Leitfaden

Open Source Reifegrade

Juni 2021

Zentralverband Elektrotechnik- und Elektronikindustrie

Inhalt

1. Herausforderungen bei der Nutzung von Open Source Software

Im Rahmen der Softwareentwicklung von Unternehmen ist in den vergangenen Jahren eine verstärkte Nutzung von Free Libre Open Source Software (FLOSS) zu verzeichnen. Diese kann als kostensparende Alternative zu proprietären Anwendungen verstanden werden. Abgesehen von den kostenfreien Nutzungsrechten enthalten Open Source Lizenzen jedoch auch konkrete Vorgaben, die durch nutzende Unternehmen eingehalten werden müssen.

Im Hinblick auf den Grad der Nutzung und die Einhaltung der entsprechenden Vorgaben weisen Unternehmen allerdings unterschiedliche Vorgehensweisen auf. Während in einigen Fällen kein Ansatz zur Verwendung von FLOSS vorliegt, existieren in anderen Unternehmen bereits festgelegte Nutzungs- und Compliance-Strategien. Trotz dieser vorhandenen und zum Teil sehr ausgereiften Strategien kommt es, gerade mit Blick auf das Thema Open Source Compliance, gehäuft zu Doppelprüfungen entlang der Lieferkette. Diese Ausgangslage begründet sich durch die Abwesenheit gemeinsamer Open Source Standards und kann, gerade angesichts perspektivisch steigender Nutzungstendenzen, als wenig zufriedenstellend für Zulieferer und Hersteller eingestuft werden.

Mit der Gründung des Arbeitskreises FLOSS hat der ZVEI auf diese Ausganglage reagiert. Ziel des Arbeitskreises ist es, einen Austausch zu Best Practice Beispielen zu ermöglichen und gemeinsame Standards zu schaffen. Damit soll die Implementierung unterschiedlicher Strategien in der Handhabung von FLOSS verhindert und die vertrauenswürdige Zusammenarbeit entlang der Lieferkette gestärkt werden.

Neben dem ZVEI hat sich auch das OpenChain Projekt, als globales Netzwerk von Unternehmen, Regierungen und NGOs, die Definition gemeinsamer Open Source Standards in der Lieferkette zur Aufgabe gemacht. Durch die Übermittlung der im Rahmen des Arbeitskreises FLOSS gewonnenen Erkenntnisse an OpenChain, möchte der ZVEI aktiv zur Weiterentwicklung dieses Projekts beitragen. In diesem Zusammenhang betrachtet der ZVEI auch die Beteiligung seiner Partner an OpenChain als zielführend für eine vertrauensvolle Zusammenarbeit entlang der Lieferkette.

2. Reifegrade in der Handhabung von FLOSS

Trotz der unterschiedlichen Vorgehensweisen von Unternehmen in der Handhabung von FLOSS lassen sich, unter Einbeziehung der Nutzungsgrades, auch übereinstimmende Handlungsmuster ableiten. Auf Basis dieser Gemeinsamkeiten wurden, im Rahmen der Aktivitäten des Arbeitskreises FLOSS, verschiedene Reifegrade mit den entsprechenden Nutzungs- und Compliance-Strategien herausgearbeitet. Diese reichen von Reifegrad Level 1, der Abwesenheit von Strategien, bis hin zu Reifegrad Level 5, einer strategischen Förderung des FLOSS-Projekts. Abhängig von dem jeweiligen Reifegrad sind, mit Blick auf Regularien, Softwareprüfung, Zuständigkeiten und Lieferbeziehungen, verschiedene Aspekte in der Handhabung von FLOSS zu berücksichtigen. Diese sollen nun im Detail dargestellt werden.

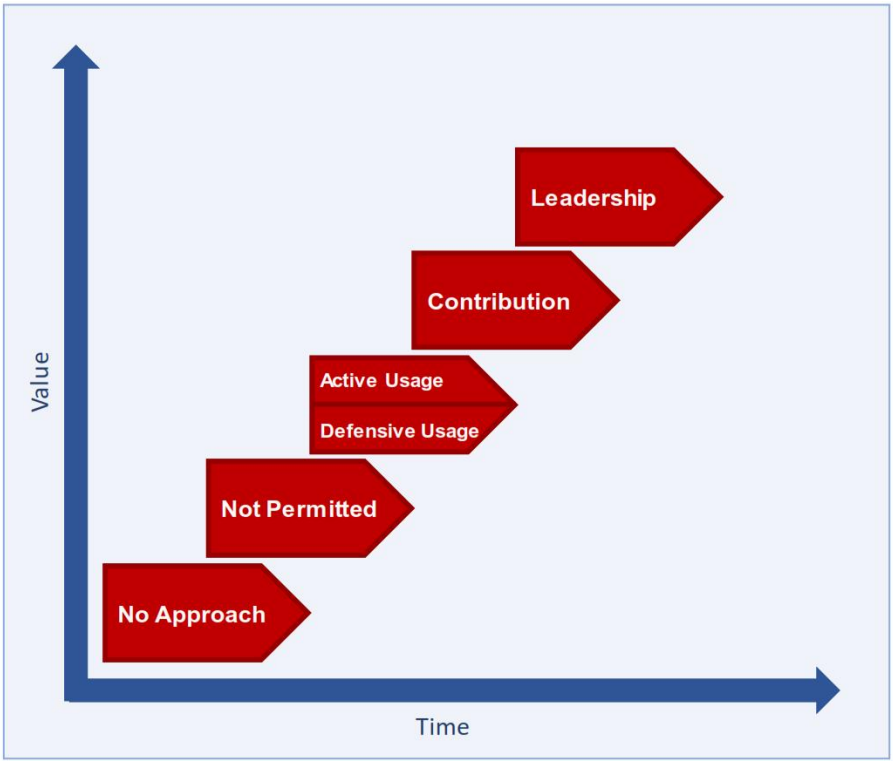

Abbildung 1 Reifegrade zum Einsatz von FLOSS im Unternehmen
(Eigene Darstellung)

2.1 Level 1: Kein allgemeines Vorgehen

Die Abwesenheit von festen Verfahrensweisen im Umgang mit FLOSS in Unternehmen kann als Basislevel verstanden werden. Da in der Handhabung von FLOSS nicht auf entsprechende Unternehmensregularien zurückgegriffen werden kann, muss die Nutzung von Fall zu Fall neu bewertet werden. In diesem Zusammenhang kann Level 1 für Unternehmen der Automobilindustrie nicht empfohlen werden. Stattdessen bietet sich eine Anhebung auf Level 2 an.

2.2 Level 2: Nichtnutzung

Ist die Nutzung von FLOSS in einem Unternehmen nicht gestattet, so gilt es, dies im Rahmen verschiedener Unternehmensprozesse zu berücksichtigen. Diese umfassen die Regularien, die Softwareprüfung und die Lieferbeziehungen eines Unternehmens.

2.2.1 Regularien

Zunächst muss der Verzicht auf die Nutzung von FLOSS in den Regularien des Unternehmens festgehalten werden. Gleichzeitig sollte das Wissen um die Hintergründe der Nichtnutzung sowie die Risiken einer Nutzung innerhalb der Organisation in periodischen Abständen aufgefrischt werden.

2.2.2 Softwareprüfung

Um die Nichtnutzung von FLOSS sicherstellen und belegen zu können, müssen verschiedene Verfahren zur Softwareprüfung implementiert werden. Diese Verfahren sind auf jede installierte Produktionssoftware anzuwenden und umfassen:

- Die Nutzung einer Scan-Software
- Die Analyse der Ergebnisse
- Eine Beurteilung anhängig von Systemgröße und Komplexität der Software
- Die Dokumentation der Ergebnisse
- Die abschließende Dokumentation der Nichtnutzung von FLOSS in der Software Freigabe

2.2.3 Lieferbeziehungen

Während sich das jeweilige Level auf eine Organisationseinheit oder ein Unternehmen bezieht, können in anderen Organisationseinheiten abweichende Level Anwendung finden. So etwa im Hinblick auf (Sub-) Zulieferer, die Teile oder die gesamte Software für ein Produkt liefern. Folgen diese demselben Ansatz (Level 2), so müssen hier ebenfalls die oben beschriebenen Verfahren durchlaufen werden. Wenden (Sub-) Zulieferer dagegen ein höheres Level an, so sind, speziell mit Blick auf die Lieferbeziehungen, die folgenden Aspekte zu berücksichtigen:

- Die Organisationseinheit muss mindestens Open Source Reifegrad Level 3 anwenden
- Die Nutzung von FLOSS muss im Vorfeld angekündigt und durch den Vertragspartner freigegeben werden
- Die Vereinbarungen müssen vertraglich festgehalten werden
- Inhalt, Lizenztyp und Auswirkungen müssen dokumentiert werden
- Ein Scanprotokoll muss vorliegen
- Aufseiten des Kunden muss eine Eingangsprüfung durchgeführt werden

2.3 Level 3: Nutzung

Die Nutzung von FLOSS in einem Unternehmen setzt ein detaillierteres Vorgehen voraus. Der Einsatz von FLOSS sollte dabei mit Blick auf die Regularien, die Softwareprüfung, die Lieferbeziehungen und ergänzend auch die Zuständigkeiten berücksichtigt werden.

2.3.1 Regularien

Wie im vorangegangenen Level muss die Nutzung von FLOSS zunächst in den Unternehmensregularien festgehalten werden. Ergänzend gilt es, konkrete Prozesse zur Handhabung von FLOSS zu definieren und diese als Teil der unternehmenseigenen Software-Wiederverwendungsstrategie anzuwenden und zu dokumentieren. Das Verankern dieser Prozesse im Bewusstsein der Organisation, stellt auch auf diesem Level eine wichtige Voraussetzung für die tatsächliche Einhaltung der definierten Verfahrensweisen dar.

2.3.2 Zuständigkeiten

Zum Zweck der Entscheidungsfindung über die Verwendung oder Nichtverwendung sowie den Anwendungsfall einer FLOSS gilt es, ein FLOSS Release Board/ FLOSS Control Board zu installieren. Dieses sollte sich aus Mitarbeitern mit den entsprechenden Kompetenzen zusammensetzen, wie zum Beispiel Compliance Beauftragte, Anwälte oder Patentanwälte.

Die Freigabe der Verwendung von FLOSS erfolgt nicht allgemein. In diesem Zusammenhang sind die Entscheidungen des Boards auf ein bestimmtes Produkt/ eine bestimmte Produktfamilie oder auf eine bestimmte Lizenz/einen bestimmten Lizenzsatz begrenzt und werden auf Basis einer Beurteilung von Optionen, Auswirkungen und Risiken getroffen. Diese Abwägungen sowie die Entscheidung über die Nutzung beziehungsweise die Nichtnutzung einer FLOSS sollten abschließend für jeden Einzelfall dokumentiert werden.

2.3.3 Softwareprüfung

Gerade mit Blick auf die Verwendung von FLOSS, müssen verschiedene Mechanismen zur Prüfung jeder Produktionssoftware implementiert werden. Diese umfassen:

- Die Nutzung einer Scan-Software
- Die Analyse der Ergebnisse
- Die Dokumentation der Ergebnisse
- Die Dokumentation der Nutzung von FLOSS in der Software Freigabe (Inhalt, Lizenz oder Lizenztyp, Lizenzversion/Scan Tool, Scan Tool Version, Scan Tool Konfiguration)
- Die Prüfung und Befolgung lizenzvertraglicher Auswirkungen

2.3.4 Lieferbeziehungen

Wie bereits beschrieben, können (Sub-)Zulieferer abweichende Reifegrade in der Handhabung von FLOSS anwenden. Mit Blick auf die Lieferbeziehungen sind dabei die folgenden Aspekte zu berücksichtigen:

- Die Produkthaftung muss reguliert werden, wobei das liefernde Unternehmen die Verantwortung trägt
- Der Kunde muss vorab über den Einsatz von FLOSS informiert werden
- Die Nutzung muss vertraglich reguliert werden

2.4 Level 3: Aktive und defensive Nutzung

Bei der Nutzung von FLOSS kann zwischen aktiver und defensiver Nutzung unterschieden werden. Die defensive Nutzung von FLOSS erfolgt nicht auf Basis einer Entscheidung des nutzenden Unternehmens sondern auf Nachfrage des Kunden. So kann beispielsweise die Einbindung einer bestimmten Library durch den Kunden gefordert werden. In diesem Fall sind alle innerhalb von Reifegrad Level 3 beschriebenen Verfahren zu berücksichtigen.

Neben der passiven Nutzung ergeben sich besonders im Fall einer aktiven Entscheidung für den Einsatz von FLOSS Besonderheiten in der Handhabung sowie verschiedene Handlungsempfehlungen im Umgang mit Lizenzen. Bei der aktiven Nutzung von FLOSS eröffnet sich zu Beginn eines neuen Softwareproduktes die Entscheidung, dieses selbst zu entwickeln, es zu erwerben oder auf eine FLOSS-Lösung zurückzugreifen. In diesem Zusammenhang muss, im Vorfeld der Entwicklung eines neuen Projektes (Produkt/Produktfamilie, Funktion, Erweiterung), speziell der Open Source Markt durch ein Expertennetzwerk auf das Vorhandensein einer entsprechenden FLOSS geprüft werden. Fällt die Entscheidung zugunsten einer FLOSS aus, so gilt es, die Hintergründe für eine Nutzung innerhalb des Entwicklungsplans festzuhalten und den geplanten Einsatz zum Abschluss der Konzeptphase erneut zu evaluieren. Gleichzeitig werden auch (Sub-) Zulieferer explizit dazu aufgefordert, den Einsatz von FLOSS zu prüfen. FLOSS kann dabei in verschiedenen Bereichen eingesetzt werden, beispielsweise zur Aktivierung einer Basisfunktion, oder zur Verbesserung eines bestimmten Produkts.

Wie eingangs beschrieben enthalten auch Open Source Lizenzen konkrete Vorgaben, die durch nutzende Unternehmen eingehalten werden müssen. Beispielsweise können sie im Rahmen sogenannter Copyleft Effekte dazu verpflichten, Weiterentwicklungen der Software ebenfalls kostenfrei zur Verfügung zu stellen. Daher lassen sich, speziell im Hinblick auf den Umgang mit Lizenzen, einige Handlungsempfehlungen festhalten:

- Lizenzen sollten wenn möglich nach Typen gruppiert werden
- Lizenzvertragliche Folgen sollten evaluiert und im Fall von Änderungen erneut geprüft werden
- Für jede Lizenz oder Lizenzgruppe sollte eine Verwendungsstrategie definiert werden (Bsp. Produkttrennung zur Vermeidung von Copyleft Effekten)
- Innerhalb der Organisationseinheit sollte eine Übersicht darüber existieren, welche Lizenzen wo genutzt werden
- Der Zugewinn durch die (Wieder-) Verwendung von FLOSS sollte analysiert, dokumentiert und kommuniziert werden (Bsp. Time to Market, Verbesserung der Qualität, Verbesserung der Kosten, Verbesserung der Wettbewerbsfähigkeit)

2.5 Level 4: Beteiligung

Bei Level 4 kommt es nicht nur zu einer Nutzung, sondern zu einer aktiven Beteiligung an FLOSS-Projekten. Im Hinblick auf Regularien, Softwareprüfung und Lieferbeziehungen werden dabei alle im Rahmen von Level 3 beschriebenen Basisverfahren angewandt. Ergänzend gilt es, Prozesse, Werkzeuge und eine Infrastruktur zum Schutz des geistigen Eigentums des Unternehmens zu implementieren.

2.5.1 Zuständigkeiten

Die Entscheidung darüber, ob es sich um ein öffentlich zugängliches oder geschlossenes Projekt handelt, unterliegt dem FLOSS Strategie Board, welches mit dem FLOSS Release Board (siehe Level 3) verglichen werden kann. Neben der Entscheidung über die Handhabung geistigen Eigentums, entscheidet dieses Board auch über den Kontext und das Ausmaß einer Beteiligung an FLOSS-Projekten oder an einer FLOSS-Community. Diese Entscheidungen werden unter Einbeziehung von Chancen und Risiken für die Businessstrategie des Unternehmens getroffen und dokumentiert.

2.6 Level 5: Führende Rolle

Unternehmen, die den Reifegrad Level 5 bei der Nutzung von FLOSS anwenden, nehmen im Rahmen von FLOSS-Projekten oder FLOSS-Communities eine führende Rolle ein, die Vorteile im Sinne der Unternehmensstrategie mit sich bringt.

Aufbauend auf den vorangegangenen Reifegrad, sind dabei alle Basisverfahren von Level 4 im Hinblick auf Regularien, Softwareprüfung, Lieferbeziehungen sowie Zuständigkeiten anzuwenden. Ergänzend gilt es, Bedeutung, Mission und Ziele des FLOSS-Projekts unter Einbeziehung des Businessmodels zu definieren.

Im Vorfeld der Führung einer FLOSS-Community steht die Entscheidung, auf eine bereits bestehende zurückzugreifen oder eine neue Community zu gründen. Da es sich bei Level 5 um offene Projekte handelt, werden auch die Ergebnisse öffentlich zugänglich gemacht. Dabei muss der Zeitpunkt der Bekanntmachung festgelegt und angekündigt werden. Dazu gilt es, entsprechende PR-Maßnahmen anzustoßen. Im Anschluss an die Aufrechterhaltung und Pflege der Community kann diese geschlossen oder an eine andere Organisation übergeben werden.

Leitfaden - Open Source Reifegrade

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Automotive
Lyoner Str. 9
60528 Frankfurt am Main

Verantwortlich:
Annika Bühls
Telefon: +49 69 6302- 464
E-Mail: annika.buehls@zvei.org

www.zvei.org

Juni 2021

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt.

Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Herausgebers unzulässig.

Das gilt insbesondere für Vervielfältigungen, Übersetzung, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.