eGovernment-Wettbewerb

ITZBund gewinnt mit LISSA

[30.09.2026] Mit LISSA entwickelt das ITZBund eine standardisierte und automatisierte Lieferkette für sichere Software. Beim eGovernment-Wettbewerb 2026 erreichte LISSA den ersten Platz in der Kategorie „Souveränität, Sicherheit und Stabilität digitaler Infrastrukturen“.

Cloud, Künstliche Intelligenz und steigende Anforderungen an Cyber-Sicherheit und digitale Souveränität verändern nach Einschätzung des Informationstechnikzentrum Bund (ITZBund) die Entwicklung und den Betrieb von Fachverfahren grundlegend. Dabei geraten zunehmend auch die Softwarelieferketten in den Blick: Einerseits soll die öffentliche Verwaltung die Kontrolle über ihre Entwicklungsprozesse behalten, andererseits müssen Anwendungen gegen Angriffe auf die Lieferkette abgesichert werden.

Für das ITZBund ist diese Herausforderung besonders relevant. Der zentrale IT-Dienstleister betreibt nach eigenen Angaben mehr als 1.400 Fachverfahren für die Bundesverwaltung. Mit LISSA – kurz für „Lieferkette ITZBund für Sichere SoftwAre“ – entsteht deshalb ein Standardprodukt für automatisierte und sichere Softwarelieferketten. Beim eGovernment-Wettbewerb 2026 erreichte das Projekt damit den ersten Platz in der Kategorie „Souveränität, Sicherheit und Stabilität digitaler Infrastrukturen“.

Sicherheitsprüfung vor dem Betrieb

LISSA setzt zwischen Softwareentwicklung und Betrieb an. Die Plattform bildet einen standardisierten Lieferweg, über den individuell entwickelte Fachverfahren in die Betriebsumgebung gelangen. Dabei überprüft LISSA die Software unter anderem auf Schwachstellen und Schadcode sowie auf Softwarequalität und Compliance-Vorgaben.

Die Entwicklungsteams können weiterhin in ihren eigenen Entwicklungszyklen und -umgebungen arbeiten. Zur Einlieferung stellen sie Quellcode und Build-Vorschriften bereit. Eine in einer demilitarisierten Zone angesiedelte Code-Schleuse holt den Quellcode automatisiert ab und prüft ihn auf Schadcode und Sicherheitslücken. Kritische Befunde führen zum Abbruch der Lieferkette. Anschließend gelangt der geprüfte Quellcode in eine geschützte Betriebsumgebung. Dort werden Sicherheitsprüfungen wiederholt und eine automatisierte Softwarequalitätsanalyse durchgeführt. Die Behörden können dafür eigene Prüfregeln festlegen.

Software wird in geschützter Umgebung gebaut

Ein wesentliches Element von LISSA ist, dass nicht lediglich fertige Softwarepakete übernommen werden. Auf Grundlage des geprüften Quellcodes und der Build-Vorschriften werden die Softwareartefakte und Container-Images innerhalb der geschützten Umgebung erstellt. Dabei erzeugt LISSA zugleich eine Software Bill of Materials (SBOM). Diese maschinenlesbare Stückliste dokumentiert die in einer Software enthaltenen Komponenten. Dadurch sollen sich beispielsweise bei Bekanntwerden einer neuen Sicherheitslücke betroffene Anwendungen schneller identifizieren lassen.

Die erstellten Softwareartefakte werden anschließend signiert und in einem geschützten Repository beziehungsweise einer Container Registry für den Betrieb bereitgestellt. Zusätzlich entsteht ein Herkunftsnachweis, der dokumentiert, woher ein Artefakt stammt und wie es erzeugt wurde. Die SBOM wird in einem eigenen Managementsystem hinterlegt.

Zero Trust für die Softwarelieferkette

Das Sicherheitskonzept folgt dem Zero-Trust-Prinzip. Software wird in unterschiedlichen Schutzzonen wiederholt überprüft, statt einer Quelle grundsätzlich zu vertrauen. Werden Schadcode oder Sicherheitslücken entdeckt, greift ein Quarantäneprozess und die Einlieferung wird gestoppt.

Auch sicherheitsrelevante Ereignisse werden protokolliert. Diese Informationen sollen zentral durch ein Security Operations Center analysiert werden können. Signierte Artefakte und Herkunftsnachweise sollen zudem verhindern, dass Software auf ihrem Lieferweg unbemerkt kompromittiert wird. Damit verbindet das ITZBund mehrere Ziele: höhere IT-Sicherheit und Betriebsstabilität, mehr Transparenz über die eingesetzte Software sowie eine größere Kontrolle über den gesamten Lieferprozess.

Automatisierung soll Entwicklung beschleunigen

LISSA ist zugleich darauf ausgerichtet, Entwicklungs- und Bereitstellungsprozesse zu automatisieren. Entwicklungsteams erhalten direktes Feedback und Security Reports. Über ein Dashboard können sie verfahrensspezifische Quality Gates überblicken. Auch das Deployment lässt sich automatisieren. Nach weiteren betrieblichen Sicherheitsprüfungen können die geprüften Artefakte aus den geschützten Repositories und Registries abgerufen und in die vorgesehenen Zielumgebungen ausgerollt werden.

Technisch setzt das ITZBund auf Container und Kubernetes. Dadurch soll die Softwarelieferkette automatisch skalierbar und aktualisierbar sein. Gleichzeitig ist LISSA modular aufgebaut. Behörden können eigene Prüfkriterien integrieren, weitere Prüfschritte sollen sich ergänzen lassen.

Unterstützung regulatorischer Anforderungen

Mit SBOM und Herkunftsnachweisen adressiert LISSA nach Darstellung des ITZBund auch regulatorische Anforderungen. Die SBOM schafft Transparenz über die Bestandteile einer Anwendung und erleichtert die Identifikation von Produkten, die von bekannten Schwachstellen betroffen sind.

Die sogenannten Provenance-Informationen dokumentieren wiederum Herkunft und Erstellung eines Softwareartefakts. Damit wird der Lieferprozess für Prüfungen und Audits nachvollziehbar. LISSA erzeugt beide Informationen automatisiert. Das ITZBund nennt als Mehrwert des Projekts neben dem Schutz vor Supply-Chain-Angriffen insbesondere „Security by Design“, Standardisierung und digitale Souveränität sowie Effizienz- und Produktivitätsgewinne durch Automatisierung.

Interesse weiterer Bundesbehörden

Zum Zeitpunkt der Wettbewerbspräsentation wurde LISSA seit sechs Monaten mit unterschiedlichen Fachverfahren pilotiert. Nach Angaben des ITZBund besteht eine hohe Nachfrage aus den Fachverfahren, während der weitere Produktaufbau läuft.

Auch andere Behörden zeigen demnach Interesse an der Lösung. In der Präsentation werden das Bundesverwaltungsamt (BVA), das Bundesministerium der Finanzen (BMF) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) als interessierte Kundenbehörden genannt.

Damit adressiert LISSA eine Aufgabe, die über einzelne Anwendungen hinausgeht: Die Softwarelieferkette selbst wird zu einem standardisierten Sicherheitsprozess. Für die Bundesverwaltung könnte damit eine gemeinsame technische Grundlage entstehen, um individuell entwickelte Fachverfahren automatisiert zu prüfen und kontrolliert in geschützte Betriebsumgebungen zu überführen.

()

Grundlage dieses Berichts ist die Wettbewerbspräsentation „LISSA – Lieferkette ITZBund für Sichere SoftwAre“, die wir mit Zustimmung des ITZBund dafür ausgewertet haben.

Stichwörter: Panorama, eGovernment-Wettbewerb, ITZBund