Open Source Vernachlässigung Manifest: Weckruf für Wandel

Category: Opinion
geschrieben von Tobias Hager | 15. Dezember 2025

Open Source Vernachlässigung Manifest: Weckruf für Wandel

Open Source – das Rückgrat des modernen Internets, das Arbeitstier hinter jedem zweiten SaaS-Startup, die geheime Superkraft von Big Tech. Und doch: Open Source wird behandelt wie der ungeliebte Stiefsohn der Digitalbranche.

Willkommen beim Manifest der Open Source Vernachlässigung – einer schonungslosen Abrechnung mit dem Status Quo, einer Kampfansage an Ignoranz und Ausbeutung, und einem Weckruf für alle, die glauben, sie könnten sich auf Kosten der Community einlullen. Wer nach weichgespültem Bullshit sucht, ist hier falsch. Hier kommt der Realitätscheck.

- Warum Open Source der Motor der digitalen Infrastruktur ist – und trotzdem systematisch vernachlässigt wird
- Die häufigsten Formen der Open Source Vernachlässigung – von fehlender Finanzierung bis toxischer Erwartungshaltung
- Wie Unternehmen, Agenturen und Entwickler von Open Source profitieren, aber kaum etwas zurückgeben
- Die technischen und wirtschaftlichen Risiken, die durch die Vernachlässigung entstehen – Stichwort: Supply Chain Security
- Warum das Open Source Ökosystem 2024 an einem Kipppunkt steht
- Welche Mythen um Open Source den Wandel blockieren – und wie man sie entzaubert
- Strategien und Best Practices für nachhaltigen Open Source Support
- Konkrete Handlungsempfehlungen für Unternehmen, Tech-Teams und Entscheider
- Wie du als Entwickler, CTO oder Tech-Lead Teil der Lösung wirst – statt Teil des Problems zu bleiben
- Ein Manifest für mehr Verantwortung, Fairness und Innovation im digitalen Zeitalter

Open Source – das klingt nach Idealismus, nach digitaler Selbstermächtigung, nach geteiltem Fortschritt. In Wirklichkeit ist es vor allem eins: die geheime, kaum gewürdigte Basis von nahezu allem, was im Web funktioniert. Vom Linux-Kernel im Rechenzentrum bis zur JavaScript-Library im Frontend, von Kubernetes bis WordPress – Open Source ist überall. Nur: Die Wertschätzung dafür ist so gering wie nie. Unternehmen, Startups und ganze Industriezweige bauen ihre Geschäftsmodelle auf kostenloser Open Source auf, investieren aber einen lächerlichen Bruchteil ihrer Budgets in deren Wartung. Das Ergebnis: Sicherheitslücken, veraltete Abhängigkeiten, Burnout bei Maintainer und eine gefährliche Verwundbarkeit der digitalen Supply Chain. Höchste Zeit, dass wir über die Open Source Vernachlässigung reden, wie sie wirklich ist – als tickende Zeitbombe und als systemische Krise, die den Fortschritt ausbremst.

Dieses Manifest ist kein Klagelied. Es ist ein Aufruf zum radikalen Umdenken. Für alle, die Open Source nutzen, verkaufen, einbauen oder davon profitieren – aber meinen, die Rechnung dafür begleiche immer jemand anderes. Spoiler: Das war einmal. Wer auch in den nächsten Jahren Innovation, Sicherheit und Stabilität will, muss jetzt liefern. Mit Geld, mit Code, mit Verantwortung. Willkommen im Real Talk der digitalen Infrastruktur.

Open Source als Fundament der

digitalen Welt – und die schleichende Vernachlässigung

Open Source ist kein Hippie-Spielplatz für Nebenbei-Entwickler. Es ist das Fundament, auf dem die digitale Wirtschaft gebaut ist. Ohne Open Source gäbe es kein modernes Cloud Computing, keine Web-Frameworks, keine Datenbanken, keine Containerisierung, keine Infrastruktur-as-Code. Tools wie Docker, Node.js, React, Nginx, PostgreSQL oder das allgegenwärtige Linux – alles Open Source. Hinter jedem erfolgreichen SaaS-Produkt, jedem Social Network und jeder E-Commerce-Plattform stecken unzählige Open Source Komponenten, die still und leise ihren Dienst tun.

Das Problem beginnt dort, wo die Wertschöpfung aufhört und die Wertschätzung nie begonnen hat. Unternehmen nehmen Open Source als selbstverständlich hin. Sie erwarten kontinuierliche Updates, Security-Patches, Kompatibilität mit den neuesten Frameworks und nahtlose Integration in ihre eigene Infrastruktur – und zahlen dafür: nichts. Maintainer werden mit Issues geflutet, Feature Requests stapeln sich, und im besten Fall gibt es ab und zu ein “Danke” als Kommentar auf GitHub. Monetäre Unterstützung? Fehlanzeige. Systematische Wartung? Selten. Wer Open Source pflegt, arbeitet oft unbezahlt, am Wochenende, zwischen bezahlten Projekten oder im Burnout-Modus.

Die Vernachlässigung ist nicht nur eine moralische, sondern eine technische und wirtschaftliche Katastrophe. Denn je weniger in Open Source investiert wird, desto maroder werden die Komponenten, desto größer werden technische Schulden, desto gravierender werden Sicherheitslücken. Die berühmten Supply Chain Angriffe – SolarWinds, Log4Shell, XZ-Backdoor – sind keine Zufälle, sondern Symptome eines Systems, das auf Ausbeutung und Ignoranz gebaut ist.

Unternehmen, die Open Source ignorieren oder nur konsumieren, sägen an dem Ast, auf dem sie sitzen. Open Source ist kein Free Lunch. Es ist ein prekäres Gleichgewicht, das kippt, wenn sich niemand mehr verantwortlich fühlt. Und dieses Kippen ist 2024 keine Theorie mehr, sondern Realität.

Die toxische Erwartungshaltung und ihre technischen Folgen: Open Source als Selbstbedienungsladen?

Open Source Vernachlässigung beginnt im Mindset. Viele Firmen und Entwickler betrachten Open Source als Selbstbedienungsladen – ein endloses Buffet an kostenlosen Tools, Libraries und Frameworks, die immer up-to-date, bugfrei und kompatibel sein sollen. Dass Maintainer Menschen mit begrenzter Zeit und

Ressourcen sind? Geschenkt. Dass Open Source keine Zauberei ist, sondern harte Arbeit? Wird gerne verdrängt.

Diese toxische Erwartungshaltung hat gravierende technische Folgen. Sie führt zu veralteten Dependencies, zu fehlenden Security-Patches, zu inkompatiblen API-Änderungen und zu einer gefährlichen Fragmentierung des Ökosystems. Wer glaubt, Open Source "funktioniert schon", ohne dass man investiert, landet zwangsläufig in der Dependency-Hölle, wo jedes Update potenziell das eigene Produkt zerlegt.

Die Realität sieht so aus:

- Maintainer können nicht jeden Bug sofort fixen, weil sie bezahlt arbeiten müssen
- Security-Patches werden manchmal erst Wochen nach dem Bekanntwerden einer Lücke eingespielt
- Breaking Changes passieren, weil niemand Zeit für vollständige Backwards-Kompatibilität hat
- Dokumentation ist oft lückenhaft, weil sie mühselig und unbeliebt ist

Die Folge? Wer Open Source nur konsumiert, ohne zurückzugeben, baut seine Systeme auf Sand. Und wenn der Maintainer ausbrennt oder das Projekt verlässt, steht das digitale Kartenhaus plötzlich ohne Fundament da.

Die technische Schuld wächst exponentiell – und mit ihr das Risiko für Sicherheitsvorfälle, Systemausfälle und teure Notfall-Refactorings. Open Source ist keine Einbahnstraße. Wer nicht investiert, verliert.

Unternehmen am Pranger: Wer profitiert – und wer zahlt die Zeche?

Fakt ist: Die Big Player der Branche verdienen Milliarden auf dem Rücken der Open Source Community. Amazon, Google, Microsoft und Co. integrieren Open Source Software tief in ihre Cloud-Stacks, bieten Managed Services auf Basis von Open Source Tools an – und geben oft kaum etwas zurück. Aber auch Mittelständler und Startups profitieren massiv, ohne die Kosten zu tragen. Sie sparen Entwicklungskosten, reduzieren Time-to-Market, umgehen Lizenzgebühren – und halten die Hand auf, wenn etwas schiefgeht.

Die Verantwortung wird systematisch nach unten delegiert. Maintainer sind für Bugs verantwortlich, für Security-Fixes, für Feature-Requests, für Support – ohne Vertrag, ohne SLA, ohne Gegenleistung. Unternehmen argumentieren: "Es ist ja Open Source, wir sind nicht verpflichtet." Übersetzt: "Wir nehmen alles, zahlen nichts und beschweren uns, wenn's nicht läuft." Dieses Modell ist nicht skalierbar. Es ist toxisch. Und es untergräbt die Innovationskraft der gesamten Branche.

Warum? Weil immer weniger Maintainer bereit sind, sich für lau ausbeuten zu

lassen. Immer mehr Open Source Projekte werden “abandoned”, weil die Last zu groß wird. Die Folge: Sicherheitslücken bleiben offen, kritische Komponenten veralten, Innovation verlangsamt sich. Die Kosten für Ausfälle, Notfall-Patches und Refactorings sind am Ende ein Vielfaches dessen, was ein minimaler Open Source Support gekostet hätte.

Unternehmen, die Open Source nutzen, aber nicht investieren, handeln kurzsichtig – und riskieren ihre eigene digitale Zukunft. Wer heute Open Source ignoriert, zahlt morgen mit Sicherheit, Reputation und Wettbewerbsfähigkeit.

Supply Chain Security, technische Schulden und das offene Scheunentor für Angriffe

Die technische Vernachlässigung von Open Source ist längst kein Randproblem mehr. Sie ist ein massives Sicherheitsrisiko – nicht nur für Nerds im Keller, sondern für ganze Industrien. Die Supply Chain Angriffe der letzten Jahre haben das brutal offengelegt. Der XZ-Utils-Backdoor, der SolarWinds-Hack, die Log4Shell-Lücke – allesamt direkte Folgen von mangelnder Wartung, fehlender Kontrolle und toxischer Erwartungshaltung gegenüber Open Source.

Die technische Supply Chain ist heute ein undurchsichtiger Dschungel aus Abhängigkeiten, Transitive Dependencies, Third-Party-Modulen und Build-Tools. Jede Komponente, jedes NPM-Package, jede Library kann zur Schwachstelle werden – insbesondere, wenn sie niemand pflegt, auditiert oder finanziert. Unternehmen wissen oft nicht einmal, welche Open Source Komponenten in ihrer Infrastruktur stecken – geschweige denn, wie aktuell oder sicher sie sind.

Typische Risiken der Open Source Vernachlässigung:

- Ungepatchte Sicherheitslücken durch veraltete Libraries
- Malicious Code Injections durch kompromittierte Packages
- Unklare Ownership und fehlende Kommunikation bei Incidents
- Plötzlicher Projektabbruch durch Maintainer-Burnout
- Kompatibilitätsprobleme bei Major Updates ohne Vorwarnung

Wer glaubt, Open Source Security sei “nice to have”, hat Supply Chain Security nicht verstanden. Die Angreifer von heute suchen nicht mehr nach Schwachstellen im eigenen Code, sondern in den Abhängigkeiten, die niemand kontrolliert. Die Kosten für einen einzigen erfolgreichen Angriff durch eine ungepatchte Library können die Ersparnis aus zehn Jahren “kostenloser” Nutzung pulverisieren.

Die Wahrheit ist: Wer Open Source vernachlässigt, öffnet Hackern die Tür und sabotiert die eigene IT-Landschaft. Technische Schulden in Open Source sind

keine hypothetische Gefahr, sondern ein reales Geschäftsrisiko.

Mythen, Ausreden und die Realität: Was Open Source wirklich braucht

Die Diskussion um Open Source ist von Mythen und Selbstbetrug durchsetzt. Die gängigsten Ausreden: “Open Source ist ja freiwillig.” – “Maintainer machen das doch aus Leidenschaft.” – “Wenn’s nicht läuft, nehmen wir halt ein anderes Projekt.” Klingt nach Startup-Romantik, ist aber toxisch naiv.

Die Realität ist eine andere:

- Open Source lebt nur, wenn jemand die Arbeit macht – und diese Arbeit muss bezahlt werden
- “Freiwilligkeit” endet da, wo die Community ausbrennt oder ausstirbt
- Alternativen sind selten wirklich kompatibel oder sicher
- Forken löst keine strukturellen Probleme, sondern dupliziert nur die Arbeit
- Innovation entsteht nur, wenn Wartung, Doku und Security dauerhaft gewährleistet sind

Was Open Source wirklich braucht:

- Verlässliche, regelmäßige Finanzierung von Unternehmen, die profitieren
- Vertragliche Zusagen für Support, Security und Weiterentwicklung
- Technische Audits und automatisierte Security-Checks in der CI/CD-Pipeline
- Klare Ownership-Strukturen und Kommunikationswege für Incidents
- Öffentliche Wertschätzung und Karrierechancen für Maintainer

Wer Open Source als “Kollektivgut” behandelt, das niemandem gehört und für das niemand zuständig ist, bekommt genau das: ein marodes Ökosystem voller technischer Leichen.

Strategien für nachhaltige Open Source – von Lippenbekenntnissen zu echter Verantwortung

Es reicht nicht, auf der Firmenwebsite ein Open Source Logo zu platzieren oder gelegentlich ein Pull Request zu machen. Nachhaltiger Open Source Support ist kein Marketing-Stunt, sondern eine strategische Notwendigkeit.

Wer wachsen, innovieren und sicher bleiben will, muss investieren – und zwar systematisch, planbar und transparent.

So geht nachhaltiger Open Source Support in der Praxis:

- 1. Budgetierung fest einplanen: Lege einen festen Prozentsatz jedes IT- oder Entwicklungsbudgets für Open Source Support, Sponsoring oder Wartungsverträge fest.
- 2. Direkte Finanzierung: Unterstütze Maintainer und Projekte via GitHub Sponsors, Open Collective oder eigene Grants. Keine Alibi-Spenden, sondern substanzielle Beiträge.
- 3. Contribution als Pflicht: Entwickle interne Policies, die Contribution zu Open Source Projekten ausdrücklich fördern und honorieren – auch in der Arbeitszeit.
- 4. Security-Checks automatisieren: Integriere Dependency-Scanning, Vulnerability-Alerts und License Audits fest in die CI/CD-Pipeline.
- 5. Open Source Governance etablieren: Bestimme interne Verantwortliche für das Open Source Management, inklusive Risk Assessment und Incident Response.
- 6. Transparenz schaffen: Dokumentiere, welche Open Source Komponenten genutzt werden, wie alt sie sind und wie sie gewartet werden.

Diese Schritte sind keine Raketenwissenschaft – aber sie machen den Unterschied zwischen nachhaltigem Wachstum und digitaler Insolvenz.

Wer Open Source als strategischen Asset begreift, gewinnt an Resilienz, Innovationsfähigkeit und Sicherheit. Wer weiter nur konsumiert, landet früher oder später auf der Liste der nächsten Supply Chain Opfer.

Fazit: Das Manifest für einen echten Wandel in der Open Source Kultur

Open Source ist das Fundament der digitalen Moderne – und wird doch behandelt wie eine billige Ressource, die niemals versiegt. Diese Haltung ist nicht nur ignorant, sondern brandgefährlich. Die Vernachlässigung von Open Source untergräbt Innovation, Sicherheit und Wettbewerbsfähigkeit. Sie ist keine Bagatelle, sondern ein systemisches Risiko für Unternehmen, Branchen und ganze Volkswirtschaften.

Das Manifest der Open Source Vernachlässigung ist ein Weckruf: Wer die Früchte kostenloser Software ernten will, muss sich an der Pflege des Gartens beteiligen. Mit Geld, mit Zeit, mit echter Wertschätzung. Die Zukunft der digitalen Infrastruktur entscheidet sich hier und jetzt. Und sie gehört denen, die Verantwortung übernehmen – nicht denen, die weiter konsumieren und hoffen, dass andere schon aufräumen. Die Party ist vorbei. Zeit, endlich zu bezahlen.