

Software Bill of Materials

Inhaltsliste für Software



Sebastian Hempel • 20.05.2025



**Das Ganze ist nur so sicher wie jedes
seiner Teile.**

Sebastian Hempel (in Anlehnung an Aristoteles)

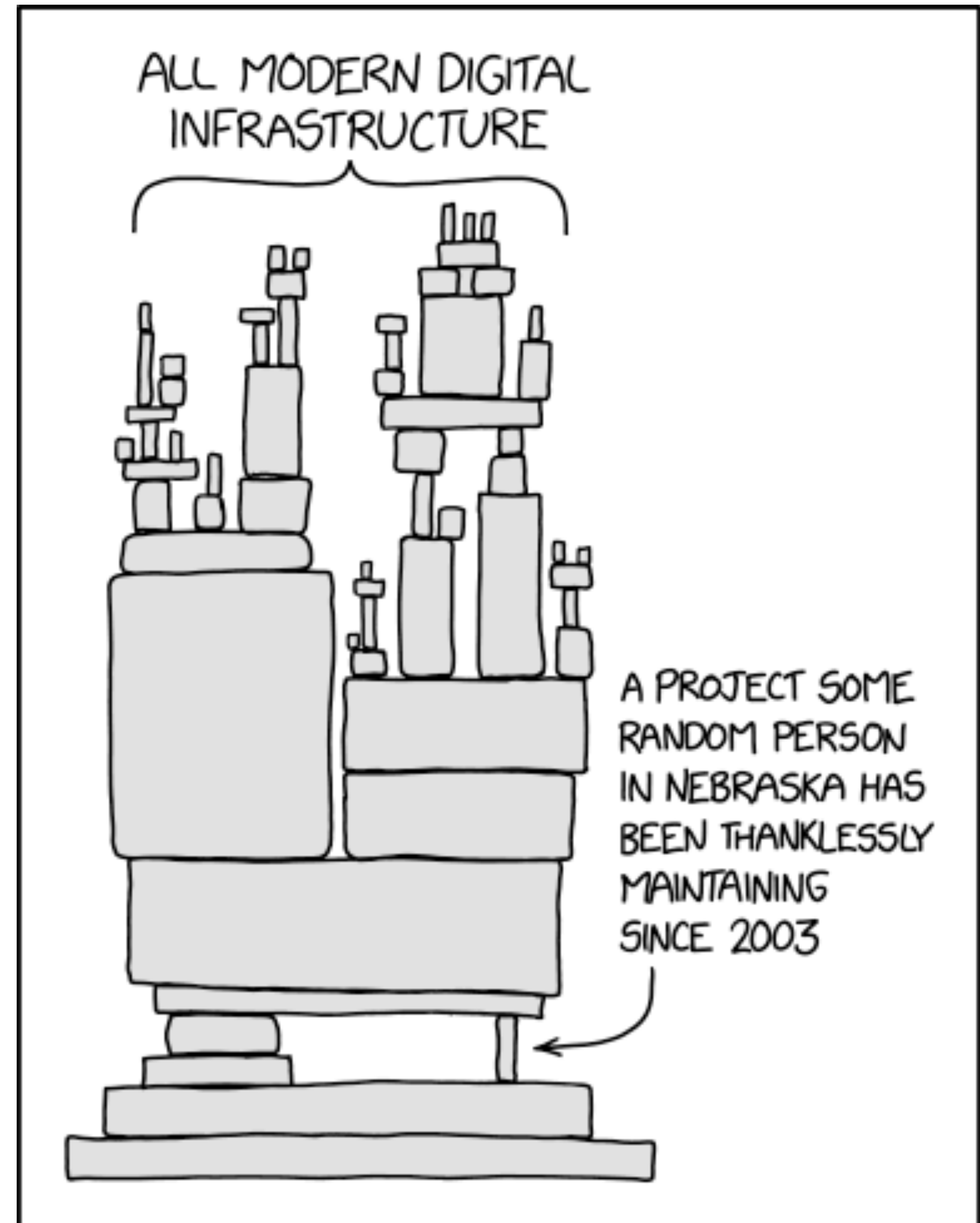
Software besteht aus mehreren Teilen

- JDK
- Framework
- Libraries
- eigene Komponenten

Software ist nie frei von Fehlern

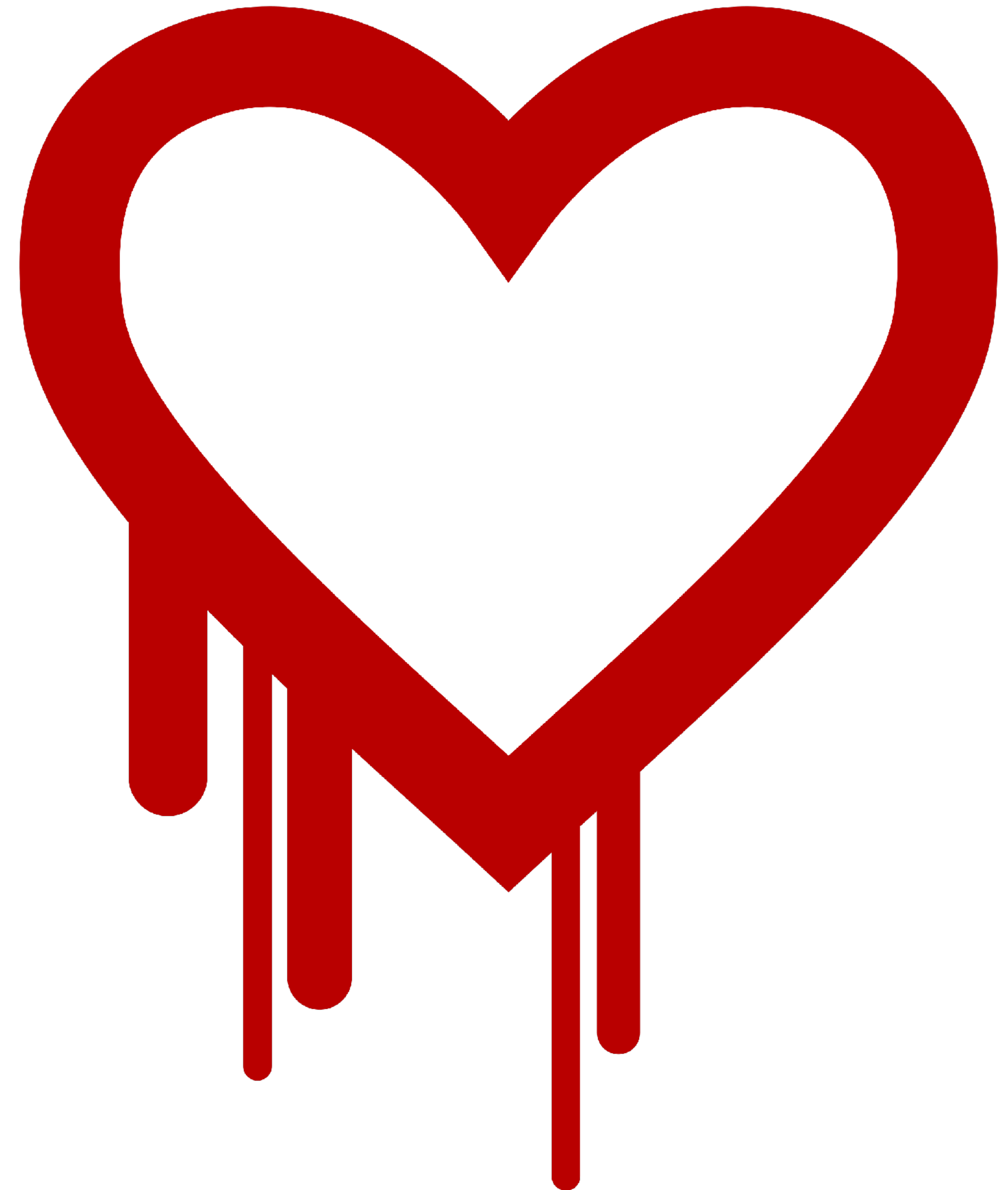
- Bugs
- CVE (common vulnerability and exposures)

Software baut aufeinander auf



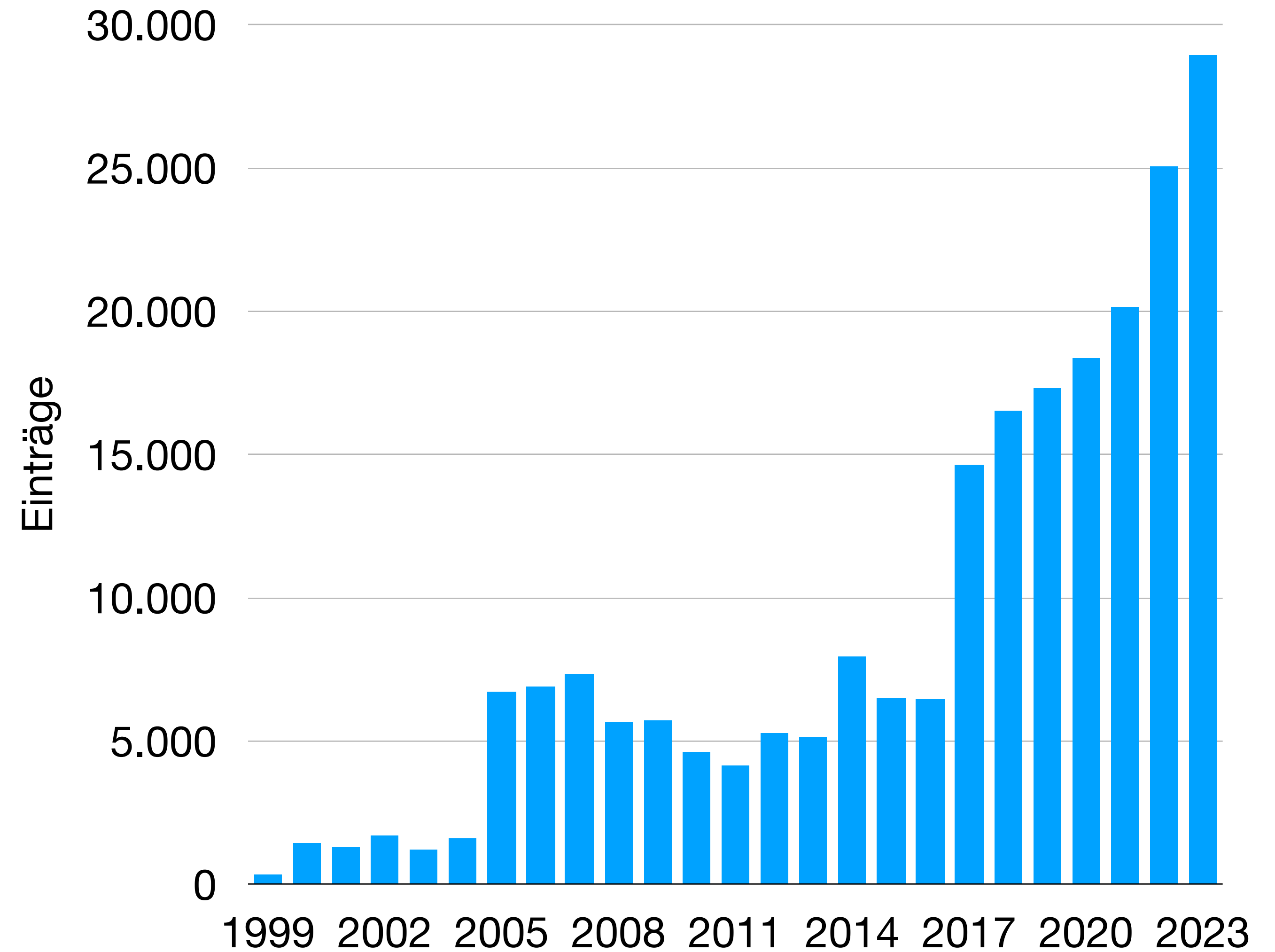
Berühmte Katastrophen

- Heartbleed (2014, CVE-2014-0160) - <https://heartbleed.com/>
- Log4Shell (2021, CVE-2021-44228)
- xz Backdoor (2024, CVE-2024-3094)



CVE Einträge pro Jahr

- komplexere Software
- mehr Angriffe
- mehr Untersuchung
- mehr Beachtung



<https://www.cve.org/About/Metrics>

BSI SBOM-Richtlinie

- TR-03182 „Cyber-Resilienz-Anforderungen“
- Empfehlung zur Gestaltung von SBOMs
- Verweis auf Cyber Resilience Act
- CISA (cybersecurity & infrastructure security agency)

