
From Code to Trust: Sichere Softwarelieferketten als Bestandteil der nationalen Sicherheitsarchitektur

Leonhard Kugler, Geschäftsführer ZenDiS
Julian Schauder, Development Lead ZenDiS



**Dieses Papier ist im Rahmen des 21.
Deutschen IT-Sicherheitskongresses 2026
des BSI entstanden und ebenfalls Teil des
publizierten Tagungsbandes.**

Inhaltsverzeichnis

Kurzfassung	4
1. Einleitung und Zielsetzung	5
2. Von der Einzelfallprüfung zur Gestaltung sicherer Ausgangsbedingungen	6
3. Das Badgeprigramm als Instrument präventiver Sicherheitsgovernance	8
4. container.gov.de als Infrastrukturbaustein sicherer Softwarelieferketten	10
5. Ausblick: Quality Gate als Ende-zu-Ende-Absicherung	12
6. Fazit	14

Kurzfassung:

Moderne Softwarelieferketten sind zu einem zentralen Angriffsziel geworden und stellen die öffentliche Verwaltung vor die Herausforderung, Sicherheit nicht mehr nur auf Ebene einzelner Anwendungen, sondern entlang der gesamten Entstehungs- und Distributionsprozesse zu gewährleisten. Der vorliegende Beitrag zeigt, wie durch den Einsatz automatisierter, standardisierter und föderal anschlussfähiger Maßnahmen Transparenz und Steuerungsfähigkeit in komplexen Softwarelieferketten geschaffen werden können.

Am Beispiel der Plattform openCode werden zwei komplementäre Instrumente vorgestellt: das **Badgeprogramm** als Infrastruktur zur kontinuierlichen, automatisierten Bewertung von Softwareprojekten sowie **container.gov.de** als souveräne Distributionsplattform für gehärtete Container-Images. Beide Ansätze folgen dem Prinzip „**Compliance as Code**“ und verlagern Sicherheit von einer nachgelagerten Prüfung hin zu einer strukturellen Eigenschaft digitaler Infrastruktur.

Gemeinsam bilden sie die Grundlage für ein übergreifendes **Quality Gate**, das die Softwarelieferkette Ende-zu-Ende absichert und damit einen operativen und Lagebildfähigen Beitrag zur Stärkung digitaler Souveränität und staatlicher Handlungsfähigkeit leistet.

1

Einleitung und Zielsetzung

Digitale Infrastrukturen haben den Status kritischer staatlicher Ressourcen erreicht. Was lange als technisches Hilfsmittel galt, ist heute unentbehrliche Grundlage für das Funktionieren von Verwaltungsleistungen, Sicherheitsbehörden und öffentlichen Diensten – und damit ein zentraler Baustein staatlicher Daseinsvorsorge. Das bedeutet auch: Die Gewährleistung von Sicherheit, Integrität und Verfügbarkeit dieser Infrastrukturen ist nicht länger eine Fachfrage der IT-Abteilungen, sondern eine Kernaufgabe des Staates. Zudem zeigen aktuelle Sicherheitsvorfälle – von SolarWinds über Log4Shell und die xz-Backdoor bis zur Kompromittierung von axios Anfang 2026 – ein verändertes Bedrohungsbild: Angriffe adressieren zunehmend nicht mehr einzelne Systeme oder Anwendungen, sondern die vorgelagerten Lieferketten, also Build-Prozesse, Abhängigkeiten und Distributionswege. Die Kompromittierung einer einzigen Komponente kann sich über Tausende nachgelagerter Systeme ausbreiten. Risiko wird damit systemisch, und nicht mehr punktuell.

Das eigentliche Problem liegt also weniger in der einzelnen Schwachstelle als in einer grundlegenden strukturellen Intransparenz: Für öffentliche Institutionen ist häufig nicht nachvollziehbar, welche Softwarekomponenten in welchen Systemen zum Einsatz kommen, woher diese stammen, wer sie pflegt und ob bekannte Schwachstellen adressiert werden. Abhängigkeiten, Build-Prozesse und Distributionswege sind oft undokumentiert oder liegen außerhalb staatlicher Kontrolle. Die Konsequenz: Ein belastbares gesamtstaatliches Lagebild existiert nicht, weil die Datenbasis, die dies erfordern würde, nicht zugänglich ist.

Open Source kann hier eine strukturelle Voraussetzung schaffen, die proprietäre Ansätze nicht bieten können, denn Quellcode, Abhängigkeiten und Entstehungsprozesse sind prinzipiell einsehbar und maschinenles- und auswertbar. Dieses Potential wird jedoch nur dann eingelöst, wenn die entsprechenden Rahmenbedingungen (standardisierte Prüfverfahren, gemeinsame Infrastrukturen, verbindliche Anforderungen an Transparenz und Nachvollziehbarkeit) aktiv geschaffen werden. Genau hier setzt der vorliegende Ansatz an.

Die bestehenden Sicherheitsansätze in der öffentlichen Verwaltung – punktuelle Prüfungen, vertragliche Zusicherungen und lokal organisierte Einzelfallbewertungen – sind notwendig und haben ihre Berechtigung. Sie stoßen jedoch angesichts wachsender Interdependenz, steigender Angriffsgeschwindigkeit und begrenzter Ressourcen an strukturelle Grenzen. Sie sind nicht skalierbar genug, um die Komplexität moderner Softwarelieferketten systematisch zu erfassen, und sie adressieren das fertige Produkt – nicht die Bedingungen, unter denen es entsteht. Was fehlt, ist keine Alternative zu diesen Verfahren, sondern eine ergänzende Infrastruktur, die das adressiert, was Einzelfallprüfungen strukturell nicht leisten können: eine übergreifende, kontinuierliche und automatisierbare Bewertungsebene.

Ziel dieses Beitrags ist es, aufzuzeigen, wie Softwarelieferketten als Teil einer nationalen Sicherheitsarchitektur verstanden und präventiv abgesichert werden können. Zentrale Fragestellung ist, wie durch automatisierte, standardisierte und föderal anschlussfähige Verfahren Risikotransparenz geschaffen wird, die staatliches Handeln gezielt unterstützt, und zwar jenseits isolierter Projekt- oder Produktbetrachtungen.

Dazu werden zwei komplementäre Instrumente vorgestellt, die auf der Plattform openCode entwickelt und bereitgestellt werden:

1. Das Badgeprogramm als Instrument standardisierter Qualitäts- und Sicherheitsbewertung sowie

2. container.gov.de als souveräne Distributionsinfrastruktur für gehärtete Container-Images mit der Möglichkeit der Anbindung relevanter Sicherheits-Infrastrukturen zur Erfassung und Nachverfolgung von Lieferkettenangriffen (z.B. seitens des BSI).

[Zum
Badgeprogramm](#)

container.gov.de

Beide Instrumente werden im Kontext eines übergreifenden Ansatzes eingeordnet, der Sicherheit nicht als nachgelagerte Maßnahme, sondern als strukturelle Eigenschaft digitaler Infrastruktur begreift. Die Steuerung der Software-Lieferkette ermöglicht erstmalig defensive Maßnahmen durch gezielte Ansprache von Betroffenen und Nachverfolgung detektierter Kompromittierungen.

openCode ist die zentrale Entwicklungs-, Prüf- und Bereitstellungsplattform für Open-Source-Software der öffentlichen Verwaltung in Deutschland. Mit über 13.500 Nutzenden und 5.700 Projekten ist openCode der größte Open-Source-Hub der deutschen Verwaltung. Die Plattform wird durch das Zentrum für Digitale Souveränität (ZenDiS) betrieben und versteht sich als operativer Infrastrukturbaukasten für die Umsetzung digitaler Souveränität.

2

Von der Einzelfallprüfung zur Gestaltung sicherer Ausgangsbedingungen

Die heutige sicherheitspolitische Herausforderung moderner Softwarelieferketten erfordert eine Erweiterung der etablierten Ansätze. Die bisherige Praxis – nachgelagerte Prüfung fertiger Produkte, reaktive Bewertung nach Bekanntwerden von Schwachstellen, projektbezogene Einzelfallanalysen – bleibt notwendig, reicht jedoch alleine nicht mehr aus. Sie setzt am Output an, also dort, wo das Risiko bereits materialisiert ist – und kann damit die vorgelagerten Entstehungsbedingungen, in denen systemische Risiken aufkommen können, nicht adäquat erfassen.

Der hier vorgestellte Ansatz verschiebt den Fokus: von der Bewertung fertiger Artefakte hin zur Gestaltung der Bedingungen, unter denen sichere Software entsteht. Nicht das einzelne Endprodukt steht im Mittelpunkt, sondern der Prozess, die Komponenten und die Infrastruktur, die dieses Produkt erst möglich machen. Sicherheit wird damit von einer Eigenschaft, die im Einsatz geprüft wird, zu einer Eigenschaft, die in den Entstehungsbedingungen und -prozess verankert ist.

Diese Erweiterung der Sicherheitsstrategie auf die gesamte Lieferkette hat eine technische und eine strategische Dimension.

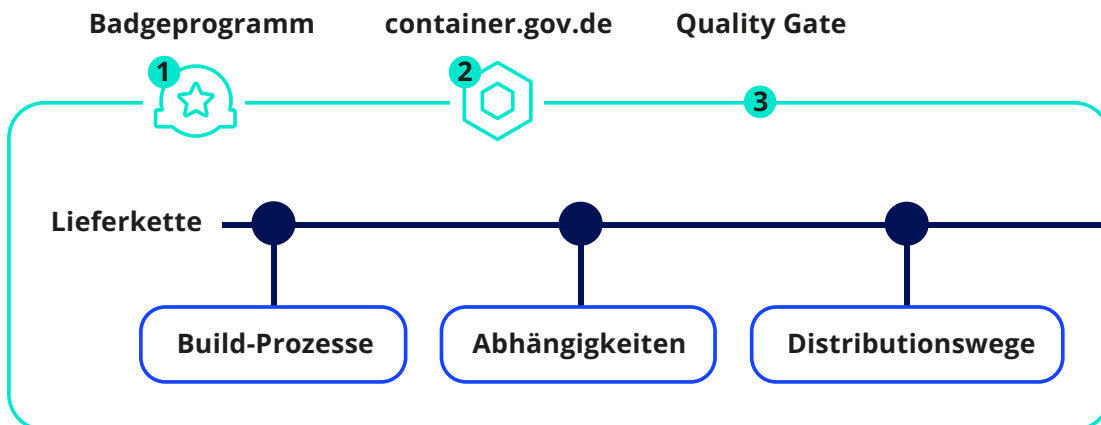


Abbildung 1: Schrittweise Absicherung der Softwarelieferkette durch Bewertung (Badgeprogramm) und kontrollierte Bezugsquellen (container.gov.de).

Technisch bedeutet er: Verifizierbare Artefakte – Software Bills of Materials (SBOM), Vulnerability Exploitability Exchange (VEX), kryptografische Attestierungen – machen Herkunft, Zusammensetzung und Sicherheitsrelevanz von Software systematisch und automatisiert erfassbar. Nicht menschliche Gutachter prüfen Einzelfälle individuell, sondern maschinenlesbare Nachweise ermöglichen kontinuierliche, reproduzierbare und skalierbare Bewertung. Der Einsatz von VEX-Dokumenten zur kontextuellen Schwachstellenbewertung stellt dabei in der öffentlichen Verwaltung eine Innovation dar: openCode etabliert hier eine Praxis, die es in dieser Form bislang nicht gab.

Strategisch bedeutet das: Der Staat verlagert seinen Steuerungsansatz. Statt Sicherheit am fertigen Produkt nachzuweisen – was bei komplexen, mehrfach verschachtelten Lieferketten ohnehin nur eingeschränkt möglich ist – gestaltet er die Bedingungen, unter denen Software entwickelt, geprüft und bereitgestellt wird. Sicherheitsanforderungen werden nicht primär administrativ oder rechtlich definiert und ex post kontrolliert, sondern technisch operationalisiert und in die Infrastruktur selbst eingebettet.

Dieses Vorgehen folgt dem Prinzip Compliance as Code: Prüfprozesse werden reproduzierbar, skalierbar und organisationsübergreifend nutzbar. Was als Anforderung definiert wird, wird zugleich als automatisierter Prüfmechanismus implementiert. Sicherheit wird damit von einer reaktiven und betriebsorientierten Maßnahme zu einem kontinuierlichen Bestandteil digitaler Infrastruktursteuerung.

Die Tragweite dieses Ansatzes reicht über den Bereich der IT-Sicherheit hinaus. Kritische Infrastrukturen – Energie, Verkehr, Wasserversorgung – werden seit jeher als Gegenstand aktiver staatlicher Gestaltung verstanden: Der Staat definiert nicht nur Mindestanforderungen, sondern gestaltet die Bedingungen, unter denen diese Infrastrukturen sicher und resilient betrieben werden können. Für digitale Infrastrukturen gilt dieser Blick bislang nur eingeschränkt. Angesichts ihrer wachsenden und heute bereits zentralen Bedeutung und der strukturellen Intransparenz, die sie kennzeichnet, ist es an der Zeit, digitale Softwarelieferketten mit demselben Gestaltungsanspruch zu behandeln. Damit verlagert sich staatliche Steuerung notwendigerweise von der Prüfung einzelner Ergebnisse auf die Gestaltung von Rahmenbedingungen – das muss heute auch explizit für digitale Infrastrukturen gelten. Der hier beschriebene Ansatz geht einen Schritt in diese Richtung: Handlungsfähigkeit entsteht nicht durch die vollständige Kontrolle

einzelner Artefakte, sondern durch den Aufbau von Infrastrukturen, die transparente Rahmenbedingungen schaffen und informierte Bewertungen sowie gezielte Reaktionen ermöglichen. Dieses Vorgehen folgt zentralen Prinzipien wie Transparenz, Attestierung, Überprüfbarkeit und Nachvollziehbarkeit sowie Skalierbarkeit, Automatisierung und der Nutzung offener Daten und Verfahren.

3

Das Badgeprogramm als Instrument präventiver Sicherheitsgovernance

Eine zentrale Rolle in diesem Ansatz spielt das openCode-Badgeprogramm. Es fungiert als Übersetzungsschicht zwischen sicherheitspolitischen Anforderungen und technischer Umsetzung: Definierte Kriterien in den Dimensionen Sicherheit, Wartung, Lizenzierung und Nachnutzung werden automatisiert geprüft und in standardisierter Form dargestellt. Dabei werden die auf openCode verfügbaren Repositories kontinuierlich und automatisiert analysiert, sodass die Vergabe von Badges nicht auf freiwilligen Einzelfallprüfungen beruht, sondern systematisch und flächendeckend erfolgt.



Abbildung 2: Bewertungsstufen von Softwareprojekten durch das openCode-Badgeprogramm anhand definierter Qualitäts- und Sicherheitskriterien.

Der entscheidende Beitrag des Badgeprogramms liegt dabei nicht in der Prüfung selbst – Audits sind kein neues Instrument. Er liegt in der Standardisierung und Aggregierbarkeit der Prüfergebnisse. Bislang erzeugen Sicherheitsbewertungen in der öffentlichen Verwaltung isolierte Einzelergebnisse: Ein Projekt wird geprüft, das Ergebnis liegt bei der prüfenden Stelle, es ist weder vergleichbar noch übertragbar. Das Badgeprogramm erzeugt demgegenüber eine gemeinsame, maschinenlesbare Bewertungsebene über Projekt- und Organisationsgrenzen hinweg – die Grundlage für ein übergreifendes Lagebild, das bislang nicht existiert.

Anstelle binärer Sicherheitsbewertungen – sicher oder unsicher – macht das Programm den Erfüllungsgrad definierter Kriterien kontinuierlich und gestuft sichtbar. Damit übernimmt es eine Governance-Funktion: Es ergänzt punktuelle Einzelfallprüfungen durch standardisierte Verfahren, schafft eine gemeinsame Bewertungslogik und unterstützt informierte Entscheidungen bei Beschaffung, Betrieb und Nachnutzung. Dadurch werden Skalierbarkeit, Nachvollziehbarkeit und die Erstellung eines übergreifenden Lagebilds ermöglicht.

Besonders deutlich wird der prozessorientierte Charakter auf den höheren Badge-Stufen. Während die unteren Stufen primär statische Merkmale eines Repositories prüfen (Vorhandensein von Lizenzen, Dokumentation, grundlegende Sicherheitsmerkmale), erfordert die Erreichung höherer Stufen den Nachweis etablierter und kontinuierlich gelebter Entwicklungs- und Wartungsprozesse. Dazu zählen beispielsweise ein nachvollziehbares Schwachstellenmanagement, kurze Reaktionszeiten auf gemeldete Issues sowie regelmäßige Code-Reviews und aktive Pflege des Projekts.

Damit verschiebt sich der Prüfgegenstand: Nicht das Release zu einem bestimmten Zeitpunkt wird bewertet, sondern die Qualität des Prozesses, der Releases hervorbringt und aktuell hält. Das ist die konkrete technische Umsetzung des oben beschriebenen Perspektivwechsels – von der Produktprüfung zur Prozessgovernance.

Die sicherheitsbezogene Bewertung im openCode-Badgeprogramm folgt einem automatisierten, regelbasierten Prüfansatz. Sicherheitsanforderungen werden dabei als definierte Kriterien modelliert und kontinuierlich auf Repository-Ebene überprüft. Im Mittelpunkt steht nicht die einmalige Prüfung eines Artefakts, sondern die Bewertung von Prozessen und Projektzuständen – etwa ob bekannte Schwachstellen adressiert werden, ob Sicherheitspraktiken etabliert sind und ob ein Projekt aktiv gepflegt wird.

Die Bewertung erfolgt entlang mehrerer Dimensionen, insbesondere Sicherheit, Wartbarkeit, Nachnutzung und Rechtssicherheit, und wird in Form gestufter Badges visualisiert. Diese gestufte Logik ermöglicht eine differenzierte Einschätzung des Reifegrads eines Projekts und schafft Anreize zur kontinuierlichen Verbesserung.

Technisch basiert das System auf einer modularen Architektur aus Metrik-Erhebung, regelbasierter Bewertung und standardisierter Ausgabe. Die Ergebnisse werden sowohl visuell als Badges als auch maschinenlesbar bereitgestellt und können in bestehende Entwicklungsprozesse integriert werden.

Damit fungiert das Badgeprogramm als skalierbare, föderal anschlussfähige Bewertungsinfrastruktur, die Qualitäts- und Sicherheitskriterien automatisiert überprüfbar macht und eine vergleichbare Entscheidungsgrundlage für die Nachnutzung von Software schafft. Durch seine Umsetzung als Open-Source-basierte, RESTful-API ist das System nicht an eine einzelne Plattforminstanz gebunden, sondern kann flexibel in unterschiedliche Umgebungen integriert und eigenständig betrieben werden. Diese Architektur ermöglicht eine organisationsübergreifende Nutzung und stellt eine zentrale Voraussetzung für den Einsatz des Badgeprogramms als Bestandteil gesamtstaatlicher Sicherheitsarchitekturen dar.

4

container.gov.de als Infrastrukturbaustein sicherer Softwarelieferketten

Moderne Verwaltungssoftware basiert zunehmend auf Container-Technologie: standardisierte Einheiten, die Software zusammen mit allen Abhängigkeiten „verpacken“ und so eine konsistente Ausführung in unterschiedlichen Umgebungen ermöglichen. Die Deutsche VerwaltungscLOUD-Strategie (DVS) setzt explizit auf containerbasierte Lösungen. Jede dieser Komponenten erfordert jedoch kontinuierliche Härtung: regelmäßige Prüfung und Absicherung gegen neu bekanntwerdende Schwachstellen.

Mit container.gov.de entsteht hierfür eine souveräne Distributionsinfrastruktur für geprüfte und gehärtete Container-Images in der öffentlichen Verwaltung. Die Plattform stellt einen zentralen Bezugsort für standardisierte, sicherheitsgeprüfte Artefakte dar und verknüpft diese mit nachvollziehbaren Prüf- und Bewertungsinformationen.

Die Umsetzung erfolgt im Rahmen der Secure Government Container Initiative (SGCI), einem Kooperationsnetzwerk aus Bund, Ländern, öffentlichen IT-Dienstleistern und weiteren Akteuren. Ziel dieses Netzwerks ist es, gemeinsame Standards für die Erstellung, Härtung und Bewertung von Container-Images zu entwickeln, Ressourcen zu bündeln und einen organisationsübergreifend nutzbaren Bestand geprüfter Softwarekomponenten aufzubauen.

Während das Badgeprogramm Transparenz über den Zustand von Software schafft, adressiert container.gov.de die Kontrolle über deren Herkunft und Distribution. Die komplementäre Frage dazu lautet: Woher beziehen wir die Komponenten, aus denen unsere Systeme bestehen – und unter wessen Kontrolle steht dieser Bezugsweg?

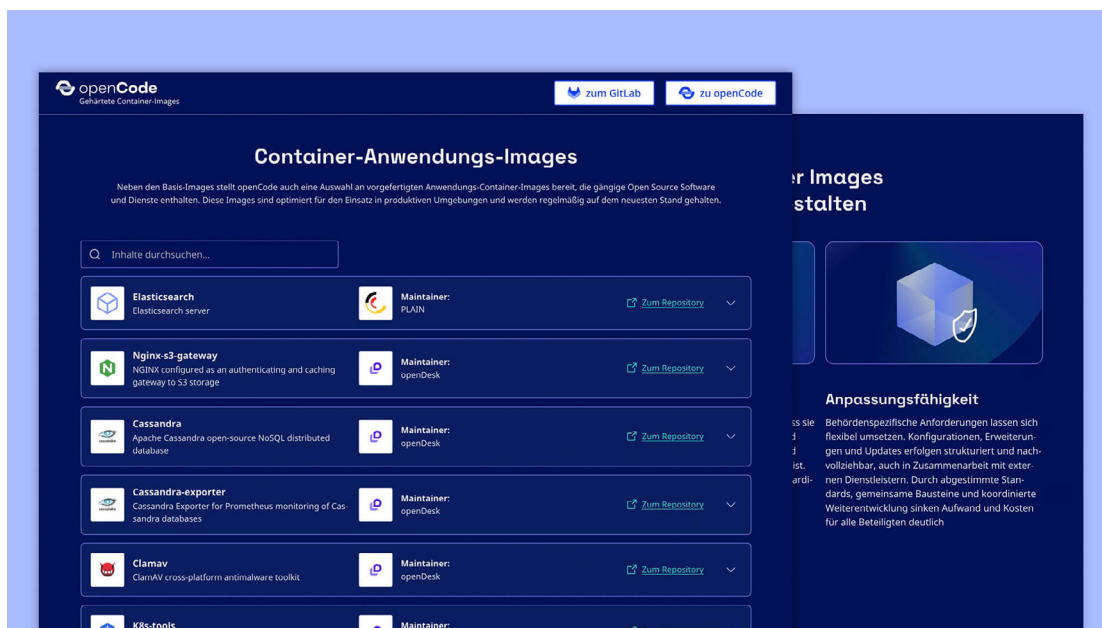


Abbildung 3: container.gov.de als zentraler Bezugsort für geprüfte und gehärtete Container-Images der öffentlichen Verwaltung.

Dieser Prozess geschieht derzeit fragmentiert und redundant. Die Container-Image-Lieferketten der öffentlichen Verwaltung werden faktisch von wenigen privatwirtschaftlichen, überwiegend nicht-europäischen Anbietern kontrolliert. Jede Organisation, die containerbasierte Software betreibt, muss entweder in kostenintensiver Eigenregie härten oder externe Dienstleister beauftragen. Die öffentliche Verwaltung zahlt vielfach für denselben Aufwand und verfügt dabei jeweils über Kontrolle im eigenen Zuständigkeitsbereich. Was fehlt, ist eine übergreifende Sicht: Herkunft, Integrität und Härtingsstandards der eingesetzten Komponenten sind nicht konsolidiert erfassbar, belastbare organisationsübergreifende Lagebilder lassen sich auf dieser Basis nicht erstellen.

Mit `container.gov.de` entsteht ein souveräner, föderal anschlussfähiger Bezugsraum für geprüfte und gehärtete Container-Images in der öffentlichen Verwaltung. Die Plattform verknüpft standardisierte Härtings- und Prüfprozesse mit verifizierbarer Herkunft und klar definierten Qualitätskriterien. Gehärtete Images werden durch automatisierte Prozesse auf `openCode` erzeugt, orientiert an Marktstandards wie SLSA (Supply-chain Levels for Software Artifacts) und den Anforderungen des Cyber Resilience Acts.

Die sicherheitsbezogene Bewertung von Container-Images auf `container.gov` baut auf dem in Kapitel 2 beschriebenen Compliance-as-Code-Ansatz auf, bei dem Sicherheitsanforderungen als maschinenlesbare Policies formuliert und automatisiert überprüft werden. Die zugrunde liegende Compliance-Policy ist in der Policy-Sprache Rego implementiert und prüft eine zentrale Bedingung: Alle bekannten Schwachstellen mit hohem oder kritischem Schweregrad dürfen sich nicht im Status einer unbehandelten Bewertung befinden.

Zentrale Grundlagen dieser Bewertung sind standardisierte Artefakte wie SBOM (Software Bill of Materials) und VEX (Vulnerability Exploitability Exchange). Die SBOM bildet ein vollständiges, maschinenlesbares Inventar aller im Container enthaltenen Komponenten und ermöglicht die automatisierte Zuordnung bekannter Schwachstellen. VEX ergänzt diese Informationen um eine kontextuelle Bewertung und beantwortet die entscheidende Frage, ob eine identifizierte Schwachstelle im konkreten Nutzungskontext des Images tatsächlich ausnutzbar ist.

Damit verschiebt sich der Fokus von einer rein detektiven Betrachtung („Welche Schwachstellen existieren?“) hin zu einer bewertungsbasierten Risikotransparenz, bei der jede relevante Schwachstelle explizit klassifiziert und begründet werden muss. Unbewertete Schwachstellen sind im Sinne der Compliance nicht zulässig, unabhängig davon, ob sie technisch behoben wurden.

Die Einhaltung dieser Anforderungen wird vollständig automatisiert überprüft und kann direkt in CI/CD-Pipelines integriert werden. Die Ergebnisse werden in standardisierten Formaten bereitgestellt und ermöglichen eine reproduzierbare, skalierbare Sicherheitsbewertung über Organisationsgrenzen hinweg.

Ergänzt wird dieser Ansatz durch systematische Härtingsprozesse, die darauf abzielen, die Angriffsfläche von Container-Images zu minimieren und die Auswirkungen erfolgreicher Angriffe zu begrenzen. Härtung folgt dabei dem Prinzip der „Post-Exploit-Sicherheit“: Selbst im Fall einer Kompromittierung wird der Handlungsspielraum eines Angreifers durch reduzierte Systemkomplexität und restriktive Laufzeitumgebungen gezielt eingeschränkt.

In Kombination mit standardisierten Attestierungen, kryptografischen Signaturen und etablierten Spezifikationen entsteht so eine Infrastruktur, in der Container-Images nicht nur bereitgestellt, sondern als nachvollziehbar geprüfte und kontextualisierte Sicherheitsartefakte ausgeliefert werden. Dies bildet die Grundlage für vertrauenswürdige und

skalierbare Softwarelieferketten in der öffentlichen Verwaltung.

Als Referenz für die praktische Umsetzung dienen Projekte wie openDesk und PLAIN, deren Komponenten systematisch analysiert, gehärtet und in die Distributionsinfrastruktur integriert werden. Diese Integration zeigt exemplarisch, wie bestehende Softwarebausteine aus realen Verwaltungsprojekten entlang definierter Sicherheitsstandards weiterverarbeitet, überprüft und organisationsübergreifend zur Nachnutzung bereitgestellt werden. Damit wird die Verbindung zwischen Entwicklungsumgebung, Prüfmechanismen und Distribution konkret operationalisiert und die angestrebte durchgängige Absicherung der Softwarelieferkette erstmals praktisch umgesetzt.

Die Verknüpfung mit dem Badgeprogramm ist dabei konstitutiv, nicht optional: Ergebnisse automatisierter Prüfungen – SBOM, CVE-Status, VEX-Informationen – werden direkt mit den bereitgestellten Container-Images verbunden. container.gov liefert also nicht nur Artefakte, sondern Artefakte mit nachvollziehbarer Bewertungshistorie. Verwaltungen können auf geprüfte Komponenten zurückgreifen, ohne Sicherheitsbewertungen jeweils neu durchführen zu müssen, weil die Bewertung als standardisierter, maschinenlesbarer Nachweis an das Artefakt gebunden ist.

Damit bilden das Badgeprogramm und container.gov.de zwei komplementäre Seiten desselben Ansatzes: Monitoring und Sourcing. Das Badgeprogramm schafft die Bewertungsgrundlage – es macht prüfbar, was vorher intransparent war. container.gov.de schafft die Bezugsgrundlage – es stellt bereit, was vorher aus unkontrollierten Quellen stammte. Gemeinsam adressieren sie die beiden Kernprobleme struktureller Intransparenz in Softwarelieferketten: Wir wissen nicht, was drin ist, und wir kontrollieren nicht, woher es kommt.

Über den operativen Nutzen hinaus erfüllt container.gov.de eine strategische Funktion. Die Plattform reduziert Abhängigkeiten von extern kontrollierten Distributionsinfrastrukturen, schafft zentrale Lagebilder über eingesetzte Container-Komponenten und unterstützt koordinierte Reaktionen im Sicherheitsvorfall. Wo vorher notwendigerweise Vertrauen aus Alternativlosigkeit bestand (Komponenten wurden bezogen, weil keine geprüfte Alternative existierte), entsteht nun die Möglichkeit einer informierten und damit auch demokratisch legitimierbaren Entscheidung auf Basis nachvollziehbarer Prozesse.

5

Ausblick: Quality Gate als Ende-zu-Ende-Absicherung

Das Badgeprogramm etabliert Prüfkriterien und eine gemeinsame Bewertungsebene. container.gov.de stellt gehärtete, bewertete Artefakte bereit. So wird die Grundlage für eine umfassende Klammer gelegt: ein Quality Gate, das die gesamte Softwarelieferkette – von der Entwicklung über die Prüfung bis zur Bereitstellung – unter eine kohärente Sicherheitsarchitektur stellt.

Technisch als „Secure Software Development Lifecycle (sSDLC)“ bezeichnet, umfasst dieses Quality Gate drei zentrale Komponenten:

1. **Common Distribution Infrastructure:** Eine gemeinsame Verteilungsinfrastruktur stellt sicher, dass geprüfte Software-Artefakte zuverlässig und sicher an alle Nutzer verteilt werden.

2. Common Build Infrastructure: Eine gemeinsame Build-Infrastruktur gewährleistet, dass Software unter definierten und nachvollziehbaren Bedingungen erstellt wird. Transparente und dokumentierte Build-Prozesse ermöglichen es, die Entstehung von Artefakten zu verstehen und bei Bedarf selbst nachzuvollziehen oder erneut auszuführen.

3. Common Standard for Quality: Ein gemeinsamer Qualitätsstandard definiert, welche Anforderungen Software erfüllen muss, um das Quality Gate zu passieren. Dieser Standard wird automatisiert geprüft.

Das Quality Gate schließt den Bogen:

- **Mission 1** (Badgeprogramm) definiert die Bewertungskriterien
- **Mission 2** (container.gov.de) stellt gehärtete Artefakte bereit und
- **Mission 3** sichert den gesamten Prozess Ende-zu-Ende ab.

Software, die das Quality Gate passiert hat, ist verbindlich geprüft – von der Herkunft ihrer Komponenten über den Build-Prozess bis zur Distribution.

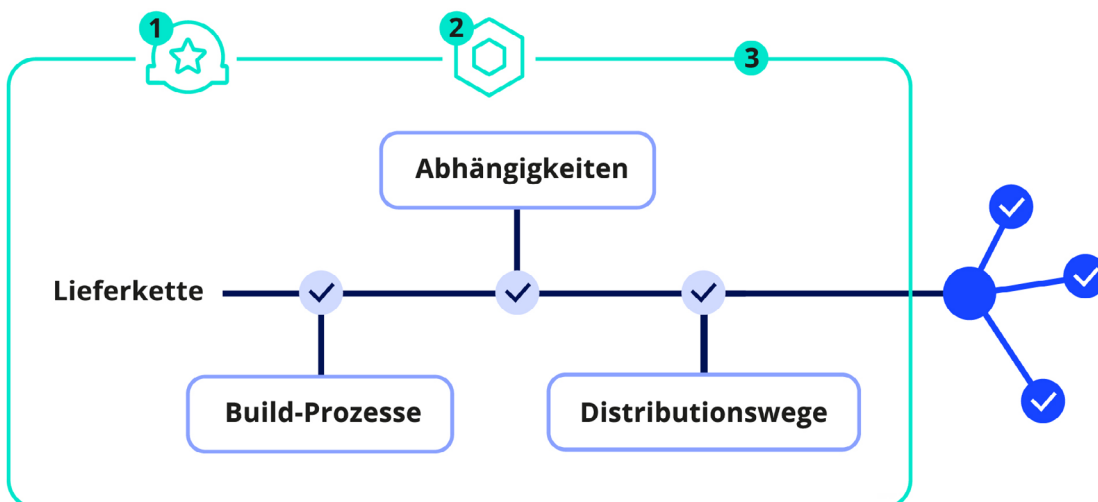


Abbildung 4: Durchgängige Absicherung der Softwarelieferkette durch ein Quality Gate entlang aller zentralen Komponenten.

Dieses Zielbild befindet sich derzeit in der Konzeptphase. Ein Grobkonzept liegt vor. Die sequenzielle Struktur – 1) Bewertungskriterien, 2) gehärtete Artefakte, 3) durchgängige Absicherung – ist dabei nicht beliebig, sondern folgt einer technischen und organisatorischen Aufbau-logik: Jede Stufe schafft die Voraussetzung für die nächste.

Die konsequente Umsetzung dieses Ansatzes schafft eine Fähigkeit, die bislang nicht existiert: Sicherheitsrelevante Informationen aus der Lieferkette – Komponenten, Schwachstellen, Härtungsnachweise – können systematisch in die operative Betriebsebene übergeben und dort mit bestehenden Sicherheitsprozessen verknüpft werden. Reaktive und präventive Ansätze wachsen so zu einer kohärenten Sicherheitsarchitektur zusammen: Prävention schafft die Grundlage für informierte Reaktion, und Reaktion profitiert von der Transparenz, die Prävention erzeugt. Das Lagebild, das daraus entsteht, ist nicht das Ergebnis nachträglicher Analyse, sondern in die Infrastruktur selbst eingebettet.

6

Fazit

Sichere Softwarelieferketten sind keine rein technische Fragestellung. Im 21. Jahrhundert sind sie eine zentrale Voraussetzung für die Fähigkeit des Staates, seine digitalen Infrastrukturen zu verstehen, zu gestalten und im Krisenfall handlungsfähig zu bleiben.

Der in diesem Beitrag vorgestellte Ansatz zeigt, wie dieser Anspruch operativ eingelöst werden kann. Der Perspektivwechsel – von der nachgelagerten Prüfung einzelner Produkte zur vorgelagerten Gestaltung sicherer Bedingungen – wird durch das Badgeprogramm und container.gov-Instrumente konkretisiert und komplettiert durch lagebildfähige Transparenz der Lieferkette. Perspektivisch schließt ein Quality Gate (sSDLC) diese beiden Säulen zu einer durchgängigen Sicherheitsarchitektur zusammen: gemeinsame Build-Infrastruktur, gemeinsame Distribution, gemeinsame Qualitätsstandards.

Das Zusammenspiel dieser Instrumente macht Software-Supply-Chain-Sicherheit von einer reaktiven Einzelmaßnahme zu einem strategischen Bestandteil staatlicher Infrastruktur. Durch Lagebilder entlang der Lieferkette werden erstmals defensive Maßnahmen möglich: Die gezielte Ansprache betroffener Institutionen und die Nachverfolgung erkannter Angriffe schaffen ein neues Niveau an Reaktionsfähigkeit – in einer Zeit, in der Angriffe auf die Software-Lieferkette zunehmend das Niveau staatlicher und nachrichtendienstlicher Akteure erreichen. Handlungsfähigkeit entsteht nicht durch den Versuch umfassender Kontrolle jedes einzelnen Artefakts, sondern durch die Gestaltung von Bedingungen, unter denen Transparenz, Bewertbarkeit und gezielte Reaktion möglich werden.

In einer vernetzten Welt bedeutet digitale Souveränität nicht Autarkie, sondern die Fähigkeit des Staates, seine kritischen digitalen Infrastrukturen jederzeit selbstbestimmt zu verstehen, zu gestalten und zu kontrollieren. Der hier vorgestellte Ansatz liefert dafür einen konkreten operativen Baustein.

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
Geschäftsführer
leonhard.kugler@zendis.de
www.opencode.de

Stand

August 2026

www.zendis.de



www.opencode.de



www.container.gov

