SUSE

White Paper

Digitale Souveränität und Resilienz durch Einsatz von Open Source Software stärken

Angesichts der aktuellen geopolitischen Dynamik wird die Abhängigkeit der deutschen Verwaltung von einzelnen internationalen Software- und IT-Anbietern zu einem immer größeren Risiko. Durch den Einsatz von Open Source Software (OSS) können eine vollumfängliche Wechselfähigkeit zwischen unterschiedlichen Anbietern gesichert und somit politische Gestaltungsspielräume geschaffen werden.

Darüber hinaus stärkt das Prinzip der quelloffenen Software die Resilienz gegenüber externen Angriffen und bietet weitreichende Potenziale für den Ausbau einer nationalen und europäischen Softwareindustrie.

Digitale Souveränität und insbesondere der Einsatz von OSS müssen daher als Kernbestandteile einer nationalen Sicherheitsarchitektur und Beitrag zur langfristigen Sicherung der Wettbewerbsfähigkeit betrachtet werden.

Was ist zu tun?

1. **Schaffung gesetzlich verbindlicher Rahmenbedingungen für den vermehrten Einsatz von Open Source Software in der öffentlichen Verwaltung**
   Erforderlich ist ein gesetzlicher Vorrang von OSS bei allen öffentlichen Beschaffungen (verbindlicher Mindestanteil).

2. **Aktive Unterstützung des Einsatzes von OSS in der öffentlichen Verwaltung**
   Wir benötigen einen Bewusstseinswandel bei Behördenleitungen und Mitarbeitern. Dazu gehört es, alte Gewohnheiten, eingefahrene Geschäftsbeziehungen und kulturelle Vorbehalte zu überwinden. Innovative Ideen und Projekte müssen sichtbare Anerkennung erhalten.

3. **Nachhaltige und regelmäßige Investitionen des öffentlichen Sektors in das OSS-Ökosystem**
   Ein robuster und zukunftsfähiger Softwaremarkt in Deutschland erfordert ein klares Bekenntnis von Politik und Verwaltung zu einem flächendeckenden Wechsel von proprietären zu quelloffenen Anwendungen und Services.

4. **Nationale Open Source-Strategie**
   Ziele, Meilensteine und Rollen sind zu definieren, eindeutige Zuständigkeiten festzulegen sowie eine klare Governance und Evaluierung zu etablieren. Die in der Strategie formulierten Maßnahmen benötigen dedizierte Haushaltsmittel.

5. **Schaffung eines nationalen OSS-Zentrums**
   Das Zentrum für Digitale Souveränität (ZenDiS) sollte zur zentralen nationalen OSS-Anlaufstelle ausgebaut werden. Damit sichert es Interoperabilität, entwickelt ein Risikomanagement und wirkt bei der Definition von Sicherheitsanforderungen mit. Zu seinen Aufgaben zählen zudem die Marktbeobachtung, der Austausch von Best Practices sowie die Weiterbildung der öffentlichen Verwaltungen. Darüber hinaus organisiert das ZenDiS ein nationales OSS-Netzwerk unter Einbindung von Verwaltungen, Wissenschaft und OSS-Unternehmen.

6. **Einrichtung einer verantwortlichen Stelle in Behörden (Chief OSS-Officer)**
   Diese Person agiert als zentraler Ansprechpartner (behördenintern und -übergreifend) für die Beschaffung, den Einsatz und die Sicherheit von OSS-Software.

Die Bedeutung von Open Source Software für die digitale Resilienz und die Stärkung des digitalen Staates

Digitale Technologien haben in den vergangenen Jahrzehnten unser wirtschaftliches, politisches und soziales Leben grundlegend verändert. Sie haben maßgeblich zu Innovation, Wettbewerbsfähigkeit und Wohlstand beigetragen.

Zugleich werden Deutschlands wachsende Abhängigkeiten von anderen Staaten und einzelnen Anbietern entlang der technologischen Wertschöpfungsketten im Digitalbereich sichtbar – vor allem durch die zunehmende Nutzung von Cloud Computing sowie den Fortschritt bei KI, Big Data, IoT und Plattformtechnologien. In einer vernetzten, digitalisierten Welt erfordert die steigende Verwundbarkeit von IT-Infrastrukturen und Anwendungen daher eine kontinuierliche Stärkung der Resilienz auf allen Ebenen, von digitaler Infrastruktur bis hin zur Sicherheitsarchitektur.

Digitale Resilienz bedeutet, schnell auf Krisen reagieren zu können, um deren negative Auswirkungen zu minimieren. Darüber hinaus umfasst sie die Fähigkeit von Individuen, Institutionen und Unternehmen, digitale Technologien souverän zu nutzen, um Innovationen zu fördern und die Wettbewerbsfähigkeit zu sichern.

Digitale Souveränität ist eine wesentliche Voraussetzung für Resilienz. Auf der technischen Ebene von IT-Infrastrukturen und digitalen Anwendungen bedeutet sie in erster Linie die Vermeidung einseitiger Abhängigkeiten und damit verbunden die Fähigkeit, problemlos zwischen Technologien und Anbietern wechseln zu können. So vermeiden Organisationen Lock-in-Effekte und sichern die Kontrolle über Technologie und Daten. OSS bietet daher für staatliche Anwendungen erhebliche Vorteile, insbesondere dort, wo Sicherheit, Resilienz und Souveränität von entscheidender Bedeutung sind.

Open Source fördert Transparenz und eine Kultur der Zusammenarbeit und Überprüfbarkeit. Die öffentliche Verwaltung gewinnt Gestaltungsfreiheit, kann die Datenverarbeitung jederzeit nachvollziehen und hat die Möglichkeit, die eingesetzten Systeme bei Bedarf auszutauschen.

Darüber hinaus ist OSS das Rückgrat und der branchenübergreifende Motor der Digitalisierung weltweit und ein entscheidender Faktor für eine erfolgreiche digitale Transformation. Zudem sind die wirtschaftlichen Auswirkungen von OSS enorm: Eine Studie der EU-Kommission schätzt, dass jeder in OSS investierte Euro mehr als das Vierfache an Nutzen bringt.

Was ist Open Source Software?

Die folgenden Kriterien müssen erfüllt sein, damit eine Software als Open Source Software (OSS) bezeichnet werden darf:

- Der Quellcode liegt frei und öffentlich zugänglich vor.
- Die Software und Kopien dürfen ohne Einschränkungen genutzt werden.
- Die Software darf angepasst, verbessert und weitergegeben werden.

Transparenz, Sicherheit und Qualität

Die Tatsache, dass Informationen (z.B. Quellcode) für jedermann einsehbar und zugänglich sind, bedeutet nicht, dass jeder auch schreibend auf das Quellcode-Kontrollsystem zugreifen kann. Zugriffsrechte werden über entsprechende Governance-Strukturen festgelegt.

Datenhoheit, Transparenz und Sicherheit stehen bei OSS im Mittelpunkt. OSS-Lösungen fördern die Datensouveränität, indem sie Personen und Organisationen die Kontrolle über die Nutzung, Speicherung und den Zugriff auf ihre Daten ermöglichen. Der offene Quellcode erlaubt es Behörden, Anwendungen zu prüfen, Fehler zu beheben und Sicherheitslücken schnell zu schließen. OSS bietet somit ein hohes Maß an Sicherheit.

Da der Code öffentlich zugänglich ist, trägt eine große Gemeinschaft von Entwicklern und Sicherheitsexperten („Community“) durch ihr “Viel-Augen-Prinzip” dazu bei, dass Sicherheitslücken in der Regel schneller erkannt und behoben werden als bei proprietärer Software. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft Open Source-Systeme als sicherer ein, weil die öffentliche Überprüfbarkeit ein wirksames Mittel zur Qualitätssicherung ist.

Open Source-Anwendungen unterliegen schnellen Innovationszyklen. Eine der größten Herausforderungen beim Einsatz von OSS besteht daher in der häufig mangelnden Kompetenz von Organisationen und Verwaltungen, Anwendungen auf dem aktuellen Stand der Technik zu halten, anzupassen und permanent weiterzuentwickeln.

Ein wesentlicher Erfolgsfaktor für den Einsatz von OSS in der öffentlichen Verwaltung ist daher die Sicherung von Aktualität und Integrität der Anwendungen – entweder durch entsprechend qualifiziertes eigenes Personal oder durch spezialisierte Dienstleister, die eine hohe Qualität bei Support, Wartung und Zertifizierung garantieren.

Herstellerunabhängigkeit und Kosteneffizienz

In der Diskussion um digitale Souveränität stehen häufig Datenschutzaspekte und Datensouveränität im Vordergrund. Der Lock-in-Effekt, also die Abhängigkeit von Anbietern proprietärer Software, ist dagegen kaum präsent. Die damit verbundenen Nachteile sollten jedoch nicht unterschätzt werden.

Wenn einzelne Anbieter in der Lage sind, Lizenzbedingungen, Preise und sogar den Einsatz von Technologien zu diktieren, schränkt dies die Souveränität der öffentlichen Verwaltung erheblich ein.

OSS reduziert die Abhängigkeiten von proprietären Anbietern und fördert Interoperabilität, Modularität und Anpassbarkeit durch offene Standards und Schnittstellen. Dies stärkt auch die Handlungsfähigkeit in Krisensituationen .

Für viele proprietäre Produkte ist nicht der vollständige Quellcode verfügbar und interne Informationen werden nur sparsam kommuniziert. Der Einsatz von Lösungen, die ausschließlich auf OSS basieren, reduziert dagegen die Abhängigkeit von einzelnen Softwareanbietern. Anwender vermeiden so die Gefahr von Vendor Lock-ins, bei denen ein Wechsel zu anderen Produkten oder Dienstleistungen schwierig und teuer werden kann.

Ein weiterer Vorteil von OSS ist die Kosteneffizienz. Durch den Wegfall von Lizenzgebühren reduzieren sich die finanziellen Aufwände auf die (maßgeschneiderte) Entwicklung von Anwendungen und deren permanente Wartung. Darüber hinaus ermöglichen Open Source-Entwicklungsmodelle eine Arbeitsteilung – auch über unterschiedliche Institutionen hinweg – und damit eine Aufteilung der Kosten. Beispiele aus anderen europäischen Ländern zeigen, dass der Einsatz von OSS zu erheblichen Kosteneinsparungen führt.

Bedeutung und Potenziale von OSS für die Nutzung von Cloud-Technologien in der öffentlichen Verwaltung

Die Umstellung auf cloudbasierte Lösungen stellt öffentliche Verwaltungen gleich vor mehrere Herausforderungen. Sie müssen Anwendungen, die bisher auf eigener Hardware betrieben wurden, in die Cloud migrieren, diese Dienste sicher integrieren und dabei Abhängigkeiten von einzelnen Anbietern vermeiden. Open Source und offene Standards fördern auch in Cloud-Architekturen die digitale Souveränität, Sicherheit und Transparenz.

Open Source-Lösungen vereinen die Flexibilität und Skalierbarkeit der Cloud mit den Kontrollmöglichkeiten eines eigenen Rechenzentrums. Sie bieten umfassende Sicherheitsfunktionen und ermöglichen Exit-Strategien, die langfristige Unabhängigkeit und eine souveräne digitale Infrastruktur sichern.

Künstliche Intelligenz und Open Source

Der Einsatz künstlicher Intelligenz (KI) wird der Digitalisierung einen enormen Schub versetzen, bringt jedoch auch neue Herausforderungen für den Staat und die öffentliche Verwaltung mit sich – etwa im Bereich des Datenschutzes. Behörden sollten daher konsequent auf souveräne KI-Anwendungen setzen.

Dabei gelten die Anforderungen hinsichtlich Software- und Systemsicherheit unverändert auch für KI-Systeme und müssen konsequent umgesetzt werden.

OSS ist der Motor der Innovation im KI-Bereich. Sie sorgt dafür, dass Wissen, Tools und Technologien weltweit zugänglich sind und von einer breiten Gemeinschaft weiterentwickelt werden können. Daher ist Open Source Software essenziell, um eine faire, offene und nachvollziehbare KI-Entwicklung voranzutreiben. Behörden schaffen damit die notwendige Transparenz und das erforderliche Vertrauen.

Im Kontext der öffentlichen Verwaltungen muss der Fokus insbesondere auf folgenden Aspekten liegen:

- **Erklär- und Nachvollziehbarkeit:** Die technische Logik von Algorithmen ist komplex. Deshalb müssen die Informationsquellen und Entscheidungskriterien transparent und nachvollziehbar sein.
- **Flexibilität und Wahlmöglichkeit:** KI-Infrastrukturen sollten sich schnell an die Anforderungen der öffentlichen Verwaltung anpassen lassen. Dies erfordert Wahlfreiheit bei Large Language Models (LLMs) und eigenen KI-Komponenten.
- **Vertrauen auf allen Ebenen:** Der durchgängige Schutz personenbezogener Daten und die Einhaltung hoher Datenschutz-Standards sind Grundvoraussetzungen für die Bereitstellung vertrauenswürdiger KI-Anwendungen.
- **Transparenz der Trainingsdaten, mit der ein KI-System trainiert wurde.** KI-Anbieter sollten klar und verständlich darlegen, unter welchen Bedingungen ihr System funktioniert, damit Anwender dessen Eignung für ihren Zweck bewerten können. Der richtige Einsatz von KI bietet ein großes Potenzial für Behörden und unsere Wirtschaft. Die Demokratisierung von KI auf der Basis des Open Source-Modells ist daher ein entscheidender Faktor für die digitale Souveränität sowie für die Sicherung von Datenhoheit und Datenschutz.

Zusammenfassung

Open Source ist eine wesentliche Voraussetzung für Innovation und eine florierende Wirtschaft im digitalen Wandel. Nur durch Offenheit und Wahlmöglichkeiten können wir unabhängige Technologien in Deutschland und der EU vorantreiben, belastbare digitale Infrastrukturen schaffen und einen offenen und demokratischen Ansatz für neue Technologien fördern.

SUSE Software Solutions Germany GmbH

Frankenstraße 146
90461 Nürnberg
Deutschland

www.suse.com