Bitkom AK Software Engineering & Software Architektur
Datum: 10. März 2025 | **Ort:** Webkonferenz

Cyber-Security in Software Engineering & Software Architektur

Cyber-Security ist längst kein Add-on mehr – sie muss von Beginn an integraler Bestandteil jeder Software-Entwicklung und -Architektur sein. Doch wie setzen wir das in der Praxis um? Welche Best Practices, Tools und Strategien helfen, sichere Systeme zu entwickeln? Und welche Fehler sollten wir unbedingt vermeiden?

Diesen Fragen beleuchtete der AK Software Engineering & Software Architektur gemeinsam mit Expert:innen in einer Sitzung am 10. März 2025 zum Thema moderne Cyber-Security in der Software-Entwicklung. Es wurde diskutiert, wie sich Sicherheitsstandards praxisnah umsetzen lassen, welche Maßnahmen die Software-Supply-Chain schützen und wie Künstliche Intelligenz die Sicherheitsanalyse in DevSecOps-Prozesse optimieren kann. Dabei ging es nicht nur um Konzepte, sondern um konkrete Lösungen für den Entwicklungsalltag.

1. EU Cyber Resilience Act (CRA): Herausforderungen für den Entwicklungsprozess

Jan Hansmann, Systemum GmbH & Co. KG

Einleitung

Der Cyber Resilience Act (CRA) bringt weitreichende Veränderungen für die Softwareentwicklung mit sich. Neben der Einführung eines CE-Kennzeichens für Software stehen Entwicklungsteams vor neuen Pflichten in Bezug auf Dokumentation, Risikoanalyse und Patch-Management.

Key Takeaways

- Der Cyber Resilience Act (CRA) tritt am 09.12.2024 in Kraft; ab 11.09.2026 gilt eine Reportingpflicht, und bis zum 11.12.2027 müssen alle Anforderungen erfüllt sein.
- Softwareprodukte müssen künftig mit einem sichtbaren CE-Kennzeichen versehen werden.
- Neue Prozessschritte im Entwicklungsprozess umfassen unter anderem die Erstellung einer SBOM, das Bereitstellen von Sicherheitspatches und eine Risikoanalyse für jedes Produkt.

- Für die CRA muss die technische Dokumentation (Anforderungen, Architektur, Nutzerhandbuch) um Security-Aspekte erweitert werden.
- Der CRA formuliert auch konkrete Security-Anforderungen, die in den Produkten umgesetzt werden müssen (Zugriffsschutz, sichere Konfiguration, ...).
- Die Anforderungen des CRA an die Software sind handhabbar, aber es gibt einen hohen zusätzlichen Prüf- und Dokumentationsaufwand.

2. Regulatorische Anforderungen & Compliance – Entwickler sollen es umsetzen, aber wer erklärt es ihnen?

Manuel Fischer, Adinger IT Trainings GmbH

Einleitung

Komplexe Vorgaben wie ISO 27001 oder DSGVO wirken in der Praxis oft unverständlich und schwer umsetzbar. Der Vortrag zeigte, wie technische Teams durch frühzeitige Einbindung und klare Kommunikation aktiv zur Compliance beitragen können.

Key Takeaways

- Folgende Regelungen werden aktuell im Bezug auf Softwareentwicklung diskutiert: NIS2, DORA, DSGVO, ISO 27001, CRA, DSA, GPSR, EU AI Act
- Definition von »EU Richtlinien«: Müssen erst in nationales Recht übersetzt werden.
- Zur erfolgreichen Umsetzung müssen Stakeholder früh einbezogen, klare Kommunikationsstrategien definiert und Mitarbeitende gezielt geschult werden.
- Regelmäßige Prüfungen, transparente Zielsetzungen und kontinuierliches Feedback helfen, Compliance nachhaltig zu etablieren.

3. Better Safe Than Sorry: Using SBOMs to Strengthen Supply Chain Security

Julia Gätjens, GitLab GmbH

Einleitung

SBOMs schaffen Transparenz in Software-Lieferketten und ermöglichen eine schnellere Reaktion auf Sicherheitslücken. Der Vortrag stellte dar, wie SBOMs helfen, regulatorische Vorgaben zu erfüllen und die Sicherheit zu verbessern.

Key Takeaways

- Die wachsende Komplexität von Software erhöht die Risiken innerhalb der Supply Chain – Transparenz ist essenziell.

- Bei Sicherheitslücken ist die Reaktionszeit entscheidend, weshalb SBOMs eine schnelle Identifikation betroffener Komponenten ermöglichen.
- In Regulierungsvorgaben wie NIS2 und dem CRA sind SBOMs bereits vorgeschrieben – bei Nichteinhaltung drohen Sanktionen.
- SBOMs sollten integraler Bestandteil der AppSec-Strategie sein und idealerweise bereits früh im Entwicklungsprozess (Shift Left) berücksichtigt werden.
- Auch Basis-Images in containerisierten Umgebungen müssen regelmäßig geprüft werden, da sie häufig übersehen werden.
- Entwickler:innen sollten aktiv in Sicherheitsprozesse integriert werden, z. B. durch Scans direkt in Merge Requests.
- Die drei zentralen SBOM-Formate sind CycloneDX, SPDX und SWID – je nach Kontext können unterschiedliche Vorteile bestehen.

4. Effiziente Schwachstellenklassifikation durch KI in DevSecOps

Simon Müller, XITASO GmbH

Einleitung

Die präzise Erkennung von Sicherheitslücken ist eine zentrale Herausforderung in der modernen Softwareentwicklung. Static Application Security Testing (SAST) Tools liefern häufig viele Fehlalarme, was die Arbeitssicherheit erschwert. Der Vortrag zeigte, wie Large Language Models (LLMs) eingesetzt werden können, um False Positives effizient zu filtern, Schwachstellenbewertungen zu verbessern und die Integration von KI in bestehende CI / CD-Pipelines zu ermöglichen.

Key Takeaways

- SAST-Tools verursachen viele Fehlalarme, was zu unnötiger Belastung bei Entwickler:innen und Sicherheitsteams führt.
- Durch den Einsatz von KI lassen sich laut aktuellen Tests rund 30 Prozent der False Positives zuverlässig herausfiltern.
- LLMs eröffnen neue Möglichkeiten zur Schwachstellenbewertung, befinden sich aber insbesondere bei logischem Reasoning noch in einer frühen Phase.
- Die Integration von KI in CI / CD-Pipelines kann Effizienz und Präzision in der Sicherheitsanalyse deutlich verbessern.

5. Ökosystem vertrauenswürdige IT – Cyberagentur-finanzierte Forschungsprojekte für beweisbare Cybersicherheit

Dr. Sebastian Jester, Agentur für Innovation in der Cybersicherheit GmbH

Einleitung

Formale Verifikation kann Sicherheitseigenschaften von Software und Hardware mathematisch nachweisbar machen. Die Cyberagentur fördert Forschungsprojekte, um diese Ansätze praxistauglich zu machen.

Key Takeaways

- Die Cyberagentur fördert derzeit Projekte, die die beweisbare Cybersicherheit auf Software- und Hardware-Ebene erforschen.
- Im Fokus stehen Methoden zur formalen Verifikation, die Sicherheitsgarantien mathematisch absichern sollen.
- Ziel ist eine durchgängige Security-by-Design-Architektur, die sich auch im Entwicklungsalltag etablieren lässt.

Zusammenfassung

Die Sitzung verdeutlichte, wie Cyber-Security von einer Querschnittsaufgabe zur strategischen Schlüsselkomponente in der Softwareentwicklung wird. Von regulatorischen Rahmenwerken über sichere Lieferketten bis hin zu KI-gestützten Analysen wurden praxisnahe Lösungsansätze vorgestellt. Die zentrale Erkenntnis: Sicherheit muss ganzheitlich, frühzeitig und teamübergreifend gedacht werden – sowohl technisch als auch organisatorisch.

Felix Ansmann
Referent Software &
IT-Services
T 030 27576-098
f.ansmann@bitkom.org