BSI/ZenDiS

Sichere Softwarelieferketten

[11.04.2025] Software besteht mitunter aus tausenden Einzelkomponenten – eine komplexe Softwarelieferkette. Deren Sicherheit ist ein wichtiges Element von IT-Sicherheit und digitaler Souveränität. ZenDiS und BSI zeigen nun in einem Strategiepapier samt Umsetzungsplan, wie die Überprüfung automatisiert werden kann.

In Zeiten zunehmender geopolitischer Spannungen wird die Gewährleistung der Sicherheit und Beständigkeit digitaler Infrastrukturen zu einem zentralen Baustein der Daseinsvorsorge. Mit einer gemeinsamen Initiative rücken das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun die Bedeutung sicherer, souveräner Softwarelieferketten in den Fokus. Nahezu jede Software greift auf hunderte oder gar tausende bestehende Einzelkomponenten, Bibliotheken und Tools zurück – in der Gesamtheit die Softwarelieferkette. Wird ein Teil dieser Kette kompromittiert oder fällt weg, entstehen erhebliche Risiken für alle Nutzenden. Angesichts ihrer Komplexität ist eine vollständige Prüfung von Softwarelieferketten bisher für einzelne Softwareanbieter kaum realisierbar. Daher, so das BSI, sei ein grundlegend neuer Ansatz notwendig, der Fachkenntnisse von Sicherheitsexperten, Entwicklern und Behörden bündelt und gemeinsame Sicherheitsanalysen mit standardisierten Prüfverfahren erlaubt.

openCode als Kernbaustein

Zentraler Baustein in dem nun von BSI und ZenDiS vorgeschlagenen Konzept ist die Plattform openCode. Sie etabliert verbindliche Sicherheitsstandards, macht Abhängigkeiten transparent und schafft nachvollziehbare Herkunftsnachweise für kritische Softwarekomponenten. Dank der Transparenz von Open Source können viele der bisher manuellen Prüfprozesse automatisiert ablaufen. Damit wird die Skalierbarkeit von Sicherheitsüberprüfungen der Softwarelieferkette erheblich verbessert. Das ZenDiS zeigt mit seinem neuen Badge-Programm für Software auf openCode, wie eine solche Prüfung realisiert werden kann: Qualitätsmerkmale von Software – etwa zu Wartung und Nachnutzung – werden dabei automatisch aus dem Code abgeleitet.

Rückmeldung erwünscht

Während viele gängige Ansätze zur Softwaresicherheit weitgehend reaktiv sind, erlaubt openCode einen präventiven Ansatz durch kontinuierliche, automatisierte Sicherheitsprüfungen und transparente Softwarelieferketten. Bei einem Sicherheitsvorfall können dadurch Artefakte und Betroffene zuverlässig identifiziert und Echtzeitlagebilder erstellt werden, sodass gezielt gewarnt werden kann. So wird openCode zu einem Schlüsselelement einer resilienten digitalen Infrastruktur in Deutschland. Ihr Konzept für eine sichere und souveräne Softwarelieferkette haben das BSI und das ZenDiS in einem gemeinsamen Strategiepapier inklusive Umsetzungsplan dargelegt. Rückmeldungen aus der Fachöffentlichkeit sind ausdrücklich erwünscht. Kontaktmöglichkeiten gibt es auf opencode.

(sib)

• Strategiepaper „Sichere Softwarelieferketten“

Stichwörter: IT-Sicherheit, BSI, Digitale Souveränität, Lieferketten, Software, ZenDIS