Sovereign Tech Agency

Dezember 2024

Stellungnahme
zum Fragenkatalog für die Öffentliche Anhörung “Open Source”
im Ausschuss für Digitales des Deutschen Bundestages
am 04. Dez 2024

Adriana Groh

CEO

Sovereign Tech Agency

Sovereign Tech Agency GmbH · Gartenstr. 7 · 10115 Berlin · www.sovereign.tech · info@sovereigntechfund.de
Geschäftsführung: Adriana Groh & Luisa von Beust
Amtsgericht Charlottenburg HRB 268739 · **USt-ID:** DE346614449 · **St-Nr**.: 231/105/18404
IBAN: DE95 3705 0198 1935 9416 80 · Sparkasse Köln Bonn · **BIC:** COLSDE33XXX

Sovereign Tech Agency

Frage 1) Welche Vor- und Nachteile hat Open Source-Technologie allgemein und besonders im Hinblick auf technische, sicherheitsrelevante, konzeptionelle, soziale, finanz-, außenpolitische und gesellschaftliche Aspekte? Welche der genannten Vor- und Nachteile kommen besonders zum Tragen, wenn Open Source-Technologien im staatlichen Kontext eingesetzt werden?

Freie und Open-Source-Software (FOSS) bildet das Fundament der digitalen Infrastruktur. Sie stellt die grundlegenden Technologien bereit, die die Entwicklung und Wartung anderer Software ermöglichen. Open Source spielt eine entscheidende Rolle in der Gestaltung der digitalen Landschaft und bietet insbesondere für staatliche Anwendungen erhebliche Vorteile – dort, wo Sicherheit, Resilienz und Souveränität von größter Bedeutung sind.

Open Source fördert Transparenz, Zusammenarbeit und Nachprüfbarkeit, indem sie es Regierungen ermöglicht, Quellcode einzusehen und anzupassen, um spezifische Anforderungen zu erfüllen, ohne von einzelnen Anbietern abhängig zu sein. Diese Flexibilität unterstützt die Interoperabilität durch die Einhaltung offener Standards, die für eine souveräne digitale Infrastruktur unverzichtbar sind. Allerdings erfordert die Integration und Wartung solcher Lösungen technisches Know-how und Ressourcen. Mit **70–90 % der modernen Software, die Open-Source-Komponenten enthält**, unterstreicht ihre Allgegenwärtigkeit ihre kritische Bedeutung.

Die offene Natur des Quellcodes ermöglicht eine globale Überprüfung, wodurch das Risiko versteckter Schwachstellen oder Hintertüren verringert wird. Diese Vorteile treten jedoch nicht automatisch ein; allein der Zugang zum Quellcode garantiert keine erhöhte Sicherheit. Laut dem **Open Source Security and Risk Analysis Report 2022** enthielten **81 % der geprüften Codebasen mindestens eine bekannte Schwachstelle**, was den Bedarf an gezielten Unterstützungsmechanismen wie dem Resilience-Programm der Sovereign Tech Agency verdeutlicht. Investitionen in die Verbesserung der Sicherheitslage, die aktive Einbindung der Community und die Einhaltung von Best Practices sind essenziell, um die Vorteile von Open Source voll auszuschöpfen.

Open Source reduziert die Anfangskosten erheblich, da Lizenzgebühren entfallen und die Abhängigkeit von einzelnen Anbietern verringert wird. Frankreich spart beispielsweise **50 Millionen Euro pro Jahr**, indem es Open-Source-IT-Infrastrukturen einsetzt. Eine **Studie der Harvard University** schätzt, dass die Nachbildung weitverbreiteter Open-Source-Software **4,15 Milliarden Dollar** kosten würde, während ein Ersatz durch proprietäre Alternativen **8,8 Billionen Dollar** erfordern würde – eine Einsparung von fast dem 3,5-Fachen der aktuellen Ausgaben für Software.

Über Kosteneinsparungen hinaus bietet Open Source gesellschaftliche Vorteile, indem es Inklusivität, Partizipation und Transparenz fördert. Initiativen wie das **UNESCO Open Solutions Program** zeigen, wie offene Technologien digitale Kluften überbrücken, marginalisierte Gemeinschaften stärken und gleichen Zugang zu Werkzeugen und Wissen sicherstellen können. Dennoch stellen Nachhaltigkeitsprobleme eine Herausforderung dar, da Open Source stark auf freiwillige Beiträge angewiesen ist. Programme wie das Sovereign Tech Fellowship adressieren diese Herausforderungen, indem sie Maintainer*innen und Mitwirkende langfristig unterstützen.

Aus einer außenpolitischen Perspektive verringert Open Source die Abhängigkeit von einzelnen Anbietern, stärkt die Autonomie und fördert gleichzeitig internationale Zusammenarbeit. National betrachtet minimiert die Unterstützung lokaler Open-Source-Ökosysteme Risiken, die mit externen Abhängigkeiten

verbunden sind. Allein in der EU trägt Open Source jährlich **65–95 Milliarden Euro** zur Wirtschaft bei und unterstreicht so seinen Wert für Innovation und das Gemeinwohl.

Indem Herausforderungen wie Nachhaltigkeit und Governance angegangen werden, kann Open Source weiterhin das Fundament für eine resiliente, sichere und inklusive digitale Infrastruktur bilden. Die strategischen Investitionen und Instrumente der Sovereign Tech Agency gewährleisten, dass diese Technologien auch für künftige Generationen erhalten bleiben.

Frage 2) Welche Voraussetzungen und Infrastrukturen braucht der erfolgreiche Einsatz von Open Source-Technologien im staatlichen Kontext?

Der erfolgreiche Einsatz von Open-Source-Technologien im öffentlichen Sektor erfordert eine robuste Infrastruktur und strategische Bedingungen, die eng mit dem Ziel der Erlangung digitaler Souveränität verknüpft sind.

Die wichtigste Maßnahme sind **nachhaltige Investitionen des öffentlichen Sektors in das Open-Source-Ökosystem**, das Lösungen für die öffentliche Verwaltung entwickelt und pflegt. Die Bundesregierung sollte Open Source in die routinemäßigen Beschaffungsprozesse integrieren. Durch die Umverteilung bestehender IT-Budgets können Ressourcen nachhaltiger genutzt werden, was die Kosten senkt und den Übergang zur digitalen Souveränität fördert. Diese Investition stärkt das Open-Source-Ökosystem und ermöglicht es Anbietern, kritische Technologien zu skalieren, zu innovieren und zu unterstützen.

Ein weiterer Eckpfeiler ist die **technische Bereitschaft**. Die Gewährleistung der Interoperabilität durch die Verwendung offener Standards und abwärtskompatibler Schnittstellen ist entscheidend für die Förderung der Integration und die Vermeidung von Anbieterabhängigkeit. Sicherheit ist ein weiteres wichtiges Anliegen; kontinuierliche Überwachung, regelmäßige Updates und zeitnahe Patches sind notwendig, um die mit jeder Software verbundenen Schwachstellen zu minimieren. Plattformen wie **Open CoDE, initiiert vom BMI**, die Zugang zu einer breiten Palette von Open-Source-Software bieten, senken die Eintrittsbarrieren und vereinfachen den Prozess der Beschaffung und Bereitstellung dieser Lösungen.

Der Rechtsrahmen für die öffentliche Beschaffung spielt ebenfalls eine entscheidende Rolle bei der Nutzung von Open-Source-Technologien. Priorisierungsrichtlinien, wie sie im **Thüringer Vergabegesetz** zu finden sind, zeigen, dass es sowohl machbar als auch vorteilhaft ist, Open-Source-Software den Vorzug zu geben, sofern sie die technischen und wirtschaftlichen Anforderungen erfüllt.

Ebenso wichtig für eine erfolgreiche Einführung von Open Source ist die **organisatorische Bereitschaft**. Der öffentliche Sektor muss die Flexibilität haben, den Anbieter zu wechseln, und die Fähigkeit besitzen, Software mitzuentwickeln oder an spezifische Bedürfnisse anzupassen. Diese Eigenschaften – in der **Marktanalyse 2019 des BMI** als Grundpfeiler der digitalen Souveränität identifiziert – unterstreichen die einzigartigen Vorteile von Open-Source-Software bei der Bewältigung dieser Herausforderungen. Langfristige Strategien sind unerlässlich, um die Nachhaltigkeit von Open-Source-Projekten zu gewährleisten. Initiativen wie das **Sovereign Tech Fellowship und das Munich Open Source Sabbatical**, die einzelne Maintainer*innen kritischer Open-Source-Projekte unterstützen, sind von unschätzbarem Wert, um die Stabilität dieser Technologien für die öffentliche Nutzung zu sichern.

Weiterführende Quellen:

- ZenDiS: Digitale Souveränität im Vergaberecht https://zendis.de/2024_06_05-zendis_positionspapier-dis-und-vergaberecht_a4_web.pdf
- IDABC European eGovernment Services: Guideline on public procurement of Open Source Software https://interoperable-europe.ec.europa.eu/sites/default/files/document/2011-12/OSS-procurement-guideline%20-final.pdf
- Frank Nagle (Harvard Business School): Government Technology Policy, Social Value, and National Competitiveness: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355486
- OSBA: Gutachten zur vorrangigen Beschaffung und Entwicklung von Open Source Software in der Bundesverwaltung https://osb-alliance.de/wp-content/uploads/2023/06/Studie-Wiebe-OSS-OSBA-Var8.pdf

- European Commission's Joint Research Centre: Assessing the interoperability of digital public services in the EU: the sooner, the better https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/assessing-interoperability-digital-public-services-eu-sooner-better-2024-05-24_en

Frage 3) Können Sie Beispiele für Open Source-Projekte nennen, die in den vergangenen Jahren besonders zum Gemeinwohl beigetragen haben und welche Erfolgsfaktoren und Best Practices lassen sich aus diesen Projekten ableiten? Im Gegenzug: Woran scheitern Open Source-Projekte und Projekte, die auf Open Source-Technologien aufbauen häufig? Welche Fallstricke sehen Sie?

Curl, ein Kommandozeilenwerkzeug und eine Bibliothek für Datenübertragungen, ist in Milliarden von Geräten eingebettet – sogar in mehreren Apps auf dem eigenen Smartphone – und damit unverzichtbar für Webdienste und alle Produkte mit digitalen Elementen. Curls Erfolg basiert auf starker gemeinschaftlicher Governance, umfangreichen Tests zur Sicherung der Zuverlässigkeit und seiner weiten Verbreitung dank der Open-Source-Lizenzierung.

Ähnlich verhält es sich mit **FFmpeg**, einer Sammlung von Tools zur Verarbeitung von Multimedia, die zahlreiche Plattformen unterstützt, da sie praktisch jedes Medienformat abdeckt. Die schnellen Veröffentlichungszyklen, umfassende Dokumentation und die offene Zusammenarbeit zwischen Expert*innen und der Industrie haben FFmpeg als Grundpfeiler der digitalen Infrastruktur etabliert. Genau diese Art der Zusammenarbeit ermöglicht Open Source.

Im Gegensatz dazu haben einige Open-Source-Projekte mit Schwierigkeiten zu kämpfen oder sind in bestimmten Fällen sogar gescheitert. Ein Beispiel ist **Log4j**: Die Entdeckung der „Log4Shell"-Sicherheitslücke hat die Risiken aufgezeigt, die mit der Abhängigkeit von unterfinanzierten und personell unterbesetzten Projekten verbunden sind, obwohl diese eine zentrale Rolle in Software-Ökosystemen spielen. Die Maintainer*innen konnten den Ressourcenbedarf für proaktive Sicherheitsmaßnahmen und Governance nicht decken, was zu weitreichenden Konsequenzen führte. Tatsächlich konnte erst zwei Jahre nach dem Vorfall, mit Investitionen des Sovereign Tech Fund, die Sicherheit von Log4j ausreichend verbessert werden, um das Risiko einer weiteren Schwachstelle wie Log4Shell zu minimieren. Bis dahin war keine andere Institution in der Lage, die dringend benötigten Ressourcen bereitzustellen.

Ein weiteres Beispiel ist das **Matrix-Protokoll**, ein technisch innovatives, dezentrales Open-Source-Kommunikationsprotokoll, das von vielen Organisationen, darunter auch öffentlichen Verwaltungen und der deutschen Bundeswehr, übernommen wurde. Doch ein Mangel an ausreichender Reinvestition in das Protokoll zwang die Maintainer*innen Ende 2023 dazu, eine weniger permissive Lizenz zu adoptieren. Während dies keineswegs ein Scheitern darstellt, war dieser Schritt notwendig, um den Ressourcenengpass zu bewältigen, und verdeutlicht die Herausforderungen, die mit der langfristigen Nachhaltigkeit offener digitaler Infrastrukturen verbunden sind.

Die Lehren sind eindeutig: Erfolgreiche Open-Source-Projekte gedeihen durch nachhaltige Finanzierung, proaktive Sicherheitsmaßnahmen und starke gemeinschaftliche Governance. Scheitern resultiert häufig aus Unterfinanzierung, fehlenden umfassenden Sicherheitsstrategien und Schwierigkeiten, technische Komplexität mit Benutzerfreundlichkeit in Einklang zu bringen. Diese Risiken müssen gemindert werden, indem Finanzierungsmechanismen gefördert werden, um Ressourcenengpässe zu beheben, wichtige Projekte aktiv unterstützen, regelmäßige Sicherheitsüberprüfungen für weit verbreitete Software vorschreiben und Best Practices in Governance und Entwicklung innerhalb des Open-Source-Ökosystems fördern.

Frage 4) Für wie relevant halten Sie das Problem des „Open-Washings“, in Anlehnung an „Greenwashing“, also vermeintliche Open Source Entwicklung, die dann schlussendlich doch wieder in proprietärem Code endet? Welche anderen Probleme sehen Sie bei der Entwicklung von Open Source Technologien?

Open-Washing ist ein Symptom oder ein spezifischer Fall einer größeren Debatte innerhalb der Open-Source-Community: Es gibt keine universell anerkannte Definition von „Open“ oder Offenheit. Während Open-Source-Lizenzen eine grundlegende Garantie für Transparenz und Zugänglichkeit bieten, schützen sie nicht unbedingt vor allen Formen von Missbrauch oder dem schleichenden Verlust von Offenheit. So verhindern zwar von der **Open Source Initiative (OSI)** genehmigte Lizenzen die rückwirkende Schließung von Open-Source-Software, aber zukünftige Entwicklungen oder Add-ons können proprietär sein. Außerdem ermöglichen **Contributor License Agreements (CLAs)** es Projektverantwortlichen, von der Community beigetragenen Code neu zu lizenzieren. Governance spielt hierbei eine entscheidende Rolle: Projekte können zwar formal als Open Source lizenziert sein, aber dennoch von einem einzigen Anbieter oder einer dominanten Instanz streng kontrolliert werden, was Fragen zur tatsächlichen Offenheit aufwirft. Diese Dynamiken erfordern eine differenzierte, fallbezogene Bewertung statt pauschaler Urteile.

Es ist auch wichtig, zwischen absichtlichem oder böswilligem „Open Washing“ und einer pragmatischen Entscheidung eines Projekts zur Änderung der Lizenzierung aufgrund eines Ressourcenmangels zu unterscheiden. In vielen Fällen, in denen Projekte ihre Lizenzierungsbedingungen ändern oder Einschränkungen einführen, geht es weniger um Täuschung und mehr um die Bewältigung eines strukturellen Ressourcenmangels. Die Open-Source-Infrastruktur leidet trotz weitverbreiteter Nutzung, insbesondere durch große Organisationen, unter chronischer Unterfinanzierung. Viele dieser Organisationen tragen nicht aktiv zur Weiterentwicklung der Technologien bei, die sie verwenden. Angesichts begrenzter Ressourcen und unzureichender Investitionen greifen einige Projekte zu Lizenzänderungen, um ihre Nachhaltigkeit zu sichern, während sie gleichzeitig versuchen, ein gewisses Maß an Offenheit zu bewahren. Diese Spannung spiegelt systemische Probleme wider und weniger eine grundsätzliche böse Absicht. Es gibt auch Beispiele, in denen Projekte später zu Open-Source-Lizenzen zurückgekehrt sind, nachdem sich ihre Ressourcensituation verbessert hatte.

Ein Beispiel dafür ist der Fall von **Redis Labs** im Jahr 2023. Das Unternehmen hinter der populären In-Memory-Datenbank Redis sah sich mit Konkurrenz durch große Cloud-Anbieter konfrontiert, die Redis als Service anboten, ohne aktiv zur Weiterentwicklung des Projekts beizutragen. Um diese Ressourcenschwäche zu beheben und die Nachhaltigkeit des Projekts zu sichern, änderte Redis Labs die Lizenz von einer Open-Source-Lizenz zu einer restriktiveren. Im Jahr 2024, nach Rückmeldungen aus der Community und der breiteren Industrie, kehrte Redis Labs schließlich zur Open-Source-Lizenz zurück. Diese Rückkehr erfolgte, nachdem das Unternehmen nachhaltigere Finanzierungsquellen und Partnerschaften aufgebaut hatte. Dieser Fall verdeutlicht die Komplexität des Themas und wie der Mangel an Ressourcen die Offenheit kritischer Komponenten beeinflussen kann.

Die Herausforderungen des „Open-Washing“ und verwandte Probleme machen letztlich deutlich, dass klarere Standards für Offenheit, mehr Investitionen in die Nachhaltigkeit von Open Source und gerechtere Governance-Modelle notwendig sind. Während Open-Source-Lizenzen eine solide Grundlage bieten, erfordert echte Offenheit eine Ausrichtung von rechtlichen, wirtschaftlichen und gemeinschaftlichen Praktiken, die Zugänglichkeit, Nachhaltigkeit, Interoperabilität und Fairness in Einklang bringen.

Transparenz in der Governance zu fördern, Finanzierungsmechanismen zur Überwindung von Ressourcenmängeln zu etablieren, sicherzustellen, dass offene Technologien auf offenen und interoperablen Standards basieren, sowie eine Kultur der offenen Zusammenarbeit anstelle eines „Wettbewerbs nach unten“ zu schaffen, sind entscheidende Schritte zur Stärkung des Open-Source-Ökosystems gegen solche Fallstricke.

Weiterführende Quellen:

- https://www.theregister.com/2024/09/12/redis_justifies_open_source_shift/

Frage 5) In welchem Zusammenhang stehen Open Source-Technologien und Fragen der digitalen Souveränität und wäre eine Bevorzugung von Open Source-Technologien in diesem Zusammenhang erstrebenswert – wo liegen konkret die Chancen und Risiken?

Was ist Open Source?

Freie und Open-Source-Software (FOSS) wird durch Lizenzen definiert, die den Benutzenden die Freiheit garantieren, den Quellcode einzusehen, zu ändern, zu verwenden und weiterzugeben. Diese Grundsätze stellen sicher, dass digitale Systeme **transparent, anpassungsfähig und interoperabel** sind, sodass Einzelpersonen, Regierungen und Unternehmen die Kontrolle über ihre Infrastruktur behalten können. Im Gegensatz zu proprietärer Software ist Open Source nicht an einen einzigen Anbieter gebunden, wodurch geschlossene Technologie verhindert und der Wettbewerb gefördert wird.

Die Rolle von Open Source in der digitalen Souveränität

Digitale Souveränität ist die **selbstbestimmte Nutzung digitaler Technologien und Systeme durch Einzelpersonen, Industrie und Regierungen** und ein entscheidendes Ziel für Deutschland und die Europäische Union in einer zunehmend digitalen und vernetzten Welt. Digitale Souveränität ist ohne Open Source nicht erreichbar.

Angesichts geopolitischer Spannungen und der Dominanz außereuropäischer Technologiegiganten ist Open Source unerlässlich, um kritische Infrastrukturen zu schützen und Unabhängigkeit zu gewährleisten. Die Transparenz von FOSS stellt sicher, dass Regierungen und Unternehmen die Kontrolle über ihre digitale Infrastruktur behalten, wodurch die Abhängigkeit von ausländischen Anbietern verringert und die Dominanz von Hyperscalern angegangen wird. Die Einhaltung **offener Standards** durch FOSS erleichtert die Interoperabilität und verhindert die Bindung an einen Anbieter – beides ist für die Selbstbestimmung im digitalen Bereich unerlässlich.

Darüber hinaus werden Open-Source-Projekte von **globalen Entwicklergemeinschaften** (Communitys) unterstützt, was schnellere Innovationen fördert und die mit proprietären Lieferketten verbundenen Risiken mindert. FOSS ist ein bewährter Motor für wirtschaftliches Wachstum, wobei Richtlinien wie die FOSS-Beschaffungsstrategie Frankreichs erhebliche Auswirkungen zeigen: mehr IT-Start-ups (+9 %–18 % jährlich), mehr IT-Beschäftigung (+6,6 %–14 %) und mehr Innovation (Nagle). Diese Eigenschaften machen Open Source zu einem **grundlegenden Bestandteil** für wirtschaftliche Widerstandsfähigkeit, demokratische Regierungsführung und Teilhabe im digitalen Zeitalter.

Warum die Bevorzugung von Open Source unerlässlich ist

Die Priorisierung von Open-Source-Technologien ist nicht nur wünschenswert, sondern unerlässlich, um digitale Souveränität zu erreichen. Open Source bietet die **Transparenz, Flexibilität und Unabhängigkeit**, die erforderlich sind, um die Kontrolle über digitale Systeme zu behalten. Diese Präferenz muss jedoch durch Folgendes unterstützt werden:

- **Strategische Investitionen**: Gezielte Finanzierung zur Gewährleistung der langfristigen Aufrechterhaltung und Nachhaltigkeit kritischer Open-Source-Projekte.
- **Kompetenzentwicklung**: Umfassende Schulungsprogramme, um öffentliche Verwaltungen mit dem Fachwissen auszustatten, das sie benötigen, um Open-Source-Lösungen effektiv zu übernehmen und zu verwalten.

- **Koordinierte Steuerung**: Starke nationale und europäische Steuerungsrahmen, um die Bemühungen zu vereinheitlichen, die gemeinsame digitale Infrastruktur zu stärken und eine Fragmentierung zu verhindern.

Um diese Ziele zu erreichen, sind neben der Sovereign Tech Agency weitere Initiativen erforderlich:

- **Ausbau der Finanzierungsmechanismen**: Etablierung nachhaltiger Finanzierungsmodelle zur Unterstützung der Wartung und Weiterentwicklung von Open-Source-Technologien, die für die öffentliche Infrastruktur von entscheidender Bedeutung sind.
- **Europäische Zusammenarbeit**: Ausweitung der Bemühungen auf ganz Europa, um kollektive Ressourcen zu nutzen, die grenzüberschreitende Zusammenarbeit zu fördern und die gemeinsame digitale Infrastruktur zu stärken.
- **Öffentliche Gelder, öffentlicher Code**: Institutionalisierung von Beschaffungspraktiken, die sicherstellen, dass öffentlich finanzierte Software offen, wiederverwendbar und zugänglich ist, um den gesellschaftlichen Nutzen zu maximieren.

Durch die Verankerung von Open Source als Eckpfeiler der öffentlichen Beschaffung und strategische Investitionen in sein Ökosystem können Deutschland und Europa widerstandsfähige, transparente und souveräne digitale Infrastrukturen schaffen. Open Source ist mehr als eine technische Lösung – es ist das Rückgrat der digitalen Souveränität.

Weiterführende Quellen:

- Frank Nagle (Harvard Business School): Government Technology Policy, Social Value, and National Competitiveness: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355486

Frage 6) Welche Vorteile oder Herausforderungen für die Verwaltungsdigitalisierung ergeben sich durch die Nutzung von Open Source-Technologien?

Open-Source-Technologien bieten erhebliche Vorteile für die Digitalisierung der öffentlichen Verwaltung. Open Source gewährleistet:

- **Flexibilität**, in dem es maßgeschneiderte Lösungen ermöglicht,
- **Interoperabilität**, für eine bessere Zusammenarbeit zwischen Behörden und Regierungsstellen,
- und mehr **Transparenz**, durch gemeinsames Schreiben und Pflegen des Codes

Entscheidend ist, dass Open Source die digitale Souveränität stärkt, indem es die Abhängigkeit von einzelnen Anbietern verringert, geopolitische Risiken mindert und der Bundesregierung mehr Kontrolle und Transparenz über die für die öffentliche Verwaltung entscheidende digitale Infrastruktur verschafft.

Die Vorteile der gemeinsamen Nutzung sind ein entscheidend. So ermöglicht beispielsweise das **„Einer-für-Alle-Prinzip“**, dass von einer Behörde entwickelte Lösungen von anderen wiederverwendet oder angepasst werden können, wodurch unnötige Kosten vermieden und die Digitalisierung der Verwaltung beschleunigt wird. Dieser Ansatz fördert die Zusammenarbeit und sorgt für eine schnellere Skalierung öffentlicher Dienste über verschiedene Zuständigkeitsbereiche hinweg.

Viele Open-Source-Projekte sind jedoch auf kleine, unterfinanzierte Entwicklergemeinschaften angewiesen, was Bedenken hinsichtlich der langfristigen Nachhaltigkeit aufwirft. Ohne strukturierte Steuerung kann es schwierig sein, in einem fragmentierten Markt zuverlässige Anbieter zu finden. Darüber hinaus fehlt den Mitarbeitenden der öffentlichen Verwaltung möglicherweise das Fachwissen, um Open-Source-Lösungen effektiv zu verwalten und zu warten.

Um diese Herausforderungen zu bewältigen, sollte die Bundesregierung **nachhaltige Investitionen in das Open-Source-Ökosystem** ausweiten und nicht nur Innovationen finanzieren, sondern auch die Wartung und die Menschen hinter dem Code unterstützen, wie die Sovereign Tech Agency bereits macht. Strukturierte Beschaffungsprozesse sollten Open-Source-Lösungen mit klaren Nachhaltigkeits- und Sicherheitsmaßstäben integrieren, damit Regierungen zu einem widerstandsfähigen und vielfältigen Ökosystem beitragen können. Initiativen wie **„Public Money, Public Code“** stellen sicher, dass öffentlich finanzierte Software das digitale Gemeinwesen bereichert und der Gesellschaft und der Wirtschaft zugutekommt.

Durch die Anerkennung von Open-Source-Software als kritische Infrastruktur kann die Bundesregierung transparente, effiziente und souveräne digitale öffentliche Dienste fördern.

Frage 7) Welche Vergabekriterien sollten im Vergaberecht mit Blick auf die Beschaffung digitaler Produkte und Dienstleistungen reformiert werden und welche Gründe sprechen dafür oder dagegen, hier einen Mindestanteil von Open Source-Technologien einzuführen?

Öffentliche Vergabegesetze sollten Kriterien priorisieren, die Transparenz, Interoperabilität und langfristige Nachhaltigkeit bei digitalen Produkten und Dienstleistungen fördern. Dazu gehört die Bevorzugung offener Standards, die Vermeidung von Vendor-Lock-in und die explizite Bewertung der Lebenszykluskosten von proprietären gegenüber Open-Source-Lösungen.

Die Einführung eines **Mindestanteils an Open-Source-Technologien** könnte ein starkes Bekenntnis zu digitaler Souveränität und Innovation signalisieren. Ein flexiblerer und gestufter Ansatz—wie die Berücksichtigung von Open Source in allen Vergabeprozessen und die Festlegung von schrittweisen Zielen (z. B. 20 % Open-Source-Nutzung bis 2025)—stellt jedoch sicher, dass die besten Lösungen gefunden werden, während der Wettbewerb erhalten bleibt.

Die Bundesregierung sollte Open-Source-freundliche Klauseln in die Vergabegesetze aufnehmen, wie sie beispielsweise im französischen Digitalministerium umgesetzt wurden. Reformen könnten Folgendes umfassen:

- **Public Money, Public Code**

Die Bundesregierung sollte sicherstellen, dass alle Softwareanpassungen und Neuentwicklungen, die mit öffentlichen Mitteln finanziert werden, unter einer Open-Source-Lizenz veröffentlicht werden. Der Quellcode sollte über Plattformen wie **Open CoDE** öffentlich zugänglich gemacht werden. Dies ermöglicht es anderen öffentlichen Institutionen, diese Lösungen wiederzuverwenden und weiterzuentwickeln, wodurch die Effizienz öffentlicher Mittel maximiert wird. Indem die Ergebnisse öffentlich finanzierter Softwareentwicklungen der breiten Gemeinschaft zur Verfügung gestellt werden, profitieren die Gesellschaft insgesamt und die Zusammenarbeit sowie Innovation im öffentlichen Sektor werden gefördert.

- **Digitale Souveränität als zentrales Vergabekriterium**

Digitale Souveränität—verstanden als die Fähigkeit, Software- und Cloud-Dienste frei zu nutzen, zu gestalten, anzupassen und zu kontrollieren—sollte als zentrales Kriterium in der öffentlichen Beschaffung etabliert werden. Open-Source-Lösungen und offene Standards sollten während des Vergabeprozesses höhere Bewertungspunkte erhalten, um sicherzustellen, dass sie mit den Zielen der digitalen Souveränität übereinstimmen. Diese Priorisierung stärkt die Kontrolle über kritische digitale Infrastrukturen und reduziert die Abhängigkeit von proprietären Anbietern, was die langfristige Resilienz und Anpassungsfähigkeit der öffentlichen IT-Systeme erhöht.

- **Verpflichtende offene und transparente Standards**

In öffentlichen IT-Beschaffungs- und Entwicklungsprojekten muss die Bundesregierung die Verwendung offener und transparenter Standards vorschreiben. Diese Anforderung stellt sicher, dass lokal entwickelte Software, die mit öffentlichen Geldern finanziert wurde, auch der lokalen Wirtschaft zugutekommt. Unternehmen können diese Software wiederverwenden, erweitern und zusätzliche Funktionalitäten anbieten. Eine solche Politik fördert Innovation, stärkt das heimische IT-Ökosystem und sorgt dafür, dass öffentliche Investitionen maximalen Nutzen für den öffentlichen Sektor und die Wirtschaft bringen.

Pro

Freie und Open-Source-Software (FOSS) fördert die digitale Souveränität, indem es die Abhängigkeit von proprietären Anbietern verringert, Transparenz durch öffentlich einsehbaren Code schafft und Innovation durch Zusammenarbeit vorantreibt. Forschung zur Open-Source-Vergabepolitik Frankreichs zeigt deren Vorteile: jährlich fast 600.000 zusätzliche Beiträge zu Open-Source-Software (im Wert von 20 Millionen USD) und ein erhebliches Wirtschaftswachstum, darunter ein jährlicher Anstieg der IT-Start-ups um 9–18 % und der IT-Beschäftigung um 6,6–14 %. Diese Ergebnisse zeigen, wie die Priorisierung von Open Source in der öffentlichen Beschaffung nicht nur das heimische IT-Ökosystem und die nationale Wettbewerbsfähigkeit stärkt, sondern auch globale Gemeingüter und Effizienz fördert.

Contra

Starre Quoten könnten die Flexibilität einschränken und proprietäre Lösungen ausschließen, die möglicherweise besser für spezifische Anforderungen geeignet sind. Sie könnten auch die Vergabeprozesse verkomplizieren und den Wettbewerb durch eine Verengung des Anbieterspektrums einschränken. Zudem erfüllen nicht alle Open-Source-Lösungen die Qualitäts-, Sicherheits- oder Supportanforderungen der öffentlichen Verwaltung. Um diese Herausforderungen anzugehen, könnte die Zertifizierung nachhaltiger und verlässlicher Open-Source-Anbieter—etwa durch das Zentrum für Digitale Souveränität (ZenDiS) in Zusammenarbeit mit dem Beschaffungsamt (BeschA)—sicherstellen, dass die öffentliche Verwaltung Zugang zu qualitativ hochwertigen und vertrauenswürdigen Optionen hat, während der Wettbewerb offen bleibt.

Weiterführende Quellen

- Frank Nagle (Harvard Business School): Government Technology Policy, Social Value, and National Competitiveness: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355486

Frage 8) Wie bewerten Sie die Fragen der Cybersicherheit im Kontext von Open-Source-Technologien, insbesondere mit Blick auf den Einsatz in öffentlichen Verwaltungen?

Die Sicherung von Software, ob Freie und Open-Source-Software (FOSS) oder proprietär, erfordert ähnliche Ansätze. Dies beinhaltet Investitionen in umfassende Sicherheitsmaßnahmen, einschließlich Code-Reviews, strenger Tests, Audits, Einhaltung von Standards und bewährten Best Practices sowie die Umsetzung solider Richtlinien für Contributions. Open-Source-Softwareprojekte, die bewährten Best Practices folgen, akzeptieren Contributions nicht blind. Genauso wie proprietäre Technologien innerhalb ihrer Organisationen gründlichen Qualitätssicherungsprozessen unterzogen werden, wenden gut gepflegte FOSS-Projekte ähnliche Sicherheitsvorkehrungen an, um Integrität und Sicherheit zu gewährleisten.

FOSS bietet jedoch einzigartige Sicherheitsvorteile für öffentliche Verwaltungen, wie z. B. die Möglichkeit, die Sicherheit eines Produkts unabhängig zu überprüfen und zu verifizieren. Diese Vorteile ergeben sich jedoch nicht automatisch; allein der Zugriff auf den Quellcode garantiert keine erhöhte Sicherheit. Investitionen in die Verbesserung der Sicherheitslage, aktives Engagement in der Community und die Einhaltung von Best Practices sind unerlässlich, um diese Vorteile zu genießen.

Die Sicherheitsstandards können sowohl bei Open Source als auch bei proprietären Technologien stark variieren. Mit der Einführung des Cyber Resilience Act (CRA) soll diese Variabilität durch die Einführung harmonisierter Sicherheitsstandards und Zertifizierungen in ganz Europa angegangen werden. Dadurch können öffentliche Verwaltungen und andere Nutzer*innen sichere digitale Produkte besser von weniger sicheren unterscheiden, was ein stabileres Tech-Ökosystem fördert.

Kleinere Open-Source-Projekte stehen vor besonderen Herausforderungen, vor allem wenn es darum geht, genügend Ressourcen bereitzustellen, um Sicherheitslücken in ihrer Software effektiv zu bewältigen. Durch die Erfahrungen der Sovereign Tech Agency mit dem Bug-Resilience Programm zum Schwachstellenmanagement konnten Dienstleistungen entwickelt werden, die diesen Projekten dabei helfen, widerstandsfähig und sicher zu bleiben. Eine weitere interessante Initiative in diesem Zusammenhang ist die Open Source Security Foundation (OpenSSF https://openssf.org), die Tools und Best-Practice-Verfahren für Open-Source-Projekte entwickelt, um deren Sicherheit zu gewährleisten. Öffentliche Verwaltungen sollten mit solchen Initiativen zusammenarbeiten, um sicherzustellen, dass die Projekte, auf die sie bauen, angemessen unterstützt werden und Sicherheitsanforderungen erfüllt werden.

Viele essenzielle Cybersicherheitstools und -komponenten zum Schutz vor digitalen Bedrohungen basieren auf Open-Source-Technologien, wie etwa Intrusion-Detection-Systeme, Schwachstellen-Scanner und Spam-Filter. Eine regelmäßige Wartung und ein reibungsloser Betrieb dieser grundlegenden Tools sind entscheidend für den Schutz der gesamten digitalen Infrastruktur. Angesichts der sich ständig weiterentwickelnden Bedrohungslage sind Investitionen in ihre Pflege und Weiterentwicklung unverzichtbar.

Frage 9) Welche Herausforderungen beim Thema Skalierung und Rollout von Open Source Software Projekten im staatlichen Einsatz sind Ihnen begegnet und welche strukturellen Maßnahmen schlagen Sie vor, um diesen zu begegnen?

Die Skalierung und Einführung von Open-Source-Projekten im staatlichen Einsatz ist oft mit Herausforderungen verbunden, die stark kontextabhängig sind, darunter fallen zum Beispiel komplexe Beschaffungsprozesse, organisatorische Kapazitäten und unterschiedliche Anwendungsfälle. Unsere Arbeit adressiert ein fundamentaleres Problem: die Abhängigkeiten innerhalb des Open-Source-Ökosystems.

Nicht nur Regierungen sind häufig auf kritische Open-Source-Projekte angewiesen, die von kleinen Teams oder einzelnen Freiwilligen betreut werden. Diese Abhängigkeit birgt Risiken wie Stagnation, verzögerte Aktualisierungen und Sicherheitslücken. Dabei sind diese Projekte keine isolierten Einheiten, sondern Teil eines komplexen Netzwerks von Abhängigkeiten, das tief in die Systeme des öffentlichen Sektors eingebettet ist. Digitale Software-Infrastruktur ist dabei als eine grundlegende, horizontale Ebene zu verstehen – eine essenzielle Basis, die den sicheren und nachhaltigen Einsatz von Software in allen Bereichen der Entwicklung und Nutzung trägt.

Um dieses Problem anzugehen, setzt die Sovereign Tech Agency sich für eine **gezielte Finanzierung zur Stärkung des gesamten Open-Source-Ökosystems** ein. Die Programme der Sovereign Tech Agency wie der Sovereign Tech Fund und das Sovereign Tech Fellowship bieten Modelle zur Unterstützung grundlegender Komponenten und ihrer Maintainer*innen. Ein ganzheitlicher Ansatz ist unerlässlich – die Vernetzung von Open-Source-Tools muss anerkannt und eine nachhaltige Finanzierung für kritische Abhängigkeiten sichergestellt werden.

Durch strategische Investitionen und enge Zusammenarbeit mit der Open-Source-Community können Regierungen stabile, interoperable und innovative Open-Source-Lösungen entwickeln und skalieren, die speziell auf die Bedürfnisse der öffentlichen Verwaltung zugeschnitten sind.

Frage 10) Welche vergaberechtlichen und verwaltungsrechtlichen Möglichkeiten werden derzeit nicht ausreichend genutzt, um den Einsatz von Open Source Software im staatlichen Bereich zu fördern und proprietäre Software perspektivisch durch quelloffene Alternativen zu ersetzen? Welche zusätzlichen gesetzlichen Vorgaben wären wünschenswert, um diesen Übergang zu unterstützen?

Ein zentraler Hebel zur Förderung von Freier und Open-Source-Software (FOSS) im staatlichen Bereich liegt in der Anpassung vergaberechtlicher Instrumente, um Basisinfrastruktur im Sinne der **digitalen Daseinsvorsorge** zu sichern. Open-Source-Software spielt eine entscheidende Rolle, um die technologische Souveränität und Unabhängigkeit des Staates zu stärken. Vor diesem Hintergrund sollte im Rahmen des geplanten Vergabetransformationspakets die einzigartige Rolle von FOSS in der digitalen Infrastruktur explizit berücksichtigt werden. Dies könnte durch die Integration von Kriterien zur digitalen Souveränität in die Leistungsbeschreibung sowie als Bestandteil der Zuschlagskriterien geschehen.

Frage 11) Welche Auswirkungen und Folgen sehen Sie voraus für den Fall, dass die Entwicklung und der Betrieb quelloffener Software als gemeinnütziger Zweck in der Abgabenordnung aufgenommen wird? Halten Sie dies für wünschenswert?

Die Anerkennung der Entwicklung und des Betriebs von Freier und Open-Source-Software (FOSS) als gemeinnützigen Zweck wäre ein wichtiger Schritt, um Open-Source-Projekte zu stärken, die dem öffentlichen Interesse dienen. Diese Projekte stellen wesentliche digitale Infrastrukturen bereit, die für Regierungen, Unternehmen und die Gesellschaft unverzichtbar sind – und das, ohne Gewinnabsichten zu verfolgen.

Eine Änderung der steuerlichen Regelungen könnte diesen Projekten und den Organisationen, die sie tragen, größere finanzielle Stabilität bieten und bestehende rechtliche Unsicherheiten beseitigen. Ein Beispiel hierfür ist die dezentrale Kommunikationsplattform Mastodon, die Open-Source-Software zum öffentlichen Nutzen und ohne Gewinnabsicht entwickelt, der jedoch im April 2024 von den Steuerbehörden ohne klare Begründung die Gemeinnützigkeit aberkannt wurde. Dieser Fall verdeutlicht eine potenzielle Regelungslücke, die solche Projekte anfällig macht. Eine Lösung dieses Problems würde ihre Resilienz stärken und die digitale Souveränität fördern, indem sie unabhängige, offene Technologien unterstützt, die dem Gemeinwohl dienen.

Die Sovereign Tech Agency erachten diese Maßnahme als wünschenswert, da sie dazu beitragen würde, die digitalen Gemeingüter zu sichern und weiterzuentwickeln.

Frage 12) Welche institutionellen Strukturen, wie z.B. Stiftungen oder NGOs wären im Bereich der Open Source Förderung wünschenswert und welche Aufgaben oder Ziele sollten diese hypothetischen Strukturen erreichen?

Wünschenswerte institutionelle Strukturen für die Finanzierung von Open-Source sollten die vielfältigen Bedürfnisse des FOSS- (Freie und Open-Source-Software) Ökosystems berücksichtigen. Dabei müssen zwei zentrale Prioritäten angegangen werden: eine stärkere finanzielle Unterstützung wichtiger Institutionen sowie der Aufbau vielfältiger Unterstützungsinitiativen, die auf die spezifischen Anforderungen der (FOSS)-Communitys zugeschnitten sind.

Zunächst ist ein stärkeres finanzielles Engagement für Organisationen wie die Sovereign Tech Agency, ZenDiS und ähnliche Einrichtungen in anderen Ländern sowie für supranationale Organisationen wie die EU und die UNO erforderlich. Regierungen, Unternehmen und Gesellschaften auf der ganzen Welt verlassen sich auf grundlegende Open-Source-Software. Für deren Wartung und Sicherheit sind alle gemeinsam verantwortlich. Die genannten Institutionen spielen eine entscheidende Rolle bei der gemeinsamen Unterstützung einer offenen digitalen Infrastruktur, der Förderung von Innovationen und der Stärkung der digitalen Souveränität auf nationaler und globaler Ebene.

Zweitens sind verschiedene Strukturen erforderlich, um den spezifischen Bedürfnissen der zahlreichen FOSS-Gemeinschaften gerecht zu werden. Dazu gehören:

- Administrative Dachorganisationen (Fiscal Hosts), wie die Software Freedom Conservancy, die Communitys ohne eigene rechtliche Strukturen dabei unterstützen, Spenden zu erhalten, Verträge abzuschließen und Ausgaben zu decken
- Unterstützende Organisationen, die Schulungen, Beratung und andere Dienstleistungen für Personen und Gruppen anbieten, die an kritischen Technologien arbeiten
- Stiftungen wie die Linux, Eclipse und Apache Software Foundations, die die erforderliche technische Infrastruktur, Unterstützung bei der Verwaltung und Fürsprache bieten,
- und gewinnorientierte Unternehmen wie die Mitglieder der OSBA, die ihre Geschäftsmodelle an Open-Source-Prinzipien ausrichten.

Insbesondere administrative Dachorganisationen (Fiscal Hosts) sind für eine effektive FOSS-Governance unerlässlich, da sie die Verwaltungskosten teilen, operative Unterstützung leisten und den Zugang zu Finanzmitteln und Ressourcen für Maintainer*innen and Mitwirkende verbessern.

Durch die Sicherstellung vielfältiger, gut finanzierter und kooperativer institutioneller Rahmenbedingungen kann die Sovereign Tech Agency Open-Source-Projekte besser unterstützen, Schwachstellen beheben und die Communitys unterstützen, die die grundlegenden Technologien für Innovation und Digitalisierung im öffentlichen Interesse entwickeln.

Frage 13) Sollte auf Bundesebene ein Open-Source-Advisory-Board initiiert werden, von dem aus auch OS-Entwicklungen monitored werden, um Probleme wie in der Vergangenheit (Log4j-Attacke) zu minimieren?

Ein Open-Source-Beirat auf Bundesebene ist möglicherweise nicht der effektivste Weg, um Open-Source-Entwicklungen zu überwachen und Herausforderungen wie die Log4j-Schwachstelle anzugehen. Bestehende Strukturen wie das CERT-Bund beim BSI und andere Programme sind bereits vorhanden, um Reaktionen auf Cybersicherheitsverletzungen auf Bundesebene zu koordinieren. Darüber hinaus wird das Open-Source-Ökosystem und kritische Infrastruktur bereits von der Sovereign Tech Agency überwacht. Sie verfügt über die erforderlichen Tools und Rahmenbedingungen wie z.B. das Resilience-Programm, um Probleme wie Unterversorgung und unzureichende Sicherheit bei der Open-Source-Entwicklung anzugehen. Das ZenDiS befasst sich mit der Frage, wie die Entwicklung von Open-Source-Software für die öffentliche Verwaltung sichergestellt werden kann.

Diese Organisationen verfügen über das Fachwissen und etablierte Verfahren zur Überwachung, Identifizierung und Minderung von Bedrohungen für die Softwareentwicklung, einschließlich, aber nicht beschränkt auf Schwachstellen in Open-Source-Software.

Die Sovereign Tech Agency ist der Meinung, dass der Schwerpunkt auf der Stärkung und Investition in bestehende Strukturen wie BSI, ZenDiS und die Sovereign Tech Agency selbst liegen sollte. Diese Behörden sind in der Lage, die Komplexität des Open-Source-Ökosystems und Bedrohungen von Cybersicherheit auf integrierte und effizientere Weise anzugehen. Daher würde eine Umverteilung von Ressourcen auf die bestehenden Mechanismen wahrscheinlich zu besseren Ergebnissen führen als die Einrichtung neuer Organe.

Frage 14) Inwiefern könnte Open Source-Software als Katalysator für innovative Ansätze in der Verwaltung fungieren? Welche neuen Dienstleistungen oder Modelle könnten durch Open Source realisiert werden, um die Bürger besser zu bedienen?

Freie und Open-Source-Software (FOSS) bietet Flexibilität, Transparenz und Zusammenarbeit und schafft so die Grundlage für innovative Ansätze im öffentlichen Sektor.

FOSS ist nicht nur eine Frage des Codes, sondern auch der ko-kreativen Form der Produktion. Der offene, gemeinschaftliche Entwicklungsprozess bringt Akteur*innen aus unterschiedlichen Bereichen zusammen – von Behörden über Unternehmen bis hin zu Zivilgesellschaft und Wissenschaft. Dieser kollaborative Ansatz fördert den Austausch von Wissen, das Teilen von Ressourcen und die gemeinsame Lösung komplexer Probleme.

Offene Standards erleichtern die Zusammenarbeit zwischen Behörden und ermöglichen maßgeschneiderte, anpassbare Lösungen anstelle starrer Einheitslösungen. Durch die Bereitstellung offener Daten und Quellcodes können Unternehmen, Forschungseinrichtungen und die Zivilgesellschaft innovative Anwendungen entwickeln, die Bürger*innen besser bedienen – etwa durch nutzerfreundliche Portale, transparente Informationsplattformen oder Werkzeuge für partizipative Verwaltungsprozesse.

Zudem erhöht Open Source die Transparenz, stärkt das Vertrauen der Bürger*innen und unterstützt eine nachhaltige, souveräne IT-Infrastruktur. So wird die Verwaltung effizienter, moderner und bürgernäher.

Frage 15) Bei der Entwicklung von Open Source Software (OSS) kann durchaus auch unbemerkt Schad-Software eingebaut werden, zB ist dann von sogenannter Protestware die Rede. Wie sicher ist OSS im Vergleich zu proprietärer Software, gibt es dazu empirische Befunde, wer haftet für etwaige Folgeschäden und mit welcher Zunahme von Protestware rechnen Sie, angesichts des allgegenwärtigen Aktivismus der sogenannten Zivilgesellschaft?

Bei Fragen wie diesen wird Open Source oft Closed Source gegenübergestellt, als gäbe es für Softwarenutzer*innen und -Entwickler*innen eine Wahlmöglichkeit. Wenn man über ein Grundverständnis für Softwarentwicklung verfügt, versteht man, dass dies aber für einen Großteil der genutzten Open-Source-Technologien nicht gilt. Es handelt sich um offene und frei zur Verfügung gestellte Basistechnologien, für die es keine proprietäre Alternative gibt - und auch niemals geben wird. Selbst wenn es nur ein Gedankenspiel ist: Die Kosten, um auch nur die kritischsten offene Technologien neu zu schreiben wären immens. Open Source ist die Grundlage einer digitalen Gesellschaft und in den meisten Fällen alternativlos. Diese Realität muss zunächst verstanden und anerkannt werden, dann können wir uns Gedanken darüber machen, wie diese kritischen Technologien sinnvoll absichert, unterstützt und mit den notwendigen Ressourcen ausstattet werden.

Open-Source-Software wird oft in einer kollaborativen Umgebung entwickelt, die Prozesse wie Peer-Reviews, kontinuierliche Integration und Tests umfasst. Obwohl es theoretisch möglich ist, Malware einzuschleusen, würde sie in den meisten Fällen entdeckt und behoben werden. In den Jahren 2022 und 2023 gab es einige Fälle, in denen populäre Softwarebibliotheken gelöscht oder beschädigt wurden. Diese „Protest-Aktionen“ kamen aber nicht von externen Akteur*innen, sondern von einzelnen Maintainer*innen, die die kleinen, aber weit verbreiteten Open-Source-Komponenten betreuten. Einzelverantwortlichkeiten bergen nicht nur ein Risiko der Sabotage, sondern auch viele anderen Risiken. Deshalb ist es so wichtig, sich auf die Governance von Open-Source-Software zu konzentrieren, um solche Szenarien zu vermeiden, indem Maßnahmen wie mehrere Maintainer*innen und ein formeller Überprüfungsprozess eingeführt werden.

Open-Source-Software ist nicht grundsätzlich sicherer oder unsicherer als proprietäre Software. Die Sicherheit hängt in beiden Fällen oft von der Einhaltung derselben bewährten Best Practices ab, wie z. B. Codeüberprüfung, Tests, die Verwendung derselben Entwicklungs-Tools wie Compiler und Virtualisierung sowie die Verwendung von Sicherheitstools wie Fuzzern, statischen Analysetools und Schwachstellenscannern – von denen viele selbst Open-Source basiert sind. Untersuchungen haben gezeigt, dass Open-Source-Komponenten 70–90 % der modernen Softwareanwendungen ausmachen, wodurch die Unterscheidung zwischen „offen“ und „proprietär“ zunehmend verwischt.

Es ist davon auszugehen, dass Fälle, in denen Malware unentdeckt in Open-Source-Software eingeschleust wird, mit der Einführung des Cyber Resilience Act, deutlich zurückgehen werden. Die Sicherheitsstandards im gesamten Software-Ökosystem werden durch das Cyber Resilience Act einheitlicher angewendet. Die Personen, die Open-Source-Software nutzen, werden sich auf eine höhere Sicherheit in der von ihnen angewendeten Software verlassen können. Diese neue Verordnung muss mit Investitionen in die Sicherheit kritischer Open-Source-Komponenten einhergehen, wie sie aktuell hauptsächlich nur von der Sovereign Tech Agency geleistet werden, um sicherzustellen, dass sie nicht zum Hindernis für Innovation und die Adoption von Open-Source-Software wird.

Frage 16) Die Bildgenerierungssoftware Stable Diffusion ist eine quelloffene Lösung, die ähnlich gute und verblüffende Ergebnisse liefert wie ihre proprietären Pendants; gleiches gilt für den Textgenerator Mistral. Wäre es aus Ihrer Sicht möglich, im Bereich generativer KI mit quelloffenen Lösungen die sich abzeichnenden Oligopole der großen Technologiekonzerne zu brechen?

Die Dominanz großer Technologie-Oligopole im KI-Bereich beruht nicht nur auf ihrer proprietären Lizenzierung, sondern auch auf ihrer Kontrolle über die Infrastruktur, die diese KI-Systeme antreibt. Unternehmen wie Amazon, Google und Microsoft beherrschen die Cloud-Computing-Infrastruktur – vor allem durch eigene Rechenzentren und Partnerschaften mit Cloud-Anbietern – und erschweren es damit Open-Source-Projekten erheblich, im großen Maßstab zu konkurrieren. Diese Unternehmen besitzen die umfangreichen Rechenressourcen, einschließlich spezialisierter Hardware wie GPUs und TPUs, die essenziell für das Training und den Betrieb großer KI-Modelle sind. Dadurch haben sie einen inhärenten Vorteil bei der Entwicklung und Bereitstellung fortschrittlicher KI und gestalten zugleich die wirtschaftlichen und technologischen Rahmenbedingungen, denen kleinere Akteure unterworfen sind.

Diese Infrastruktur ist nicht nur tief mit den KI-Modellen dieser Unternehmen verflochten, sondern überhaupt der Grund, warum solche Modelle existieren können. So stützt sich OpenAI stark auf Microsofts Azure-Cloud-Dienste, die die notwendige Rechenleistung für Modelle wie GPT bereitstellen. Diese Integration erlaubt es den Tech-Giganten, ihre Position nicht nur in der KI-Entwicklung, sondern auch in den Bereichen Hosting und Betrieb von KI-Diensten zu konsolidieren. Sie profitieren von einem erheblichen Vorsprung in diesem Bereich und verfügen über die finanziellen Mittel, ihre Dominanz langfristig zu sichern.

Selbst Lösungen wie Mistral und Stable Diffusion, die vergleichbare KI-Modelle produzieren können, bleiben stark von der Infrastruktur der großen Tech-Konzerne abhängig, wenn es um Skalierung und Einsatz geht. Dies untergräbt ihr disruptives Potenzial. Tatsächlich tragen diese Modelle oft zur wachsenden Dominanz der Big Tech bei, wie das Beispiel von Mistrals Partnerschaft mit Microsoft zeigt – ein Arrangement, das den Anschein von Open-Source-Fortschritt erweckt, letztlich aber dem Oligopol zugutekommt.

Die Herausforderung, die Dominanz von Big Tech im KI-Bereich zu brechen, liegt nicht darin, die ressourcenintensive, zentralisierte Infrastruktur dieser Unternehmen zu replizieren. Stattdessen sollte der Fokus auf der Förderung von Technologien liegen, die auf Dezentralisierung und Autonomie setzen und die Abhängigkeit von zentralisierten Systemen reduzieren. Dieses Konzept steht im Einklang mit der Idee eines „Eurostack“ – einem Rahmenwerk souveräner Technologien, das offene, verteilte und dezentrale digitale Anwendungen ermöglicht. Ein solches Modell fördert nicht nur die technologische Vielfalt, sondern auch die Entwicklung von Anwendungen, die Privatsphäre, Transparenz und Nutzerkontrolle priorisieren und damit der Dominanz dieser Technologiegiganten entgegenwirken.

Frage 17) Welche Barrieren sehen Sie gegen einen höheren Einsatz Open Source bei staatlichen Stellen, und wie bewerten Sie insbesondere folgende Barrieren:

- **„harte“ Lock-In-Effekte zum Beispiel durch technische Abhängigkeiten, wenn**
- **Hardware nur mit bestimmter Software läuft, oder Software nur mit bestimmter**
- **proprietärer Software interoperabel ist,**
- **weiche Abhängigkeitsfaktoren wie Gewöhnungseffekte,**
- **mangelnde IT-Kompetenz im Einkauf, was zur Verlängerung von Rahmenverträgen oder mehr Einkauf von Vertrautem führt, weil man Alternativen nicht kennt oder ihre Risiken überschätzt,**
- **mangelnde IT-Kompetenz im Betrieb, weil es weniger Erfahrung mit Open-Source-Dienstleistenden gibt,**
- **Folgen von Lobbyismus großer Hersteller proprietärer Software,**
- **fehlende Transparenz zum Einsatz von Open Source und proprietärer Software,**
- **mangelnde strategische Weitsicht beziehungsweise Überschätzung von kurzfristigem Nutzen bei Unterschätzung langfristiger Risiken?**

Um die Hindernisse für die Einführung von Open-Source-Software in der öffentlichen Verwaltung zu überwinden, ist ein schrittweises Vorgehen von entscheidender Bedeutung. Es ist wichtig, mit Bildungsinitiativen und strategischer Gesetzgebung zu beginnen, die Open-Source-Lösungen in überschaubaren Schritten fördern und dafür sorgen, dass die Anwender*innen Vertrauen in diese Technologien aufbauen.

Durch die Einführung kleinerer Open-Source-Projekte oder Pilotprogramme können Regierungen die praktischen Vorteile aufzeigen, wie z. B. verbesserte Transparenz, Sicherheit und Kosteneinsparungen. Weiterbildungen sind unerlässlich, um Beamten und Entscheidungsträger*innen das technische Wissen zu vermitteln, um Open-Source-Software effektiv zu bewerten und zu integrieren, und auch um den Widerstand aufgrund mangelnder Gewöhnung oder wahrgenommener Risiken zu überwinden. Darüber hinaus kann eine Gesetzgebung, die lokale Open-Source-Anbieter unterstützt und die Nutzung von Open-Source-Lösungen fördert, dazu beitragen, eine florierende lokale Wirtschaft rund um diese Technologien zu schaffen.

Die Stadt München dient als Beispiel für die Effektivität eines schrittweisen Übergangs zu Open-Source-Software. Anfänglich stieß die Stadt noch auf erheblichen Widerstand. Unter anderem verzögerte die Lobbyarbeit großer proprietärer Softwareunternehmen, die Implementierung der Open-Source-Lösungen. Trotz des Widerstands setzte die Stadt ihre Bemühungen um die Umstellung auf Open Source fort, was auch die Resilienz der Initiative untermalte. Durch die schrittweise Einführung von Open-Source-Tools, die Konzentration auf Interoperabilität und die Unterstützung lokaler Anbieter konnte München Vertrauen aufbauen und die langfristigen Vorteile der digitalen Souveränität aufzeigen. Obwohl der Fortschritt durch Lobbyarbeit zeitweise verlangsamt wurde, zeigen die anhaltenden Bemühungen der Stadt, dass

schrittweise Veränderungen, unterstützt durch Bildung und Gesetzgebung, immer noch zu einem erfolgreichen Übergang zu einer sichereren, kostengünstigeren und widerstandsfähigeren digitalen Infrastruktur führen können.

Weiterführende Quellen:

- Open Source Observatory der Europäische Kommission: Munich's Long History with Open Source in Public Administration https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/munichs-long-history-open-source-public-administration

18) Inwiefern kann eine Stärkung der Verbreitung von Open Source Anwendungen auch positive soziale Effekte haben und Grundrechte fördern, und welche Rolle spielen dabei und generell eine hohe Interoperabilität und Maßnahmen zur Erleichterung der Nachnutzung bereits existierender Open Source Software?

Die verstärkte Nutzung von Open-Source-Anwendungen, insbesondere offener digitaler Infrastrukturen, trägt erheblich zur sozialen Gerechtigkeit bei und fördert grundlegende Rechte, indem sie sicherstellt, dass kritische Technologien für alle zugänglich, sicher und transparent bleiben. Die Sovereign Tech Agency hat in mehrere Technologien investiert, die eine wichtige Rolle bei der Förderung digitaler Souveränität spielen und gleichzeitig Rechte wie Datenschutz, Meinungsfreiheit und den Zugang zu Informationen schützen. So wurde beispielsweise in ***OpenMLS*** investiert, das die Verschlüsselung in Gruppennachrichten verbessert und sicherstellt, dass Einzelpersonen sicher und privat kommunizieren können – ein grundlegendes Recht. Ebenso sind Technologien wie ***curl, rustls und PGP*** weit verbreitet und bilden das Rückgrat der digitalen Infrastruktur, die sichere digitale Interaktionen wie Online-Banking sowie die Bereitstellung von Sicherheitsupdates für Online-Produkte ermöglicht. Damit sind sie von entscheidender Bedeutung für das Recht auf Privatsphäre und Sicherheit.

Darüber hinaus befähigt die Verbreitung von Open-Source-Anwendungen mehr Menschen, aktiv als Gestalter*innen von Technologie aufzutreten und nicht nur als reine Nachnutzer*innen. Diese Mitgestaltung verändert, wer und wie unsere Gesellschaft digital prägt, und stärkt gleichzeitig das Vertrauen in digitale Systeme sowie den gesellschaftlichen Zusammenhalt.

Die Vorteile offener digitaler Infrastrukturen werden durch Interoperabilität und Wiederverwendbarkeit weiter verstärkt. Diese Eigenschaften fördern die positiven sozialen Effekte der Zusammenarbeit über verschiedene Gemeinschaften hinweg und verbessern zugleich die Sicherheit und Skalierbarkeit digitaler Lösungen. So wurde beispielsweise die ***ActivityPub Test Suite*** unterstützt, die die Interoperabilität zwischen dezentralen sozialen Netzwerken wie Mastodon oder Pixelfed, die das ActivityPub-Protokoll nutzen, verbessert. Dies stärkt die Möglichkeit für Nutzer*innen, plattformübergreifend Inhalte nahtlos zu teilen und zu kommunizieren, und fördert digitale Rechte wie die Meinungsfreiheit und den Zugang zu Online-Communities.

Durch die Unterstützung der Modernisierung von ***Fortran***, einer Programmiersprache, die zentral für die wissenschaftliche Forschung ist, trägt die Sovereign Tech Agency dazu bei, sicherzustellen, dass Werkzeuge zur Förderung von Wissen in Bereichen wie Gesundheitswesen und Klimawissenschaften offen und zugänglich für eine vielfältige und globale Gemeinschaft von Forschenden bleiben.