TIMETOACT
SOFTWARE & CONSULTING

Open Source Compliance

Herausforderungen beim Einsatz von Open Source Software

TIMETOACT
Performance Strategy

Was ist Open Source?

Open Source heißt „quelloffen“ und meint entsprechend Software, deren Quellcode öffentlich zugänglich ist. Um als Open Source zu gelten, muss es Usern möglich sein, die Software a) auszuführen, b) zu analysieren, c) an die eigenen Bedürfnisse anzupassen und d) weiterzugeben – auch in veränderter Form.

Was sind die Vorteile?

Open Source Produkte erfreuen sich auch in Unternehmen immer größerer Beliebtheit und bieten eine ganze Reihe an Vorteilen:

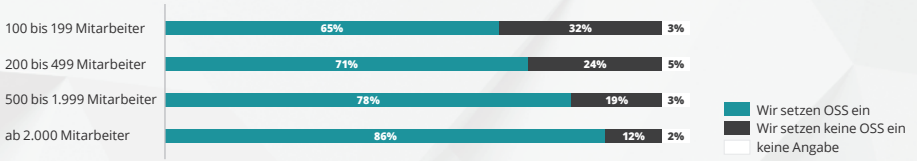
Unabhängigkeit von Dienstleistern ✔
Meist kostenlose Nutzung ✔
Einblick in den Quellcode ✔
Möglichkeit zur Anpassung des Quellcodes ✔
Große Community ✔
Hoher Reifegrad der Anwendung durch ständige Weiterentwicklung ✔

Welche Bedingungen sind an die Nutzung geknüpft?

Entgegen der allgemeinen Meinung gibt es sehr wohl Bedingungen und Fallstricke bei der Nutzung von Open Source Software. So ist deren Einsatz wie bei proprietärer Software von Lizenzvorschriften abhängig. Sogenannte Permissive Lizenzen bieten Endanwendern große Freiheiten und erlauben eine Nutzung gegen minimale Auflagen. Demgegenüber stehen Copyleft Lizenzen, deren Nutzung an strikte Voraussetzungen geknüpft ist.

Wie verbreitet ist Open Source Software?

Die Nutzung von Free and Open Source Software (FOSS) nimmt rasant zu. Mittlerweile setzen nahezu alle großen Unternehmen weltweit auf entsprechende Lösungen.



Einsatz von OSS nach Unternehmensgröße, Quelle: Bitkom Research 2019

Wurde Open Source früher noch als Ersatzlösung für Proprietäre Software gesehen, z. B. Libre Office anstatt Microsoft Office, integrieren heute immer mehr Unternehmen Open Source-Produkte in eigene Anwendungen. Diese Entwicklung bringt neue Herausforderungen mit sich.

Welche Herausforderungen gehen mit der Nutzung einher?

Pauschal zu behaupten, Proprietäre sei sicherer als Open Source Software ist sicherlich nicht richtig. Allerdings fehlen im Falle der frei zugänglichen Software regelmäßige Updates und Patches vom Hersteller und die einsetzenden Unternehmen sind selbst für die Sicherheit verantwortlich. Schwachstellen können weitreichende Konsequenzen haben, wie der **Log4J-Vorfall 2022** eindrucksvoll gezeigt hat.

Wie angedeutet, bedeutet Open Source nicht, dass Unternehmen die Software verwenden dürfen, wie sie möchten. So gestattet es die Copyleft Lizenz im Normalfall zwar, Open Source Software zu verändern oder in unternehmenseigene Produkte einzubauen und anschließend weiterzugeben, allerdings oftmals unter der Voraussetzung, dass die daraus entstehende Software ebenfalls frei – nach Open Source-Regeln – lizenziert werden muss.

Dies kann dazu führen, dass Firmen, welche Copyleft Lizenzen falsch einsetzen, dazu gezwungen sein könnten, den Source Code offenzulegen bzw. an alle weiterzugeben, die auch die Software erhalten. Der Kommerzielle Schaden kann für Unternehmen, die eigene Software entwickeln, durchaus erheblich sein. Das betrifft alle Geräte, die mit Software ausgeliefert werden, seien es Autobetriebssysteme, Maschinensteuerungen oder Fernsehgeräte. Auch Webanwendungen sind hiervon möglicherweise nicht mehr ausgenommen.

Wie kann ich mich absichern?

Als Hilfestellung für Unternehmen, die ein Open Source Compliance-Programm etablieren und die Risiken minimieren wollen, gibt es seit 2020 den ISO Standard 5230 als Leitlinie. Die ISO Norm selbst definiert allerdings lediglich Anforderungen und bietet wenig Hilfe bei der Implementierung. Die Norm selbst wird von der Open Chain Organisation erstellt und überwacht.

www.openchainproject.org

OPENCHAIN

Wie kann die TIMETOACT unterstützen?

TIMETOACT nutzt selbst seit Jahren Open Source- Technologien für die Softwareentwicklung. Darüber hinaus berät sie große Mittelständer und Großkonzerne zu Lizenz Compliance für Proprietäre sowie Open Source Produkte und bringt umfangreiche Expertise in dem Bereich mit.

TIMETOACT selbst ist Partner der Openchain Organisation und hilft Unternehmen dabei die Anforderungen der ISO Norm zu erfüllen.

Gerne beraten unsere Expert*innen Sie zu Open Source Lizenzen und unterstützen Sie bei der Umsetzung Ihres Open Source Compliance Programms.

TIMETOACT
SOFTWARE & CONSULTING

Die TIMETOACT Services umfassen:

Open Source Consulting	Generelle Beratungsleitung Projektspezifisch oder auf Abrufbasis.
Implementierung Open Source Compliance Management	Unterstützung bei der Implementierung von Open Source Lizenzmanagement. Definition von Governance, Policies und dazugehöriger Prozesse.
Open Source Auditierung (Toolgestütz)	Auditierung von Software (Quellcode) um Compliance Risiken aufzudecken.
Security Auditierung (Toolgestütz)	Auditierung des Quellcodes um Sicherheitslücken zu identifizieren.
Managed Service	Komplettservice bezüglich Open Source Lizenzmanagement. Inkludiert Implementierung und regelmäßiges Review, sowie strategischer Ausbau.
Reifegrad-Assessment nach ISO/IEC 5230	Durchführung eines Assessment um den aktuellen Reifegrad der Organisation im Bezug zur ISO/IEC 5230 zu bewerten.
Implementierung ISO/IEC 5230	Unterstützung bei der Umsetzung von Maßnahmen für den ISO/IEC 5230 Standard.
Open Source Lizenzkatalog	Eigener Lizenzkatalog mit Risikobewertung von über 600 Open Source Lizenzen.

TIMETOACT
SOFTWARE & CONSULTING

Sprechen Sie uns gerne an!

Simon Pletschacher
Manager Performance Strategy
TIMETOACT

simon.pletschacher@timetoact.de
0176 75860472

www.timetoact.de/details/open-source-lizenzmanagement