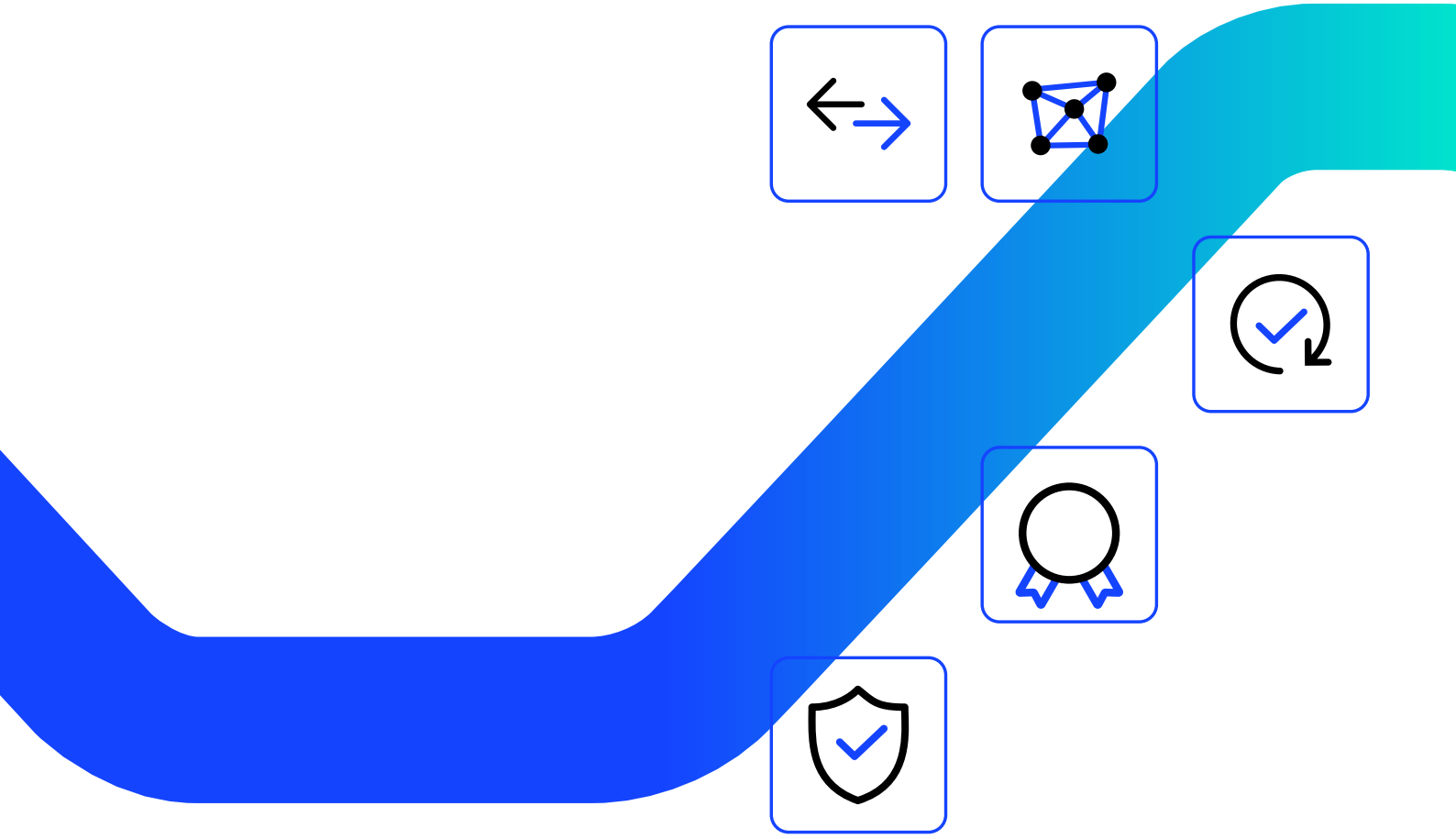
Sichere Softwarelieferketten:

openCode als Baustein einer souveränen digitalen Infrastruktur



openCode

Bundesamt
für Sicherheit in der
Informationstechnik

Inhaltsverzeichnis

Dieses Papier ist in Zusammenarbeit zwischen dem ZenDiS und BSI entstanden, um aufzuzeigen, wie das Sicherheitsniveau für Softwareprodukte in der Öffentlichen Verwaltung erhöht und harmonisiert werden kann.

www.opencode.de

openCode

www.zendis.de

Zen DiS Zentrum Digitale Souveränität

www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik

Die digitale Zeitenwende erfordert neue Sicherheitsstrategien

Deutschland und Europa stehen an einem Wendepunkt. Geopolitische Spannungen, strategische Technologiekonkurrenz und die steigende Zahl komplexer Cyberangriffe erfordern eine Neuausrichtung unserer digitalen Sicherheitsarchitektur. Gleichzeitig wächst die Bedeutung digitaler Dienste für Verwaltung, Wirtschaft und Zivilgesellschaft: Digitale Infrastruktur hat längst den Status der Systemrelevanz erreicht – sie ist nicht mehr nur technisches Hilfsmittel, sondern unentbehrliche Grundlage für das Funktionieren von Staat, Wirtschaft, Gesellschaft und Demokratie im 21. Jahrhundert.

In dieser digitalen Zeitenwende wird die Gewährleistung der Sicherheit und Beständigkeit digitaler Infrastrukturen zu einem zentralen Baustein für die Daseinsvorsorge – und damit zur Kernaufgabe des Staates. Gleichzeitig bietet der Aufbau eigener digitaler Kapazitäten erhebliches wirtschaftliches Entwicklungspotenzial und kann als Innovationsmotor für den Digitalstandort Deutschland wirken. Während auf europäischer Ebene an übergreifenden Strategien für technologische Unabhängigkeit gearbeitet wird,[1] liegt es an uns in Deutschland, diese Visionen durch konkrete Implementierungsschritte zu unterstützen und die praktischen Grundlagen für eine gemeinsame digitale Souveränität zu schaffen.

Ein zentraler Baustein ist dabei die Kontrolle über **Softwarelieferketten**.

Der „SolarWinds“-Vorfall hat 2020 eindrücklich gezeigt, wie angreifbar diese Lieferketten sind und wie schwer solche Angriffe zu erkennen sind. Bei diesem hochkomplexen Angriff wurden durch legitime Software-Updates Schadcode-Komponenten eingeschleust, die sich monatelang unbemerkt in den Systemen zahlreicher Regierungsbehörden und Unternehmen festsetzen konnten. Eine vollständige Prüfung solcher Softwarelieferketten ist angesichts ihrer Komplexität für einzelne Anbieter einer Software kaum realisierbar, egal ob es um Open-Source- oder proprietäre Software geht. Dies erfordert einen grundlegend neuen Ansatz, der über die Möglichkeiten einzelner Organisationen hinausgeht und die Fachkenntnisse von Sicherheitsexpert:innen, Entwickler:innen und Behörden gezielt bündelt, standardisierte Prüfverfahren etabliert und gemeinsame Sicherheitsanalysen ermöglicht.

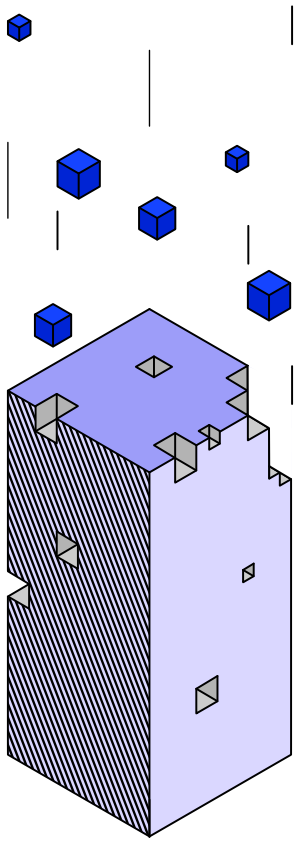
1 https://www.euro-stack.info

Fehlende Bausteine unserer digitalen Infrastruktur

Die Sicherheit digitaler Systeme hängt maßgeblich von der Qualität der Komponenten ihrer Lieferkette ab. Insbesondere im Cloudbereich besteht dabei derzeit eine problematische Abhängigkeit: Die Infrastruktur nahezu aller Container-Image-Lieferketten wird von wenigen privatwirtschaftlichen Anbietern kontrolliert. Diese Marktkonzentration führt zu einer faktischen Monopolstellung, die fundamentale Fragen zur digitalen Souveränität aufwirft.

Diese strukturellen Abhängigkeiten schaffen mehrfache systemische Risiken:

1. **Sicherheitsrisiken:** Kaum Transparenz und Verlässlichkeit in der Lieferkette.
2. **Handlungsunfähigkeit bei Vorfällen:** Behörden können nur allgemein warnen, nicht gezielt reagieren.
3. **Verlust der digitalen Souveränität:** Abhängigkeit von nicht-europäischen Diensten für kritische Infrastruktur, Kontrolle über wesentliche digitale Infrastruktur nicht gegeben.
4. **Fehlende Lagebilder:** Ein zentrales Lagebild der Lieferkette ist hinsichtlich der aktuellen zahlreichen unkoordinierten Teillösungen kaum realisierbar, bzw. die einzigen Lagebilder liegen beim privatwirtschaftlichen Dienstleister der Infrastruktur.
5. **Mangelnde Skalierung:** Manuelle Prüfprozesse können mit der Menge der auszuwertenden Daten im Rahmen moderner Cyberangriffe nicht Schritt halten. Sie erfordern einen unverhältnismäßig hohen Ressourceneinsatz bei gleichzeitig geringerer Zuverlässigkeit.



Konkret: Unsere Verwaltungen und Unternehmen sind derzeit von wenigen Technologieanbietern abhängig, deren zum Teil kostenlose Infrastrukturleistungen und Produkte wir nutzen, aber nicht kontrollieren können. Die aktuellen geopolitischen Entwicklungen machen deutlich, dass es das Ziel sein muss, Abhängigkeiten zu minimieren und Kontrolle und Einfluss auf Regularien und Sicherheitsstandards auszuweiten. Je wichtiger digitale Technologien für unsere Infrastruktur werden, desto kritischer wird diese fehlende Kontrolle.

openCode: Zentraler Baustein für eine souveräne digitale Infrastruktur

Die Plattform openCode stellt einen entscheidenden Baustein für den Aufbau einer souveränen digitalen Infrastruktur in Deutschland dar. Sie adressiert gezielt die kritischen Schwachstellen in der Softwarelieferkette und ermöglicht so einen strategischen Vorteil für souveränes staatliches Handeln in der digitalen Zeitenwende.

openCode etabliert verbindliche Sicherheitsstandards, macht Abhängigkeiten transparent und schafft nachvollziehbare Herkunftsnachweise für kritische Softwarekomponenten. So wird Open-Source Software zu einem Schlüsselelement einer resilienten digitalen Infrastruktur in Deutschland.

Die Plattform schafft erstmals einen Ort, der nicht nur die Prüfaufwände reduziert und die Softwarelieferkettensorgfalt zentral unterstützt, sondern auch die Beschaffenheit von Softwarekomponenten bewertbar machen kann.

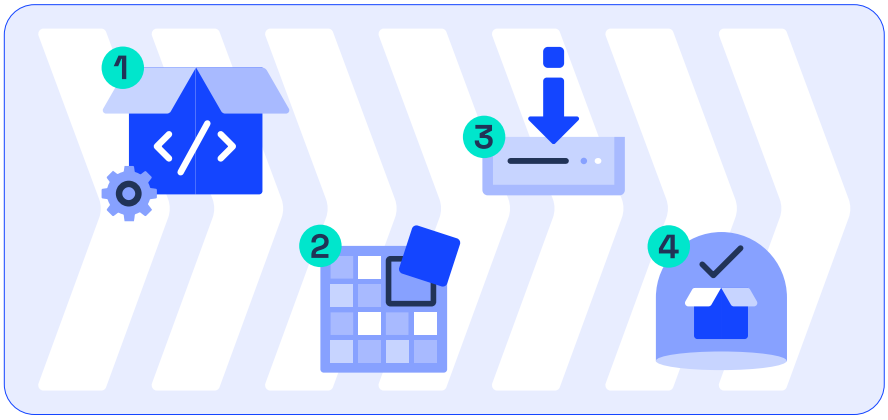
Dies bietet für Sicherheitsbehörden entscheidende Vorteile:

- Vollständiger Einblick in die Softwarelieferkette.
- Transparenz über verfügbare und geprüfte Container-Images der Öffentlichen Verwaltung.
- Ein umfassendes Lagebild durch Einblick in den zentralen Distributionsort und Verknüpfung von Sicherheitsrisiken.
- Zentrale Überwachungs- und Auditierungsmöglichkeiten, einschließlich des Monitorings verdächtiger Vorgänge.
- Effizientere Ressourcennutzung durch Bündelung von Audits und automatisierte Qualitätsprüfungen an einem zentralen Ort statt über viele verteilte Quellen.

Diese Vorteile ermöglichen es dem BSI und anderen Sicherheitsorganisationen, ihre gesetzlichen Aufgaben im Bereich der digitalen Sicherheit effizienter zu erfüllen und den wachsenden Bedrohungen wirksamer zu begegnen.

Paradigmenwechsel von Reaktion zu Prävention

Derzeitige Ansätze zur Softwaresicherheit sind weitgehend reaktiv: Nach einem Sicherheitsvorfall erfolgt eine allgemeine Warnung, ohne dass klar ist, welche Systeme betroffen sind. openCode kann einen präventiven Ansatz durch kontinuierliche, automatisierte Sicherheitsprüfungen und transparente Softwarelieferketten ermöglichen: Bei einem Sicherheitsvorfall können Artefakte und Betroffene zuverlässig identifiziert werden, sodass gezielt gewarnt werden kann.



Container Images und ihre Lieferkette

Was sind Container-Images?
Container-Images sind standardisierte, ausführbare Softwarepakete, die alle notwendigen Komponenten enthalten, um eine Anwendung auszuführen – einschließlich Code, Ausführungsumgebung, Bibliotheken und Konfigurationsdateien. Sie ermöglichen, dass Anwendungen zuverlässig in unterschiedlichen IT-Umgebungen laufen.

Container-Image-Lieferketten – So funktioniert's:
1. Erstellung: Entwickler bauen Container Images auf Basis von Grundlagen-Images (Base Images)

2. Speicherung: Die Images werden in spezialisierten Datenbanken (Registries) abgelegt

3. Verteilung: Bei Bedarf werden Images auf den Zielserver heruntergeladen

4. Ausführung: sogenannte "Container-Runtime-Systeme" starten die Images als isolierte Container

Sicherheitsrelevanz für die digitale Infrastruktur:
Container-Images bilden heute das Fundament moderner Cloud-Infrastrukturen und digitaler Dienste

Die Integrität der Container-Image-Lieferkette ist entscheidend für die Sicherheit der gesamten digitalen Infrastruktur

Manipulierte Container-Images können als Einfallstor für weitreichende Systemkompromittierungen dienen

Fehlende Transparenz über Herkunft und Inhalt von Container-Images erschwert Sicherheitsbewertungen

Bei Störungen in der Container-Image-Lieferkette können zahlreiche abhängige Dienste gleichzeitig ausfallen

Integration in die europäische Digitalstrategie

Im Kontext einer europäischen Digitalstrategie kann das Modell openCode als praktische Umsetzung der geforderten digitalen Souveränität dienen. Die Plattform verkörpert Prinzipien wie Datenhoheit, Interoperabilität und Sicherheit durch offene Standards und transparente Prozesse.

Resilienz durch Dezentralisierung

Im Gegensatz zu bisherigen, zentralisierten Infrastrukturen[2] setzen wir bei openCode auf ein Modell mit verteilter Verantwortung und Kontrolle. Diese Verteilung stärkt nicht nur die Widerstandsfähigkeit gegen Ausfälle, sondern reduziert auch geopolitische Abhängigkeitsrisiken. Durch eine dezentrale Verbundsinfrastruktur und abgestimmte Governance-Strukturen kann die digitale Handlungsfähigkeit Deutschlands auch in Krisenszenarien gewährleistet werden, ohne von einzelnen ausländischen Anbietern abhängig zu sein.

Skalierung und Automatisierung

Die wachsende Komplexität moderner Softwarelieferketten und die Vielzahl digitaler Projekte in der öffentlichen Verwaltung machen nicht nachnutzbare und vollständig manuelle Sicherheitsprüfungen zunehmend unpraktikabel bis unmöglich. openCode adressiert diese Herausforderung durch intelligente Automatisierung: Das Badge-Programm ist Teil eines breiteren Ansatzes, der Zugang zu Metadaten und Quellcode ermöglicht. So können etwa Behörden bei Sicherheitsvorfällen nicht nur allgemein warnen, sondern gezielt betroffene Systeme identifizieren und Gegenmaßnahmen einleiten. Diese Skalierbarkeit verbessert nicht nur die Effizienz, sondern erhöht auch die Reaktionsfähigkeit bei neuen Sicherheitsbedrohungen – ein entscheidender Vorteil in einer Zeit, in der die Geschwindigkeit digitaler Angriffe stetig zunimmt.

→ https://badges.opencode.de/de

Das Badge-Programm von openCode

Was sind Badges?
Badges sind Qualitätssiegel, die automatisiert den Status von Software-Projekten bewerten und visualisieren. openCode prüft dafür Softwareprojekte anhand definierter Kriterien und vergibt entsprechende Badges in den Bereichen Sicherheit, Wartung und Nachnutzung.

Das Badge-Programm – So funktioniert's:

Automatisierte Prüfung:
Software-Repositories werden nach festgelegten Kriterien durchsucht

Transparente Darstellung:
Die Ergebnisse werden in Form von Badges visualisiert

Sichtbare Einbindung:
Badges werden im Softwareverzeichnis angezeigt

Nachvollziehbare Erklärung:
Detaillierte Begründung zeigt, welche Kriterien erfüllt wurden

Warum ist das hilfreich?
Badges schaffen Orientierung bei der Bewertung von Software-Qualität

Transparente Qualitätskriterien erleichtern Entscheidungen bei der Softwarebeschaffung

Entwicklungsteams erhalten einen klaren Anreiz zur Einhaltung von Sicherheits- und Qualitätsstandards

Die Nachnutzung von qualitätsgeprüfter Software wird gefördert

2 Beispiel: DockerHub ist eine der weltweit meistgenutzten Registries für Container-Images. Container-Images sind standardisierte, portable Softwarepakete, die Anwendungen mit allen benötigten Abhängigkeiten in einer isolierten Umgebung bereitstellen – ein fundamentales Element moderner Cloud-Infrastrukturen. Neben DockerHub existieren zwar auch die Registries großer Cloud-Anbieter, jedoch bleibt DockerHub besonders für Open-Source-Projekte dominant. Die Marktkonzentration auf wenige, nicht-europäische Anbieter führt zu mangelnder Transparenz über Herkunft und Sicherheit der Images und schafft kritische Abhängigkeiten in der globalen digitalen Infrastruktur.

Unser Lösungsansatz: openCode als Kernbaustein für sichere Softwarelieferketten

Um die Vision von openCode als Baustein einer souveränen digitalen Infrastruktur zu verwirklichen, schlagen wir folgende vier Umsetzungsschritte vor:

Ein sicheres System zur Softwareprüfung und -herstellung mit Verifikationsprozess

Eine hochsichere Entwicklungsumgebung und Build-Infrastruktur mit automatisierten Prüfverfahren bietet:

- Transparenten Einblick in Entstehungsprozesse von Software
- Standardisierte, skalierbare Sicherheitsprüfungen statt Einzelfallbetrachtungen
- Sofortiges Feedback zu Sicherheitsrisiken für Entwickler:innen
- Reduzierte Compliance-Aufwände durch standardisierte und automatisierte Prozesse

Souveräne Container-Registry mit einheitlichen Standards

Ein dezentrales Verzeichnis für geprüfte Container-Images mit klaren Sicherheitskriterien ermöglicht:

- Unabhängigkeit von externen Anbietern in Krisenszenarien
- Einheitliche Bewertungsgrundlage für die öffentliche Verwaltung
- Garantierte Compliance mit europäischen Regulierungen

Resiliente Verteil-Infrastruktur für Software

Eine dezentrale Bereitstellungslösung gewährleistet:

- Aufrechterhaltung kritischer digitaler Dienste auch in Krisensituationen
- Höhere Zuverlässigkeit und Verfügbarkeit von Diensten
- Schnellerer Zugriff durch lokale Bereitstellung
- Integration in bestehende Sicherheitsarchitekturen

Gemeinsame Qualitätskriterien und Prüfstandards

Eine mit dem BSI abgestimmte Definition von Qualitätskriterien für Container-Images und Software-Komponenten:

- Klare Standards für „zuverlässige Container-Images"
- Einheitliche Grundlage für automatisierte Prüfverfahren
- Transparente und nachvollziehbare Einschätzungen für alle Beteiligten

Gemeinsam für Digitale Souveränität

Die digitale Zeitenwende erfordert entschlossenes Handeln. Mit openCode steht bereits heute eine Plattform bereit, die zum Fundament einer souveränen digitalen Infrastruktur ausgebaut werden kann. Für eine erfolgreiche Umsetzung ist eine enge Zusammenarbeit zwischen allen beteiligten Behörden und Institutionen erforderlich.

Wir sind überzeugt: Die Stärkung digitaler Souveränität ist eine Aufgabe von nationaler Bedeutung. In einer vernetzten Welt bedeutet Souveränität nicht die vollständige Autarkie, sondern die Fähigkeit des Staates, seine digitalen Infrastrukturen jederzeit selbstbestimmt zu gestalten und zu kontrollieren.

Ein handlungsfähiger Staat muss seine kritischen Systeme verstehen, beeinflussen und im Krisenfall unabhängig betreiben können – eine Grundvoraussetzung, um seine Kernaufgaben im digitalen Zeitalter zu erfüllen und die Interessen seiner Bürgerinnen und Bürger zu schützen.

Wir laden alle Stakeholder ein, diesen wichtigen Prozess mitzugestalten. Nur gemeinsam können wir eine digitale Infrastruktur aufbauen, die unsere staatliche Handlungsfähigkeit sichert, unsere demokratischen Grundwerte stärkt und die notwendige Resilienz für die Herausforderungen der Zukunft bietet.

Umsetzungsplan

Um den Herausforderungen zu begegnen, schlagen wir eine Schrittweise Implementierung vor. Aufgrund der gebotenen Dringlichkeit, mahnen wir schnelles Handeln und mutige Schritte, die Abhängigkeiten zu adressieren, an.

2025: Grundlagen schaffen

- Einführung und Ausbau des Badge-Programms[3] für automatisierte Qualitäts- und Sicherheitsprüfungen
- Aufbau einer ersten Container-Registry als souveräne, verlässliche Bezugsquelle für Container-Images Implementierung grundlegender Signierungsmechanismen
- Gemeinsame Entwicklung von Qualitätskriterien in Abstimmung mit dem BSI für sichere Container

2025–2026: Ausbau der Infrastruktur

- Etablierung einer hochsicheren Build-Umgebung
- Proof of Concept für die Prüfung von Qualitätskriterien in Abstimmung mit dem BSI
- Integration der europäischen Compliance-Anforderungen
- Entwicklung von Lagebildern zur Erkennung und Bewertung von Sicherheitsrisiken

Ab 2026: Strategische Integration

- Ausbau zu einer krisenfesten Infrastruktur (mit Verteidigungsfallniveau)
- Integration in die nationale Sicherheitsarchitektur
- Unterstützung für kritische Infrastrukturen
- Aufbau einer Dezentralen und Föderierten Infrastruktur für Softwarelieferketten

3 https://badges.opencode.de/de

Das Badge-Programm von openCode ist ein innovatives Qualitätssicherungssystem, das Software-Repositories automatisiert auf Sicherheits- und Qualitätskriterien prüft. Ähnlich wie Gütesiegel im Handel kennzeichnen die Badges (Bronze, Silber, Gold) unterschiedliche Qualitätsstufen, die auf transparenten, messbaren Kriterien basieren. Entwickler erhalten sofort detailliertes Feedback, welche Kriterien ihr Projekt bereits erfüllt und welche Verbesserungen für die nächste Stufe notwendig sind. Das System automatisiert Prozesse, die bisher überwiegend manuell oder in jeweils nur aufzubauenden Umgebungen durchgeführt werden, und macht so hochwertige Sicherheitsüberprüfungen skalierbar.

Open Source als Grundlage für Digitale Souveränität

Die Digitale Souveränität der Öffentlichen Verwaltung basiert auf drei strategischen Zielen, die durch den Einsatz von Open-Source-Software maßgeblich unterstützt werden:

Wechselmöglichkeiten

Open Source bietet der Öffentlichen Verwaltung Flexibilität bei der Wahl von IT-Lösungen und -Anbietern:

- Durch offene Standards entsteht echte Wahlfreiheit
- Open-Source-Lizenzen sichern die langfristige Nutzung
- IT-Architekturen können bedarfsgerecht angepasst werden
- Interoperable Systeme erleichtern den Austausch von Lösungen

Gestaltungsfähigkeit

Open Source stärkt die Fähigkeit der Verwaltung, ihre IT aktiv mitzugestalten:

- Transparenz durch Einblick in den Quellcode
- Aufbau von IT-Expertise durch praktische Erfahrung
- Möglichkeit zur bedarfsorientierten Weiterentwicklung
- Förderung der verwaltungsübergreifenden Zusammenarbeit

Einfluss auf Anbieter:innen

Open Source stärkt die Position der Verwaltung gegenüber im Dialog mit IT-Anbieter:innen:

- Förderung eines vielfältigen Marktes durch offene Standards
- Einbringen spezifischer Anforderungen zu Funktionalität und Datenschutz
- Option zum Betrieb in eigenen Rechenzentren der Verwaltung
- Partnerschaftliche Zusammenarbeit bei der Weiterentwicklung

Über das ZenDiS

Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) unterstützt die Öffentliche Verwaltung in Bund, Ländern und Kommunen dabei, sich aus kritischen Abhängigkeiten von einzelnen Technologieanbietern zu lösen.

Dazu stellt es neben Kompetenzen, Services und Beratung auch eine Kooperations- und Entwicklungsplattform sowie leistungsfähige, skalierbare und leicht zugängliche Open-Source-Lösungen bereit. Zudem bündelt das ZenDiS die Anforderungen der Öffentlichen Verwaltung und stellt gemeinsam mit seinen Partnern sicher, dass Lösungen bedarfsgerecht weiterentwickelt und zuverlässig betrieben werden.

Herausgeber

Zentrum für Digitale Souveränität der Öffentlichen Verwaltung GmbH
(ZenDiS)
Suttner-Nobel-Allee 4
44803 Bochum
E-Mail: hallo@zendis.de
Web: www.zendis.de

Ansprechpartner

Leonhard Kugler
Abteilungsleitung Open-Source-Plattform
leonhard.kugler@zendis.de
www.opencode.de

Stand

März 2025