominanz amerikanischer Cloud-Anbieter gefährdet zudem – wie oben beschrieben – die europäische Infrastruktur- und Datensouveränität. Angesichts des Bedarfs an einer krisenresistenten Softwarelandschaft ist der Aufbau alternativer Infrastrukturen erforderlich, da bei bestehenden Lösungen häufig keine ausreichenden Garantien hinsichtlich Verfügbarkeit und Vertraulichkeit bestehen. Wie in Abschnitt 3 ausgeführt, kann OSS dabei eine zentrale Rolle spielen.

6 Konzeptioneller Vorschlag: Förderstrukturen für ein nachhaltiges OSS-Ökosystem

Dieses Kapitel skizziert ein Referenzmodell für Förderstrukturen, die das bestehende OSS-Ökosystem professionalisieren und nachhaltig stärken. Obwohl die nachfolgende Darstellung generisch gehalten ist, ist es für Software-Produkte mit spezifischen Anforderungen – etwa in der Büroautomatisierung oder im ERP-Umfeld – erforderlich, jeweils angepasste Förderstrukturen zu entwickeln. Weiter hinten in der Software-Lieferkette können

[76] https://www.tagesschau.de/wirtschaft/unternehmen/jaguar-cyberangriff-100.html

[77] https://www.odni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf

[78] https://en.wikipedia.org/wiki/Log4Shell

[79] https://arxiv.org/abs/2412.05887

[80] https://interoperable-europe.ec.europa.eu/sites/default/files/news/2022-04/Development%20of%20a%20Funding%20Mechanism%20for%20Sustaining%20Open%20Source%20Software%20for%20European%20Public%20Services.pdf

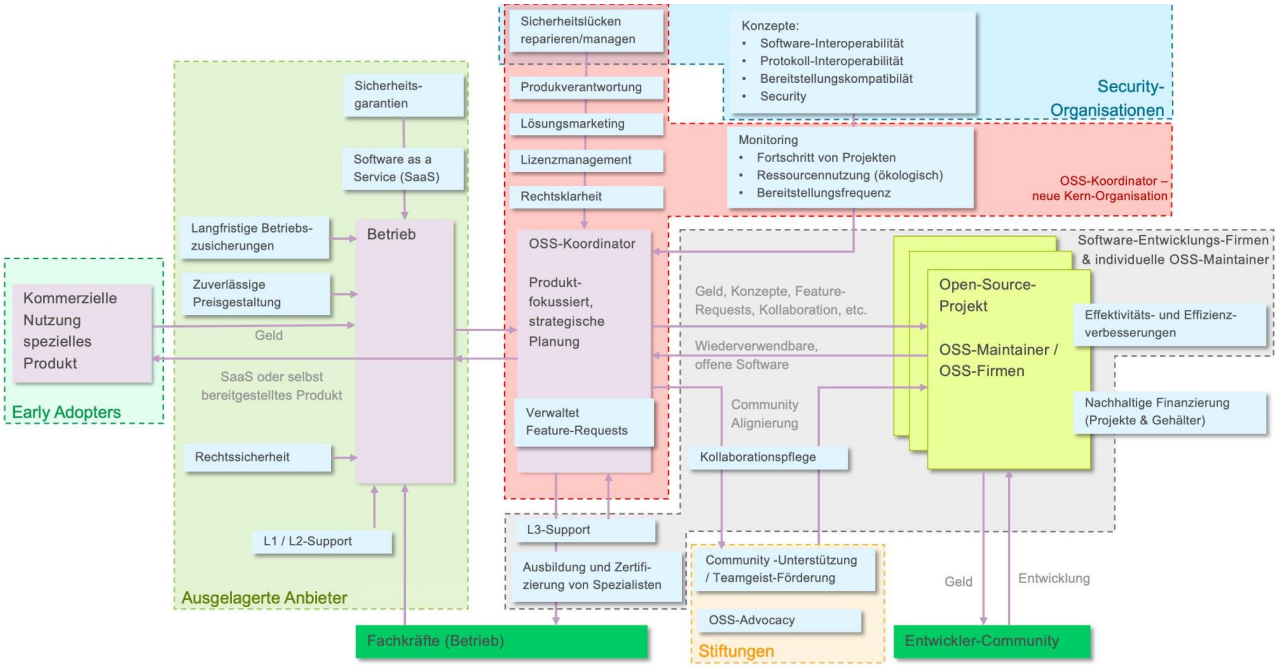

Abbildung 3: Vorgeschlagenes Ökosystem mit Geld- und Güterflüssen. Diese Arbeit fokussiert sich auf den OSS-Koordinator im Zentrum (in rot), welcher als zentrale Organisation die fehlenden organisatorischen Komponenten und Garantien bereitstellt und damit den Konflikt zwischen konkurrierenden Unternehmen und kollaborativer Software-Entwicklung überbrückt.

sich jedoch Ökosysteme unterschiedlicher Produkte überschneiden, da häufig dieselben Bibliotheken und Frameworks genutzt werden.

Der Kern des Referenzmodells ist die Etablierung einer neuen Art von Organisation, die – orientiert an den Marktanforderungen und im Interesse der Allgemeinheit – fehlende organisatorische Bausteine bereitstellt und belastbare Garantien für OSS schafft. Die Schaffung einer solchen Organisation leitet sich aus der Anforderung ab, dass langfristig resiliente Software-Lösungen ohne dauerhafte Bindung an bestimmte Anbieter betreibbar sein sollten. Voraussetzung hierfür sind austauschbare Komponenten, migrierbare Datenformate sowie offene Protokolle. Eine zentrale Organisation kann zudem den strukturellen Zielkonflikt zwischen konkurrierenden Unternehmensinteressen und kollaborativer Software-Entwicklung wirksam überbrücken.

Das vorgeschlagene Referenzmodell verfolgt darüber hinaus die folgenden Ziele:

Existenz von Software-Alternativen: Reduktion von Lock-In-Effekten, Flexibilität beim Betrieb von Software-Komponenten und Freiheiten über die abgelegten und prozessierten Daten, soweit gesetzeskonform.

Interoperabilität und Modularität: Austauschbarkeit von Infrastruktur-Komponenten dank offener Protokolle, Modularisierung und standardisierter Schnittstellen.

Sicherheit und Verfügbarkeit: Reduktion der Risiken bezüglich Ausfall, Datenabfluss und externer Manipulation der IT-Systeme und Technologien.

Digitale Nachhaltigkeit: Maximierung des Nutzens für die Gesellschaft.

6.1 Prinzipien des Ökosystems

Der OSS-Koordinator fokussiert sich auf die Regelung von Software-Entwicklung und Infrastrukturbetrieb und folgt im Idealfall den folgenden Prinzipien:

Markttauglichkeit und Finanzierung: Das Ökosystem muss sich langfristig selbst tragen können, mit finanziellen Anreizen, die eine wirtschaftlich lohnende Teilnahme gewährleisten.

Offenheit und Wettbewerb: Innovationszyklen werden beschleunigt und Lock-in-Effekte werden durch Interoperabilität und Kontrolle über Daten reduziert.

Nachhaltige Maintenance: Die langfristige Pflege bestehender Software – Sicherheitsupdates, Bugfixes, Anpassung an neue Abhängigkeiten – wird als eigenständige, finanzierungswürdige Leistung anerkannt und systematisch sichergestellt. Maintenance darf nicht dem Zufall oder dem Engagement einzelner Freiwilliger überlassen bleiben.

Komplette Transparenz: Alle Entscheidungen, Strukturen und Geldflüsse sind klar definiert und transparent. Missbrauch wird vermieden durch die Kontrolle seitens der OSS-Communities und zahlenden Nutzern.

Trennung von Entwicklung und Betrieb: Eine Entkopplung der Verantwortlichkeiten Entwicklung und Betrieb verringert die Abhängigkeit von wenigen Software-Anbietern, da weitere Akteure Dienstleistungen bereitstellen, was die Basis für eine souveräne IT-Infrastruktur schafft.

Mehrwert durch Einfachheit: Eine Vereinfachung der Software-Nutzung wird dank Klärung von Lizenz- und Kostenfragen erreicht.

Priorisierung durch Community: Wie Entwicklungsziele im Ökosystem priorisiert werden, ist noch nicht abschliessend geklärt. Der OSS-Koordinator nimmt eine zentrale Steuerungsrolle ein, was unweigerlich die Frage aufwirft, inwieweit Community und zahlende Nutzer tatsächlich Einfluss auf Entscheidungen haben — und wie Interessenskonflikte zwischen diesen Gruppen aufgelöst werden. Zudem ist fraglich, ob ein einheitlicher Priorisierungsmechanismus für alle Projekttypen und -grössen taugt. Diese Governance-Fragen müssen im Rahmen der weiteren Ausarbeitung der Förderstrukturen explizit adressiert werden.

Minimale administrative Hürden: Ermöglichen unkomplizierten Einstieg, schaffen Anreize für Beteiligungen und erlauben flexible Auszahlung finanzieller Kompensationen.

Serviceneutralität: Ermöglicht den Wechsel zwischen Betriebsanbietern und Software, ähnlich der Netzneutralität.

Kontrolle über Daten: Lösungen erlauben Datenextraktion und -migration. Die Trennung von Entwicklung und Betrieb ermöglicht zudem eine eigene Infrastruktur und volle Datenkontrolle.

Um eine angemessene Finanzierung zu erreichen, ist eine gezielte Unterstützung kleinerer Anbieter von Vorteil, da diese oft innovativer und ressourceneffizienter arbeiten können.[81]

Um kommerziellem Missbrauch der Förderstrukturen vorzubeugen, sind stabile Strukturen und umfassende Transparenz erforderlich; gleichzeitig müssen Entscheidungswege kurz bleiben, um übermässige Bürokratie zu vermeiden.

Politische Unterstützung ist dabei entscheidend, um die durch Marktdynamiken bedingten Abhängigkeitsverhältnisse zu verändern. Rechtliche Verpflichtungen und Lizenzkosten sind wesentliche Bestandteile des Ökosystems. Im extremen Krisenfall bleibt dank der Offenheit des Quellcodes der

[81] Siehe dazu den Forschungskorpus zum Stichwort *Diseconomies of Scale*.

zugrunde liegenden Software-Komponenten deren Verfügbarkeit dennoch gewährleistet. Ziel ist ein selbsttragendes Ökosystem, das – sobald es eine kritische Grösse erreicht hat – allen Beteiligten messbare Vorteile bietet, wie dies beispielsweise beim Linux Kernel der Fall ist. Solche Unterstützungsnetzwerke wie um den Kernel müssen gezielter aufgebaut und gefördert werden.

6.2 Ausgestaltung des Ökosystem

Das Ökosystem umfasst neben den Kunden und Nutzern von Software (links in Abb. 3) die folgenden Stakeholder:

Open Source Projekte und Entwickler (rechts): Zuständig für Entwicklung und Wartung der OSS, unterstützt durch konstanten und vorhersehbaren Geldfluss zur Planung und Sicherheitslückenbehebung sowie zur Funktionserweiterung.

Betrieb (links): Verantwortlich für Betrieb und Verfügbarkeit sowie rechtliche Sicherheiten der Software.

OSS-Koordinator (Mitte): Zentrale Organisation, welche die fehlenden organisatorischen Komponenten und Garantien bereitstellt und damit den Konflikt zwischen konkurrierenden Unternehmen und kollaborativer Software-Entwicklung überbrückt. Sie vermittelt zwischen Anbieter-, Kunden- und Entwicklerbedürfnissen, strukturiert OSS-Förderung und ist finanziert durch Feature Requests.

Unabhängige IT-Sicherheitsüberprüfer (oben): Überprüfen den Zustand der Software in der Organisation und unterstützen den Aufbau besserer Sicherheitsinfrastruktur.

Externe, nicht-profitorientierte Geldgeber (unten Mitte): Unterstützen besonders in traditionell finanziell schwachen Bereichen wie Vernetzung und Community-Aufbau.

Spezialisierte Fachkräfte (unten links): Aufbau eines Fachkräfte-Kontingents zur Technologie- und Betriebsanwendung in Unternehmen.

OSS Communities (unten rechts): Die Entwickler-Community ist zentral, oft ehrenamtlich organisiert und sollte explizit gefördert werden.

Die Förderstrukturen sollen OSS Communities und Entwickler nicht ersetzen, sondern gezielt unterstützen — insbesondere dort, wo der Markt derzeit keine ausreichenden Strukturen und Anreize bietet.

Der OSS-Koordinator übernimmt dabei eine vermittelnde Rolle zwischen Anbietern, Kunden sowie OSS Communities; er deckt dabei Aufgaben ab, die über die eigentliche Software-Entwicklung hinausreichen. Dazu gehören insbesondere die Integration geeigneter rechtlicher Strukturen, die Übersetzung von Marktanforderungen in Software-Funktionalitäten sowie das Management von Lizenzen. Ergänzend überwacht der OSS-Koordinator den Fortschritt von Vorhaben, schafft rechtliche Klarheit und koordiniert die Ausbildung sowie den Aufbau notwendiger Fachkompetenzen.

Sofern nicht anderweitig geregelt, stellt der OSS-Koordinator zudem strategische Übersicht, Koordination und Wissensaustausch mit Partnerorganisationen sicher und ermöglicht agile Anpassungen an Nutzer- und Entwicklerbedürfnisse, wie im EuroStack Governance Framework[82] beschrieben. Kontroll- und Auditfunktionen zur Sicherstellung von Transparenz und Rechenschaftspflicht sind ebenfalls integraler Bestandteil.

Eine weitere zentrale Aufgabe des OSS-Koordinators besteht darin, Fachkräfte bereitzustellen und zu vernetzen, die Systeme entwickeln und betreiben können. Obwohl grundsätzlich qualifizierte Fachkräfte verfügbar sind, fehlen bislang effiziente Strukturen für deren koordinierte Zusammenarbeit und Vermittlung.

[82] https://www.euro-stack.info/docs/EuroStack_2025.pdf

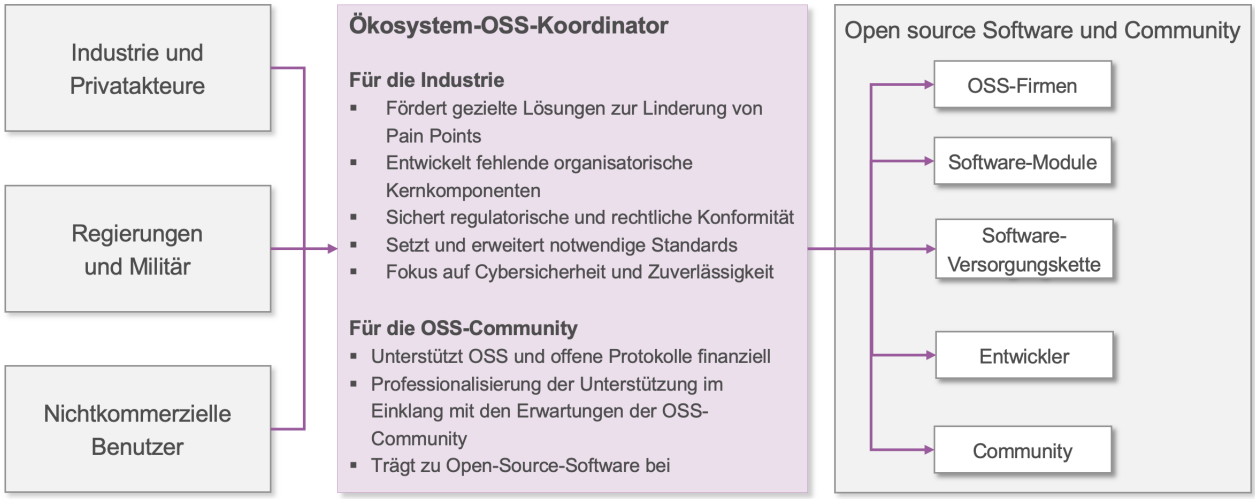

Abbildung 4: Der OSS-Koordinator dient als Brücke zwischen den unterschiedlichen Zielen der Welten: Markt (Ausschluss und Kontrolle) und Open Source (Kollaboration).

Darüber hinaus kann es sinnvoll sein, kommerzielle und private Nutzungen lizenzrechtlich unterschiedlich zu behandeln, um die Rechte von Entwicklern zu schützen und gleichzeitig die Verbreitung der Software zu fördern. Eine solche Differenzierung erhält den Wert der Software, ermöglicht ein niedrigschwelliges Ausprobieren und stärkt zugleich Weiterentwicklung und Innovation.

Damit das Ökosystem im profitorientierten Markt tragfähig funktionieren kann, müssen geeignete Anreizstrukturen geschaffen werden. Finanzielle Mittel sollen gezielt an Projekte fliessen, die das Software-Ökosystem wesentlich prägen, sei es durch breite Nutzung oder durch eine integrale Rolle innerhalb der Lieferkette. Als Mindestanforderung gilt dabei die nachhaltige Wartung der Software. Nutzer sollten zudem durch geeignete Lizenzbedingungen oder konkrete Vorteile dazu ermutigt werden, das Ökosystem auch für begleitende Dienstleistungen zu nutzen.

Zusätzlich sind Fördermittel für neue Technologien erforderlich, die entweder durch staatliche Programme oder durch Venture Kapital bereitgestellt werden können. Transparente und klar nachvollziehbare Geldflüsse innerhalb des OSS-Koordinators sind dabei essentiell. Über die Mittelverwendung und Verteilungskriterien soll gemeinsam mit der Entwicklungs-Community und den Nutzern entschieden werden, gestützt durch geeignete Verteilungsmetriken und Partnerschaften (vgl. Abschnitt 4.2.2).

Eine abflachende Verteilungskurve der Mittel kann zur Stabilität des Ökosystems beitragen: Kleinere Projekte werden stärker berücksichtigt, während grössere Projekte Anreize erhalten, modularer zu entwickeln. Dies fördert Wettbewerb, Wiederverwendbarkeit und Innovation.

6.3 Rolle der Cybersicherheit

Die Cybersicherheits-Community begrüsst offene Strukturen, da in solchen Umgebungen Sicherheitsprüfungen kosteneffizienter und einfacher durchgeführt werden können und Schwachstellen dank kollaborativer Prozesse häufig schneller behoben werden. Die beiden wesentlichen Tätigkeitsfelder entsprechender Experten umfassen zum einen die Verbesserung und Automatisierung von Sicherheitsüberprüfungen während der Softwareentwicklung und zum anderen das externe Testen fertiger Lösungen.

Die Auswirkungen des EU Cyber Resilience Act[83] (CRA) auf Open Source Software sind derzeit noch nicht abschliessend geklärt[84]. Der OSS-Koordinator kann jedoch als unterstützende Struktur dienen, indem es regulatorische Orientierung bietet und – wo erforderlich – finanzielle Unterstützung für Compliance- und Sicherheitsaufwände bereitstellt. Die daraus resultierenden, niedrigeren Sicherheitskosten könnten insbesondere Innovationen in KMU und Start-ups fördern.

Diese Bestrebungen werden durch das Ökosystem finanziert und können durch externe Geldgeber, wie Stiftungen oder staatliche Programme, zusätzlich gestärkt werden. Während die kontinuierliche Prozessverbesserung ein integraler Bestandteil wirksamer Cybersicherheit ist, sollte das nachgelagerte Testen als eigenständiger Aufgabenbereich betrachtet und entsprechend organisiert werden.

Das Testen erfolgt dabei in mehreren Schritten: Zunächst müssen Schwachstellen sowohl innerhalb der Softwarekomponenten des Ökosystems als auch in der zugrunde liegenden Infrastruktur systematisch identifiziert werden. Anschliessend ist die koordinierte Behebung der Schwachstellen sicherzustellen. Dies kann etwa durch die Information ehrenamtlicher Entwickler erfolgen, damit diese die notwendigen Patches erstellen. Alternativ können Entwickler vergütet werden, um Patches zur Verfügung zu stellen. Eine weitere Option besteht darin, die Behebung gemeinsam mit professionellen Anbietern zu koordinieren. In allen Fällen umfasst der Prozess auch die Überwachung des Fortschritts sowie die Qualitätssicherung der eingereichten Änderungen. Schliesslich ist eine abgestimmte Priorisierung der Testverfahren erforderlich, um Ressourcen effektiv und effizient einzusetzen.

Wesentlich ist dabei, dass nicht nur Schwachstellen identifiziert, sondern deren Behebung auch nachhaltig in die Code-Basis integriert wird. Dies wird durch die Offenheit der Software sowie den transparenten Zugang zu den relevanten Artefakten und Prozessen der Softwareentwicklung ermöglicht, oder durch Kollaboration mit Unternehmen, die bereits in die Entwicklung der Komponente involviert sind.

6.4 Rolle der Philanthropie

Philanthropie kann gezielt Aktivitäten fördern, die künftig strategisch relevant sind oder sich aufgrund ihres Wesens nur unzureichend über Marktmechanismen finanzieren lassen — insbesondere Community-Building und Advocacy. Eine unabhängige Finanzierungsquelle stärkt zudem die Resilienz des OSS-Koordinators und kann als ergänzender Mechanismus zur Sicherung von Neutralität und Kontrolle dienen. Vielversprechende Einsatzgebiete philanthropischer Mittel sind:

- Initiale Anschubfinanzierung zur Stärkung und Weiterentwicklung des OSS-Ökosystems und -Koordinators.
- Lageberichte zur aktuellen Situation sowie zur Bündelung und Übersicht laufender Aktivitäten.
- Potenzialanalysen sowie überzeugende Kennzahlen und Evidenz für Entscheidungsträger.
- Aufbau, Moderation und Verstetigung von Communities in priorisierten Lösungsgebieten.
- Nachgelagerte Massnahmen wie unabhängige Tests, Audits und Evaluierungen von Ökosystem und Software (z.B. Security-Testing).

6.5 Rolle des Staates

Analog zur Philanthropie kann der Staat die Anschubfinanzierung zur Stärkung des OSS-Ökosystems sicherstellen. Darüber hinaus kann er folgende Rollen einnehmen:

[83] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
[84] https://www.linuxfoundation.org/blog/understanding-the-cyber-resilience-act

- Gezielte Förderung relevanter Technologien und Systemarchitekturen, einschliesslich des Aufbaus entsprechender Fachkompetenzen.
- Analyse bestehender Abhängigkeiten und Bewertung der damit verbundenen Risiken sowie Integration der Erkenntnisse in Fördermassnahmen.
- Verknüpfung öffentlicher Beschaffungen und Aufträge mit Souveränitäts- und Offenheitskriterien, um das Ökosystem direkt oder indirekt zu fördern.
- Aufbau und Pflege internationaler Kooperationen zur Entwicklung souveräner und offener Lösungen.
- Sicherstellung der Krisenreaktionsfähigkeit bei Ausfällen und Bedrohungen, einschliesslich der Verfügbarkeit ausreichend qualifizierter Fachkräfte.

Die staatliche Förderung sollte das Open Source Ökosystem unterstützen, ohne es zu ersetzen oder zu kontrollieren. Unternehmen und Freiwillige treiben Innovationen voran, während staatliche Mittel Stabilität und Sicherheit gewährleisten sollten[85].

6.6 Rolle des NTC

Das NTC bringt sich in mehrfacher Hinsicht ein: (a) als unabhängige Testing-Organisation, welche entwickelte Software prüft und die Behebung identifizierter Schwachstellen aktiv begleitet, (b) als Interessensvertretung, die Cybersicherheitsaspekte in den politischen Diskurs einbringt, sowie (c) als Schlüsselpartner, der relevante Entscheidungsträger miteinander vernetzt.

Im Rahmen dieser Arbeit wurden bereits Gespräche zum Potential einer offenen Software-Infrastruktur geführt, die vom NTC gezielt weitergeführt werden können. Erste Ergebnisse dieser Gespräche sind in das vorliegende Diskussionspapier eingeflossen.

7 Relevanz der Künstlichen Intelligenz

Die Fortschritte im Bereich der Künstlichen Intelligenz verwandeln die IT-Landschaft in unbestreitbare Weise in Hinsicht auf Software-Entwicklung[86] und -Testing[87].

Die automatisierte Generierung von Software stellt keine tragfähige Alternative zum Einsatz von Open-Source-Lösungen dar. Auch bei einem Einsatz von generativer KI ist fundierte technische Expertise erforderlich, um qualitativ hochwertige, wartbare und sichere Software zu gewährleisten. Darüber hinaus führen die mit einer individuellen Weiterentwicklung und Instandhaltung verbundenen Kosten sowie der erhöhte organisatorische Aufwand in der Regel zu einer geringeren Wirtschaftlichkeit im Vergleich zu gemeinschaftlich entwickelter und gepflegter Open Source Software.

Während der Aufwand zur Behebung und Analyse von Sicherheitslücken langfristig zwar abnehmen dürfte, werden hingegen Anzahl und Komplexität der Angriffe voraussichtlich zunehmen. Somit wird sich die Dringlichkeit der im Diskussionspapier analysierten Problematiken mittelfristig wohl weiter verschärfen.

Daher sollte folgendes Dreigespann in Betracht gezogen werden: (a) Die Einrichtung einer dedizierten Forschungsstelle, die sich mit den Möglichkeiten zur gewinnbringenden Nutzung von KI zur Stärkung von Open Source Software und souveränen Ökosystemen beschäftigt. (b) Forschung zur Anwendung von KI bei der Erkennung von Schwachstellen im Code, sowohl beim Pushen als auch in

[85] https://dri.es/funding-open-source-like-public-infrastructure

[86] https://www.cnbc.com/2025/04/29/satya-nadella-says-as-much-as-30percent-of-microsoft-code-is-written-by-ai.html

[87] https://aisle.com/blog/aisle-discovered-12-out-of-12-openssl-vulnerabilities

bestehendem Code, um potenziellen Angreifern effektiv und rechtzeitig entgegenzuwirken. (c) Weitere Forschungsinitiativen zur Erkennung und Behebung bestehender Schwachstellen durch den Einsatz von KI-Technologien.

8 Empfehlungen

Basierend auf den Einsichten dieses Diskussionspapiers werden zusammenfassend die folgenden Punkte empfohlen. Die Empfehlungen richten sich primär an Schweizer Akteure, sind jedoch teilweise nur im europäischen oder internationalen Verbund wirksam umsetzbar — dies ist bei der Lektüre entsprechend zu berücksichtigen.

- Finanzierung der Folgearbeit dieses Diskussionspapiers, konkret die genauere Analyse der praktischen marktwirtschaftlichen Implikationen auf OSS sowie das daraus abgeleitete Target Operating Model des vorgeschlagenen Ökosystems.
- Durchführung eines Pilotprojektes als Proof of Concept in kleinem Rahmen zum Sammeln von Erfahrung und Etablieren eines Netzwerkes.
- Investition in Forschung, wie Dynamiken zwischen Open Source Software und dem Markt für Softwareprodukte heute funktionieren, zukünftig ausgestaltet werden können und wie die Gleichgewichte zu setzen sind. Dies schliesst insbesondere die Analyse von Anreizsystemen für ein funktionierendes Ökosystem mit ein.
- Investition in den aktiven Aufbau von Cybersicherheitskapazität, inklusive Testing, um nachhaltig stabile IT-Infrastruktur zu schaffen und zu betreiben. Für eine vereinfachte Umsetzung sollten offene Systemarchitekturen berücksichtigt werden.
- Investition in Forschung zum Verhältnis zwischen bezahlten und freiwilligen Entwicklern innerhalb von OSS-Projekten. Die Einführung bezahlter Arbeit in eine bestehende Freiwilligen-Community birgt erhebliche Risiken: Sie kann intrinsische Motivation verdrängen, Ungleichgewichte und Ressentiments erzeugen oder die Entwicklungsrichtung zugunsten der zahlenden Akteure verschieben — und damit die Community, die das Projekt erst ermöglicht hat, nachhaltig schädigen. Gleichzeitig sind finanzielle Anreize für eine professionelle Maintenance unerlässlich. Wie dieses Spannungsfeld konstruktiv aufgelöst werden kann, ist noch unzureichend verstanden und muss bei der Ausgestaltung des OSS-Koordinators explizit adressiert werden.
- Investition in Forschung zu offenen Lizenzrechtsfragen, die der Markt nicht von selbst löst: insbesondere zur rechtlichen Kompatibilität beim Kombinieren von Komponenten unter verschiedenen Lizenzen, zur empirischen Wirksamkeit neuer Hybridmodelle wie Fair Source oder Fair Core sowie zu praktikablen Methoden der Lizenz-Compliance für Unternehmen mit vielen OSS-Abhängigkeiten.
- Identifikation und Risikoanalyse von gesellschaftlich notwendiger IT-Infrastruktur durch staatliche oder staatsnahe Organisationen. Daraus sollten Strategien zur längerfristigen Digitalpolitik abgeleitet werden.
- Generell wirtschaftliche Förderung von Schlüsseltechnologien, Produkten und Unternehmen für offene Lösungen. Schaffen entsprechender Anreize und Ökosysteme. Förderung von Fachkräften und deren Vernetzung.

Diese Empfehlungen richten sich zwar an Stiftungen, privatwirtschaftliche sowie staatliche Organisationen, doch liegt im derzeitigen politischen und wirtschaftlichen Klima die Initiative primär beim Staat.

9 Weiteres Vorgehen und Ausblick

Auf dem Weg zu einem nachhaltig gestärkten OSS-Ökosystem sind die folgenden Schritte zu verfolgen:

Detaillierte Ausarbeitung des OSS-Koordinators: Im nächsten Schritt ist das Target Operating Model unter Einbezug der relevanten rechtlichen Strukturen, der Governance sowie der administrativen Anforderungen zu konkretisieren. Darüber hinaus ist durch die Durchführung einer Wirtschaftlichkeitsanalyse und die Etablierung geeigneter Transparenzmechanismen die Akzeptanz bei den beteiligten Stakeholdern sicherzustellen.

Ausarbeitung der Aufbaustrategie: Zudem ist die Grundfinanzierung zu sichern und eine Strukturierung der ersten organisatorischen Schritte sowie der wesentlichen Meilensteine vorzunehmen.

Aufbau strategischer Partnerschaften: Weiterhin ist die Integration wesentlicher Partner aus der Schweiz, der EU und dem europäischen Umfeld sicherzustellen, wobei Akteure aus Politik, Wirtschaft und der OSS-Community einzubeziehen sind.

Eine substanzielle Verbesserung der Benutzbarkeit offener Software dürfte deren Verbreitung massgeblich beschleunigen und zur Positionierung des Industriestandorts Schweiz als Technologiezentrum beitragen. Trotz vergleichsweise hoher Lohnkosten könnte die Schweiz aufgrund einer im Vergleich zur EU weniger ausgeprägten Regulierung einen attraktiven Standort für die Entwicklung und Steuerung eines OSS-Ökosystems darstellen.

Autoren

Dr. sc. ETH David M. Sommer: Cyber-Security Experte beim Innovationsdienstleister Zühlke, Product Owner und Tech Lead, engagiert bei der Digitalen Gesellschaft Schweiz, Fachexperte an der Fachhochschule Nordwestschweiz beim Studiengang Data Science, Organisator von mehrtägigen Events im Bereich Digitalisierung und Gesellschaft.

Florian Kubiak: Theoretischer Physiker und Programmierer in der Computersimulation und angewandter Statistik, engagiert in gesellschaftlichen Fragen rund um digitale Themen.

Dr. Raphael M. Reischuk: Mitgründer und Vorstandsmitglied des Nationalen Testinstituts für Cybersicherheit NTC, Mitglied des Innovationsrates von Innosuisse, Mitglied des Beirats Cybersicherheit der Schweizerischen Akademie der Technischen Wissenschaften SATW, sowie Partner beim Innovationsdienstleister Zühlke.