Digitale Nachhaltigkeit: Digitale Souveränität und Open Source Software beim Einsatz von PM-Tools

Guido Bacharach[1], Jakob Jäger[2], Harald Wehnes[3]

Abstract: Digitale Nachhaltigkeit ist eine grundlegende Voraussetzung für die Zukunftsfähigkeit unseres Landes, der Gesellschaft und Wirtschaft. Die steigende digitale Abhängigkeit Deutschlands und Europas von marktdominanten, nicht-europäischem Recht unterliegenden IT-Unternehmen ist besorgniserregend. In diesem Beitrag werden zunächst die Risiken und potentiellen Konsequenzen digitaler Abhängigkeit aufgezeigt. Danach werden verschiedene Lösungsansätze vorgestellt, die aus dieser Abhängigkeit führen können. Eine wichtige Rolle spielen dabei der Einsatz von Open Source Software (OSS) und die Governance von OSS Communities. Darüber hinaus stellen wir einen Souveränitätsscore (MVP) vor, mit dem man seine persönliche Digitale Souveränität bzw. die seines Unternehmens oder seiner Organisation messen kann. Abschließend geben wir Empfehlungen, insbesondere zum verantwortungsbewussten Tool-Einsatz in der Projektarbeit und darüber hinaus.

Keywords: Souveränitätsscore, Digitale Nachhaltigkeit, Digitale Souveränität, Innovationen, Projektmanagement, Tools, Open Source Software (OSS), Standards, Governance von OSS Projekten

1 Einleitung

Das generelle Bewusstsein für Abhängigkeiten ist in letzter Zeit durch verschiedene Ereignisse (Ukraine-Krieg, Trump-Regierungszeit, Musk/Twitter etc.) sprunghaft gestiegen. Das „Lessons learned“ aus der Abhängigkeit von russischem Gas: Wir müssen professionelles Präventions- und Risikomanagement anwenden, um wann immer möglich, Vorsorge zu treffen, bzw. Abhängigkeiten frühzeitig zu identifizieren, um rechtzeitig gegensteuern zu können und Risikominderungsmaßnahmen einzuplanen und umzusetzen. In diesem Beitrag wollen wir die digitalen Abhängigkeiten Deutschlands und Europas beleuchten. **Im Gegensatz zum Gas können digitale Abhängigkeiten irreversibel sein und können zu massiven dauerhaften wirtschaftlichen und gesellschaftlichen Schäden führen.**

Die Konsequenzen aus dem Wegfall von russischem Gas sind uns allen noch im Bewusstsein (Ergebnisauszug aus einem Workshop beim PM Forum 2023 der GPM Deutsche Gesellschaft für Projektmanagement e.V. am 15.06.2023 in Köln):

- „Mondpreise“ für Gas, Strom und andere Energieträger; Preisaufschläge über die komplette Value Chain → Inflation
- Mediale Panikmache: Verbreitung von Verunsicherungen; Existenzängste

[1] Netzwerk Digitale Nachweise, Westminsterstraße 60, D-45470 Mülheim, g.bacharach@gpm-ipma.de
[2] Universität Würzburg, Institut für Informatik, Am Hubland, D-97074 Würzburg, jaeger@informatik.uni-wuerzburg.de
[3] Universität Würzburg, Institut für Informatik, Am Hubland, D-97074 Würzburg, wehnes@informatik.uni-wuerzburg.de

- Rezession; Insolvenzen; Arbeitslosigkeit
- Massive Einsparaktionen; Energiedrosselung am Arbeitsplatz
- Einsatz von Fracking Gas; umstrittenes Heizungsgesetz.

Was waren die Sofortlösungen, und welche Lösungsmöglichkeiten wurden auf den Weg gebracht? Ergebnisauszug aus dem o.g. Workshop:

Sofortlösungen	Mittel-/langfristige Lösungsmöglichkeiten
➢ Nutzung vorhandener Gasreserven ➢ Energiesparmaßnahmen bei Gas und Strom	➢ Ausbau erneuerbarer Energien: Solar- und Windenergie, Brennstoffzellen, Wasserstoff, Wärmepumpen etc. ➢ Verträge mit (politisch z.T. nicht ganz unkritischen) Ersatzlieferanten ➢ Gebäudedämmung und ähnliche Maßnahmen ➢ Förderprogramme: Energiesparmaßnahmen, Investitionen in erneuerbare Energien, Energieforschung u.ä.

Abb. 1: Lösungsmöglichkeiten für die Abhängigkeit von russischem Gas

Bei digitalen Abhängigkeiten können die Konsequenzen wesentlich dramatischer sein, z.B. wenn der „Digitale Hahn“ für lebensnotwendige Dienste von ausländischen Unternehmen oder Politikern abgedreht wird. Sofortlösungen hierfür sind aktuell nicht in Sichtweite. Es gibt noch keinen Plan B. Mittel- und langfristige Lösungen benötigen Vorlauf.

Sofortlösungen	Mittel-/langfristige Lösungsmöglichkeiten
➢ **Keine**	➢ Awareness für die Risiken und Konsequenzen digitaler Abhängigkeit stärken ➢ Vorrang in der Beschaffung von Softwareprodukten, die digitale Souveränität stärken, z.B. Open Source Software ➢ Schaffung von Rahmenbedingungen, die den Wettbewerb am Softwaremarkt stärken

Abb. 2: Lösungsmöglichkeiten für digitale Abhängigkeit

Abgeleitet aus dieser Problemstellung haben wir uns vorrangig mit den folgenden **Forschungsfragen** befasst:

F1: *Wie kann der Grad der Digitalen Souveränität einer Software gemessen werden?*

F2: *Welche Lösungsansätze und Handlungsempfehlungen gibt es zur Stärkung von Digitaler Souveränität?*

Unser Beitrag gliedert sich wie folgt: In Kapitel 2 werden die Risiken und Konsequenzen digitaler Abhängigkeit analysiert. Kapitel 3 widmet sich der Forschungsfrage F1. Es wurde ein Souveränitätsscore (MVP) konzipiert und programmtechnisch umgesetzt, mit dem man die Digitale Souveränität einer Software messen kann. In Kapitel 4 werden die Ergebnisse zur Forschungsfrage F2 vorgestellt: Vorgehensempfehlung, Risikocheckliste, Maßnahmenkatalog zur Verringerung digitaler Abhängigkeiten und Softwareproduktempfehlungen. Mit einem Fazit und Ausblick auf zukünftige Forschungsarbeiten und Folgeaktivitäten (Kapitel 5) wird der Beitrag abgeschlossen.

2 Digitale Abhängigkeiten: Risiken und Konsequenzen

Wir beginnen dieses Kapitel mit Begriffsklärungen, die für die nachfolgenden Abschnitte wichtig sind. Um das Bewusstsein für digitale Abhängigkeiten und deren Konsequenzen zu stärken, betrachten wir anschließend den Status der „Digitalen Kolonie Deutschland" und analysieren die Risiken und potentiellen Konsequenzen digitaler Abhängigkeit.

2.1 Begriffe

Was versteht man unter „Digitaler Souveränität"?

„*Digitale Souveränität*" beschreibt „*die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können*" (Definition des IT-Planungsrats der Bundesregierung [IT21]).

Warum ist digitale Souveränität von zentraler Bedeutung für Unternehmen, Institutionen und Bürgerinnen und Bürger?

Digitale Souveränität gewährleistet Sicherheit, Datenschutz und Unabhängigkeit von ausländischen politischen und wirtschaftlichen Einflussnahmen. Sie stärkt die Wettbewerbsfähigkeit von deutschen und europäischen Unternehmen, schützt geistiges Eigentum und fördert Innovationen. Insgesamt trägt sie zur wirtschaftlichen Prosperität, Sicherheit und zu nachhaltigem Wohlstand in der digitalen Welt bei.

Was ist Open Source Software (OSS)?

Open-Source-Software (OSS) bezeichnet Software, deren Quellcode für die Öffentlichkeit zugänglich ist: Benutzer können den Code einsehen, für ihre Zwecke ändern und verteilen. Investitionen in die Entwicklung von Open-Source-Software sowie deren Einsatz (kostenfreie Lizenzen) sind für Unternehmen und Institutionen im Vergleich zu proprietärer Software in der Regel wirtschaftlich nachhaltiger, da keine teuren Dauerverpflichtungen (z.B. Abogebühren) anfallen. Ergänzende kostenpflichtige Services (Releases, Betrieb, Support u.ä.) werden von verschiedenen Dienstleistern angeboten.

Was versteht man unter proprietärer Software?

Proprietär nennt man Software, deren Quellcode und Nutzungsrechte im Besitz eines Unternehmens oder einer Organisation liegen. Die genaue Funktionsweise ist intransparent und der Code ist nicht öffentlich zugänglich. Proprietäre Lösungen "Made in Germany" sind im Kontext von Digitaler Souveränität positiv zu bewerten, wenn diese der vollen Kontrolle des europäischen Rechtsraums unterliegen und auch das Hosting in Deutschland oder der EU stattfindet. Wie OSS helfen diese Lösungen digital unabhängiger zu werden.

Welche Auswirkungen haben Softwaremonopole?

Im Kontext Digitaler Souveränität sind Software-Monopole und -Oligopole äußerst problematisch, da diese u.a. mit ihrer Kapitalstärke in die politischen Entscheidungsprozess stärker eingreifen können, wettbewerbsverzerrend wirken, hohe Abhängigkeiten generieren und das Risiko von Kontrollverlust über die eigenen Daten sowie Erpressbarkeit schaffen → siehe ***Vendor und Cloud Lock-in***

Welche grundlegende Bedeutung hat OSS für die Digitale Souveränität?

Mit Open Source Software (OSS) können Unternehmen und Institutionen die Kontrolle über ihre Daten und Technologien sichern und die Unabhängigkeit von marktdominierenden Anbietern fördern. OSS ermöglicht Flexibilität und Anpassungsfähigkeit und erhöht die IT-Sicherheit und Interoperabilität. Darüber hinaus fördert sie lokale Wertschöpfung, Innovationskraft und sichert zukünftigen Wohlstand.

Was versteht man unter Vendor Lock-in?

Ein Vendor Lock-in ist eine gefährliche Situation, in der ein Kunde in sehr hohem Maße von den Produkten eines Anbieters abhängig ist und ohne massive Kosten und Schwierigkeiten nicht kurzfristig den Anbieter wechseln kann. Ein Vendor Lock-in kann Kunden erpressbar machen.

Was versteht man unter Cloud Lock-in?

Ein Cloud Lock-in ist eine übermäßige Abhängigkeit eines Unternehmens oder einer Institution von einem bestimmten Cloud-Anbieter, die es praktisch unmöglich macht, zu einem anderen Anbieter zu wechseln, wodurch die Kontrolle über Daten und Prozesse verloren gehen kann und Erpressbarkeit möglich wird.

2.2 Digitale Kolonie

Die Themen Digitale Souveränität, Datensouveränität, geopolitische Abhängigkeit, Offenheit von Daten, Standards und Code sind sowohl in der Wirtschaft als auch in der politischen Diskussion angekommen: Im Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP [BU21] haben Digitalen Souveränität und der verstärkte Einsatz von Open Source einen hohen Stellenwert. Die Stärkung der technologischen und Digitalen Souveränität Deutschlands ist zum Leitmotiv der Digital- und Innovationspolitik (Digitalstrategie 2022) der Bundesregierung erhoben worden [BU22].

In jüngster Zeit mehren sich die Warnungen hochkarätiger IT-Experten, Forschungseinrichtungen und Politiker, Deutschland und Europa drohe eine „Digitalen Kolonie“ oder „Digitale Datenkolonie“ zu werden:

- Manfred Broy: *Deutschland ist auf dem Weg, ein digitales Entwicklungsland, eine digitale Kolonie zu werden*. [Br20]
- Helmut Krcmar: *Droht Europa eine digitale Kolonialisierung*? [Kr20]

Maximilian Mayer und Yen-Chi Lu von der Konrad-Adenauer Stiftung e.V. kommen in einer Studie zum Ergebnis, dass Europa die Konsequenzen seiner digitalen Abhängigkeit noch kaum erkannt hat [ML22].

2.3 Risiken aus digitaler Abhängigkeit

Recht eindrucksvoll beschreiben Jan Mahn und Christian Wölbert [MW20] die möglichen Konsequenzen digitaler Abhängigkeit:

Washington, Herbst 2020: In der heißen Phase des US-Wahlkampfs verschärft Donald Trump die Sanktionen gegen die Ostsee-Pipeline Nord Stream 2 und verbietet amerikanischen Digitalkonzernen die Zusammenarbeit mit staatlichen Stellen in Deutschland. Kurz darauf verlieren Hunderte Behörden, Krankenkassen und Schulen den Zugriff auf Cloud-Dienste wie Microsoft Office 365, Google Docs und Cisco Webex.

Abb. 3: Fiktives Beispiel [MW20]

Johann Bizer, Chef von Dataport, einem IT-Dienstleister für Behörden in Norddeutschland meint dazu: „Was gestern unvorstellbar und als platter Antiamerikanismus ausgelegt worden wäre, ist heute möglich und denkbar geworden.“ Und er weist auf Beispiele von digitalen US-Embargos hin: Venezuela, Iran, China. Mit Blick auf die Präsidentschaftswahl in den USA 2024 kann auch eine Renaissance der "America First"-Politik nicht ausgeschlossen werden.

Der Wirtschaftsverband BITMi Bundesverband IT-Mittelstand e.V. warnt vor den wachsende digitalen Abhängigkeiten, die inzwischen ein „besorgniserregendes Ausmaß“ erreicht haben, weist auf „konkrete Gefahren für unsere politische Selbstbestimmung“ hin und fordert „Deutschland darf im Digitalen nicht zu einer reinen Anwendungs-Volkswirtschaft werden“. [BI22]

Die wirtschaftlichen Folgen der Monopolisierung und dem damit einhergehenden fehlenden Wettbewerb am digitalen Markt werden insbesondere bei den halbjährlichen Preissteigerungen, die häufig im 2-stelligen Prozentbereich liegen, überdeutlich. [Ke22], [JK23].

Wir haben eine Risikoanalyse digitaler Abhängigkeiten und deren potentielle Konsequenzen vorgenommen und als Ergebnis eine **Checkliste zur Risiko-Identifizierung** für Unternehmen und Institutionen abgeleitet. Sie wird hier auszugsweise wiedergegeben:

- **Dauer-Abhängigkeit, z.B. durch Verlust bzw. Freisetzung eigener IT-Spezialisten aus „wirtschaftlichen“ Gründen**
- Eingeschränkte Informationssicherheit, rechtliche Unsicherheit, eingeschränkte Flexibilität, fremdgesteuerte Innovation [PwC19]
- Wirtschaftliche und politische Erpressbarkeit
- Unkontrollierbare Kosten durch Verlust der Verhandlungsfähigkeit: Jedes Preisangebot muss akzeptiert werden. Kein Einfluss auf Vertragsinhalte und Konditionen.
- Verlust von Eigentums- bzw. Urheberrechten, IP (Intellectual property), Wissen, Patenten, Informationen zur Beantragung von Patenten
- Verlust der Datenhoheit, Industriespionage etc..

Der erste Punkt ist besonders kritisch: Unternehmen oder Institutionen, die z.B. aus „Kostengründen“ eigene IT-Bereiche schließen und ihre Daten und Prozesse („Kronjuwelen“) in Only-Cloud-Modelle von Unternehmen mit juristischen Hauptsitz außerhalb der EU verlagern, können schnell in irreversible und unverhältnismäßig teure und dauerhafte Abhängigkeiten geraten und ihre Innovationsfähigkeit verlieren, wenn kein eigenes digitales Know-how mehr vorhanden ist und die Voraussetzungen für Gestaltungsfähigkeit fehlen.

2.4 Risiken aus der Nutzung „kostenfreier“ Tools

„Kostenfreie“ Software-Tools werden in der Projektarbeit und darüber hinaus gerne eingesetzt, um bewusst oder unbewusst Kosten zu sparen. Die Tatsache, dass man mit dem Gold des 21. Jahrhunderts, seinen eigenen persönlichen Daten und Verhaltensweisen bezahlt, ist vielen bekannt und wird aber häufig verdrängt [WB20]. Welche Risiken man mit der Nutzung „kostenfreier“ Tools eingeht, zeigt beispielhaft der folgende Auszug aus der Datenschutzerklärung von Discord (https://discord.com/privacy). Produktnutzung bedeutet automatisch die Einverständniserklärung zu diesen Bestimmungen.

Wortlaut der Datenschutzbestimmung	Klartext
Informationen, die Sie bereitstellen: *Wir sammeln Informationen von Ihnen, die Sie freiwillig zur Verfügung stellen (z. B. sobald Sie sich für die Dienste registrieren oder bestimmte Dienste nutzen). Zu den von uns gesammelten Informationen gehören unter anderem Benutzername, E-Mail-Adresse und alle Nachrichten, Bilder, temporäre VoIP-Daten (um die Kommunikation zu ermöglichen) und andere Inhalte, die Sie über die Chat-Funktion verschicken.*	Sämtliche anfallende Daten werden gespeichert
Daten, die wir automatisch sammeln: *Wenn Sie mit uns über die Dienste kommunizieren, erhalten und speichern wir bestimmte Informationen wie IP-Adresse, Geräte-ID und Ihre Aktivitäten innerhalb der Dienste. Wir sind berechtigt, diese Informationen zu speichern. Die können auch in Datenbanken aufgenommen werden, die im Besitz von Tochtergesellschaften, Agenturen und Dienstleistern sind, und von diesen verwaltet werden.*	Daten können an Dritte weitergeleitet werden
Gesammelte Informationen: *Um unsere Nutzer besser verstehen und unsere Dienste optimieren zu können, untersuchen wir auf der Grundlage der gesammelten Informationen demografische Daten, Interessen und Verhaltensweisen unserer Nutzer. Diese Ergebnisse können zusammengestellt und analysiert werden. Wir können diese gesammelten Daten mit unseren Tochtergesellschaften, Agenturen und Geschäftspartnern teilen. Wir können auch gesammelte Benutzerstatistiken offenlegen, um unsere Dienstleistungen aktuellen und potenziellen Geschäftspartnern zu präsentieren und sie anderen Dritten für andere rechtmäßige Zwecke zur Verfügung zu stellen.*	Aus den Daten können Profile erstellt und an Dritte weitergegeben werden.
Das Unternehmen hat seinen Sitz in den Vereinigten Staaten. *Unabhängig von Ihrem Standort stimmen Sie der Verarbeitung und Weitergabe Ihrer Daten in den USA und anderen Ländern zu. Die Datenschutzgesetze in den USA und in anderen Ländern können im Hinblick auf Sicherheit und Umfang von denen Ihres Landes abweichen.*	Ungesteuerter Abfluss von Daten und Wissen an Dritte

Abb. 4: Datenschutzbestimmung von Discord: Wortlaut vs. Klartext

Der Abfluss von Daten und Wissen an Dritte ist besonders kritisch zu bewerten. Neben persönlichen Daten kann dies auch Projekt- und Unternehmensdaten betreffen sowie Daten von Geschäftspartnern. Auch Eigentums- und Urheberrechte sind damit gefährdet.

Erschwerend kommt für Anwender hinzu, dass sie selbst aufgrund dieser Bestimmung für jegliche Konsequenzen von Datenschutzverletzungen verantwortlich sind, die durch die Nutzung relativ leicht entstehen können, und nicht das Unternehmen Discord.

3 Digitaler Souveränitätsscore

Wie lässt sich Digitale Souveränität stärken? Mit dieser Frage haben sich Jakob Jäger und Ralf Schweifler, zwei Studierende der Universität Würzburg, im Rahmen eines Master-Informatik-Praktikums [JS23] befasst und ein Tool (MVP) zur Messung der Digitalen

Souveränität von Softwareprodukten entwickelt. Die zugehörige Plattform *digital-sovereignty.net* gibt darüber hinaus noch wertvolle Tipps, wie man als Einzelperson, Unternehmen oder Institution seinen Score verbessern und damit seine Digitale Souveränität steigern kann. Die Berechnung des Scores basierte auf einem rudimentären Ansatz, der lediglich zwischen Open Source und proprietärer Software unterschied.

Im Rahmen einer anschließenden Masterarbeit [Jä23] hat Jakob Jäger, Mitautor dieses Beitrags, diesen Ansatz verfeinert und auf proprietäre Lösungen ausgedehnt. Er hat insbesondere ein qualitatives Bewertungsmaß für die Digitale Souveränität entwickelt und dieses implementiert. Mit diesem Souveränitätsscore ist es Nutzern möglich, eine Einschätzung über den Grad der Digitalen Souveränität der von ihnen eingesetzten Software zu erhalten. Jede Software wird anhand der folgenden 6 Kriterien bewertet und daraus der Souveränitätsscore berechnet:

- **Monopolisierung und Wettbewerb:**
  Hat die Software eine Monopolstellung innerhalb ihrer Kategorie?
- **Quelloffenheit:**
  Nutzt die Software eine quelloffene Lizenz?
- **Standardisierte Dateiformate:**
  Bietet die Software volle Unterstützung für offene, standardisierte Dateiformate?
- **Standardisierte Schnittstellen:**
  Nutzt die Software offene APIs/Schnittstellen zur Bereitstellung von Daten?
- **Rechtsstandort und Datensicherheit:**
  Hat der Anbieter der Software seinen juristischen Hauptsitz in der EU?
- **On-Premise:**
  Kann die Software im On-Premise Betrieb eingesetzt werden?

Die **Scoreberechnung** erfolgt mittels der folgenden Formel:

$$\text{Score}(S) = \frac{\sum_{k_1 \in K_1} e(k_1)}{|K_1|} \cdot \prod_{k_0 \in K_0} e(k_0)$$

Erläuterung

- Unterscheidung zwischen Ko-Kriterien K_0 sowie Standardkriterien K_1
- Erfüllungsfunktion e(k) hat Wert 1, falls die Bedingung erfüllt ist, ansonsten den Wert 0
- Berechnung via Prozent der erfüllten Standardkriterien multipliziert mal Ko-Kriterien
- Ergebnis: Wert zwischen 0 und 1, wobei 0 schlechtestes und 1 bestes Ergebnis
- Je höher der Score, desto besser unterstützt die Software die Digitale Souveränität!

Abb. 5: Formel zur Scoreberechnung mit Legende

Um Verstärkungen von Abhängigkeiten und von Lock-in Effekten zu vermeiden sowie die Marktmacht von Monopolisten nicht noch weiter zu steigern, wurde das Kriterium ”Wettbewerb und Monopolisierung“ als Ko-Kriterium gewählt. Alle anderen Kriterien gehen als Standardkriterien in die Formel ein.

Es muss angemerkt werden, dass es neben den oben genannten Kriterien weitere gibt, wie Nutzerakzeptanz, Cybersicherheit, Maintenance und Support, die über den Grad der Digitalen Souveränität einer Software hinaus beachtet werden müssen. Auch könnten einige Kriterien granularer definiert werden. Das würde allerdings die einfache Handhabbarkeit beeinträchtigen.

Die neue Version der Website *digital-sovereignty.net* enthält ergänzend zur Bewertungsmöglichkeit von Software:

- Eine Liste von bereits mit dem Score bewerteten Softwareprodukten
- Hintergrundinformationen zu „Digitaler Souveränität" und zum Souveränitätsscore
- Empfehlungen zur Steigerung der Digitalen Souveränität
- Mitmachmöglichkeit im Rahmen einer Community.

4 Lösungsansätze und Handlungsempfehlungen zur Stärkung der Digitalen Souveränität

Grundvoraussetzung für Entwicklung von Maßnahmen zur Stärkung der Digitalen Souveränität ist das Bewusstsein der Verantwortlichen für die Bedeutung und Kritikalität des Themas für das jeweilige Unternehmen, für die jeweilige Organisation, für jeden Einzelnen und für die gesamte Gesellschaft.

Im Folgenden werden dazu verschiedene Ansätze und Hilfestellungen angeboten: Vorgehensempfehlung, Risikocheckliste, Maßnahmenkatalog und Liste alternativer, vorzugsweiser Open-Source-basierter Produkte. Diese Informationen finden sich auch auf *digital-sovereignty.net* und werden durch Feedback der Community ständig weiterentwickelt.

4.1 Vorgehensempfehlung

1. **Messen Sie den Grad der Digitalen Souveränität Ihres Software-Portfolios** (mit *digital-sovereignty.net).* Konzentrieren Sie sich dabei auf die Produkte, von denen ihr Unternehmenserfolg abhängig ist bzw. die den Hauptteil Ihrer Ausgaben für Software-Lizenzen ausmachen.
2. Führen Sie eine umfassende **Risikoanalyse** durch.
3. Erstellen Sie einen **Maßnahmenplan** (Abschnitt 4.2) für besonders kritische Abhängigkeiten und monitoren Sie die Umsetzung und den Erfolg dieser Maßnahmen. Je später Sie anfangen, umso teurer und aufwändiger wird es.
4. Verstärken Sie in Ihrem Unternehmen, Ihrer Organisation und Ihrem Umfeld das **Bewusstsein** für digitale Abhängigkeiten und die damit verbundenen Risiken.

4.2 Risikoanalyse für digitale Abhängigkeiten

Für die Identifikation und Analyse der Risiken sind Leitfragen sowie eine **Risiko-Checkliste** besonders hilfreich:

- **Existieren potentiell irreversible Abhängigkeiten, z.B. durch Verlust bzw. Freisetzung eigener IT-Spezialisten aus „wirtschaftlichen Gründen“**
- Wo besteht die Gefahr eines Cloud Lock-ins?
- Wo besteht die Gefahr eines Vendor Lock-ins?
- Besteht die Gefahr, dass Sie Ihre Gestaltungs- und Innovationsfähigkeit durch digitale Abhängigkeiten verlieren?
- Ist die Vermeidung von Industriespionage sichergestellt?
- Ist Ihre Datenhoheit sichergestellt?
- Gibt es Compliance-Risiken (DSGVO) durch die Verarbeitung und Speicherung von Daten in Rechenzentren, die nicht dem europäischen Rechtssystem unterliegen?

Sind sie „verhandlungsfähig“? Oder müssen Sie jedes Preisangebot akzeptieren? Kann Ihr Vertragspartner den Vertrag einseitig ändern. Welche finanziellen Konsequenzen ergeben sich, wenn bisher gewährte (hohe) Rabatte wegfallen oder sie in andere Preiskategorien eingestuft werden. Können Sie den Einsatz der Lizenzen vertragskonform monitoren?

4.3 Maßnahmenkatalog zur Verringerung digitaler Abhängigkeiten

Nachdem die kritischsten Risiken analysiert wurden, ist der nächste Schritt, hierfür angemessene Maßnahmen zu planen und auf den Weg zu bringen. Als **Sofortmaßnahme** bietet sich die Vermeidung verstärkter oder neuer digitaler Abhängigkeiten an.

Weiter Maßnahmen können z.B. sein:

- Zwei- oder mehrgleisige Einkaufsstrategie
- Alternative Anbieter durch Kauf deren Produkte und Serviceleistungen sowie konstruktive Kritik im Reifeprozess fördern
- Vermeidung von Vendor und Cloud Lock-in
- Innovationen mit Open Source entwickeln.

4.4 Mit Open Source Software die Zukunft gestalten

Open Source Softwareprodukte (OSS) stellen – insbesondere für die Öffentliche Verwaltungen – eine Alternative zum Einkauf und Betrieb von Produkten von Monopolisten dar. Dies vermeidet digitale Abhängigkeit, stärkt die Digitale Souveränität und fördert digitale Kompetenz [Ba23]. Eine pauschale Empfehlung für OSS kann allerdings nicht gegeben werden. Neben der Qualität der Software sind weitere Kriterien zu berücksichtigen, die für eine nachhaltige Nutzung stehen.

Von besonderer Bedeutung sind dabei auch das Governance- und das Lizenzmodell der Software [Ba23]. Governance definiert einen Ordnungsrahmen, der insbesondere die Mitsprache und Mitentscheidung regelt. Eine Governance beinhaltet eine Organisationstruktur mit festgelegten Rollen mit Verantwortlichkeiten, Richtlinien und Prozessen. Staatliche Einrichtungen sollten grundsätzlich nur in solche Open Source Projekte investieren, die digitale Nachhaltigkeit sicherstellen [Ba23].

Die Zahlen des Bitkom Open Source Monitors von 2021 belegen, das Open Source in der deutschen Wirtschaft angekommen ist: Der Einsatz und die Nutzung von Open Source gehört für die große Mehrheit der Unternehmen und Organisationen zum täglichen Geschäft [BI21] geworden.

Der Expertenkreis „Transformation der Automobilwirtschaft“, ein hochkarätig besetztes Beratungsgremium des BMWK spricht sich in einer Empfehlung vom Juni 2023 für einen ganzheitlichen Mindset Change hin zur Open-Source-Entwicklung aus, um den Automobilstandort Europa zu stärken [ET23]. Er schlägt u.a. vor, Open-Source freundliche rechtliche Rahmenbedingungen zu schaffen, die die Entwicklung und Nutzung von Open-Source-Software fördern (insbesondere IP-Recht, Haftungsrecht, Kartellrecht).

In den Öffentlichen Verwaltungen wird zunehmend das **Einer-für-alle-Prinzip (EfA-Prinzip)** praktiziert, d.h. Fachanwendungen werden einmalig entwickelt und allen anderen zur Verfügung gestellt. Das ZenDiS (Zentrum für Digitale Souveränität) unterstützt den Austausch von Programmen durch die Plattform OpenCoDE *www.opencode.de*.

Kollaborative Entwicklungen bringen Synergien, indem Kompetenzen organisations- bzw. unternehmensübergreifend gebündelt werden. Sie sparen Ressourcen, Kosten und Zeit. Durch den Austausch wird zudem die Qualität der gemeinsam entwickelten Produkte erhöht. Darüber hinaus entsprechen Investitionen in Open Source Projekte dem Prinzip der wirtschaftlichen Nachhaltigkeit.

Und nicht zuletzt sorgt OSS für **soziale Teilhabe** in allen gesellschaftlichen Schichten.

In jüngster Zeit entstehen immer mehr Communities, die sich mit Digitaler Souveränität und Open Source Software befassen, wie z.B. der AK OSS *https://ak-oss.gi.de* der GI Gesellschaft für Informatik e.V.

4.5 Empfehlung von alternativen Produkten

Um insbesondere Unternehmen und Institutionen Orientierung zum Einsatz und zur Beschaffung von Software zu bieten, haben wir eine Liste von Alternativen – meist Open Source-basierte Lösungen – auf digital-sovereignty.net zusammengestellt. Durch den vorzugsweisen Einsatz dieser Produkte wird der Wettbewerb belebt sowie Digitale Souveränität gestärkt. Auf der Basis von Feedback findet eine laufende Aktualisierung und Weiterentwicklung dieser Liste statt. Projektverantwortliche sollten bei Beschaffungen daher stets prüfen, ob bestimmte Funktionalitäten von Softwareprodukten bzw. -services nicht auch von einem europäischen Anbieter angemessen erfüllt werden.

5 Fazit und Ausblick

Zusammenfassend ist festzustellen, dass Digitale Souveränität eine grundlegende Voraussetzung für die "Enkelfähigkeit" unserer Gesellschaft und Wirtschaft ist. Wir alle sind aufgefordert, massive digitale Abhängigkeiten zu vermeiden, damit wir die digitale Zukunft frei und selbstbestimmt gestalten können.

Zur Umsetzung gehört auch Mut, neue Wege zu gehen und Verantwortung zu übernehmen. Projektmanager, Führungskräfte und für IT-Beschaffungen Verantwortliche sollten **bei der Auswahl von Software-Tools und IT-Dienstleistungen stets auch das Kriterium „Digitale Souveränität“ einbeziehen**. Insbesondere muss sichergestellt sein, dass die Datenhoheit und Innovationskraft erhalten bleiben und Erpressbarkeit unmöglich wird. Es gibt vielfältige Möglichkeiten, sich beim Aufbau und der Weiterentwicklung von Communities zu beteiligen. **Machen Sie mit**!

Zentrale Ergebnisse der hier vorgestellten Forschungsarbeiten sind:

1. Die digitale Abhängigkeiten Deutschlands und Europas haben inzwischen ein „besorgniserregendes Ausmaß“ erreicht und sind kritischer als die Abhängigkeiten von russischem Gas, da hierfür kein Plan B existiert und einige unumkehrbar sind.
2. Der vorgestellte und implementierte Souveränitätsscore ist eine pragmatische Möglichkeit, die Digitale Souveränität von eingesetzter Software zu messen.
3. Es gibt Lösungsansätze, Handlungs- und Produktempfehlungen zur Stärkung der Digitalen Souveränität (vgl. Kapitel 4).

Digitale Souveränität wird verstärkt zum Gütezeichen, mit dem Unternehmen Wettbewerbsvorteile erzielt können.

Der Souveränitätsscores ist praxisorientiert ausgerichtet, mit relativ leicht nachprüfbaren Kriterien und einer direkten Berechnungsmethode. Zwar wird zwischen Ko- und Standardkriterien unterschieden, eine weitere Unterscheidung oder Gewichtung findet allerdings nicht statt. Dies mindert die Möglichkeiten zur Abbildung des Grads der Digitalen Souveränität einer Software und legt einem unerfahrenen Nutzer nahe, alle Kriterien seien jederzeit gleich wichtig.

Weitere Limitationen und Kritikpunkte sind in [Jä23] aufgeführt. Diese bilden die Basis für **zukünftige Forschungsarbeiten und Folgeaktivitäten**:

- Souveränitätsscore um weitere messbare Kriterien erweitern
- Gewichtung von Kriterien vornehmen und/oder Subindizes für Kriterien entwickeln
- Alternativen-Finder entwickeln (Prototyp liegt bereits vor)
- Qualitätssicherung und Erweiterung der Handlungs- und Produktempfehlungen
- Ausbau der Website *digital-sovereignty.net* zu einer **zentralen Anlaufstelle und Community-Plattform für „Digitale Nachhaltigkeit“** mit zusätzlichen Funktionalitäten, wie z.B. Bewertungen der alternativen Lösungen.

Literaturverzeichnis

[AH23] Almasi N., van Helden P.: Deutschlands digitale Abhängigkeit: Von Souveränität kann keine Rede sein. https://digitaldependence.eu/wp-content/uploads/2023/03/Laenderstudie_Deutschland_Almasi_vanHelden_09032023.pdf

[Ba23] Bacharach, G. et.al.: Governance von Open Source Software, Empfehlungen für die Öffentliche Verwaltung – Diskussionsbeitrag. https://www.ossbig.at/wp-content/uploads/2023/05/2023-05-08-OpenSourceGovernance-Diskussionsberitrag-V3-1.pdf

[BI22] BITMi: Offener Brief an die Bundesregierung: BITMi warnt vor voranschreitender digitaler Abhängigkeit, 2022. https://www.bitmi.de/offener-brief-digitale-abhaengigkeiten/

[BMI20] Bundesministerium des Inneren und für Heimat, Digitale Souveränität, 2020. https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html

[Br20] Broy, M.: Deutschland ist auf dem Weg, ein digitales Entwicklungsland, eine digitale Kolonie zu werden. in TUM Forum Sustainability – Wissenschaft, Vernunft, Nachhaltigkeit, 1.7.2020, S. 112; https://mediatum.ub.tum.de/doc/1548492/1548492.pdf

[BU21] Bundesregierung: Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP von 12/2021. https://www.bundesregierung.de/breg-de/aktuelles/koalitionsvertrag-2021-1990800

[BU22] Bundesregierung: Digitalstrategie 09/2022: https://bmdv.bund.de/SharedDocs/DE/Anlage/K/presse/063-digitalstrategie.pdf?__blob=publicationFile

[ET23] Expertenkreis Transformation der Automobilwirtschaft (ETA): Durch Open-Source-Softwareentwicklung den Automobilstandort Europa stärken. https://expertenkreis-automobilwirtschaft.de/media/pages/home/8653794fe6-1686745132/expertenkreis-transformation-der-automobilwirtschaft_kurzpapier_open-source-software.pdf

[IT21] IT-Planungsrat: Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf

[Jä23] Jäger, J.: Digitale Nachhaltigkeit: Souveränitätsscore, 2023. Informatik-Masterarbeit, Universität Würzburg

[JS23] Jäger, J., Schweifler, R.: Digitale Nachhaltigkeit: Souveränitätsscore, 2023. Informatik-Master-Praktikumsbericht, Universität Würzburg

[JK23] Jahn, T., Kerkmann, C.: Microsoft hebt Preise für Geschäftskunden deutlich an. https://www.handelsblatt.com/technik/it-internet/cloud-computing-microsoft-hebt-preise-fuer-geschaeftskunden-deutlich-an/29050158.html

[Ka21] Kagermann, Henning; Streibich, Karl-Heinz; Suder, Katrin (2021): Digitale Souveränität. Status quo und Handlungsfelder. Deutsche Akademie der Technikwissenschaften (acatech). https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/

[Ka20] Kapalschinski, C.: Was passiert, wenn Google morgen entscheidet, seine Services in Europa abzuschalten?“. https://www.handelsblatt.com/autoren/christoph-kapalschinski/1986466.html

[Ke22] Kerkmann, C.: IT-Unternehmen erhöhen Preise für Software kräftig. https://www.handelsblatt.com/technik/it-internet/microsoft-oracle-sap-it-unternehmen-erhoehen-preise-fuer-software-kraeftig/28691308.html

[Kr20] Krcmar, H: Droht Europa eine digitale Kolonialisierung? CIO, 27.02.2020. https://www.cio.de/a/droht-europa-eine-digitale-kolonialisierung,3627664

[ML22] Mayer M., Lu Y.: Europa hat die Konsequenzen seiner digitalen Abhängigkeit noch kaum erkannt. https://www.kas.de/documents/252038/16166715/Europa+hat+die+Konsequenzen+seiner+digitalen+Abh%C3%A4ngigkeit+noch+kaum+erkannt.pdf/664c8d2d-48e4-e864-fafa-a16bfa5bdc37?version=1.3&t=1651564960080

[MS21] Murphy M., Scheuer S.: Datenschutzbeirat der Telekom warnt: Europa droht zur „digitalen Kolonie“ zu werden. Handelsblatt, 27-04-2021. https://www.handelsblatt.com/technik/it-internet/cloud-dienste-datenschutzbeirat-der-telekom-warnt-europa-droht-zur-digitalen-kolonie-zu-werden/27035912.html

[MW20] Mahn, J.; Wölbert, C.: Die riskante Abhängigkeit der Bundesrepublik von amerikanischen IT-Riesen; https://www.heise.de/hintergrund/Die-riskante-Abhaengigkeit-der-Bundesrepublik-von-amerikanischen-IT-Riesen-4881155.html

[PwC19] PwC: Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Berlin. https://wibe.de/wp-content/uploads/20190919_strategische_marktanalyse-compressed.pdf

[WB20] Wehnes, H.; Beger, A.: Die Wette ist eröffnet: Wird „Datenspende“ Wort des Jahres 2020? – GPM Online-Debatte mit dem Bundesdatenschutzbeauftragten Prof. Ulrich Kelber: Blindflug? Virtuelles Arbeiten im Kontext Datenschutz & Informationsfreiheit