



**ARBEITSKREIS**  
OPEN SOURCE SOFTWARE



**PRÄSIDIUMSARBEITSKREIS**  
DIGITALE SOUVERÄNITÄT

Deutscher Bundestag

Ausschuss für Digitales

Ausschussdrucksache

20(23)307

77. Sitzung (öA) am 04.12.2024

02.12.2024

**01.12.2024**

## **Stellungnahme**

**der Arbeitskreise „Open Source Software“ und  
„Digitale Souveränität“ der Gesellschaft für Informatik e.V.**

**zum Fragenkatalog**

**Öffentliche Anhörung „Open Source“**

**Ausschuss für Digitales des deutschen Bundestags**

**am 04.12.2024**

**Im ersten Teil unserer Stellungnahme stellen wir die Gesellschaft für Informatik e.V, den GI-Präsidiumsarbeitskreis „Digitale Souveränität“ und den GI-Arbeitskreis „Open Source Software“ vor.**

**Im zweiten Teil betrachten wir die Problemfelder der massiven digitalen Abhängigkeit, die die Notwendigkeit des Einsatzes von Open Source Software begründen.**

**Im Teil 3 werden die Fragen des Fragenkatalogs aus fachlicher Sicht beantwortet.**

## 1. Über die Gesellschaft für Informatik e.V., den Präsidiumsarbeitskreis „Digitale Souveränität“ und den Arbeitskreis „Open Source Software“

Die **Gesellschaft für Informatik e.V. (GI)** ist mit mehr als 17.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatiker\*innen.

Mit [14 Fachbereichen](#), über [30 aktiven Regionalgruppen](#) und [unzähligen Fachgruppen](#) ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Präsidentin der GI ist Frau Regine Regitz.

Die zunehmende Abhängigkeit von großen Technologieanbietern bedroht unsere Digitale Souveränität sowie die wirtschaftliche und gesellschaftliche Stabilität: <https://gi.de/themen/beitrag/deutschland-als-digitale-kolonie>. Vor diesem Hintergrund hat das Präsidium der GI Mitte 2024 den **Präsidiumsarbeitskreis „Digitale Souveränität“** mit dem Sprecher Prof. Dr. Harald Wehnes, [wehnes@informatik.uni-wuerzburg.de](mailto:wehnes@informatik.uni-wuerzburg.de), eingerichtet.

Der **Arbeitskreis Open Source Software (AK OSS)** hat die Ziele, über Open Source Software (inkl. Hardware, Daten) relevante Themen zu informieren und zu beraten, ein Netzwerk für Gleichgesinnte zu schaffen, den Nachwuchs zu fördern, regelmäßig Veranstaltungen zu organisieren sowie wissenschaftlich fundierte Positionen für die Politik zu entwickeln und zu vertreten. Prof. Dr. Julian Kunkel, [julian.kunkel@gwdg.de](mailto:julian.kunkel@gwdg.de), ist der Sprecher dieses Arbeitskreises.

## 2. Digitale Souveränität oder digitale Kolonie? Problemfelder der digitalen Abhängigkeit

Expert:innen aus Wissenschaft und Wirtschaft warnen bereits seit Längerem davor, dass wir uns auf dem Weg in eine **digitale Kolonie** befinden. So betonte etwa der Wirtschaftsverband BITMi (Bundverband IT-Mittelstand) die wachsenden digitalen Abhängigkeiten, die ein „besorgniserregendes Ausmaß“ erreicht haben, und weist auf „konkrete Gefahren für unsere politische Selbstbestimmung“ hin.<sup>1</sup> Bitkom-Präsident Ralf Wintergerst wird ebenfalls deutlich: „Wir dürfen keine **digitale Kolonie** werden“, sagt der Chef des Digitalverbands zur Präsentation einer Studie, die genau das befürchten lässt.<sup>2</sup> Diese Zukunftssorgen und geopolitische Erpressbarkeitsszenarien nehmen immer realistischere Formen an.

In diesem Abschnitt werden die wichtigsten **Problemfelder der digitalen Abhängigkeit** beleuchtet. Nachfolgend werden Lösungsansätze vorgestellt.

### **Problemfeld 1: Die Datenfalle führt zum Verlust der Souveränität eines Landes**

In einem Interview mit der BBC<sup>3</sup> im Jahr 2021 beschreibt der britische Geheimdienstchef Sir Richard Moore, MI6, die Gefahren digitaler Abhängigkeiten. Dabei erklärt er die „Datenfalle“ wie folgt:

**„Wenn Sie einem anderen Land erlauben, Zugang zu wirklich kritischen Daten über Ihre Gesellschaft zu erhalten, wird das mit der Zeit Ihre Souveränität aushöhlen, da Sie keine Kontrolle mehr über diese Daten haben.“**

Die Datenfalle schließt sich zum Beispiel, wenn die Planungen einiger Bundesländer zur Migration in die Microsoft Cloud Azure verwirklicht werden. Durch diese Verlagerung öffentlicher Infrastrukturen und Daten in die Cloud eines US-Unternehmens unterliegen die Daten nicht nur den heimischen, sondern auch den Rechtsvorschriften der USA.

Der **US CLOUD Act**<sup>4</sup> ermächtigt US-Behörden, ganz legitim auch auf Daten zuzugreifen, die in Rechenzentren von US-Dienstleistern außerhalb der USA gehalten werden. Dabei sind diese Dienstleister zum Stillschweigen über Zugriffe verpflichtet! Wer Daten in diesen „Clouds“ speichert, verliert somit die Kontrolle über seine eigenen Daten. Er muss davon ausgehen, dass er damit ein hohes Risiko eingeht und unfähig wird, seine Zukunft selbständig gestalten zu können. Betriebsgeheimnisse und persönliche Daten könnten in falsche Hände geraten.

### **Problemfeld 2: Die Kostenfalle führt zu unüberschaubaren Dauer-Belastungen für die Haushalte des Bundes, der Länder und Kommunen**

Durch diese irreversible Abhängigkeit geht auch die Verhandlungsfähigkeit verloren. Es gibt keinen wirklichen Einfluss auf Vertragsinhalte und Konditionen. De facto muss zukünftig jedes Preisangebot und jede Preissteigerung akzeptiert werden. Das impliziert unüberschaubare Ausgabensteigerungen für die Haushalte des Bundes, der Länder und Kommunen. Auch Erpressungsszenarien sind nicht auszuschließen.

Die jüngsten Preiserhöhungen der marktbeherrschenden Virtualisierungssoftware VMware<sup>5</sup> verdeutlichen, wie Monopolstellungen wirtschaftlich ausgenutzt werden. Davon sind auch Bund, Länder und

---

<sup>1</sup> <https://www.bitmi.de/offener-brief-digitale-abhaengigkeiten>

<sup>2</sup> <https://www.rnd.de/wirtschaft/digitalimporte-aus-china-und-den-usa-firmen-ueber-deutsche-abhaengigkeit-besorgt-CWZHOHBJSJBDPFA5MUXRO2OINQ.html>

<sup>3</sup> <https://www.bbc.com/news/uk-59474365>

<sup>4</sup> <https://www.justice.gov/criminal/cloud-act-resources>

<sup>5</sup> <https://www.golem.de/news/preiserhoehung-bei-vmware-nutzer-kritisieren-verachtung-und-brutalitaet-von-broadcom-2404-184194.html>

Kommunen erheblich betroffen<sup>6</sup>. Die Nutzer beschwerten sich anlässlich **bis zu zwölffacher Preiserhöhungen** über „Verachtung und Brutalität“ von Broadcom.

Bei den Microsoft Produkten besteht ebenfalls eine extrem hohe Abhängigkeit der Bundesverwaltung, wie der Abschlussbericht der PwC-Marktanalyse<sup>7</sup> „zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern“ dokumentiert, der im Auftrag des BMI erstellt wurde. Allein im Zeitraum von 2015 bis 2021 (sieben Jahre) haben sich die Ausgaben der Bundesverwaltung für Microsoft fast verfünffacht<sup>8</sup>.

Mitte November 2024 hat **Microsoft Preiserhöhungen von bis zu 40 %** angekündigt<sup>9</sup>. Aufgrund der Abhängigkeit besteht de facto kein Verhandlungsspielraum, d.h. jeder Preis und jede Vertragskondition muss akzeptiert werden. Wenn hier nicht zeitnah – z.B. durch den Einsatz von Open Source Produkten –entgegengesteuert wird, kommen in den nächsten Jahren unüberschaubare Dauerkosten auf die öffentlichen Haushalte zu. Die Microsoft-Lizenzkosten belasten inzwischen viele Unternehmen, u.a. den Kliniksektor: „Was Microsoft ab 2025 für die Bereitstellung seiner Softwarelizenzen vorsieht, könnte Betriebe des Gesundheitswesens an den Rand ihrer finanziellen Möglichkeiten bringen.“<sup>10</sup>

### **Problemfeld 3: Die Datenmissbrauchsfälle**

In der ZDF-Dokumentation „Wie Amazon seine Konkurrenz zerstört“<sup>11</sup> wird belegt, wie z.B. Amazon systematisch **vertrauliche Daten von Anbietern**, die in Amazon Rechenzentren (AWS) gespeichert werden, auswertet, Kopien der Produkte herstellt und diese „Eigenprodukte“ aggressiv auf der eigenen Plattform vermarktet. Kein Einzelfall, wie auch von Reuters<sup>12</sup> umfassend nachgewiesen wurde.

Es stellt sich daher auch die Frage, inwieweit vertrauliche Daten in den Rechenzentren von Microsoft und Co. ausreichend vor Missbrauch geschützt sind. Auch Behörden speichern dort sensible Daten über Bürger und Unternehmen, z.B. Finanzämter.

Unternehmen, die ihre Geschäfts- und Prozessdaten in den Rechenzentren (Clouds) von außereuropäischen Hyperscalern speichern, gefährden ihre Existenz. **Am gefährdetsten sind die deutschen Weltmarktführer.**

Einen einzigartigen Einblick in den globalen Datenhandel gibt ein Dokument, das von netzpolitik.org analysiert und veröffentlicht wurde<sup>13</sup>. Über Microsofts Datenmarktplatz Xandr können Werbetreibende **Personendaten kaufen** und dabei die Personengruppe im Detail beschreiben, bspw. mit "Gebrechliche Senioren", "LGBTQ" oder "Moms who shop like crazy". Es gibt auch Listen zu Einkommen, Militäranghörigkeit und psychischer Gesundheit.

### **Problemfeld 4: Versteckte Sicherheitsprobleme und mangelnde Kommunikation; selbst US-Behörden sind alarmiert über Microsofts Sicherheitslücken in der Cloud**

Selbst das Vertrauen der US-Behörden in Microsoft scheint durch massive Sicherheitsprobleme und mangelhafte Kommunikation<sup>14,15</sup> erschüttert zu sein. Die Cyber Security and Infrastructure Security

---

<sup>6</sup> <https://netzpolitik.org/2024/digital-unsouveraen-bundesregierung-legt-sich-an-broadcoms-kette/>

<sup>7</sup> [https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/marktanalyse-reduzierung-abhaengigkeit-software-anbieter.pdf?\\_\\_blob=publicationFile&v=2](https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/marktanalyse-reduzierung-abhaengigkeit-software-anbieter.pdf?__blob=publicationFile&v=2)

<sup>8</sup> <https://www.spiegel.de/wirtschaft/kosten-fuer-microsoft-softwarelizenzen-des-bundes-seit-2015-fast-verfuenffacht-a-e685382a-e694-4748-bb66-e191a00e468e>

<sup>9</sup> <https://www.heise.de/news/Bis-zu-40-Prozent-teurer-Microsoft-plant-saftige-Preiserhoehungen-10039322.html>

<sup>10</sup> <https://ap-verlag.de/softwarelizenzen-microsoft-lizenzkosten-belasten-den-kliniksektor/89265/>

<sup>11</sup> <https://www.youtube.com/watch?v=ieOgOESfU0U>

<sup>12</sup> <https://www.reuters.com/investigates/special-report/amazon-india-rigging/>

<sup>13</sup> <https://netzpolitik.org/2023/microsofts-datenmarktplatz-xandr-das-sind-650-000-kategorien-in-die-uns-die-online-werbeindustrie-einsortiert/>

<sup>14</sup> <https://www.heise.de/hintergrund/Gestohlener-Master-Key-Der-kleingeredete-GAU-der-Microsoft-Cloud->

Agency (CISA) – amerikanisches Pendant zum BSI – hat die Directive "ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System" erlassen. Diese verdeutlicht, dass fremde staatliche Akteure in Microsofts E-Mail-Systeme über längere Zeit eindringen konnten. Nach wie vor ist unklar, ob die Risiken vollständig beseitigt sind<sup>16</sup>.

### **Problemfeld 5: Steuervermeidungsstrategien der digitalen Monopole**

Durch die intensive Nutzung von Produkten digitaler Monopolisten verlieren wir unsere Fähigkeit, die digitale Transformation selbstbestimmt zu gestalten. Die lokale Wertschöpfung verringert sich. Statt Steuereinnahmen werden verstärkte wirtschaftliche Abhängigkeit und Erpressbarkeit generiert. Die Steuervermeidungsstrategien der digitalen Monopole sind hinreichend bekannt. Für 44 Milliarden Euro Umsatz in Europa im Jahr 2020 hat Amazon keinen Cent Steuern gezahlt<sup>17,18</sup>.

### **Problemfeld 6: Ausbau der Monopolmacht auf weitere Wirtschaftssektoren**

Mit der enormen Finanzmacht können die digitalen Monopole Millionen für Lobbyarbeit ausgeben und damit die Gesetzgebung beeinflussen. Dies belegt die von Lobby Control durchgeführte Studie „Lobbymacht von Amazon, Google & Co. wird immer größer“. Mehr als 113 Millionen Euro jährlich gibt die Digitalindustrie allein für Lobbyarbeit in Brüssel aus<sup>19</sup>.

Hinzu kommt, dass die digitalen Monopole ihre Marktmacht rasant auf weitere Wirtschaftssektoren wie Medien, Banken, Bezahldienste, Logistik, Gesundheitswesen, Bildung usw. ausdehnen und auch hier immer dominanter werden. Damit einher gehen der Verlust von Wettbewerbsfähigkeit, Wertschöpfung, Wachstum und Wohlstand, was zwangsläufig zu sinkenden Steuereinnahmen und Beiträgen für die Sozialkassen führt.

### **Fazit:**

1. Für die Politik besteht dringender Handlungsbedarf, um die digitale Zukunftsfähigkeit von Deutschland zu sichern.
2. Lösungen bieten Open Source Software-Produkte sowie Software-Produkte „Made in D/EU“ – betrieben in eigenen Rechenzentren (on-prem) oder in Rechenzentren, die europäischem Recht unterliegen und von Firmen mit europäischem Firmensitz betrieben werden.
3. Der Staat muss sein Einkaufsverhalten ändern:  
Der Erwerb von Produkten, die digitale Souveränität fördern, muss Priorität haben vor dem Erwerb von Produkten von digitalen Monopolen, die unsere Abhängigkeit verstärken und zugleich Wettbewerb sowie lokale Wertschöpfung verhindern. Insbesondere sollte vom Staat geförderte Open Source Software, wie z.B. open-Desk und Sovereign Cloud Stack (SCS), von ihm selbst als „Ankerkunde“ - wann immer möglich - eingesetzt werden. Damit stellt er zugleich die Nachhaltigkeit der Förderung mit Steuermitteln sicher.

---

[9234601.html?seite=all](#)

<sup>15</sup> <https://www.heise.de/news/Nach-Microsoft-Hack-muessen-US-Behoerden-gross-aufraeumen-9682556.html>

<sup>16</sup> <https://www.heise.de/news/Nach-Microsoft-Hack-muessen-US-Behoerden-gross-aufraeumen-9682556.html>

<sup>17</sup> <https://kurier.at/wirtschaft/amazon-bezahlte-im-coronajahr-keine-koerperschaftssteuer-in-europa/401371661>

<sup>18</sup> <https://www.heise.de/news/Alle-Jahre-wieder-Alphabet-spart-weiter-Steuern-in-Milliardenhoehe-4266075.html>

<sup>19</sup> [https://www.lobbycontrol.de/macht-der-digitalkonzerne/lobbymacht-von-amazon-google-co-wird-immer-groesser-111173/?mtm\\_campaign=2023-10-02&mtm\\_kwd=digital-1](https://www.lobbycontrol.de/macht-der-digitalkonzerne/lobbymacht-von-amazon-google-co-wird-immer-groesser-111173/?mtm_campaign=2023-10-02&mtm_kwd=digital-1)

### 3. Beantwortung des Fragenkatalogs

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?

Die **Vorteile** liegen

a) in der **intrinsischen Eigenschaft** einer grundsätzlichen **Wiederverwendbarkeit** von Open Source Software und damit einem erheblich **geringeren Risiko** für **Monopolbildungen**, da Softwarefirmen Support als auch Weiterentwicklungsdienste anbieten können, sowie

b) in der Zugänglichkeit des Codes für Prüfungen und dem „**mehr Augen**“-Prinzip bei der Erstellung, das bei korrekter Anwendung zu einem erheblich höheren **erreichbaren Sicherheitsniveau** führen kann.

c) in der – insbesondere im öffentlichen Verwaltungssektor – möglichen **Bündelung von Entwicklungsressourcen**, um ein Gegengewicht zu den dominierenden Marktführern aufbauen zu können. Aufgrund der (zumindest formal) fehlenden Konkurrenz zwischen den öffentlichen Dienststellen könnten Ressourcen aus einem großen Kreis von Entwicklern an einem gemeinsamen Code arbeiten. Sobald die Zahl der Nutzer pro „Zeile Code“ in die Größenordnung von proprietären Anwendungen kommt, wird ein **schnelles Aufholen** ohne weiteres **möglich**. Das Einer-für-alle-Prinzip wird somit auf ein „**Alle für Alle**“-Prinzip erweitert, was die Akzeptanz der Arbeitsergebnisse deutlich erhöhen kann (=> Partizipation als Akzeptanzfördernde Maßnahme). Ebenfalls könnten Entwickler bei Behörden als auch unabhängige Softwarefirmen die speziellen Anforderungen der Behörde in Open Source Software integrieren.

d) Open Source fördert zudem die **Zugänglichkeit von Informatikfragestellungen** in der Gesellschaft insgesamt und kann so zur Ausbildung von Programmierkenntnissen als Grundlage zukünftiger Technologiebeherrschung („**fünfte Grundrechenart**“, MINT-Förderung) dienen.

Die **Nachteile** liegen

a) in einer **möglichen Verantwortungsdiffusion** unter den Entwicklern, wenn die Code-Entwicklung als „Hobby“-Aktivität, ohne finanzielle Kompensation und ohne Kontrolle ausgeführt wird. Durch Finanzierung kann dies vermieden werden!

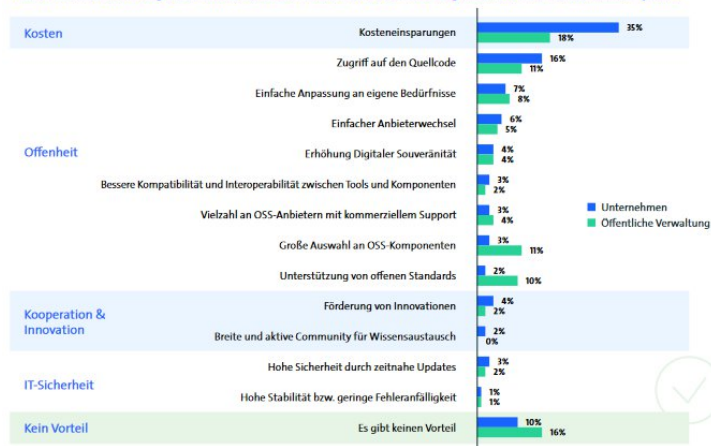
b) das zugrundeliegende Hierarchiemodell („**Meritokratie**“) **fördert die Durchsetzung von „Fleißigen“**, aber **nicht** unbedingt von **begabten** Mitentwicklern. Dies ist aber für eine **langfristige Stabilität des Codes** unter den sich ändernden Nutzungsbedingungen und Anforderungen (Erweiterbarkeit etc.) unabdingbar. Diese Kompetenz muss also gezielt gefördert werden. In einem professionalisierten Open Source Entwicklungsmodell würde deshalb ein **paritätisches Gremium mit hoher Architekturkompetenz** nicht nur die Anwendung selbst (bzgl. ihrer Architekturqualität) prüfen, sondern auch die beteiligten Personen bzgl. deren Fähigkeiten beaufsichtigen. Gegenseitige Begutachtung der Fähigkeiten findet zwar auch in der Meritokratie statt, jedoch geschieht dies nicht explizit. Durch die Etablierung von Governance-Strukturen kann dieser Nachteil vermieden werden.

c) analog zu proprietärer Software, gibt es die **Gefahr** von **gezielt eingebrachten Schwachstellen** durch staatliche oder private kriminelle Akteure. Um hier auf das Sicherheitsniveau zu erhöhen kann im Gegensatz zu proprietärer Software :

- die **Provenienz-Kontrolle** (Verifikation des Autors jeder Zeile Code und deren Änderungshistorie) konsequent professionalisiert werden => Aufgabe für Open CoDE
- die **kontinuierliche** Prüfung der **beteiligten Personen** erfolgen (siehe Sicherheitsüberprüfung Ü1-Ü3). Dies muss bei sicherheitskritischen Anwendungen durch den übergeordneten Träger des Projektes erfolgen.

Die Bitkom Studie „Open Source Monitor“<sup>20</sup> von 2023 gibt einen sehr guten aktuellen Überblick über die Vor- und Nachteile von OSS im Unternehmenseinsatz und in der Öffentlichen Verwaltung:

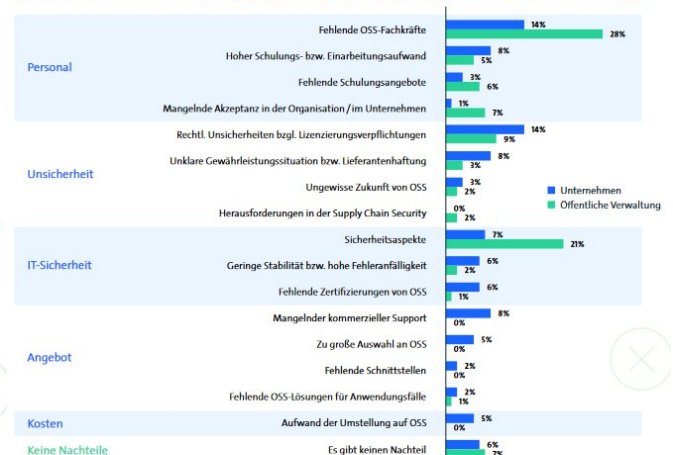
Was ist aus Ihrer Sicht der größte Vorteil, der für den Einsatz von OSS in Ihrer Organisation / Ihrem Unternehmen spricht?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Offene Abfrage, nur eine Antwort möglich | fehlende Werte: „Weiß nicht / k. A.“  
Quelle: Bitkom Research 2023

Abbildung 39 – Vorteile von Open-Source-Software aus Sicht der Öffentlichen Verwaltung

Was ist aus Ihrer Sicht der größte Nachteil, der gegen den Einsatz von OSS in Ihrer Organisation / Ihrem Unternehmen spricht?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) sowie alle Befragten der Öffentlichen Verwaltung (n=102) | Offene Abfrage, nur eine Antwort möglich | fehlende Werte: „Weiß nicht / k. A.“ | Quelle: Bitkom Research 2023

Abbildung 40 – Nachteile von Open-Source-Software aus Sicht der Öffentlichen Verwaltung

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

Die wichtigste Voraussetzung ist eine **breite Awareness in Politik, Wirtschaft und Gesellschaft** über die in Abschnitt 2 aufgezeigten Risiken und Konsequenzen digitaler Abhängigkeit (Zusammenfassung: „Digitale Kolonie“).

Aus dieser Awareness müssen **nachhaltig wirkende politische Handlungen** – mit messbarer Zielsetzung und unterstützt von professionellem Controlling und Steuerung – abgeleitet werden. Ein **parteiübergreifendes konkretes Commitment** und die **Umsetzung im Beschaffungswesen** wären die besten politischen Voraussetzungen.

Weitere wichtige Voraussetzungen sind:

- Die formalen Möglichkeiten zu einer schrankenlosen, dynamischen Kooperation über Behörden Grenzen hinweg (die technischen Möglichkeiten sind hier bereits vollständig vorhanden) muss organisatorisch und rechtlich gewährleistet werden. Beiträge einzelner Einrichtungen müssen im Sinne einer Amtshilfestruktur ohne monetäre Kompensation möglich sein.
- Einrichtung von Leitungsstrukturen (Stiftung, Genossenschaft), deren Akteure persönlich über hervorragende Entwicklungskennntnisse verfügen, sodass eine diesbezügliche Einschätzung des entstehenden Codes und der beteiligten Entwickler (entsandt aus den

<sup>20</sup> <https://www.bitkom.org/sites/main/files/2023-09/bitkom-studie-open-source-monitor-2023.pdf>

Einrichtungen) möglich wird. Entsprechende Anpassungen und Weichenstellungen müssen hohe Priorität genießen. Zur Erinnerung: heutige, auch die marktführenden proprietären Systeme befinden sich auf einem suboptimalen Niveau im Verhältnis zwischen Programmumfang und tatsächlich benötigter Anzahl von Programmzeilen. Bei regelmäßiger Überarbeitung der Architektur sind erheblich kleinere und somit überschaubarere Programme ohne weiteres möglich. Dies muss neben dem Projektmanagement fester Bestandteil der Qualitätssicherung sein.

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?

Hierzu gibt es unzählige Beispiele. Dies fängt bei der Bereitstellung von Entwicklungsumgebungen für die Codeerstellung und Verwaltung an (alle wichtigen Umgebungen für die Entwicklung von Python sind Open Source Produkte jeweils mit einem sehr hohen Stabilitätsniveau) und hört bei der Verbreitung großer Plattformen für die Verkehrsforschung (SUMO, FIWARE) auf. Dazwischen gibt es eine Vielzahl von Produktivitätstools. Die Produkte der „Digital Leader“ des Open Source Markts sind in der Software Suite „openDesk“ verbaut.

Das bekannteste und erfolgreichste OSS-Projekt ist das Betriebssystem Linux und die damit verbundenen offenen Betriebssysteme im Server-, Desktop- und Smartphonebereich. Ein sehr gutes Beispiel für ein Gemeinwohlprojekt ist das von 24 Hochschulen getragene BigBlueButton-Projekt<sup>21</sup> für die gleichnamige DSGVO-konforme Video-Konferenzlösung.

Für das Scheitern von Open Source Projekten (im oben diskutierten Sinne) gibt es verschiedene Gründe. Die Wichtigsten werden durch die wirtschaftlichen Interessen von proprietären Softwareanbietern verantwortet:

- a) Ein Akteur „kauft“ sich in den Kreis der Entwickler ein - für große, finanzstarke Anbieter ist dies durch Beistellung von Ressourcen und der Mitgliedschaft in Steuerungskreisen großer OSS Projekte absolut kein Problem. Unter dem Deckmantel der Meritokratie entsteht eine Dominanz einer dann sehr professionellen und mit unbegrenztem Zeiteinsatz arbeitenden Entwicklergruppe, die gleichzeitig die Spezifikationshoheit („was wird jetzt als nächstes gebaut“) an sich reißt. Wenn die lizenzrechtlichen Bedingungen es gestatten, dass der Code auch für proprietäre, darauf aufbauende Produkte verwendet werden kann, werden die peripher beteiligten Entwickler („Hobbyisten“) zu kostenlosen Ressourcen für ein im Grunde proprietäres Produkt. Auch ohne dass es eine unmittelbare Monetarisierung nach sich zieht, hat die Übernahme der Kontrolle über ein weit verbreitetes Open Source Produkt große Vorteile für einen Anbieter. Im Fall Google Chrome ermöglicht dies die Unterstützung / Bevorzugung eigener bereits kommerzialisierter Produkte (youtube, google maps, google search, google workspace) aus dem Browser heraus („bei Google anmelden?“).
- b) Eine Steigerung dieser Fehlentwicklung ist die Übernahme der kompletten Codebasis durch einen proprietären Anbieter (Beispiel „Docker“). Dies geschieht vornehmlich bei

---

<sup>21</sup> <https://zenodo.org/records/7624015>



bereits weit verbreiteten Systemen, bei denen man hoffen kann, dass Anwender bereit sind Lizenzgebühren zu zahlen, weil sie die entsprechenden Komponenten bereits tief in ihren Anwendungslandschaften verbaut haben. Es gibt eine gewisse „Gegenwehr“ der Anwendergemeinschaft, wenn die Lizenz Einführung zu „ungeschickt“ und für alle sichtbar unfair durchgeführt wird (im Grund eignet sich eine Firma ein Wirtschaftsgut an, das von Freiwilligen kostenlos zur Reife gebracht wurde. Beispiel: Fa. Oracle mit Java.

c) Manchmal scheitern OSS Projekte auch an Meinungsverschiedenheiten zwischen Entwicklern. Führt dies zu dem gefürchteten „Fork“, also der Weiterverwendung und Abwandlung des Codes in einem neuen Produkt mit dann ähnlichen Fähigkeiten, so sinkt für beide Seiten die Nutzerzahl pro „Zeile Code“ und damit die positiven, motivationsfördernden Einflüsse auf die Entwicklergruppe (Verbreitungsgrad, Bekanntheit, Zahl der Rückmeldungen für Verbesserungen etc.). Prominentes Beispiel LibreOffice und OpenOffice.

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 sehr relevant, weil dies auch durch Akteure geschieht, die den Bonus des „NGOs“ und Heilsbringers ausnutzen. Immer wieder schaffen es einzelne kleine Dienstleister eine vermeintliche Open Source Lösung so zu spezialisieren, dass trotz des öffentlichen Zugangs zu dem zugrundeliegenden Source Code keine Chance für die Übernahme des Codes bei vertretbaren Kosten besteht. Im Bereich der Hyperscaler ist das „Open Washing“ an der Tagesordnung. Alle stützen sich auf große Anteile an Open Source und monetarisieren diese. Die Kriterien des Nutzens von OSS zu Gunsten der Anwender sind dabei absolut nicht mehr gegeben, der wirtschaftliche Gewinn steht im Vordergrund.

Noch kritischer als „Open-Washing“ sehen wir das „**Souveränitäts-Washing**“: Die Verursacher der massiven digitalen Abhängigkeit, die digitalen Monopolisten, statten ihre Abhängigkeitsverstärkenden Produkte immer häufiger mit dem Attribut „souverän“ aus oder promoten Narrative, dass die Software Souveränität ermöglichen würde. Dies hat den Charakter von massiver Verbrauchertäuschung, vergleichbar: „*Raucht mehr, umso gesünder werdet ihr*“. Dabei werden auch Akteure aus dem vermeintlich „staatstreuen“ Umfeld (Bundesdruckerei, Rode&Schwarz, SAP) als Hilfe für die Argumentation mit hinzugezogen.

Eine große Menge kleiner Dienstleister aus dem Bereich Beratung und Implementierung von Cloud-Diensten werden ebenfalls instrumentalisiert, um die unterstellte „Seriösität“ der souveränen Angebote zu bekräftigen. Große proprietäre Softwareanbieter promoten vielfältig falsche Narrative, welche von der breiten Bevölkerung und der Politik nicht reflektiert werden. Ein Beispiel: Auf der Informatik Konferenz 2024 war das Hauptthema „Digitale Souveränität“, in den Eröffnungsreden der Politiker wurden bedauerlicherweise verschiedene falsche Narrative inkludiert.

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?

Open Source Technologie ist grundsätzlich gut geeignet, dem Einfluss von einzelnen Machthabern entzogen zu werden. Im Bereich der Chip-Herstellung ist das leuchtende Beispiel RISC-V (<https://riscv.org/>), ein Open Source Konzept zum Entwurf hoch verdichteter integrierter Schaltkreise. Dies ist geeignet, die Dominanz der wenigen, weit überwiegend US-basierten Marktteilnehmer zu brechen. Die Organisation hat deshalb vorsichtshalber ihren Sitz in die Schweiz verlegt, um dem Einfluss der US-Regierung zu entkommen<sup>22</sup>.

Für die Gewinnung von Souveränität ist zunächst die Wiederherstellung eines funktionierenden Marktes entscheidend, auf dem sich dann ein Staat bzw. die Wirtschaft eines Staates souverän bedienen kann. Je nach geopolitischer Lage können sich dann ganze Wirtschaftsräume dem Einfluss einer fremden Macht entziehen, wenn es im eigenen Rechtsraum genügend Alternativen gibt. Voraussetzung für den Aufbau eines solchen **Wettbewerbs** (der heute im Wesentlichen zum Erliegen gekommen ist!) ist die **Erzwingung von Kompatibilität, offene Schnittstellen und die Austauschbarkeit von Komponenten und Modulen**. Ein neuer Anbieter auf dem Markt muss sich darauf verlassen können, dass ein genutzter Standard „offen“ in dem Sinne ist, dass nicht der „Platzhirsch“ in der Lage ist, diesen so abzuändern, dass ein neues Produkt bei Markteintritt obsolet bzw. nicht mehr konkurrenzfähig ist (hierzu ist das OOXML-Format von Microsoft zur Speicherung von Bürodokumenten ein konkretes Beispiel, eine ca. 6.000-seitige Spezifikation ist kaum von Konkurrenten umzusetzen). Mit „offen“ ist bei Standards immer gemeint: ein paritätisch besetztes Konsortium bestimmt die Weiterentwicklung und sorgt für maximale Aufwärts/Abwärtskompatibilität (Beispiel: USB mit Abwärtskompatibilität besteht nun über nunmehr 25 Jahre). Standards müssen genau genug formuliert sein, um im Ergebnis die Kompatibilität wirkungsvoll sicher zu stellen.

Vorbildliche Rahmenvoraussetzungen für den Einsatz von Open Source hat die Schweizer Bundesregierung geschaffen. Das neue Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG)<sup>23</sup> enthält einen eigenen Abschnitt zu Open Source mit dem Grundsatz „Public Money – Public Code“: Die von Behörden entwickelte Software soll als OSS der Allgemeinheit zur Verfügung gestellt werden. Das Parlament erwartet niedrigere Kosten, eine effizientere Zusammenarbeit im Gemeinwesen und qualitativ bessere Software.

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

Siehe Antwort zu 1)

Hauptsächlich müssen die Auftraggeber die Vertragsgestaltung mit den Entwicklungsdienstleistern dahingehend umstellen, dass die Arbeitsergebnisse vollständig in das geistige Eigentum des Auftraggebers bzw. der Öffentlichkeit übergeht und keine spätere Nutzung in ggf.

---

<sup>22</sup> <https://www.heise.de/news/Die-RISC-V-Foundation-verlegt-ihren-Sitz-aus-den-USA-in-die-Schweiz-4596534.html>

<sup>23</sup> <https://www.fedlex.admin.ch/eli/fga/2023/787/de>

kommerziellen Projekten mehr möglich ist. Dies bedroht automatisch etwaige Alleinstellungsmerkmale bestimmter Dienstleister, was im Sinne des Auftraggebers ist. Die Hürden für einen Dienstleisterwechsel werden deutlich herabgesetzt, was sich positiv auf die Qualität und Leistung der Dienstleister auswirkt.

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?

Das Vergaberecht stellt die entsprechenden Vergabeoptionen bereits heute bereit. Die genutzten Vertragsformen sind bisher aber eher Lizenzverträge oder Werkverträge mit der Möglichkeit einer kommerziellen Nachnutzung des entstehenden Programmcodes.

Mit einem prozentualen Mindestanteil an Open Source steht dies nicht in Zusammenhang. Diese Forderung ist aber insofern sinnvoll, als die bisher noch selten genutzten Vertragsformen einer Dienstleistung ohne Rückhalten des geistigen Eigentums für den Anbieter bisher wenig geübt ist. Die aus Sicht des Auftraggebers zweifellos ökonomischer Vergabeform des Open Source Projektes ist ungewohnt und (wie oben beschrieben) schwächt die Position der Dienstleister. Die Festlegung eines Mindestanteils ist also zum heutigen Stand sehr sinnvoll. In Bereichen, wo es bisher definitiv kein Angebot in OSS gibt, darf natürlich die Vergabe an einen proprietären Anbieter nicht verwehrt werden.

Bei Ausschreibungen müssen stets **offene Schnittstellen** und die Möglichkeit des kostenfreien Datenexports ausgeschrieben werden. So muss der Datenexport von Hyperscalern bspw. kostenlos bei Beendigung des Vertrags möglich sein (vgl. DataAct). Entgegen von Narrativen ist den Experten hier kein Fall bekannt, wo dies technisch unmöglich wäre, wirtschaftlich ist ein solches Feature natürlich stark gegen die Interessen der Anbieter.

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

Für den Einsatz von OSS im öffentlichen Bereich ist eine strenge Kontrolle der Herkunft von Code-Segmenten unabdingbar. Ziel muss es sein, die für eine möglichst große Gruppe von Anwendern bzw. für die Abbildung eines Verwaltungsprozesses benötigte Codebasis so konsolidiert und kontrolliert wie möglich zu halten. Dies erfordert die zyklische Investition in Code Revisionen unter Software-architektonischen Gesichtspunkten. Der Code muss fortwährend optimiert und sicherheitsgeprüft werden und er muss jeweils von einer möglichst großen Nutzeranzahl genutzt werden. Das entstehende gute Verhältnis zwischen Nutzerzahl, Funktionsumfang und Code-Umfang ermöglicht dabei eine hochqualitative Pflege und somit ein hohes Stabilitäts- und Sicherheitsniveau. Auch proprietäre Software sollte derlei Audits durchgeführt werden vom Anbieter, allerdings gibt es dafür keine Kontrolle und Garantie. Bei OpenSource Software können Audits allerdings stets durchgesetzt werden.

Open Source sollte unbedingt den Vorrang in der öffentlichen Verwaltung gegeben werden, um die Kontrolle über die Cybersicherheit zurück zu erlangen.

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 heute bei Fachverfahren üblichen Rolloutprinzipien sind sehr aufwendig, unabhängig von der darunterliegenden IaaS Infrastruktur (sei sie selbst gehostet oder bei einem Dienstleister als „Cloud“-Angebot organisiert). Die „one Click“-Angebote großer Hyperscaler nützen hierbei nichts, da alle öffentlichen Auftraggeber (mit wenigen Ausnahmen) keine Stoßlasten aufweisen.

Die ohnehin notwendige Optimierung des Betriebs (Stichwort DevOps) muss im Zuge von Systemumstellungen jetzt umgesetzt werden. Open Source Ansätze helfen hier, alte Strukturen („das geht nicht anders!“) aufzubrechen. Die vorhandenen Open Source Middleware Werkzeuge (Bsp.: Sovereign Cloud Stack) erlauben modernste Verteilungsverfahren (=> CI/CD, Continuous Integration and Deployment), die ganz auf die Bedürfnisse der öffentlichen Hand zugeschnitten werden können und proprietären Lösungen in keiner Weise zurückstehen.

Wichtig ist eine Professionalisierung des Arbeitens im Open Source Bereich. Das über viele Jahre kultivierte Image des „Nerds“ der auch mit schlecht betreibbarer Software zurechtkommt (da er das nötige Hintergrundwissen zur Behebung kleiner Fehler hat) muss in der Nutzung im Verwaltungsbereich abgelegt werden. Hierzu gehören Maßnahmen zur Software Qualitätssicherung (wie sie in der Medizintechnik, in der Raumfahrt wie auch im Automobilbau seit Jahren üblich sind). Eine Etablierung dieser qualitätsorientierten Grundhaltung muss auch im Umfeld der Verwaltungssoftware erfolgen. Dies bedeutet, dass bei einer Budgetierung von einer OSS-Lösung Mittel für die Qualitätssicherung und das Rollout berücksichtigt werden müssen und nicht nur ein Minimal Viable Product budgetiert wird.

Eine häufige Quelle von Akzeptanzproblemen sind Vorurteile gegenüber OSS bei den Nutzenden. Diese führen zu einer negativen Erwartungshaltung. Die unterschiedlichen Bewertungsmaßstäbe von Fehlern bei marktführenden Produkten gegenüber denen von OSS Produkten sind gravierend, psychologisch aber nachvollziehbar - Hersteller nutzen auch hier Narrative, wie bspw. „Der Fehler ist technisch unvermeidbar und nicht unsere Schuld“.

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?

Bei der Vergabe müssen die Bewertungskriterien „Erfüllung von offenen Standards“, „Bereitstellung als Open Source Produkt“ sowie „einfacher, kostenfreier und vollständiger Datenexport“ Pflichtkriterien sein.

Eine alternative Projekt-bezogene Ausschreibeform muss möglich sein:

Vergaben heben heute stark auf die Vereinbarung und Lieferung von klar definierten und abgegrenzten Liefergegenständen ab. Für gegenständliche Arbeitsergebnisse mit starker Normung und lange bekannter Umsetzungspraxis (bspw. im Baugewerbe mit einer Vielzahl

von Normen und Regelungen) ist dies zielführend. Für Arbeitsergebnisse, deren vollständige und lückenlose Beschreibung im Vorfeld einer Vergabe unter keinen denkbaren Umständen möglich ist, sind diese Standardverfahren ungeeignet. Die Vergabe von purer „Arbeitsleistung“ (=> Time-and-Material) wird ebenfalls praktiziert, führt aber häufig zu einer Vermeidung von Verantwortungsübernahme und „Spielverzögerung“.

Ein besseres Verfahren würde eine kontinuierliche gutachterliche Begleitung des Entwicklungsprozesses durch einen Treuhänder des Auftraggebers einbeziehen, dem sich die Vertragspartner unterwerfen und mit dessen Hilfe auch deutliche Änderungen in der geforderten Spezifikation rechtssicher in eine neue Vertragslage („wer schuldet wem was?“) überführt werden können. Analog zum Product Owner in der Entwicklungsmethodik SCRUM würde dies die Domänenexpertise eines Fachmitarbeiters mit den Spezialkenntnissen eines externen Softwareentwicklungsunternehmens zusammenbringen.

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?

Eine Aufnahme in die Abgabenordnung ist in jeden Fall sinnvoll und würde Open Source weiter fördern. Die steuerrechtliche Behandlung von OSS Umsetzungen muss allerdings entsprechend ausgearbeitet und erprobt werden, um zu vermeiden, dass Hersteller unter dem Deckmantel von Open Source-Entwicklungen Gewinne erwirtschaften. Hierzu liegen noch zu wenige Erkenntnisse vor. Daher ist eine vorsichtige Formulierung zu wählen, diese könnte bei Erfolg weiter ausgeweitet werden. Ein Ansatz könnte sein: „die Förderung von offenen Quellcode unter einer freien-Software-Lizenz mit CopyLeft.“

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?

Die weiter oben beschriebenen Risiken der Verantwortungsdiffusion können wirksam bekämpft werden, wenn es Plattformen gibt, die Herkunftsnachweise (Provenienz) von Software Modulen auf hohem Sicherheitsniveau unterstützen. Die Plattform „openCode“ des Zentrums für Digitale Souveränität (ZenDis) ist genau ein solches Beispiel. Ist die Plattform heute auf die Auffindbarkeit und Zugänglichkeit von Open Source Projekten ausgerichtet, so kann sie im nächsten Schritt Verantwortung für den Prüfstatus und die Herkunft von Code Angeboten übernehmen.

Der ebenfalls beschriebene Gefahr der „feindlichen Übernahme“ eines OSS Projektes durch einen finanzkräftigen kommerziellen Anbieter kann durch die Gründung von Genossenschaften begegnet werden, die ausschließlich durch Anwenderorganisationen besetzt sind. Die Genossenschaftsmitglieder können ihrerseits Unternehmen beauftragen. Diese haben aber kein Stimmrecht in Fragen der Entwicklungsroadmap eines OSS Projektes.

Weitere Aufgaben, die ggf. durch dedizierte NGOs abgedeckt werden könnten, sind:

- a) Training für OSS Entwicklung, Schulungen für Entwicklung

- b) Training für OSS Nutzung Empfehlung von Governance-Modellen
- c) Rechtsbeistände
- d) Einsatz von OSS in Bildungseinrichtungen

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?

Grundsätzlich ist proprietäre Software von den gleichen Fehlerarten bedroht wie Open Source Software. Es erschließt sich daher nicht, warum hier andere Maßstäbe angelegt werden sollen. Das z.T. größere Medienecho von Fehler in OSS ist auf zwei Gründe zurück zu führen:

- a) OSS Funktionen sind (aufgrund ihrer kostenlosen und unproblematischen Zugänglichkeit) zum großen Teil erheblich weiter verbreitet, als proprietäre Module. Entsprechend größer ist die Wirkung eines Fehlers (siehe Log4J, was häufiger genutzt wurde, als alle anderen Programme)
- b) Die Hersteller proprietärer Software haben Interesse an der Skandalisierung von OSS Fehlern und unterstützt deshalb deren Bekanntmachung durch die Presse.

Wir denken daher, dass ein OS Advisory Board für das Monitoring nicht notwendig ist. Es wäre allerdings sinnvoll ein allgemeines Advisory Board einzuführen, welches Fehler in Software monitort und auch Hersteller von proprietärer Software stärker sanktioniert, wenn diese Fehler nicht bzw. nicht zeitnah beseitigen. Insgesamt ist das bisher in kommerziellen Produkten vorzufindende Fehlerniveau und die Einschränkungen in der Betreibbarkeit (Menge an Know-How, die nötig ist, um die z.T. haarsträubenden Fehler bei Updates zu beseitigen) grundsätzlich zu hinterfragen und es sind dringend Maßnahmen zu treffen, um dieses Niveau zu erhöhen.

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?

Die proprietäre Natur der häufig in Fachverfahren eingesetzten Software hat in der Vergangenheit häufig zu festgefahrenen Verhältnissen zwischen Anbieter und Behörde geführt. Das „bequeme Geldverdienen“ in gesicherter Auftragsumgebung mit Lock-In hat mögliche Innovationen verhindert. Die mögliche Teilhabe durch weitere Akteure bis hin zu interessierten Externen oder auch einzelnen Bürgern kann hier den Innovationsdruck massiv erhöhen und so die Ergebnisse verbessern. Partizipation als motivationsförderndes Mittel könnte auch lokal stärker eingesetzt werden. Neben einem Heranführen der Bürger an die Informatik (=> MINT-Orientierung) könnten die Beiträge ansonsten Unbeteiligter zu einer größeren Bürgernähe und so zu einem größeren Vertrauen in staatliche Dienstleistungen führen, was wiederum einen direkten positiven Einfluss auf die Demokratie haben kann.

Die größten Hebel für die Verbesserung der Verwaltungsdienstleistungen liegen aber in der Prozessgestaltung von Abläufen und der Konsolidierung von Datenflüssen (once-only-Prinzip). Dies kann durch informationstheoretische Verfahren unterstützt werden. Die kritischen Veränderungen sind aber von den Eignern der Fachverfahren durchzusetzen.

15) Bei der Entwicklung von Open Source Software (OSS) kann durchaus auch unbemerkt Schad-Software eingebaut werden, z.B. 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?

Wir verstehen die Annahme nicht, dass Protestware in OSS anders zu bewerten wäre als in proprietärer Software. Entwickler schmuggeln auch heute noch sogenannte EasterEggs in kommerzielle Produkte der Anbieter. Diese bleiben in einzelnen Fällen auch über Jahrzehnte unerkannt – dies gilt auch bei Software, die millionenfach verkauft wird, wie kommerzielle Spiele.

Wir sind davon überzeugt, dass OSS hier kein Nachteil ggü. kommerzieller Software mit sich bringt. Im Gegensatz zu proprietärer Software kann allerdings „Protestware“ einfach aus OSS heraus gepatched werden - nach der Entdeckung können je nach Schwere des Falles unabhängige Firmen beauftragt werden und durch umgehende Beseitigung Folgeschäden verhindert werden.

Der kürzlich entdeckte Eintrag einer Spionagesoftware in einem OSS Produkt konnte nur gefunden werden, weil die Inspektion des Codes unmittelbar erfolgen konnte. Der gleiche Spionageversuch in einem kommerziellen Produkt hätte ggf. lange unentdeckt bleiben können. Spionage in proprietärer Software wird vielfältig vorgeworfen<sup>24</sup>. In OSS kann dies überprüft werden. Einen wichtigen Betrag zur Sicherung gegen ungewollte Veränderungen ist der Herkunftsnachweis (siehe Frage 12), mit dem kritische Software Komponenten auch in Open Source Projekten bestimmten (und ggf. sicherheitsüberprüften) Software Entwicklern zweifelsfrei zugeordnet werden können. Hierfür spielt die zweifelsfreie Identifikation von Beitragenden Entwicklern eine herausragende Rolle.

16) Die Bildgenerierungssoftware Stable Diffusion ist eine quelloffene Lösung, die ähnlich gute und verblüffende Ergebnisse liefert wie ihre proprietären Pendant; 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?

Hierbei sind mehrere Faktoren zu berücksichtigen. Große Techkonzerne investieren Milliarden USD pro Jahr in Künstliche Intelligenz. Die dabei entwickelten Lösungen und Tool Frameworks sind -abgebildete auf die Autobranche- vergleichbar mit Ferrari, bestmöglich ausgestattet. Daher können Open Source Lösungen hier aktuell nicht für alle Zwecke vergleichbar gute funktionale und nicht-funktionale Anforderungen erfüllen, bspw. alle Features und. eine benutzerfreundliche Umgebung.

Es wäre allerdings möglich, 95% der Anfragen durch Open Source Modelle zu bedienen. Damit würde die digitale Souveränität gestärkt werden.

Die Oligopole versuchen derzeit ihre KI-Werkzeuge in vorhandene Produkte zu integrieren („Bundeling“, bspw. Microsoft CoPilot), so dass diese aus Bequemlichkeit und als „Standardlösung“ von Kunden bevorzugt genutzt werden (hierdurch erhöht sich naturgemäß der Preis

---

<sup>24</sup> <https://www.heise.de/news/Huawei-laut-CIA-von-chinesischer-Regierung-finanziert-4403987.html>

der betreffenden Produkte (siehe MS365). Es ist Aufgabe der Politik (national bzw. EU), die Bündelung von Softwarekomponenten zu verbieten und den Austausch mit offenen Standards einzufordern.

Der große Vorteil für Deutschland und Europa besteht dahingehend, dass wir ein einzigartiges Domain-Wissen (bspw. Automotive, Maschinenbau, Pharmabranche) besitzen und auch über umfangreiche Datenbasen verfügen. Es ist notwendig der Forschung den Zugriff auf derlei Daten zu geben, um diese Datenschätze in generative Modelle einbringen zu können. Es wäre von Vorteil die Copyright-Regelungen dahingehend anzupassen, dass ein Zugriff auf Literatur- oder Forschungspublikationen leichter möglich wird.

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,

Besonders schwerwiegend ist der harte Lock-In von Daten durch proprietäre Schnittstellen und die Weigerung von Herstellern (Narrativ: „technisch nicht realisierbar“), Datenexports in Standardformate exportieren zu können.

Bzgl. Hardware kommt diese Form der Barriere bei OSS bisher nicht vor. Der Grund hierfür liegt darin, dass diese Inkompatibilitäten keinen realen Ursprung haben, sondern ein Teil der Marketing Strategie der Softwareanbieter sind (so wird für Windows 11 eine höherwertige Hardware verlangt, als für Windows 10. Diese Forderung, obwohl intuitiv nachvollziehbar, ist falsch: Windows 11 wurde mit entsprechenden Umgehungen erfolgreich auf sehr alten Rechnern installiert und funktioniert fehlerfrei).

Bezüglich gezielter Inkompatibilitäten zwischen proprietären Softwarekomponenten gibt es das gleiche Vorgehen. Dies ist dann nicht oder nicht ohne große Anstrengung zu umgehen. Für Open Source Software sind solche Manöver natürlich schwer möglich, wenn beide Komponenten OS sind. Bei der Kommunikation mit proprietärer Software besteht immer das Problem des Reengineering, was nach Europäischem Recht nur eingeschränkt, nach amerikanischem Recht aber erlaubt ist. In der Praxis spielt dies aber wegen des großen Risikos für den nicht kommerziellen Anbieter eine untergeordnete Rolle.

- weiche Abhängigkeitsfaktoren wie Gewöhnungseffekte,

Die „Sozialisierung“ und Bindung der Anwender an die marktführenden Plattformen (die in Schulen durchweg kostenlos, in anderen Bildungseinrichtungen mit starken Rabatten angeboten werden) ist drastisch. Alternative Produkte aus dem Open Source Bereiche müssen deshalb das gelernten Systemverhalten so weit wie irgend möglich nachmodellieren, um Akzeptanz zu finden. Dies kollidiert mit dem Selbstverständnis vieler OSS Entwickler, die -versiert im Umgang mit verschiedensten Benutzeroberflächen- die beschriebene Problematik für weniger relevant halten und ihren Schwerpunkt auf konkrete Verbesserungen gegenüber dem Status Quo richten. Am Ende benötigt der Anwender aber nicht die „bessere“ Software, sondern diejenige Version, die am wenigsten Umlernen erfordert. Die Toleranz gegenüber plötzlichen Änderungen bei den Marktführern ist dabei erheblich höher, als die gegenüber „fremder“ OSS Produkten. Kurz: „Der Marktführer darf alles, die alternative Software



darf keinen Millimeter abweichen“. In Akzeptanz dieses Verhaltens muss die OSS Entwicklung alternativer Produkte die Nutzer bestmöglich abholen.

- mangelnde IT-Kompetenz im Einkauf, was zur Verlängerung von Rahmenverträgen  
Es ist Aufgabe der Politik, die Bedeutung von Wettbewerb auch im Software Einkauf klar zu machen. Das „kleine 1x1“ des Einkaufs gehört in jedem Industriebetrieb zum Standard wissen, wenn es um den Einkauf von Fertigungsmaterialien für Produkte geht. „Second Source“ ist die wichtigste Risikovorsorge jedes Betriebes. Jeder Erfahrene Einkäufer weiß, dass er durch gezielte Vergabe mehrere Anbieter im Geschäft halten muss. Die simple Übertragung dieses Prinzips auf die Software Werkzeuge löst diese Frage.

- oder mehr Einkauf von Vertrautem führt, weil man Alternativen nicht kennt oder ihre Risiken überschätzt,

Es ist vielmehr so, dass die Risiken einer fehlenden Diversifizierung der Anbieter massiv **unterschätzt** wird. Dem gegenüber sind die Risiken einer Veränderung dann überschaubar, wenn sie koordiniert und mit einer großen Anzahl weiterer Anwender gemeinsam unternommen werden. Das „nicht kennen“ von Alternativen wird aus der Vergangenheit auch durch das „nicht glauben“ verstärkt. Vielen IT-Verantwortlichen aus der öffentlichen Verwaltung fehlt schlicht die Vorstellungskraft darüber, welche Alternativen bereits in höchster Qualität und Stabilität vorhanden ist. Mit dem Wissen, dass dies alles ohne gezielte Förderung und ohne Finanzierung entstanden ist, kann man sich leicht eine schlagkräftige staatlich unterstützte Entwicklung von Alternativen vorstellen.

- mangelnde IT-Kompetenz im Betrieb, weil es weniger Erfahrung mit Open-Source-Dienstleistenden gibt,

Es sind weniger die OSS Dienstleister als vielmehr das mühsam erworbene Wissen im Umgang mit proprietären Werkzeugen. Ein Administrator mit Zertifizierungen bei einem Hyperscaler kann (schon aufgrund der Komplexität und des hohen Aufwandes im Betrieb) hoffen, dass seine Arbeitskraft in jedem Fall benötigt wird. Empfiehlt er den Einsatz eines neuen, ggf. einfacher administrierbaren Produktes, gefährdet er/sie indirekt den eigenen Arbeitsplatz. Dies stellt eine psychologisch gut nachvollziehbare Hürde für einen Wechsel dar.

- Folgen von Lobbyismus großer Hersteller proprietärer Software,  
Die langjährige Einwirkung der Lobby auf die (zunehmend fachfremden) Entscheider im IT-Bereich hat eine massive Wirkung. So hält heute ein IT-Verantwortlicher die hohe Fehlerquote bzgl. Cyber-Sicherheit für „normal“, obwohl in Bereichen mit hohen Sicherheitsanforderungen (Medizin, Luftfahrt) ohne Probleme hochqualitative Software entsteht. Nach dem gleichen Muster wird OSS als „grundsätzlich unsicher“, unkontrollierbar etc. dargestellt, was Vorbehalte schürt. Hier ist die Politik gefragt, eine sachliche Betrachtung zu erzwingen.

- fehlende Transparenz zum Einsatz von Open Source und proprietärer Software,

Hier findet derzeit ein Nachholen des Aufbaus der erforderlichen Kenntnisse statt. Dies kann durch die Open Source Community und durch oben ebenfalls diskutierte, Genossenschaften und Konsortien erfolgen.

- mangelnde strategische Weitsicht beziehungsweise Überschätzung von kurzfristigem Nutzen bei Unterschätzung langfristiger Risiken?

Dies ist zweifellos der Fall. Für börsenorientierte Unternehmen ist dies eine logische Konsequenz der quartalsgetriebenen Optimierung der Betriebsergebnisse. Öffentli-

che Einrichtungen können hier aber mit längerfristigen Perspektiven arbeiten. Ein Verharren, auch den (monopolbedingt) z.T. überaus mangelhaften Funktionen der marktführenden Anbieter (insbesondere Sicherheit und Betreibbarkeit) ist mittelfristig weder zielführend, noch nötig. OSS-basierte Alternative (und auch kommerzielle Alternativen) sind (entgegen der gängigen „Narrative“) gut machbar, wenn dem Priorität eingeräumt wird und wenn der erforderliche Reifegrad durch intensive Verwendung solcher Systeme in der Praxis konsequent gefördert wird.

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?

In Artikel 2 (1), GG kann die freie Entfaltung der Persönlichkeit durch Open Source unterstützt werden. Nutzende können die Systeme beliebig ihrer Persönlichkeit entsprechend anpassen. Ebenfalls wird Art. 5 (1) unterstützt. Zensur wird durch Open Source verhindert, ebenfalls kann sich jede/r daraus unterrichten. Der Staat könnte OSS dazu nutzen um Art. 7 (1), die Aufsicht über Schulen zurück zu erlangen.

Eine 2021 von der EU-Kommission veröffentlichte Studie<sup>25</sup> bestätigt den **signifikanten Einfluss von Open Source Software auf die Wettbewerbsfähigkeit europäischer Unternehmen**, auf das **Wirtschaftswachstum**, auf die Start-up-/KMU-Szene und die technologische Unabhängigkeit Europas.

Der Studie zufolge trägt Open Source einen erheblichen Beitrag zum Bruttoinlandsprodukt (BIP) der EU bei: Rund 1 Milliarde Euro, die Unternehmen in der EU 2018 in Open Source investiert haben, führten demnach zu einem wirtschaftlichen Mehrwert von 65 – 95 Milliarden Euro.

---

<sup>25</sup> <https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and>