Gehärtete Container-Images für die Öffentliche Verwaltung

Secure Government Container Initiative (SGCI)

Zielsetzung

Sichere Softwarelieferketten sind heutzutage für einen handlungsfähigen digitalen Staat unabdingbar. Sie sind die Basis für Software, ohne die staatliches Handeln gefährdet wäre. Die Lieferketten beschreiben den Weg einer Software vom jeweiligen Autor bis zur Einbindung in die Verwaltungssoftware. Ist eine einzelne Komponente vulnerabel oder ungewartet, kann das Gesamtsystem gefährdet sein. Daher sind sie längst als kritische Ressourcen zu betrachten.

Um die digitale Handlungsfähigkeit der Verwaltung zu sichern, bauen wir ein gemeinsames Kooperationspartnernetzes auf. Mit Fokus auf die letzte Meile der Softwareentwicklung, der Container-Distribution, schafft dieses Netzwerk operativ einen verlässlichen und sicheren Bezugsort.

Die Container dieses Ökosystems sollen die qualitativen Anforderungen der Deutschen Verwaltungscloud (DVC) und des Cyber Resilience Acts (CRA) erfüllen. Gleichzeitig sollen sie anschlussfähig an den Deutschland-Stack sein. Dieses neue Ökosystem schafft somit einen gemeinsamen Sicherheits- und Qualitätsstandard für Container in der Verwaltung.

Damit entsteht auf openCode ein souveräner Raum für die gesamte OCI-Containerlandschaft – sicher, wiederverwendbar, überprüfbar und föderal anschlussfähig. Es ist ein entscheidender Schritt hin zu einer digitalen Verwaltung, die ihre Grundlagen selbst kontrolliert und gestaltet.

Container sind isolierte Prozesse und bündeln Anwendungscode sowie alle Abhängigkeiten, damit die Software in unterschiedlichen Umgebungen gleich läuft.

Container-Images sind Archive, die alle notwendigen Bibliotheken, Dateien und Abhängigkeiten enthalten, um den Container zu erstellen und auszuführen.

Container-Härtung reduziert Schwachstellen, indem man beispielsweise mehrstufige Sicherheitskontrollen hinzufügt, Transparenz- und Wartungsanforderungen erhöht oder unnötige Komponenten entfernt.

container.gov.de

Nutzen und Mehrwert

- **Einheitliche und nachvollziehbare Standards**
  Konsistent aufgebaute und dokumentierte Container-Images schaffen Klarheit für Entwicklung, Betrieb und Sicherheitsprüfung (z. B. CycloneDX und VEX als OCI-Attestierung).
- **Deutliche Reduktion von Sicherheitsrisiken**
  Container-Schwachstellen werden aktiv bewertet. Dadurch erreichen weniger Fehlalarme (z. B. falsch-positive CVE-Meldungen) den Betrieb.
- **Härtung nach Best Practices**
  Moderne Sicherheitsmaßnahmen wie der Verzicht auf unnötige Shells reduzieren Angriffsflächen und erhöhen die Robustheit der eingesetzten Software-Bausteine.
- **Weniger Prüfaufwand**
  Wiederverwendbare und gehärtete Container-Images reduzieren Sicherheitsprüfungen in den Verwaltungen.
- **Hohe Nachnutzbarkeit und Kompatibilität**
  Wo sinnvoll, werden bestehende Open-Source-Komponenten integriert und eine Upstream-Kompatibilität gewährleistet. Die Verwaltung agiert damit als dezentraler Integrator, statt eigene Insellösungen zu bauen.
- **Gemeinsame Weiterentwicklung**
  Das Netzwerk fungiert als Architektin und Motor des Ökosystems. Sie treibt den technischen Aufbau voran und sorgt dafür, dass Containerstandards in der Verwaltung nicht nur definiert, sondern auch praktisch umgesetzt werden.
- **Kostensenkung**
  Durch abgestimmte Vorgehensweisen, geteilte Bausteine und gemeinsame Pflege sinken Aufwand und Kosten für alle Beteiligten signifikant.

„Unsere Containerstrategie verbindet offene Standards mit föderaler Zusammenarbeit und schafft damit einen neuen Sicherheits- und Qualitätslevel für Verwaltungssoftware. Mit jedem geprüften Container wächst ein gemeinsamer, sicherer Werkzeugkasten der Verwaltung für moderne Softwareentwicklung."

Leonhard Kugler

Vorgehen

Die Plattform openCode baut durch Kooperationen mit dem BSI, Auslands-IT des Auswärtigem Amt, weiteren Ressorts, Ländern und öffentlicher IT ein **Netzwerk zur Entwicklung eines containerbasierten, geprüften und standardisierten Softwarelieferketten-Ökosystems** auf. Es werden wiederverwendbare gehärtete Container-Images erstellt und auf der Plattform bereitgestellt.

Dreh- und Angelpunkt ist die **Website** „container.gov.de“. Dort werden die Container-Images zur Nachnutzung nach Zulassung veröffentlicht und Interessierte können sich beteiligen. Die von openCode bereitgestellten Images liegen im dazugehörigen **Repository**.

Durch regelmäßigen Austausch, klare Verantwortlichkeiten und offene Beteiligung entsteht eine **belastbare Grundlage** einer sicheren, geprüften Container-Landschaft für die öffentliche Verwaltung.

Beteiligungsmöglichkeiten

→ 1. Kooperationspartner / „First Mover“ auf strategischer Ebene

Organisationen auf Policy Ebene, die mit einem initalen Investment gemeinsam mit dem ZenDiS den Aufbau einer verwaltungsweiten Container-Infrastruktur vorantreiben.

- gemeinsam genutzte Ressourcen wie abgestimmte Hardening-Guidelines, Baselines und Container-Images, um Kosten zu senken
- gemeinsame Governance-Strukturen (z. B. zukünftiges Steuerungsgremium)
- definierte Rahmenbedingungen für den verwaltungsweiten Einsatz gehärteter Images

Wie das funktioniert:

- Aktive Mitgestaltung und Einbringung eigener Anforderungen
- Teilnahme an strategischen Abstimmungen und übergreifenden Formaten

Jetzt strategischen Einstieg abstimmen!

→ 2. Auftraggebende für Härtungsleistungen (operativ / bedarfsgesteuert)

Auftraggeber, die Container-Images prüfen, analysieren oder härten lassen möchten. Dabei entstehen:

- Kooperationsverträge zwischen ZenDiS, etwaigen Dienstleistenden aus dem Ökosystem und Auftraggebenden
- sicherheitsüberprüfte, dokumentierte OSS-Container-Images
- Erstellung von SBOMs, CVE- und VEX-Analysen
- Anwendung von Härtungsmaßnahmen durch Updates, Abhängigkeitstrimmung und Minimalisierung des Basisimages
- Perspektivisch: Bezug geprüfter Images über ein vertragliches Modell (inkl. vertragliche Vereinbarungen zu Wartung & Pflege)

Jetzt Leistungsauftrag klären!

→ 3. Community Contributor mit technischer Mitarbeit

Organisationen, IT-Dienstleistende und Entwickler:innen, die aktiv geprüfte Container-Images bereitstellen. Dabei entstehen:

- nachnutzbare, standardisierte und geprüfte Container-Images
- gemeinsame technische Bausteine für die Verwaltung

Wie das funktioniert:

- Bereitstellung gehärteter Container-Images zur Listung auf container.gov.de (unter Einhaltung der definierten Kriterien)
- Mitarbeit an technischen Standards, Dokumentation und Härtungsprozessen
- Bei Bedarf Bereitstellung von Expertise oder Dienstleistern für die technische Entwicklung spezifischer Komponenten

Jetzt Container-Image bereitstellen!

→ 4. Community-Mitglied für Konsultation & Informationsaustausch

Organisationen, die verbindlich an der fachlichen Ausrichtung mitwirken, informiert bleiben und Bedarfe einbringen. Dabei entsteht:

- transparenter Austausch
- Feedbackmentalität zu vorgelegten Policies, Guidelines und Images
- Ein wachsendes, föderales Netzwerk

Wie das funktioniert:

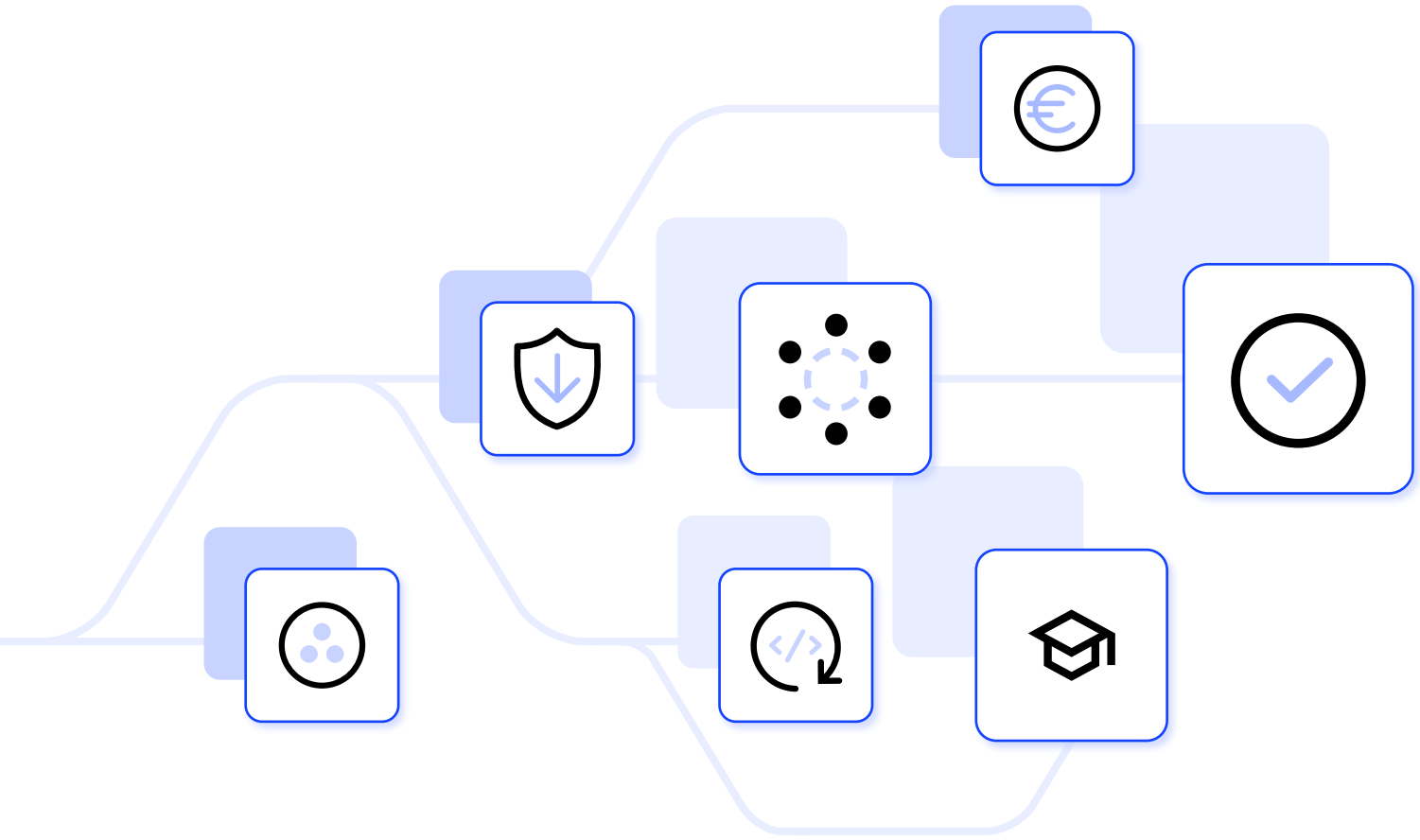
- Teilnahme an Informationsveranstaltungen, Konsultationen & Austauschformaten
- Beitrag von Feedback zu Hardening-Guidelines, Policies oder Images

Jetzt in den fachlichen Austausch einsteigen!

Gerne erläutern wir Ihnen die möglichen Beteiligungsformen im Detail und klären offene Fragen in einem persönlichen Gespräch.

Wir laden Sie herzlich ein, sich an der Ausgestaltung der nächsten Schritte zu beteiligen und freuen uns auf den weiteren Austausch!

Janou Feikens
Community Managerin
container@opencode.de



Das Zentrum für Digitale Souveränität (ZenDiS) stellt mit **openCode** eine ebenenübergreifende Plattform bereit, die Open-Source-Software nutzbar macht und veröffentlicht.

In Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik hat ZenDiS Anfang 2025 ein **Strategiepapier zu sicheren Softwarelieferketten (sSDLC)**[1] innerhalb der Öffentlichen Verwaltung veröffentlicht. Zentrales Anliegen ist der **Abbau einer problematischen 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.

1 https://opencode.de/de/wissen/publikationen/ssdlc-strategiepapier-wissen