Open-Source-Software

Die Markt(r)evolution...

Quelloffene Software ist in aller Munde. Gegner und Befürworter streiten über Vor- und Nachteile. Dabei werden Gegensätze diskutiert und zum Dogma erhoben, die das Thema im Grunde nur auf wenige Teilaspekte reduzieren. Es ist an der Zeit, die unterschiedlichen Aspekte einmal systematisch zu betrachten. Gerade im Bereich der Datensicherheit ist eine sorgfältige Analyse des Für und Wider wichtig.

Im Internet ist Open-Source-Software nicht mehr wegzudenken. So läuft weltweit auf knapp 68 % aller Webserver der quelloffene Apache. Die Abbildung der menschenfreundlichen Internet-Namen auf maschinenfreundliche IP-Adressen (z.B. www.interest.de auf 194.64.235.56) erfolgt durch DNS-Server; die darauf fast ausschließlich eingesetzte Open-Source-Software ist BIND. Auch die Mailtransportprogramme, sei es sendmail, postfix oder exim, sind im Quelltext verfügbar. Damit hat quelloffene Software bewiesen, dass sie an kritischen Stellen der Infrastruktur verlässlich eingesetzt werden kann.

Open Source – mehr als nur Linux

Häufig werden mit dem Begriff „Open Source“ Begrifflichkeiten verbunden, die damit wenig zu tun haben. Open Source ist kein Synonym für Linux. Der gesamte Linux-Kern sowie die GNU-Programme, die erst eine komplette Distribution ausmachen, sind zwar Open Source. Aber es gibt auch für Windows gute Open-Source-Software, z.B. Mozilla und Open Office.

Open Source ist nicht immer kostenlos

Auch heißt Open-Source-Software nicht notwendigerweise, dass eine Software kostenlos sein muss. Umgekehrt gibt es gute kostenlose Software, die nicht Open Source ist, z.B. Pegasus Mail für Windows und GPGshell.

PGP, OpenSSL und andere – Verschlüsselung mit Open Source

Wichtige Verschlüsselungssoftware, wie PGP, GnuPG, OpenSSL und die CryptLIB, sind Open Source. Hierbei nimmt PGP eine Sonderstellung ein. Denn PGP ist im Grunde kommerzielle Software. Der Quellcode wird offen gelegt, damit Interessenten prüfen können, ob die Software ihren eigenen Richtlinien entspricht. Bei allen vier Beispielen handelt es sich um etablierte, schon lange verfügbare Software.

Offen gelegte Quellcodes stärken das Vertrauen in die Software

Das Beispiel PGP zeigt, wie wichtig der Quellcode für das Vertrauen in die Software ist. Nachdem der zwischenzeitliche Besitzer von PGP, Network Associates, sich mit der Veröffentlichung des Quellcodes Zeit ließ, kamen alle möglichen Gerüchte auf. Die Fa. PGP Corp. macht nun als vertrauensbildende Maßnahme den Quellcode ihrer Produkte verfügbar. Ohne Quellcode wäre der gute Ruf von PGP also sehr schnell beschädigt.

Gerade in Zeiten, in denen selbst Regierungsbehörden sich an Wirtschaftsspionage beteiligen, ist die Verlässlichkeit von Verschlüsselungssoftware extrem wichtig. Und der offene Quellcode erlaubt es jedermann, selbst nach Sicherheitslücken zu suchen.

Open Source heißt nicht zwingend, keinen Support zu erhalten

Es gibt auch – in der Regel kostenpflichtigen – Support für Open-Source-Software. Die Autoren der Software entwickeln ein Geschäftsmodell, bei dem die Software kostenlos ist und der Support bezahlt wird. Häufig etablieren sich auch im Umfeld von Open-Source-Software Firmen, die

sich mit dem Produkt besonders gut auskennen und deshalb entsprechende Unterstützung anbieten können.

Lebensdauer der Software als Entscheidungskriterium für den Einsatz

Eine wichtige Frage vor der Verwendung ist, wie lange die Software noch weiterentwickelt und gepflegt wird. Besteht ein Entwicklungsteam nur aus einer Person, kann ein Projekt schnell aufhören zu existieren. Damit verschwindet nicht die Software, aber Weiterentwicklung und Pflege finden nicht mehr statt.

Mit Know-how können Sie Open Source selber weiterentwickeln

Bei Open Source hat das Unternehmen den Vorteil, über den Quellcode zu verfügen, sodass es die Entwicklung und Anpassung in die eigenen Hände nehmen und die Software so weiter nutzen kann.

Allgemeingut Open Source? Lizenzrecht in Deutschland und den USA

Auch für Open-Source-Software gibt es einen Lizenzvertrag. Die wichtigsten Lizenzen sind: GNU General Public License (GPL), GNU Lesser General Public License (LGPL), BSD License, MIT License und die Apache License. Alle Lizenzen finden sich auf der OSI-Webseite. Da diese Lizenzen im Wesentlichen vor dem Hintergrund amerikanischen Lizenzrechts entstanden sind, stellt sich die Frage nach der Gültigkeit in Deutschland. Im Mai hat

Linux contra Windows ist nur ein Teilaspekt der Diskussion.

das Landgericht München (Az. 21 O 6123/03) die GPL jedoch als rechtswirksam anerkannt.

Haftung und Gewährleistung bei Open Source

Dennoch wird zur Zeit versucht, eine „Deutsche Freie Software-Lizenz“ zu etablieren, die an das deutsche Rechtssystem besser angepasst, aber trotzdem kompatibel zur GPL ist. Nach US-Recht kann grundsätzlich jedwede Haftung ausgeschlossen werden. Dies ist mit dem deutschen Recht nicht vereinbar. Deshalb soll in einer deutschen Lizenz Haftung und Gewährleistung auf die Fälle „grober Fahrlässigkeit und Vorsatz“ beschränkt werden. Außerdem muss – da in Deutschland der Verzicht auf die sog. Urheberpersönlichkeitsrechte nicht möglich ist – die Beziehung zwischen Urheber und Werk stärker beachtet werden.

Prof. Dr. Rainer W. Gerling

Pro Open Source	Contra Open Source
Open-Source-Software ist millionenfach erfolgreich im Einsatz.	Open-Source-Entwicklung ist oft mehr vom Interesse der Entwickler als vom Bedarf des Markts getrieben.
Kritische Kernkomponenten des Internet (BIND, Mailserver) sind Open Source und haben sich bewährt.	Häufig sind Installationsroutinen nur für Experten und nicht für Endanwender durchführbar.
Quellcode erlaubt eigene Anpassungen und gegebenenfalls Fehlerkorrekturen.	Die Benutzeroberflächen sind teilweise gewöhnungsbedürftig, da das Design einer ergonomischen Oberfläche ein anderes Fachwissen als die Programmierung verlangt.
Meistens kostenlos verfügbar.	Häufig nur in Englisch verfügbar; eine deutsche Version muss selbst erstellt werden.
Ein Unternehmen kann durch Finanzierung der Entwicklung spezieller Funktionalitäten meist sehr schnell angepasste Versionen erhalten.	Falls Hardwareunterstützung erforderlich, wird neueste Hardware erst verspätet unterstützt, da die Hardwarehersteller die erforderlichen Entwicklerinformationen nicht herausgeben.
Da etablierte Open-Source-Software extrem häufig benutzt wird, besteht in der Regel hohe Stabilität; Fehler werden kurzfristig behoben.	Die Qualitätskontrolle eines großen Softwareherstellers ist systematischer.
Da es für viele Anwendungen konkurrierende Projekte (z.B. Editoren, Desktops, Mail-Programme) gibt, kann man aus einer Vielzahl von Anwendungen genau die passende finden.	Quellcode, der einmal unter der General Public License (GPL) steht, kann nicht unter eine andere Lizenz gestellt werden.
Aufgrund des Reviews und der Verfügbarkeit des Quellcodes ist das Vertrauen in die Software größer.	
Die Sicherheit ist besser, da es keine versteckten Funktionalitäten gibt.	
Man hat die Freiheit, mit der Software zu machen, was man will.	
Bei etablierten Verschlüsselungsprodukten sind die Kryptoalgorithmen wahrscheinlich fehlerfrei implementiert. Tests können entfallen.	