

Lizenz-Compliance für Open Source Software: Ein allgemeiner Leitfaden

Inhalt

Einführung

Open Source Software kennenlernen 2

Was man tun muss, um die Vorteile von OSS nutzen zu können 4

Risiken bei Mißachtung der OSS-Lizenz 6

Das Thema der Lieferkette 8

OSS-Information, die mit einer Software ausgeliefert werden muss 0

Einführung

Open Source Software (OSS) ist aus der modernen Softwareentwicklung nicht mehr wegzudenken. OSS ist in fast allen elektronischen Produkten enthalten, einschließlich Supercomputern, Cloud-Servern, Personalcomputern, Unterhaltungselektronik, Automobilen, Industrieausstattungen und IoT-Geräten. Unternehmen müssen Produkte oder Dienstleistungen mit hoher Qualität und einer schnelleren Markteinführungszeit entwickeln, auch in einem intensiven Wettbewerb. Sie müssen auch mit den neuesten Technologietrends Schritt halten. OSS ist dabei unverzichtbar.

Eine große Anzahl an OSS wird durch die Zusammenarbeit von Softwareentwicklern aus verschiedenen Organisationen auf der ganzen Welt entwickelt. OSS ist häufig ein Vehikel für fortschrittliche Innovationen in verschiedenen Bereichen. Softwareentwickler, die an der Entwicklung von Open Source teilnehmen, haben die Möglichkeit, ihre Fähigkeiten zu verbessern und diese Innovation aus erster Hand zu erleben.

OSS kann von jedem frei verwendet, modifiziert und vertrieben werden, der die entsprechenden Lizenzbedingungen einhält. Wenn OSS vertrieben wird, muss der Distributor zum Zeitpunkt des Vertriebs die Bedingungen der Lizenz einhalten. Es gab Fälle, in denen Distributoren verklagt wurden und den zugehörigen Rechtsstreit verloren haben, weil sie ihren gesetzlichen Verpflichtungen nicht nachkamen. Um die durch den Einsatz von OSS verursachten Risiken zu verringern, müssen alle in das Thema involvierten Mitarbeiter mit den Grundprinzipien von OSS vertraut sein.

Diese Broschüre wurde vom OpenChain-Projekt der Linux Foundation verfasst, um möglichst vielen Menschen die Grundprinzipien von OSS zu erläutern.

Mai 2019



Open Source Software kennenlernen

Lernen wir die Grundlagen von Open Source Software (OSS) kennen.

In dieser Broschüre wird Folgendes erklärt:

- 1 Was ist Open Source Software?
- 2 Was man tun muss, um die Vorteile von OSS nutzen zu können
- 3 Risiken im Kontext einer Nichteinhaltung von OSS-Verpflichtungen

Leider gab es Fälle, in denen Unternehmen ihren OSS-Lizenzverpflichtungen nicht nachkamen und dies zu Rechtsstreitigkeiten mit den Urheberrechtsinhabern führte.

- 4 Das Thema der Lieferkette
- 5 Was man tun muss, um sicherzustellen, dass alle von OSS profitieren

Die Punkte 3 und 4 können miteinander verflochten sein. Wenn OSS über eine Lieferkette erworben wird, müssen alle Mitglieder der Lieferkette die Lizenzverpflichtungen erfüllen. Wenn ein Kettenglied die Lizenzverpflichtungen nicht erfüllt, können Unternehmen in der weiteren Lieferkette dies aufgrund fehlender Lizenzbedingungen nicht ausgleichen. Ein Mitarbeiter oder ein Unternehmen, das alleine handelt, kann nicht alle Verpflichtungen und Anforderungen eigenständig erfüllen.

Wenn ein Artikel mit OSS-Software an Dritte geliefert wird, müssen Informationen zu jeder enthaltenen OSS bereitgestellt werden. Folgende Gruppen von Mitarbeitern müssen die ordnungsgemäßen Verfahren für Erwerb und Distribution von OSS kennen:

- **Softwareentwicklung und Engineering:** Neben Softwareentwicklern sind auch Hardwareingenieure maßgeblich an der Entwicklung von Gerätetreibersoftware, Board Support Packages (BSP) und Software Development Kits (SDKs) für ihre Hardware beteiligt.
- **Einkauf:** OSS kann in Liefergegenständen aus der Lieferkette enthalten sein, z. B. Software, Hardwaremodule, SoCs, Halbleiterprodukte und Produkte, die von ODM / OEM-Herstellern entworfen und entwickelt wurden.
- **Vertrieb:** Der Vertrieb muss die Gründe verstehen, augrund derer Kunden die OSS-bezogenen Informationen - einschließlich Urheberrechts- und Lizenzinformationen - benötigen.
- **Qualitätssicherung:** OSS, welche in einem Produkt enthalten ist, kann dessen Qualität beeinträchtigen oder Fehler verursachen. Mitarbeiter in der QS müssen sich solcher Probleme bewusst sein.
- **Rechtsabteilung / Lizenzmanagement:** Mitarbeiter der Rechtsabteilung und des Lizenzmanagements müssen Gesetze, Präzedenzfälle und Rechtsmittel kennen, die sich auf die Auslegung und Einhaltung von OSS-Lizenzen beziehen.
- **Führungskräfte und Manager:** Führungskräfte und Manager entwickeln Strategien, um Open Source zu nutzen, zu verbreiten und dazu beizutragen. Sie bilden Teams, um die OSS-Nutzung zu fördern; sie überwachen die OSS-Prozesse und investieren in die erforderlichen Software-Tools.

*ODM: Original Design Manufacturer OEM: Original Equipment Manufacturer

Definition von OSS

Es ist nicht einfach, die Frage "Was ist OSS?" genau zu beantworten. Unterschiedliche Menschen werden auf die Frage verschiedene Antworten geben. Die meisten Menschen stimmen jedoch bei folgenden Aussagen überein:

OSS ist Software, für welche der Quellcode bereitgestellt wird. Der Urheberrechtsinhaber gestattet Dritten, die Software zu verwenden, zu überprüfen, zu modifizieren und weiterzugeben.

Beispiele für OSS

Linux ist wahrscheinlich das am weitesten bekannte Beispiel für Open Source Software. Ein Betriebssystem (OS) ist Software, die dafür designt wurde, anderer Software eine Plattform zur Verfügung zu stellen. Linux ist ein solches Betriebssystem. Linux ist überall. Es ist in fast allen wichtigen Computersystemen enthalten, einschließlich Supercomputern, Börsensystemen, Internetservern, Smartphones mit Android-Softwarestack, Produkten der Unterhaltungselektronik, Automobilen und Industrieanlagen. Linux ist weltweit die Basis eines großen Teils der technologischen Kerninfrastruktur.

Linux wurde durch die Zusammenarbeit zehntausender Entwickler aus der ganzen Welt entwickelt. Die Linux-Entwicklung wird jeden Tag aktiv fortgesetzt. Jeder kann Linux frei nutzen, modifizieren und verbreiten, sofern er die Bedingungen der von den Linux-Entwicklern gewählten Lizenz einhält. Es ist sehr wichtig, dass Unternehmen, die Linux verwenden, die Lizenzbestimmungen für Linux verstehen und einhalten.

Neben Linux gibt es eine Vielzahl weiterer OSS-Projekte. Dazu gehören das für HTTP-Server verwendete Apache-Projekt, die weit verbreitete Compiler GNU Compiler Collection (GCC) und die integrierte Eclipse-Entwicklungsumgebung, um nur einige zu nennen.

OSS und Lizenzen

Ein Urheberrechtsinhaber von OSS verzichtet nicht auf sein Urheberrecht am Code, sondern gewährt Benutzern bestimmte Rechte an der Software, unter der Bedingung, dass die Software-Lizenzbedingungen durch den Benutzer eingehalten werden. In einigen Fällen kann ein Inhaber eines Urheberrechts Benutzern eine Patentlizenz erteilen. Für Benutzer von Open Source-Software ist es wichtig, die Lizenz jeder von ihnen verwendeter OSS zu verstehen.

Fast alle OSS-Lizenzen lehnen jegliche Haftung des OSS-Entwicklers ab. In fast allen Fällen übernehmen die OSS-Entwickler keine Verantwortung für die Verwendung ihrer OSS. Benutzer, Produktintegratoren und Anbieter müssen diese Verantwortung jedoch für Ihre Software ggf. übernehmen.

Nicht alle Softwareprodukte sind urheberrechtlich geschützt. Wenn Sie beurteilen müssen, ob eine bestimmte OSS urheberrechtlich geschützt ist oder nicht, sollten Sie sich an einen Rechtsanwalt oder Urheberrechtsexperten wenden.

Was eine Lizenz erlaubt (Urheberrecht)

Mit einigen OSS-Lizenzen gewährt der Inhaber des Urheberrechts Dritten das Recht, die Software zu verwenden oder zu verbreiten. Diese Lizenzgewährung erfolgt ohne direkte Kommunikation zwischen dem Urheberrechtsinhaber und dem Benutzer. Dieses Nutzungsrecht wird jedoch nur gewährt, wenn der Benutzer die vom Urheberrechtsinhaber in der Lizenz festgelegten Bedingungen einhält. Wenn ein Benutzer diese Lizenzbedingungen nicht einhält, besteht ein ernstes Problem.

Was eine Lizenz erlaubt (Patente)

Mit einigen OSS-Lizenzen gewährt der Urheberrechtsinhaber einer OSS Dritten das Recht, die Patente, die mit der Software umgesetzt werden und dem Inhaber des Urheberrechts gehören, frei zu nutzen. Nicht jede OSS-Lizenz gewährt eine solche Patentlizenz. Beispiele für Lizenzen, die eine solche Patentnutzungserlaubnis enthalten, sind die Apache-Lizenz und die GNU General Public License (GPL) Version 3.

Typische OSS-Lizenzen

Die Open Source Initiative (OSI) ist eine Organisation, die OSS fördert. Sie definiert die Kriterien für die Definition von OSS und hat Dutzende verschiedener Lizenzen als gültige OSS-Lizenzen freigegeben.

<https://opensource.org/licenses>
<https://opensource.org/osd>

Die meiste OSS wird unter einer von der OSI genehmigten Lizenz lizenziert. Darüber hinaus wird einige Software, die unter einer nicht von der OSI genehmigten Lizenz lizenziert ist, möglicherweise auch als Open Source-Software behandelt. Ob eine solche Software als OSS (oder auf andere Weise) behandelt werden soll, sollte durch Vereinbarung zwischen dem Softwarelieferanten und dem Empfänger festgelegt werden.



Was Sie tun müssen, um die Vorteile von OSS nutzen zu können

Wenn Sie OSS verwenden, ist es am wichtigsten zu wissen, welche Verpflichtungen Sie im Zusammenhang mit einer Verbreitung der Software haben.

Fast alle OSS-Lizenzen definieren Folgendes:

- Der OSS-Entwickler lehnt jede Haftung für Auswirkungen der Verwendung der Software ab
- Einige Verpflichtungen müssen erfüllt werden, wenn die Software von einer natürlichen oder juristischen Person (Distributor) vertrieben wird.

In den folgenden Abschnitten kann ein Distributor entweder eine natürliche oder eine juristische Person wie eine Firma sein.

Jeder, der die Bedingungen der Lizenz einhält, darf die Software frei nutzen und verbreiten.

Die Bedingungen sind jedoch von Lizenz zu Lizenz unterschiedlich. Bei einigen Lizenzen müssen in der weiterverbreiteten Software lediglich ein Lizenzhinweis und ein Urheberrechtsvermerk enthalten sein. Andere Lizenzen erfordern die Offenlegung des Quellcodes und ein schriftliches Angebot, diesen erhalten zu können. Einige Lizenzen haben Bedingungen, die sich darauf auswirken, mit welcher anderen OSS diese in Kombination verwendet werden kann. Ein Distributor ist verpflichtet, alle in der Lizenz festgelegten Verpflichtungen einzuhalten.

Es gibt verschiedene Möglichkeiten, Software zu verbreiten. Eine Möglichkeit besteht darin, ein Produkt zu verkaufen, welches die OSS-Software enthält. Eine andere Möglichkeit besteht darin, eine Website bereitzustellen, von der die Software heruntergeladen werden kann. Wenn ein Objekt, das OSS enthält, verbreitet wird, muss jeweiliger Distributor die Lizenz für diese OSS einhalten.



Beispiele für die Distribution von OSS

Es gibt verschiedene Möglichkeiten, wie OSS verbreitet werden kann. In jedem Fall muss der Distributor die OSS-Lizenz einhalten.

1. Eine Möglichkeit, OSS weiterzuverbreiten, besteht darin, ein Produkt mit einem SDK (Software Development Kit) zu entwickeln, welches von einem Halbleiterhersteller bereitgestellt wird. Wenn OSS, die im SDK enthalten ist, während der Entwicklung in ein Produkt integriert wird, bedeutet dies, dass der Halbleiterhersteller OSS über die Einbeziehung in sein SDK verbreitet und auch der Produktentwickler OSS über die Integration in sein Produkt distribuiert. In diesem Fall ist der Produktanbieter für die Einhaltung der Lizenz verantwortlich; ist hierbei jedoch vom Halbleiterhersteller abhängig. Wenn der Halbleiterhersteller keine entsprechenden Informationen zur im SDK enthaltenen OSS bereitstellt, kann der Produkthersteller die OSS-Lizenz nicht einhalten.
2. Eine andere Möglichkeit, OSS zu weiterzuverbreiten, besteht darin, dass von einem Hersteller ein ODM oder OEM mit Entwurf und Entwicklung eines Produkts beauftragt wird. Der ODM oder der OEM kann OSS in das Produkt integrieren, über die der Produktvertreiber Bescheid wissen muss.
Obwohl ein OEM oder ODM das Produkt hergestellt hat, distribuiert der Markeninhaber die in das Produkt integrierte OSS mit seinem Produkt. Der Markeninhaber muss die OSS-Lizenz einhalten. Wenn der ODM- oder OEM-Hersteller keine entsprechenden Informationen zu OSS bereitstellt, kann der Markeninhaber des Produkts die OSS-Lizenz nicht einhalten.
3. Andere Möglichkeiten eines Verbreitens von OSS umfassen das Versenden eines Produkts, die Veröffentlichung von Anwendungen für Mobilfunkgeräte oder das Bereitstellen eines Softwareupdates für ein zuvor ausgeliefertes Gerät.
Wenn OSS in einem Produkt, einer mobilen Anwendung oder einem Software-Update enthalten ist, handelt es sich um die Distribution von OSS. Die Entität, die das Produkt versendet oder die Software veröffentlicht, muss die OSS-Lizenz einhalten.
4. In Webseiten verwendetes JavaScript stellt eine Verbreitung dar:
Ein interessanter Fall der OSS-Distribution kann auftreten, wenn eine Webseite auf den Computer eines Benutzers übertragen wird.

In Webseiten enthaltenes JavaScript wird als Teil der Webseitendaten vom Webserver an den Browser auf dem Computer des Benutzers übertragen, wenn der Benutzer auf die Seite zugreift. Handelt es sich bei

dem JavaScript-Programm um OSS, handelt es sich um eine Distribution, und es gelten die Lizenzbestimmungen.

Verpflichtungen, die zu erfüllen sind, wenn OSS distribuiert wird

Die Verpflichtungen, die erfüllt werden müssen, wenn OSS weiterverbreitet wird, variieren von Lizenz zu Lizenz. Es ist wichtig, alle OSS-Lizenzen und zugehörigen Lizzenzen in einem Produkt oder Programm zu identifizieren, das verbreitet wird.

Dies ist erforderlich, um alle unterschiedlichen Lizenzbedingungen, die erfüllt werden müssen, klar zu verstehen.

Permissive Lizenzen

Die MIT-Lizenz, die BSD-Lizenz und die Apache-Lizenz beinhalten nur wenige Verpflichtungen. Diese Lizenzen erfordern die Weitergabe des Urhebervermerks der Software und des Lizenztextes. Der Hinweis sollte deutlich sichtbar an einer Stelle angebracht sein, an welcher die Person, die die OSS erhält, ihn lesen kann.

Wechselseitige Lizenzen

Die GPL-Lizenz, die LGPL-Lizenz, die AGPL-Lizenz und die Mozilla Public License erfordern die Offenlegung des Quellcodes für die zugehörige Software. (Lizenzangaben und Urhebervermerke im Quellcode dürfen nicht entfernt werden.) Wenn der Distributor den Quellcode geändert hat, müssen auch alle Quellcode-Änderungen offengelegt werden. Wechselseitige Lizenzen möchten eine Umgebung schaffen, in welcher Benutzer ihre Änderungen und Verbesserungen mit allen Benutzer und Entwicklern der Software teilen.

Neben der Offenlegung des Quellcodes müssen für diese Lizenzen in der Regel auch andere Verpflichtungen erfüllt werden. Um Software unter einer wechselseitigen Lizenz verbreiten zu können, müssen Sie diese Verpflichtungen verstehen. Bei Bedarf sollten Sie sich an Ihre für Recht und geistiges Eigentum zuständigen Mitarbeiter wenden.

Patentrechte, die Sie nicht erteilen können

In einigen Fällen kann eine OSS-Lizenz erfordern, dass ein Distributor seinen Benutzern eine Lizenz für Patente erteilt, die in derjenigen Software enthalten sind, die der Distributor verwendet mit einer OSS integriert. Wenn Sie ein solches Patent haben, für das Sie Ihren Benutzern keine Lizenz gewähren können, dürfen Sie OSS, für die diese Lizenzbestimmungen gelten, nicht vertreiben.

Risiken bei Mißachtung der OSS-Lizenz

Falls durch einen OSS-Urheberrechtsinhaber gegen ein Unternehmen wegen Nichteinhaltung der Lizenz ein Rechtsstreit eingeleitet wurde.

Leider kommt es vor, dass die Nichteinhaltung der OSS-Lizenz zu Rechtsstreitigkeiten der OSS-Urheberrechtsinhaber gegen den Benutzer (und den Distributor) führt. In mindestens einem Fall verlangte ein Urteil vom Beklagten, die Verbreitung ihrer OSS-beinhaltenden Produkte auszusetzen.

Im Dezember 2009 gab es eine Klage im Zusammenhang mit einer Open Source-Software namens "Busybox". Das Busybox-Programm ist weitgehend in Embedded- Systeme integriert und ist unter der GPL-Lizenz Version 2 lizenziert. In diesem Fall waren 14 Unternehmen in den Rechtsstreit verwickelt, darunter einige aus der Unterhaltungselektronik-Branche. Das Bemerkenswerte an diesem Fall war, dass einige Unternehmen aufgrund der Produkte eines ODM-Herstellers in den Rechtsstreit verwickelt waren.

In jedem Fall führte die Nichteinhaltung der OSS-Lizenz durch den Distributor zu den Rechtsstreitigkeiten. Um Rechtsstreitigkeiten zu vermeiden, sollte ein Unternehmen, das mit OSS arbeitet:

- jede OSS in der zu verbreitenden Software identifizieren
- die durch die OSS-Lizenz(en) definierten Verpflichtungen verstehen und befolgen



Was durch einen Rechtsstreit verloren geht

Wenn ein Unternehmen in einem Rechtsstreit verwickelt ist, besteht einer der größten Schäden für das Unternehmen in Reputationsverlust (Reputationsrisiko). Ein schlechter Ruf hinsichtlich einer Nichteinhaltung von Softwarelizenzbedingungen kann dazu führen, dass ein Unternehmen das Vertrauen anderer Unternehmen verliert. Je mehr ein Unternehmen die Bedeutung seiner Vertrauensbeziehungen versteht und sich bemüht, Vertrauen in seiner gesamten Branche aufzubauen, desto ernsthafter agiert es, Risiken für seine Reputation zu vermeiden.

Die Reaktion auf Rechtsstreitigkeiten erfordert viel Arbeit und Aufwand. Ohne Rechtsstreitigkeiten könnten die in den Bereichen Recht, Einkauf, Anwendungsentwicklung und Compliance tätigen Mitarbeiter für konstruktivere Aufgaben eingesetzt werden. Dies bedeutet, dass ein Unternehmen, welches sich die Zeit nehmen muss, um auf Rechtsstreitigkeiten zu reagieren, möglicherweise andere Geschäftschancen verpasst, an denen diese Mitarbeiter arbeiten könnten. Insbesondere die Anstellung eines kompetenten Anwalts für OSS-Rechtsstreitigkeiten ist sehr teuer.

Ein Vergleich oder ein Gerichtsurteil kann die Bezahlung von Geld oder einer Geldstrafe erfordern. Im Extremfall kann ein Urteil dazu führen, dass die Distribution eines Produkts ausgesetzt wird, was sehr geschäftsschädigend und kostspielig sein kann.

Wie man eine gute Beziehung zur OSS-Community aufbaut

Um das Risiko von Rechtsstreitigkeiten zu verringern, ist es wichtig, die OSS-Prinzipien zu verstehen und die Verpflichtungen aus den OSS-Lizenzen einzuhalten. Darüber hinaus wird dringend empfohlen, einen Beitrag zur OSS-Community zu leisten und gute Beziehungen zu

den Entwicklern der von Ihnen verwendeten OSS aufzubauen

Wenn Sie die Gründe, warum die Autoren eine bestimmte Open Source-Lizenz für ihre Software ausgewählt haben, und die Absichten der OSS-Community, die ein OSS-Projekt unterstützen, verstehen, werden Sie in der Lage versetzt, über ein rein wortgetreues Einhalten einer OSS-Lizenz hinauszuwachsen. Die Absichten der Entwickler zu verstehen, ist einer der wichtigsten Vorteile einer guten Beziehung zur OSS-Community.

Eine gute Beziehung zur OSS-Community kann es einem Unternehmen ermöglichen, dass eigene neue Ideen in die OSS aufgenommen werden. Die OSS-Community kann die Software basierend auf Ihren Ideen und Anforderungen verbessern. Außerdem haben Entwickler in Ihrem Unternehmen möglicherweise die Möglichkeit, mit hochqualifizierten OSS-Entwicklern zusammenzuarbeiten. Dies kann die Zufriedenheit und Kompetenz Ihrer Entwickler fördern.

Mit zunehmender Größe und Funktionalität von Systemsoftware wird diese immer komplexer. Es wird immer schwieriger, fehlerfreie Software zu erstellen. Wenn ein Unternehmen jedoch gute Beziehungen zu OSS-Entwicklern unterhält, kann die Community Ihren Softwareingenieuren bei der Entwicklung der Software unterstützen um Fehler zu finden und zu beheben.

Wie man zu OSS-Communities beiträgt

Es gibt viele Möglichkeiten, einen Beitrag zu OSS-Communities zu leisten: Bugfixes und neue Funktionen vorschlagen, Dokumente übersetzen, Orte und Foren bereitstellen, in denen Community-Mitglieder kommunizieren können, sowie ein Sponsoring von und eine Teilnahme an OSS-unterstützenden Projekten und Fachverbänden wie z. B. der Linux Foundation.



Das Thema der Lieferkette

OSS-Compliance kann nicht von einer Person allein erreicht werden.

Je größer und komplexer Software wird, desto größer und komplexer wird auch die Software-Lieferkette. Zu einer modernen Software-Lieferkette können eine OSS-Community, ein Softwarelieferant, ein Halbleiterhersteller, der ein SDK bereitstellt, und ein Hersteller eines Endproduktes gehören. Wenn ein Mitglied einer großen und komplexen Software-Lieferkette die Lizenzverpflichtungen nicht einhält oder die entsprechenden Lizenzinformationen nicht bereitstellt, hat dies erhebliche Auswirkungen auf den Anbieter, der zur Einhaltung der Lizenz verpflichtet ist (Abbildung 1). Konformitätsfehler können dazu führen, dass die Bereitstellung eines Produktes ausgesetzt wird. Wenn der Anbieter den Fehler vor Bereitstellung nicht kennt, kann er bezüglich des Fehlers Anfragen von einem Urheberrechtsinhaber oder einem Dritten erhalten, die er nicht beantworten kann.

Wenn die Software-Compliance jedoch in der vorgelagerten Lieferkette ordnungsgemäß verwaltet wird, können diese Probleme vermieden werden. Um die Einhaltung von OSS-Lizenzen zu erleichtern, müssen alle Teilnehmer an der Lieferkette ihre Pflicht erfüllen, Vertrauen in der gesamten Lieferkette aufzubauen und entsprechende Informationen zu enthaltener Software kommunizieren.

Es empfiehlt sich, dass jedes Unternehmen in der Lieferkette ein Team zusammenstellt, um die Einhaltung der OSS-Compliance in der Kette sicherzustellen. Das OpenChain-Projekt der Linux Foundation bietet ein Selbstzertifizierungsprogramm, das Unternehmen für diesen Zweck verwenden können. Die Selbstzertifizierung hilft einem Unternehmen dabei, seinen Compliance-Prozess zu überprüfen. Der Zertifizierungstest ist in mehreren Sprachen verfügbar und kann von jedem kostenlos genutzt werden.

Abbildung 1 Probleme in der Software-Lieferkette

Anforderungen an Mitglieder der Lieferkette

Wenn ein Lieferant Software vertreibt, muss dieser Lieferant jedem Empfänger die Informationen zur Verfügung stellen, die zur Einhaltung der OSS-Lizenz erforderlich sind. Ein Empfänger sollte die Daten und Dateien sorgfältig prüfen und sicherstellen, dass sie korrekt sind.

Ein Software-Distributor kann Software von mehreren Anbietern in ein einzelnes Produkt integrieren. In diesem Fall muss der Distributor zusammen mit der Software Informationen zu jeder enthaltenen OSS-Komponente erhalten.

Wenn zu einer OSS-Komponente keine Informationen empfangen werden, sollte diese OSS nicht in ein Produkt integriert werden.

Unterschiedliche Rollen in einem Unternehmen haben unterschiedliche Verantwortlichkeiten für OSS-Compliance

Softwareentwickler

Softwareentwickler sollten die Konfiguration einer Software verwalten, aufzeichnen und speichern. Dies beinhaltet Folgendes:

- OSS und ihre Lizenz
- Verlinkungen (z.B. von der Software verwendete Bibliotheken, dynamische oder statische Verlinkung, etc.)
- Bearbeitungen - das heißt, die technischen Details aller an der Software vorgenommenen Änderungen.

Diese Elemente müssen identifiziert und dokumentiert werden. Jedes Mal, wenn sich die Softwarekonfiguration ändert, sollte die Dokumentation aktualisiert werden. Die Lizenz für ein bestimmtes Projekt kann sich von einer Softwareversion zur nächsten ändern. Es wird empfohlen, die Dokumentation so zu erstellen und zu verwalten, dass jedes OSS-Element leicht referenziert und überprüft werden kann. Bei einigen Lizizenzen (z. B. der GPL-Lizenz) muss ein Distributor den Quellcode offenlegen. Es wird dringend empfohlen, eine Versions-verwaltungssoftware zu verwenden, um den ursprünglichen Quellcode und alle Änderungen am Quellcode nachzuverfolgen.

Softwareeinkäufer

Softwareeinkäufer müssen zu eingehender Software OSS-Informationen erhalten, damit Softwareentwickler diese

aufzeichnen können. OSS kann in jeglicher Software - wie dem von einem Halbleiterhersteller bereitgestellten SDK - enthalten sein.

Einkäufer müssen auf die Software bei allen Arten von Liefergegenständen achten, die das Unternehmen erhält.

Vertriebsmitarbeiter

Vertriebsmitarbeiter müssen mit Kunden in Bezug auf OSS kommunizieren. Ein Kunde kann spezielle Anforderungen in Bezug auf die Verwendung von OSS haben. Beispielsweise verfügt ein Unternehmen möglicherweise über eine OSS-Richtlinie, die die Verwendung von OSS mit bestimmten Lizizenzen verhindert.

Für Vertriebsmitarbeiter ist es wichtig, die Anforderungen der Kunden in Bezug auf OSS zu kennen und diese Informationen internen Softwareentwicklern mitzuteilen.

Rechtsberater / Lizenzmanager

Die Zusammenarbeit mit Rechtsberatern und Lizenzmanagern ist für das Verständnis von OSS-Lizenzen unabdingbar. Rechtsberater und Lizenzmanager sollten die Lizizenzen überprüfen, denen die von einem Unternehmen verwendete OSS unterliegt, und die Entwickler hinsichtlich ihrer Verwendung beraten:

- Welche Freigaben sind für die Verwendung von OSS erforderlich? (Im Allgemeinen sehen OSS-Lizenzen keine Haftung des Entwicklers der Software vor.)
- Was ist erforderlich, um die OSS distribuieren zu können?
- Kann die Integration einer OSS ein Problem verursachen, wenn die Software von weiteren Empfängern ("Downstream") verwendet wird?

Führungskräfte und Manager

Um OSS effektiv und ordnungsgemäß nutzen zu können, müssen verschiedene Mitarbeiter in einem Unternehmen zusammenarbeiten.

Führungskräfte und Manager müssen möglicherweise die Koordination zwischen Unternehmenseinheiten erleichtern und können beschließen, ein dediziertes Team für die Verwaltung von OSS-bezogenen Themen einzurichten. Dies beinhaltet Investitionen in Personal, in Weiterbildung und Entwicklungsumgebungen.

OSS-Information, die mit einer Software ausgeliefert werden muss

Um sicherzustellen, dass alle von OSS profitieren, müssen Benutzer wissen, welche Informationen in Bezug auf OSS mit auszuliefernden Softwareprodukten bereitgestellt werden müssen.

In dieser Broschüre wurde erläutert, wie wichtig es ist, eine OSS-Dokumentation zu führen und OSS-Lizenzen einzuhalten.

Welche Informationen zu OSS sollten mit auszuliefernden Softwareprodukten bereitgestellt werden? In diesem Abschnitt werden die spezifischen Informationen erläutert, die mit OSS verteilt werden müssen. Da die erforderlichen Informationen je nach Geschäfts- und Unternehmensrichtlinien unterschiedlich sind, wenden Sie sich an jedes Empfängerunternehmen, um weitere Informationen zu erhalten.

Wenn keine OSS in den Software-Liefergegenständen enthalten ist, sollten Sie den Empfängern klar mitteilen, dass der Liefergegenstand keine OSS enthält. Der Empfänger kann dann entsprechend handeln.

Wenn OSS im Lieferumfang der Software enthalten ist, müssen Sie diese Software und die jeweilige Lizenz eindeutig ausweisen. Beispielsweise kann sich die Lizenz zwischen verschiedenen Versionen einer OSS ändern. Name und Version jeder OSS-Komponente sind unverzichtbare Informationen. Für jede Komponente ist es hilfreich, eine Download-Quelle oder die Quellcode- oder Hauptprojektwebseite für die Software anzugeben. Auf diese Weise können die Empfänger die Informationen zur Software, ihrer Version und Lizenz überprüfen.

Wenn der Distributor gemäß der OSS-Lizenz zur Offenlegung des Quellcodes aufgefordert wird, geben Sie den Quellcode an. Der jeweils erforderliche Quellcode hängt von der OSS-Lizenz ab. Zum Beispiel erfordert Version 3 der GPL-/ LGPL-Lizenz, dass Sie neben dem Quellcode für die Software auch Informationen bereitstellen müssen, die auf der Grundlage des Codes für die Installation einer modifizierten Binärcodedatei erforderlich sind.

Information, die mit einer OSS verbreitet werden muss

Die folgenden Informationen müssen mit Ihren Liefergegenständen verteilt werden, die OSS enthalten.

- Liste der OSS-Komponenten

Für jede OSS-Komponente:

- Informationen für die Identifikation der Software (Versionsnummer, Quelle des Quellcodes (z. B. Website-URL) und wie die Software bezogen werden kann)
- Liste der anzuwendenden Lizenzen und (falls mehr als eine vorhanden) der Lizenz, unter der Ihr Unternehmen das OSS vertreibt
- Alle Änderungen, die Sie an der Software vorgenommen haben

Bei OSS, bei denen der Distributor laut Lizenzverpflichtung den Lizenztext und Urhebervermerke bereitstellen muss:

- Den Original-Lizenztext und den Urhebervermerk

Bei OSS, bei welcher die Lizenz eine Offenlegung des Quellcodes erfordert:

- Den erforderlichen Quellcode (Im Fall von GPL müssen Sie zusätzlich zum Quellcode auch diejenigen Skripte bereitstellen, die für die Generierung der aus dem Quellcode erstellten ausführbaren Dateien verwendet werden.)

In einigen Fällen, in denen eine OSS-Komponente selbst eine sekundäre OSS-Komponente enthält, müssen Sie auch Informationen für die sekundäre OSS-Komponente bereitstellen.

Die oben genannten Informationen sind ziemlich allgemein gehalten. Ein Kunde benötigt möglicherweise bestimmte Informationen, während ein anderer Kunde stattdessen andere Informationen benötigt. Es ist wichtig, mit Ihren Kunden über die benötigten Informationen und deren Format zu kommunizieren.

Das SPDX-Projekt

Das von der Linux Foundation gehostete, SPDX®(Software Package Data Exchange®)-Projekt stellt ein standardisiertes Format für den Austausch von Lizenzinformationen bereit.

Das Format kann von jeder Person verwendet werden, und es wird dringend empfohlen, es in der gesamten Lieferkette zu verwenden. Informationen zu diesem Format finden Sie unter:

<https://spdx.org/>

Werkzeuge zum Scannen von Quellcode

Es gibt Scan-Tools, die OSS in Software-Paketen erkennen und einige Informationen automatisch generieren können. Beispielsweise hat das von der Linux Foundation gehostete FOSSology-Projekt ein solches Scan-Tool entwickelt. Das FOSSology-Tool ist unter einer OSS-Lizenz erhältlich und kann von jedermann frei verwendet werden. Es stehen auch andere Scan-Tools mit kommerziellen Lizenzen zur Verfügung. Es wird empfohlen, solche Tools zu verwenden, um OSS-Lizenzen in Softwarepaketen während der Entwicklung und vor Auslieferung zu überprüfen.

Einige Scan-Tools können Berichte basierend auf der SPDX-Spezifikation erstellen. Diese Scan-Tools sind nützlich, um Informationen zu generieren, die direkt in den Liefergegenständen für einen Kunden enthalten sein können.



Über das OpenChain-Projekt

Das OpenChain-Projekt stärkt das Vertrauen in Open Source, indem es Open-Source-Lizenzcompliance einfacher und konsistenter macht. Die OpenChain-Spezifikation definiert einen Kernsatz von Anforderungen, die jedes Qualitätssicherungsprogramm erfüllen muss. Mit "OpenChain Conformance" können Unternehmen die Einhaltung dieser Anforderungen nachweisen. Das "OpenChain-Curriculum" unterstützt diesen Prozess, indem es umfangreiches Referenzmaterial für effektives Open-Source-Training und -Management bereitstellt. Das Ergebnis ist, dass Open-Source-Lizenzcompliance für alle Teilnehmer der Software-Lieferkette vorhersehbarer, verständlicher und effizienter wird.

Über The Linux Foundation

The Linux Foundation widmet sich der Aufgabe, ein nachhaltiges Ökosystem für Open Source-Projekte aufzubauen, um die Technologieentwicklung und die Akzeptanz in der Industrie zu beschleunigen.

The Linux Foundation wurde im Jahr 2000 gegründet und bietet Open Source-Communities beispiellosen Support durch finanzielle und intellektuelle Ressourcen, Infrastruktur, Services, Veranstaltungen und Schulungen. Gemeinsam bilden The Linux Foundation und ihre Projekte die ehrgeizigste und erfolgreichste Investition in die Schaffung von 'shared technology'.

