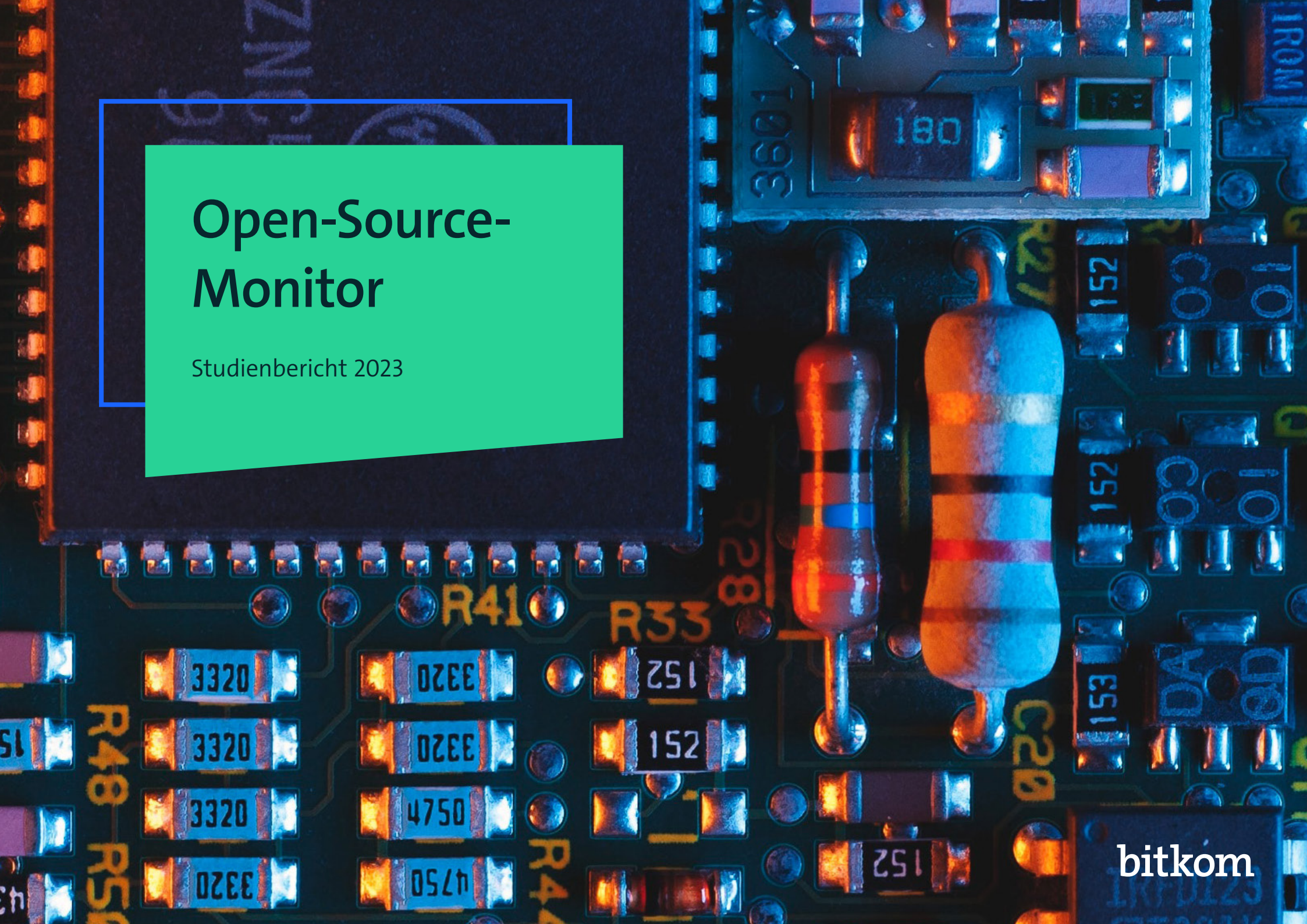


Open-Source-Monitor

Studienbericht 2023

bitkom

Inhalt

Abbildungen

Mit freundlicher Unterstützung von:

Welche Bedeutung hat Open Source in den Jahren 2023 und danach? Wer eine Antwort auf diese Frage sucht, der muss sich nur eines der aktuellen Top-Themen anschauen: Künstliche Intelligenz und die Large Language Models. Treiber waren und sind hier Unternehmen wie unter anderem das von Microsoft unterstützte OpenAI, Google oder Meta, aber inzwischen hat die Open-Source-Community aufgeholt und gibt teilweise sogar den Takt vor. Nicht wenige gehen sogar davon aus, dass Open-Source-Sprachmodelle über kurz oder lang die Qualitätsstandards setzen werden. Open Source – eine nerdige Nische in der digitalen Welt? Mitnichten.

Es gibt mehr als genug Beispiele aus anderen Bereichen. Kein Software-Entwicklungsteam kommt ohne Open-Source-Tools aus. Die großen digitalen Plattformen, von sozialen Netzwerken bis zu Streaming-Diensten, die wir täglich nutzen, basieren auf Open Source. Ohne sie gäbe es viele Dienste, die wir für selbstverständlich halten, gar nicht. Und der Datenverkehr im Internet? Er hängt zu einem großen Teil von Open-Source-Protokollen und -Software ab. Aber der Einfluss endet nicht bei Computern und Servern. Die Smartphone-Revolution, die unser Kommunikationsverhalten radikal verändert hat, wäre ohne Open-Source-Komponenten kaum denkbar. Sie ermöglichen nicht nur die Funktionalität der Geräte, sondern auch die rasante Innovation, die wir in den letzten Jahren erlebt haben.

Längst wird Open-Source-Software in Deutschland in der gesamten Breite der Wirtschaft verwendet: 7 von 10 Unternehmen setzen entsprechende Lösungen bewusst ein, die Hälfte aller Unternehmen beteiligt sich an der Weiterentwicklung von Open-Source-Software, meist durch den Bezug von kostenpflichtigem Support oder entsprechenden Enterprise-Lösungen. Mit dem »Open Source Monitor 2023«, für den mehr als 1.100 Unternehmen befragt wurden, wollen wir zum dritten Mal aufzeigen, welche Rolle Open Source für die Wirtschaft heute spielt und welche Entwicklungen zu erwarten sind. Erneut haben wir rund 100 Organisationen des Public Sector befragt, um ein Stimmungsbild zu erhalten. Dabei zeigt sich, dass Open-Source-Software auch aus Behörden nicht mehr wegzudenken ist: 59 Prozent nutzen solche Lösungen derzeit.

Da Open Source sowohl den Zugang zum Quellcode als auch die Möglichkeit beinhaltet, Verbesserungen vorzunehmen, diese der Öffentlichkeit zur Verfügung zu stellen und eigene Software rund um die Open-Source-Komponenten zu erstellen, ergeben sich eine Vielzahl von Vorteilen. Sowohl im Unternehmen, z. B. durch geringere Kosten, individuell angepasste Lösungen oder auch die Möglichkeit, die Sicherheit selbst zu überprüfen. Open Source bietet aber auch Chancen für unsere gesamte Wirtschaft und Gesellschaft:

> Open Source kann uns helfen, dem Ziel der Digitalen Souveränität näher zu kommen, indem wir die Hoheit über die eingesetzte Software behalten oder zurückgewinnen.

Dafür müssen wir Open Source aber noch stärker in den Fokus rücken und strategischer angehen. Denn nur rund jedes dritte Unternehmen (32 Prozent) gibt an, eine Open-Source-Strategie im Unternehmen zu verfolgen.

Hier gibt es noch viel Potenzial, das sich zu heben lohnt und noch viele Aufgaben für die Open-Source-Community, wozu wir mit diesem »Open Source Monitor 2023« unseren Beitrag leisten wollen.

Dr. Ralf Wintergerst
Präsident Bitkom

Methodik

Zum dritten Mal in Folge bietet der »Open-Source-Monitor 2023« aufschlussreiche Antworten auf Fragen rund um den Status Quo, die Einsatzmöglichkeiten und die Herausforderungen von Open-Source-Software in Deutschland. Wie in den Vorgängerstudien aus 2019 und 2021 liegt der Fokus auch in diesem Jahr wieder auf der deutschen Wirtschaft und den folgenden Fragen:

- Wie stehen die Unternehmen dem Thema Open-Source-Software grundsätzlich gegenüber und welche Vor- bzw. welche Nachteile sehen sie für ihre Unternehmen?
- Haben die Unternehmen eine Strategie zur Verwendung bzw. Beteiligung an Open-Source-Software?
- Inwiefern setzen Unternehmen Open-Source-Software ein und nach welchen Kriterien wird Open-Source-Software ausgewählt?
- Welche Ressourcen werden für das Open-Source-Software-Management eingesetzt? Wurde ein Open Source Programm Office eingerichtet und gibt es Analysetools zur Sicherheitsprüfung der eingesetzten Open-Source-Software-Komponenten?
- Inwiefern beteiligen sich die Unternehmen aktiv an der (Weiter-)Entwicklung von Open-Source-Software?
- Gibt es in Unternehmen niedergeschriebene Policies für Open-Source-Software?
- Wie adressieren Unternehmen das Themenfeld Compliance von Open-Source-Software?
- Und wie sieht es rund um die Etablierung und Standardisierung von Compliance-Prozessen aus?

Zur Beantwortung dieser und weiterer Fragen wurde eine Befragung von Unternehmen durchgeführt, um so den strategischen Einsatz von Open-Source-Software in deutschen Unternehmen zu untersuchen.

Gemeinsam mit den 20 Partnern Bitsea GmbH, Bundesdruckerei GmbH, Dataport AöR, DB Systel GmbH, Eclipse Foundation Europe GmbH, Fraunhofer-Gesellschaft, ITDZ Berlin AöR, Kernkonzept GmbH, KPMG AG Wirtschaftsprüfungsgesellschaft, Mercedes-Benz Group AG, {metæffekt} GmbH, NORDEMANN, Open-XChange, Osborne Clarke, publicplan GmbH, PwC GmbH, Red Hat GmbH, Siemens AG, Sonatype und SUSE Software Solutions Germany GmbH haben der Digitalverband Bitkom und Bitkom Research das Studiendesign entwickelt. Hierbei war das Ziel weiterhin repräsentative Einblicke in die deutsche Wirtschaft zu bekommen. Gemeinsam mit der Fachexpertise des Projektkonsortiums wurde hierfür zunächst ein standardisierter Fragebogen entwickelt. Im nächsten Schritt wurden im Zeitraum von Ende März bis Mitte Mai 2023 computergestützte telefonische Interviews (CATI) von geschulten Telefoninterviewerinnen und -interviewern durchgeführt.

Im Rahmen der Unternehmensbefragung wurden 1.155 Unternehmen mit mindestens 20 Beschäftigten in Deutschland befragt, die repräsentativ nach Größenklassen und Branchen ausgewählt wurden. Durch Schichtung dieser Zufallsstichprobe wurde gewährleistet, dass Unternehmen aus den unterschiedlichen Größenklassen und Branchen in für statistische Auswertungen ausreichender Anzahl vertreten sind. Die Aussagen der Befragungsteilnehmerinnen und -teilnehmer wurden bei der Analyse gewichtet, sodass die Ergebnisse ein repräsentatives Bild für alle Unternehmen ab 20 Beschäftigten in Deutschland ergeben (siehe Abbildung 1). Die gewählte Stichprobenstruktur erlaubt die Darstellung von Besonderheiten innerhalb ausgewählter Größenklassen und Branchen.

Größenklassen	Absolut Ungewichtet	Prozentual Ungewichtet	Absolut Gewichtet	Prozentual Gewichtet
20 – 99 MA	353	30,6 %	926	80,2 %
100 – 199 MA	302	26,1 %	119	10,3 %
200 – 499 MA	249	21,6 %	72	6,2 %
500 – 1.999 MA	152	13,2 %	32	2,8 %
2.000+ MA	99	8,6 %	6	0,5 %

Branchen	Absolut Ungewichtet	Prozentual Ungewichtet	Absolut Gewichtet	Prozentual Gewichtet
Automobilbau	150	13,0 %	6	0,5 %
Banken & Versicherungen	151	13,1 %	15	1,3 %
Verkehr & Logistik	150	13,0 %	74	6,4 %
IT & Telekommunikation	151	13,1 %	43	3,7 %
Handel	151	13,1 %	207	17,9 %
Sonstige Industrie	202	17,5 %	316	27,4 %
Sonstige Dienstleistungen	200	17,3 %	494	42,7 %

Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Quelle: Bitkom Research 2023

Abbildung 1 – Zusammensetzung der Unternehmensstichprobe nach Größenklassen und Branchen (ungewichtet und gewichtet)

Analog zum »Open-Source-Monitor 2021« ist die Grundgesamtheit in diesem Jahr weiterhin Unternehmen in Deutschland mit mindestens 20 Beschäftigten. Im Gegensatz zu 2019, wo die Grundgesamtheit Unternehmen in Deutschland mit 100 Beschäftigten war, kann somit wieder der Einsatz von Open-Source-Software in kleineren Unternehmen mit 20 bis 99 Beschäftigten erfasst werden. Um Zeitreihen zu Veränderungen von 2019 bis 2023 aufzuweisen, wurde die Gesamtstichprobe in den Jahren 2021 und 2023 von ehemalig ca. 800 Unternehmen auf über 1.150 Unternehmen erweitert. Die Erweiterung der Gesamtstichprobe erlaubt eine direkte Vergleichbarkeit über die Jahre, für die Ergebnisse für Unternehmen mit mindestens 100 Beschäftigten (↗ Kapitel 2).

So wie im Jahr 2021 zuerst eingeführt, wurde neben der repräsentativen Unternehmensstichprobe außerdem eine Teilstichprobe von 100 Organisationen der Öffentlichen Verwaltung befragt, um einen Einblick in den Einsatz von Open-Source-Software in der Öffentlichen Verwaltung zu erhalten (↗ Kapitel 3). Darin enthalten sind Organisationen des Wirtschaftszweiges Öffentliche Verwaltung inkl. Allgemeine Öffentliche Verwaltung, Öffentliche Verwaltung auf den Gebieten Gesundheitswesen, Bildung, Kultur und Sozialwesen, Wirtschaftsförderung, Wirtschaftsordnung und Wirtschaftsaufsicht. Nicht enthalten sind Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, Öffentliche Sicherheit und Ordnung sowie Sozialversicherung.

Die finale Stichprobe verteilt sich mit 41 Prozent auf die Ebene der Kommunalverwaltung, 42 Prozent auf die Landesverwaltung und 17 Prozent auf die Bundesverwaltung (siehe Abbildung 2).

Größenklassen	Absolut Ungewichtet	Prozentual Ungewichtet
20 – 99 MA	26	25 %
100 – 199 MA	26	25 %
200 – 499 MA	27	26 %
500+ MA	23	23 %

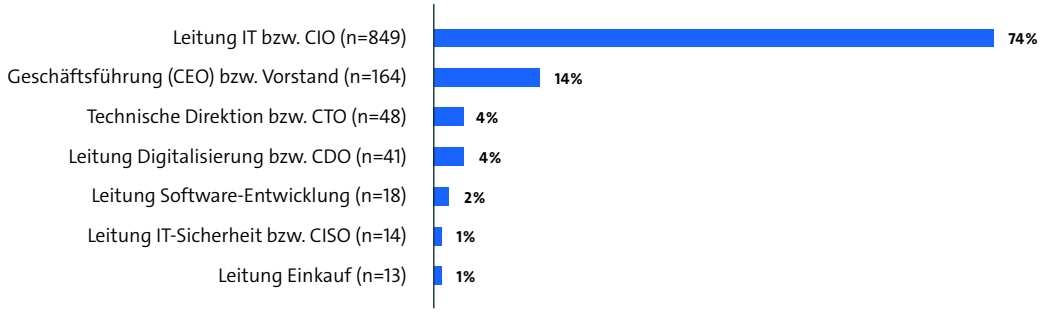
Verwaltungsebene	Absolut Ungewichtet	Prozentual Ungewichtet
Bundesverwaltung	17	17 %
Landesverwaltung	43	42 %
Kommunalverwaltung	42	41 %

Basis: Alle Befragten der Öffentlichen Verwaltung (n=102)
Quelle: Bitkom Research 2023

Abbildung 2 – Zusammensetzung der Verwaltungsstichprobe nach Größenklassen und Verwaltungsebene (ungewichtet)

Der standardisierte Fragebogen der Unternehmensbefragung wurde für die Öffentliche Verwaltung angepasst und analog dazu ebenfalls per computergestützten telefonischen Interviews (CATI) von Ende März 2023 bis Mitte Mai 2023 durchgeführt. Die Ergebnisse der Öffentlichen Verwaltung wurden nicht gewichtet und gehen nicht in das Gesamtergebnis der repräsentativen Unternehmensbefragung ein. Die Stichprobe liefert in der Größe und Verteilung kein repräsentatives Bild zum Einsatz von Open-Source-Software in der Öffentlichen Verwaltung, gibt aber ein aussagekräftiges Stimmungsbild für den Public Sector.

Die Interviews wurden mit Führungskräften durchgeführt, die in ihrem Unternehmen für das Thema Open-Source-Software verantwortlich sind. Rund die Hälfte der Unternehmen (49 Prozent) hat die Verantwortung formell oder informell an eine Person vergeben. In der Regel ist eine Person informell zuständig, wie zum Beispiel die Leitung Informationstechnik oder die Leitung Digitalisierung. Nur zwölf der befragten Unternehmen haben eine formelle Position für die Leitung des Themas Open-Source-Software geschaffen (1 Prozent).

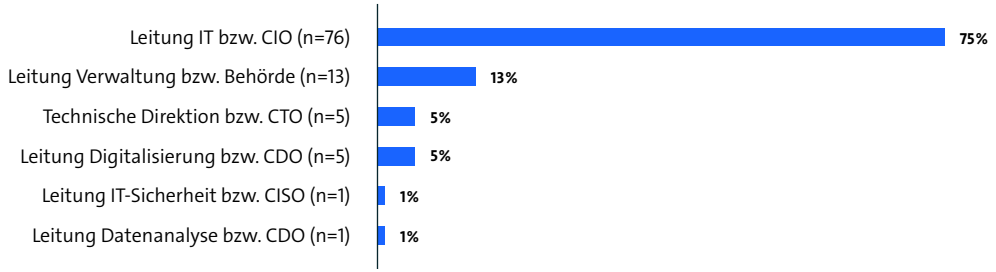


Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen
Quelle: Bitkom Research 2023

Abbildung 3 – Zusammensetzung der Unternehmensstichprobe nach Position der befragten Personen im Unternehmen (ungewichtet)

In denjenigen Unternehmen, in denen die Verantwortung für das Thema Open-Source-Software nicht formell einer Person zugeordnet ist (47 Prozent), wurden Führungskräfte befragt, die in ihrem Unternehmen für den Software-Einsatz bzw. die Software-Entwicklung verantwortlich sind. Die Zusammensetzung der Stichprobe entsprechend der Position der befragten Personen ist in Abbildung 3 dargestellt.

Bei drei Viertel (74 Prozent) der Unternehmen wurde die Führungskraft, die den Bereich Informationstechnik leitet, befragt. In der Öffentlichen Verwaltung wurden die Interviews ebenfalls in 75 Prozent der Fälle mit der Leitung Informationstechnik geführt (siehe Abbildung 4).



Basis: Alle Befragten der Öffentlichen Verwaltung (n=102) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen
Quelle: Bitkom Research 2023

Abbildung 4 – Zusammensetzung der Verwaltungsstichprobe nach Position der befragten Personen in der Organisation (ungewichtet)

Zu Beginn der beiden Befragungen wurde zunächst jeweils ein einheitliches Verständnis von Open-Source-Software für alle Befragten geschaffen. Diese Definition liegt auch diesem Studienbericht zugrunde und sei nachfolgend genannt:

> Unter Open-Source-Software verstehen wir Software, wie z. B. Programm-Module, Quellcode und Bibliotheken, Programmierwerkzeuge sowie komplette Betriebssysteme oder Software-Lösungen, deren Quellcodes offengelegt sind und deren Lizenz es den Lizenznehmenden erlaubt, die Software frei auszuführen, sie zu analysieren, anzupassen und sowohl in unveränderter als auch veränderter Form weiterzugeben. Voraussetzung hierfür ist neben dem offen zugänglichen Quell- bzw. Sourcecode auch Lizenzgebührenfreiheit.

Im vorliegenden Bericht wird – wie auch bereits im Rahmen der Befragung geschehen – in der Regel die Abkürzung OSS für Open-Source-Software verwendet.

1 Open-Source-Software im Unternehmens-Einsatz

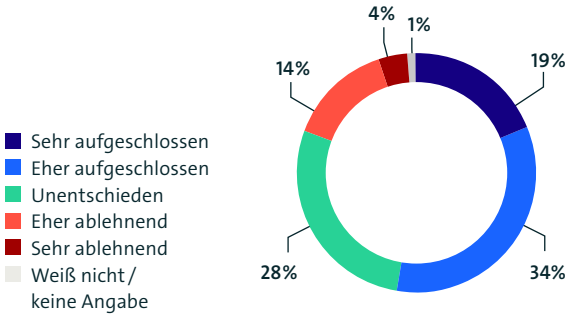
1.1 Einstellung zu Open-Source-Software

Bei der Frage, wie Unternehmen generell zum Thema OSS stehen, zeigt sich knapp die Hälfte (53 Prozent) aller Unternehmen ab einer Größe von 20 Beschäftigten aufgeschlossen (siehe Abbildung 5). Während 34 Prozent der Unternehmen eher aufgeschlossen sind, ist ein Fünftel (19 Prozent) sogar sehr aufgeschlossen. Nur 18 Prozent der Unternehmen stehen OSS ablehnend gegenüber. Ein gutes Viertel (28 Prozent) ist unentschieden gegenüber OSS.

Im Hinblick auf die verschiedenen Unternehmensgrößen lässt sich feststellen, dass die Haltung gegenüber OSS linear mit der Größe der Unternehmen im Zusammenhang steht (siehe Abbildung 6). Während kleinere und mittelständische Unternehmen (20 bis 199 Beschäftigte) zu 51 Prozent aufgeschlossen auf das Thema OSS blicken, sind es bei Unternehmen der Größenklasse 200 bis 499 Beschäftigte schon 6 von 10 Unternehmen (62 Prozent). Diese Tendenz setzt sich weiter fort und Großunternehmen zeigen somit das stärkste Interesse an OSS (500 bis 1 999 Beschäftigte: 69 Prozent, ab 2 000 Beschäftigen: 67 Prozent).

Bei der offenen Frage (d. h. einer Frage, bei der keine Antworten vorgegeben wurden) nach dem größten Vorteil, der für den Einsatz von OSS spricht, sind lediglich ein Zehntel der Unternehmen (10 Prozent) der Meinung, dass es keine Vorteile von OSS gibt (siehe Abbildung 7). Unter den Unternehmen, die OSS verwenden, integrieren, (weiter-) entwickeln oder sich auf andere Weise an OSS beteiligen, sehen de facto alle Vorteile an OSS (keine Vorteile: 0 Prozent).

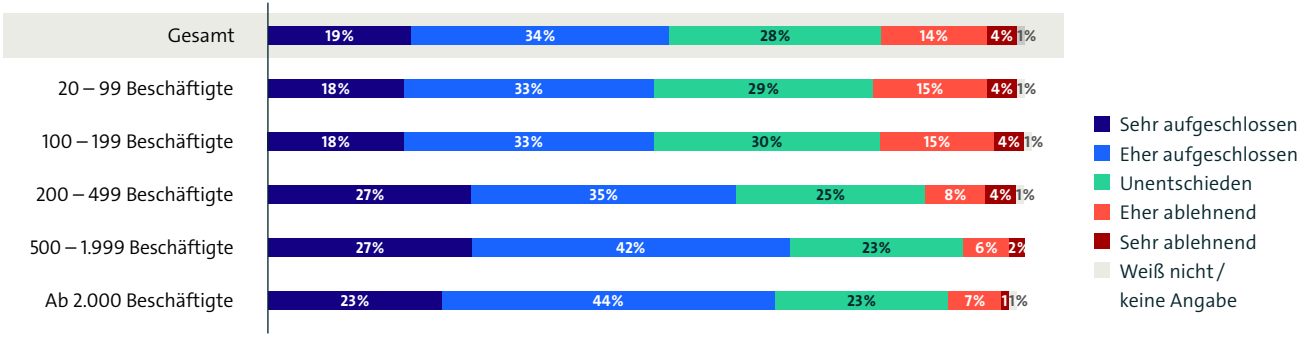
Wie steht Ihr Unternehmen generell zum Thema OSS?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen
Quelle: Bitkom Research 2023

Abbildung 5 – Einstellung zu Open-Source-Software

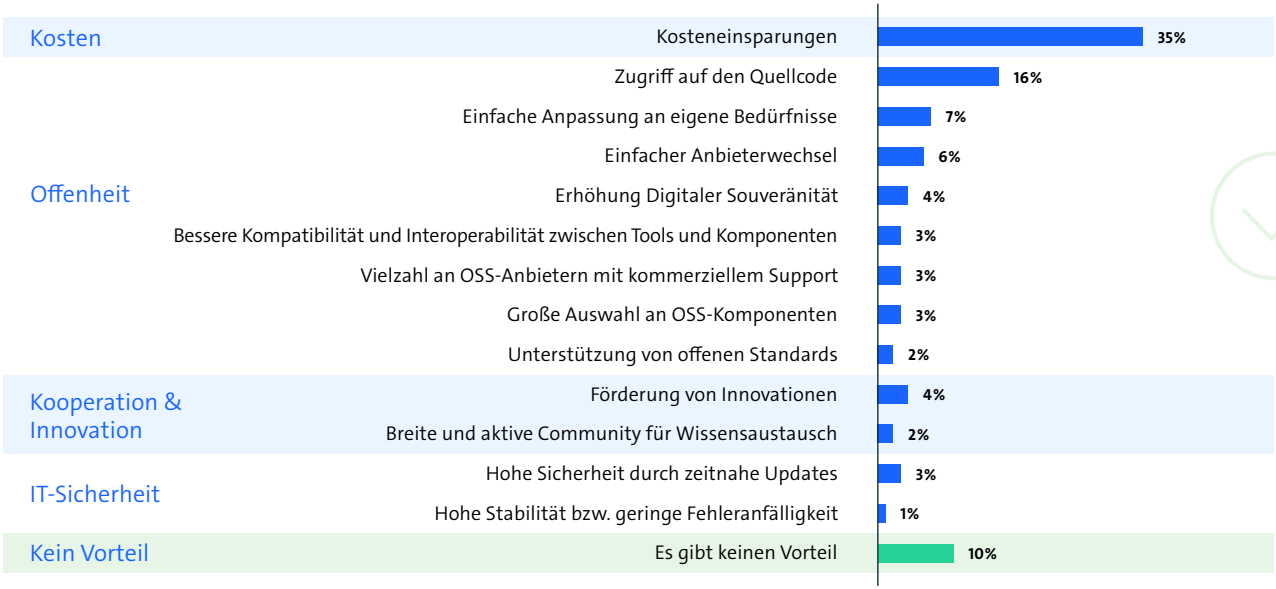
Wie steht Ihr Unternehmen generell zum Thema OSS?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen
Quelle: Bitkom Research 2023

Abbildung 6 – Einstellung zu Open-Source-Software nach Unternehmensgrößenklassen

Was ist aus Ihrer Sicht der größte Vorteil, der für den Einsatz von OSS in Ihrem Unternehmen spricht?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Offene Abfrage, nur eine Antwort möglich | fehlende Werte: »Weiß nicht / k. A.«
Quelle: Bitkom Research 2023

Abbildung 7 – Vorteile von Open-Source-Software

Betrachtet man alle befragten Unternehmen, werden von einem Drittel (35 Prozent) Kosteneinsparungen als größter Vorteil von OSS genannt. Die Lizenzgebührenfreiheit von OSS ist somit der mit Abstand am häufigsten genannte Vorteil. Die Vielzahl der weiteren genannten Vorteile zeigt, dank der offenen Fragemethodik, dass eine große Bandweite an Gründen für den Einsatz von OSS angeführt wird.

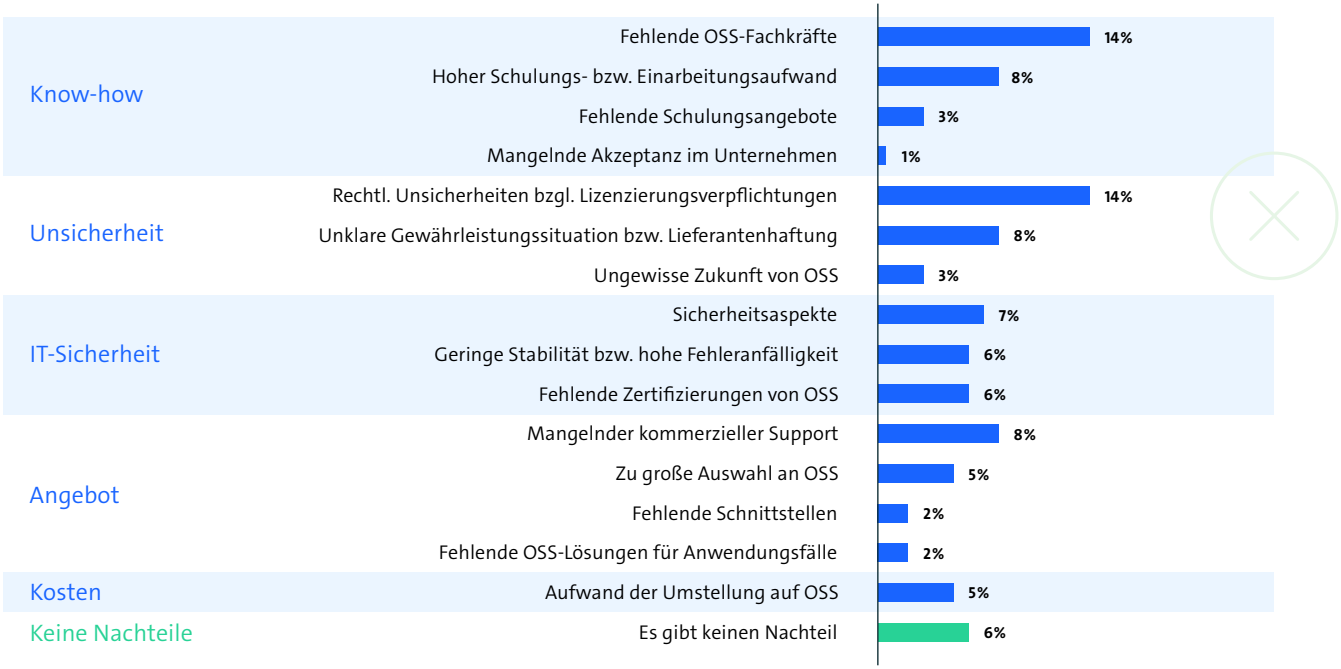
Betrachtet man die Kategorisierung der Vorteile, so lassen sich die meisten Nennungen der Offenheit von OSS zuordnen (44 Prozent). Dabei nennen 16 Prozent der Unternehmen den Zugriff auf den Quellcode als größten Vorteil. Mit 7 Prozent wird die einfache Anpassung von OSS an die eigenen Bedürfnisse der Unternehmen als nächstes genannt. Es folgen die Erhöhung der digitalen Souveränität (4 Prozent), die Kompatibilität und Interoperabilität zwischen Tools und Komponenten (3 Prozent), die Vielzahl an OSS-Anbietern mit kommerziellem Support (3 Prozent), die breite Auswahl an OSS-Komponenten (3 Prozent) sowie die Unterstützung von offenen Standards (2 Prozent).

Förderung von Kooperation und Innovation sehen insgesamt 6 Prozent der Unternehmen als größten Vorteil. Hierbei benennen 4 Prozent der Unternehmen die Förderung von Innovation als konkreten Vorteil. Weitere 2 Prozent bewerten die Breite und eine aktive OSS-Community als vorteilhaft, wenn es um den Wissensaustausch geht.

Lediglich 4 Prozent geben IT-Sicherheitsaspekte als größten Vorteil von OSS an. Konkret sehen 3 Prozent der Unternehmen die hohe Sicherheit durch zeitnahe Updates als Hauptvorteil. Nur 1 Prozent hebt die geringe Fehleranfälligkeit von OSS hervor.

Neben den Vorteilen waren für diese Studie auch die Nachteile, die Unternehmen bezüglich OSS sehen, von Interesse. Somit wurde zusätzlich eine offene Frage gestellt, die sich mit dem größten Nachteil befasst, der gegen den Einsatz OSS spricht. Anders als bei den Vorteilen steht nicht ein alleiniger Grund an der Spitze. Mit 14 Prozent sind sowohl die fehlenden Fachkräfte als auch die rechtlichen Unsicherheiten bezüglich der Lizenzverpflichtungen die am häufigsten genannten Nachteile aus Unternehmensperspektive (siehe Abbildung 8).

Was ist aus Ihrer Sicht der größte Nachteil, der gegen den Einsatz von OSS in Ihrem Unternehmen spricht?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Offene Abfrage, nur eine Antwort möglich | fehlende Werte: »Weiß nicht / k. A.«
Quelle: Bitkom Research 2023

Abbildung 8 – Nachteile von Open-Source-Software

Danach zeigt sich erneut ein differenziertes Bild mit weiteren Gründen, die sich oft nur um wenige Prozentpunkte voneinander unterscheiden. Wie auf Abbildung 8 zu sehen, lassen sich auch hier die Gründe in übergeordnete Kategorien zusammenfassen. Insgesamt ein Viertel der Unternehmen (26 Prozent) nennen Nachteile rund um das Know-how. Dabei werden neben den schon genannten fehlenden OSS-Fachkräften auch der hohe Schulungs- bzw. Einarbeitungsaufwand (8 Prozent), die fehlenden Schulungsangebote (3 Prozent) und die mangelnde Akzeptanz im Unternehmen (1 Prozent) genannt.

Für ein weiteres Viertel (25 Prozent) ist der Einsatz von OSS generell mit Unsicherheiten verbunden. Neben den lizenzrechtlichen Unsicherheiten spielt für 8 Prozent eine unklare Gewährleistung bzw. Haftung der Lieferanten bei OSS eine Rolle. Weitere 3 Prozent der Unternehmen machen sich Sorgen um die ungewisse Zukunft von OSS.

Aspekte rund um die IT-Sicherheit werden insgesamt von knapp jedem fünften (19 Prozent) Unternehmen als Nachteil genannt. Mit Blick auf die Vorteile, bei denen nur 4 Prozent der Unternehmen das Thema IT-Sicherheit nannten, zeigt sich deutlich, dass die Sorgen diesbezüglich überwiegen. Interessant ist an dieser Stelle außerdem, dass die Ergebnisse der Studie aus dem Jahr 2021 hier noch stärker ein ambivalentes Bild zeigten. Vor zwei Jahren nannten nur 9 Prozent der Unternehmen IT-Sicherheitsaspekte als Nachteil, während 9 Prozent diese Aspekte ebenso als größten Vorteile nannten. Die Unsicherheiten bezüglich des Themas IT-Sicherheit sind also in 2023 gestiegen. In diesem Jahr nennen 7 Prozent der Unternehmen sicherheitsrelevante Aspekte, im generellen Sinne, als größten Nachteil. Darauffolgend sehen jeweils 6 Prozent der Unternehmen die hohe Fehleranfälligkeit und die fehlende Zertifizierung von OSS als kritische Faktoren.

Weitere 17 Prozent der Unternehmen nannten Nachteile rund um das Angebot von OSS. Dabei steht mit 8 Prozent ein mangelnder kommerzieller Support bei OSS an erster Stelle, gefolgt von einer zu großen Auswahl (5 Prozent),

fehlenden Schnittstellen (2 Prozent) und fehlenden OSS-Lösungen für unternehmensspezifische Anwendungsfälle (2 Prozent).

Zuletzt nennen weitere 5 Prozent der Unternehmen den Aufwand der Umstellung auf OSS und die damit verbundenen Kosten als größten Nachteil, der gegen den Einsatz von OSS spricht.

Generell geben neun von zehn (92 Prozent) Unternehmen Nachteile rund um den Einsatz von OSS an. Blickt man erneut auf die Unternehmen, die OSS verwenden, integrieren, weiterentwickeln oder sich auf andere Weise an OSS beteiligen, ändert sich diese Ansicht kaum. 89 Prozent dieser Unternehmen nennen einen Nachteil hinsichtlich des Einsatzes von OSS. 6 Prozent aller befragten Unternehmen sehen allerdings keine Nachteile, die gegen den Einsatz von OSS sprechen.

Open Source – der Schlüssel zu Resilienz, Souveränität und Fortschritt

Marcel Scholze
Director, Head of OSS Management Services
PwC

Regulatoren erkennen die Bedeutung von Open Source

Der Draft des EU Cyber Resilience Acts (CRA), die Executive Order zur Cybersecurity in den USA, der Digital Operational Resilience Act (DORA) oder die ENISA Guidelines für die IoT Supply Chain sind nur wenige Beispiele für Gesetze und Verordnungen, die direkt oder indirekt Open-Source-Software (OSS) und die Bedeutung von Software Bill of Materials (SBOM) adressieren. Regulatoren haben die zentrale Bedeutung von Open Source in der digitalen Transformation erkannt und fördern den sicheren, rechtskonformen Einsatz von OSS. Dies birgt große Chancen als auch Herausforderungen für die Open Source Community und für Organisationen. Aufgrund dessen ist es unerlässlich, ein adäquates OSS-Management zu etablieren.

Regulatorik als Chance ergreifen

Für Unternehmen ist es von zentraler Bedeutung, die zuvorgenannten Anforderungen des Marktes und der Regulatoren nicht nur im Mindestmaß umzusetzen, sondern aktiv als Chance zu begreifen, um die bekannten Vorteile von Open Source strategisch zu nutzen und fest in der Unternehmenskultur zu verankern. Im Zuge dessen geht es nicht nur um die Chance zum Beispiel auf beschleunigte Innovation, Kostenreduktion oder Transparenz, sondern auch um die Förderung der eigenen Resilienz und Souveränität. Der strategische Einsatz von Open Source ermöglicht es Organisationen, flexibel auf ein dynamisches Marktumfeld zu reagieren, ihre technologische Unabhängigkeit zu stärken und langfristige Wettbewerbsvorteile zu erlangen.

Stärkung Ihrer Organisation durch ein optimiertes OSS-Managementsystem

Die neue OpenChain ISO 18974 bietet als internationaler Standard wichtige Orientierung, wie Security Management Prozesse für Open Source gestaltet werden sollten. Wie auch bei Open Source Compliance Prozessen (ISO 5230), handelt es sich um komplexe Workflows, die in der Regel mehrere Unternehmensbereiche und Tools involvieren. Eine zentrale Inventarisierung der genutzten OSS bildet hierbei einen wichtigen Dreh- und Angelpunkt. Auch wenn die beiden ISO Normen jeweils eigenständig und unabhängig sind, kann die harmonisierte Etablierung dazu beitragen, Synergieeffekte zu realisieren. Die Umsetzung von OSS Security und Compliance Strukturen erfordert dabei die Konzeption von Individuallösungen entlang etablierter Standards und deren zyklische Optimierung. Dabei sind IT-, Prozess-, Open Source- und juristisches Know-how essenziell.

Ein externer Blick auf die Organisation kann hierbei wertvoll sein, indem z. B. Regelungslücken identifiziert, Latenzzeiten optimiert oder die genutzte Toolchain neutral evaluiert wird. Wie auch schon 2021 sehen die Teilnehmenden des Bitkom Monitors eine Herausforderung bei Open-Source-Software im Mangel an qualifizierten Open Source Fachkräften. Umso wichtiger ist es daher, den vorhandenen Ressourcen ein effizientes Prozess- und Tool-Umfeld bereitzustellen.

Unabhängigkeit und interdisziplinäre Expertise für Ihr Open-Source-Management

Die strategische Umsetzung der ISO 5230 und 18974, einschließlich der Integration einer verlässlichen SBOM, erfordert individuelle Maßnahmen und umfassende technische sowie juristische Expertise.

PwC berät und implementiert oder prüft und zertifiziert Open-Source-Managementsysteme und bietet professionelle Managed Services zu Code Scanning, SBOM-Erstellung und Kuration sowie Lieferantenauditierungen an.

Open Source Compliance as a Service

Die Herausforderung

Open Source Software Compliance wird immer wichtiger – allerdings auch immer anspruchsvoller: Softwareentwicklungszyklen verkürzen sich, zudem wird immer häufiger im Wege einer automatisierten Continuous Delivery entwickelt. Gleichzeitig wird Software immer größer und komplexer. Schon relativ einfache Projekte enthalten nicht selten hunderte, wenn nicht tausende Drittkomponenten. Aus rechtlicher Sicht ist dann sicherzustellen, dass sämtliche Pflichten der Lizenzen erfüllt werden.

Viele Unternehmen beschränken sich darauf, den Lizenztext der jeweiligen Drittkomponente herauszusuchen. Oft werden dann allenfalls noch Urhebervermerke zusammengestellt und dann beides mit der Software ausgeliefert. Aus rein faktischer Sicht ist allein diese Aufgabe alles andere als trivial – aus rechtlicher Sicht ist es allerdings erst der Anfang. Denn neben der Pflicht zur Weitergabe von Lizenztexten und Urhebervermerken enthalten viele Lizenzen noch weitere Pflichten, Einschränkungen und Anforderungen, welche zu beachten sind. Das wiederum setzt allerdings eine vertiefte Prüfung der Lizenztexte voraus, was schließlich mit erheblichem Aufwand verbunden ist.

Hinzu kommt, dass viele Pflichten von der konkreten Art der Verwendung der entsprechend lizenzierten Software abhängen. Es reicht also nicht, Lizenzen einmal rechtlich zu prüfen und zu bewerten, sondern es ist immer auch der konkrete Use Case zu berücksichtigen, in welchem die Softwarekomponenten eingesetzt werden.

Unsere Lösung

Auf der Grundlage von mehr als zehnjähriger Erfahrung mit rechtlichen Fragen von Open Source Compliance haben wir mit der FOSSmatrix eine Lösung entwickelt, welche als Webservice zur Verfügung gestellt werden kann. Sie ermöglicht es, knapp 200 Lizenzen – nach insgesamt 75 Merkmalen untergliedert – automatisiert mit Blick auf die definierten Use Cases auszuwerten. Detaillierte Beschreibungen möglicher Lizenzkonflikte mit Verweis auf die zugrundeliegenden Lizenzen und weitere Quellen erlauben dann einen schnellen Überblick über Konflikte sowie das Ergreifen der nächsten Schritte zu deren Lösung.

Rechtlich komplexe Fragen wurden dabei in Teilaspekte heruntergebrochen, diese dann mit unterschiedlichen Score-Werten und Bewertungslogiken versehen. Wo erforderlich, wurden alle Schritte und Ergebnisse ausführlich schriftlich dokumentiert. So können auch rechtlich umstrittene Fragen, Zweifelsfälle und Graustufen erfasst, bewertet und visualisiert werden.

Die Lösung ist sehr flexibel: Sie kann stand-alone über ein Webinterface bedient werden oder mit einer API in eine vorhandene Tool-Infrastruktur eingebunden werden.

Ihr Vorteil

Durch die von uns entwickelte Lösung ist es möglich, schnell und übersichtlich eine große Zahl von Lizenzen automatisiert rechtlich zu prüfen und auf die Vereinbarkeit mit den eigenen Einsatzzwecken hin abzugleichen.

Osborne Clarke hat langjährige Erfahrung in der umfassenden rechtlichen und technischen Beratung zu Open Source und bietet Lösungen im Bereich Open Source Software (OSS) Compliance und Contributions.

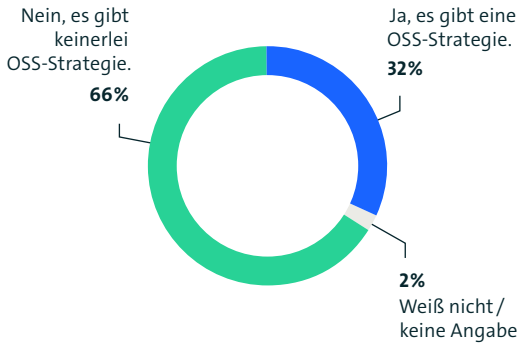
Dr. Hendrik Schöttle
Rechtsanwalt, Partner, Fachanwalt für IT-Recht

↗ osborneclarke.com/oss

1.2 Open-Source-Software-Strategie

Ein weiterer bedeutender Aspekt der befragten Unternehmen ab 20 Beschäftigen, ist die strategische Auseinandersetzung von Unternehmen mit dem Thema Open Source. In der Studie wurden Unternehmen demnach gefragt, ob sie in ihren Unternehmen eine Strategie zur Verwendung bzw. zur Beteiligung an OSS haben. Dabei wurde eine Strategie als ein Dokument mit niedergeschriebenen Zielen und Plänen definiert.

Gibt es in Ihrem Unternehmen eine Strategie zur Verwendung bzw. zur Beteiligung an OSS?



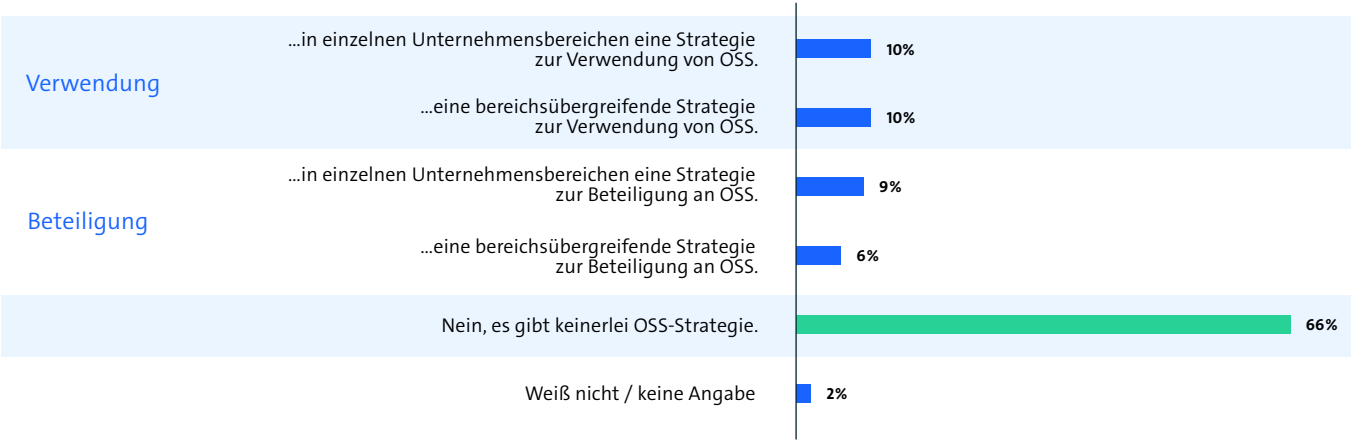
Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155)
Quelle: Bitkom Research 2023

Abbildung 9 – Open-Source-Software-Strategie

Abbildung 9 zeigt, dass bereits ein Drittel (32 Prozent) der Unternehmen eine OSS-Strategie hat. Die strategische Relevanz von Open Source für deutschen Unternehmen zeigte sich außerdem in dem ↗ Kapitel zur Methodik. Demnach haben rund die Hälfte der Unternehmen (48 Prozent) die Verantwortung für das Thema OSS informell an eine Person vergeben. Lediglich 1 Prozent der Unternehmen hat eine formelle Position für die Leitung des Themas OSS.

Einen tieferen Einblick bezüglich der vorhandenen Strategien bzw. Teil-Strategien bietet Abbildung 10. Hier ist zu erkennen, dass die inhaltliche Ausrichtung der Strategie sich für ein Fünftel (20 Prozent) der Unternehmen auf die Verwendung von OSS bezieht. Dabei ist der Umfang für Strategien rund um die Verwendung gleichmäßig auf einzelne Unternehmensbereiche und bereichsübergreifende Strategien verteilt (jeweils 10 Prozent). Weitere 15 Prozent der Unternehmen haben eine Strategie zur Beteiligung an OSS. Hier liegen Strategien in einzelnen Unternehmensbereichen mit 9 Prozent leicht vor bereichsübergreifenden Strategien (6 Prozent).

Gibt es in Ihrem Unternehmen eine Strategie zur Verwendung bzw. zur Beteiligung an OSS?



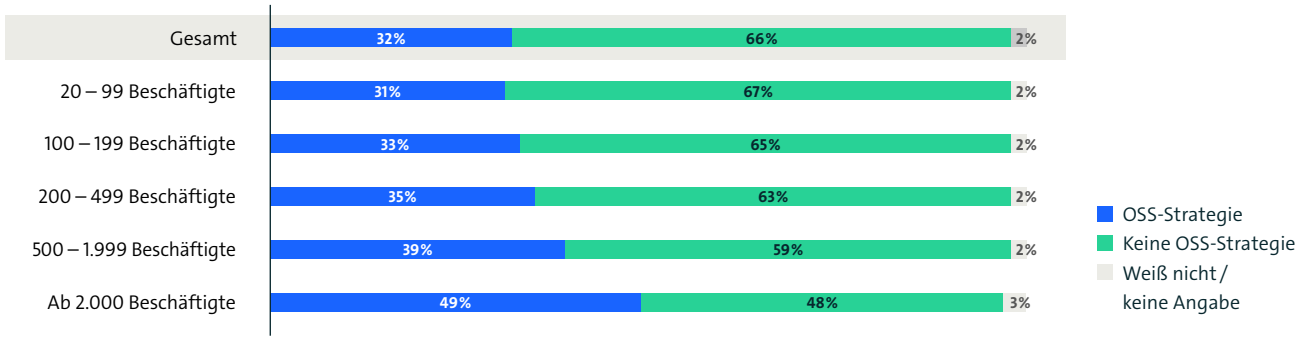
Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Mehrfachnennungen möglich
Quelle: Bitkom Research 2023

Abbildung 10 – Open-Source-Software-Strategie nach Art

Mit Blick auf die Unternehmensgrößenklassen zeichnet sich, wie auch schon bei der Einstellung gegenüber OSS (↗ Kapitel 1.1, Abbildung 6), erneut ein zur Größe der Unternehmen linearer Zusammenhang ab (siehe Abbildung 11). Bei Kleinunternehmen mit 20 bis 99 Beschäftigten haben 31 Prozent eine OSS-Strategie. Im Mittelstand sind es ebenfalls rund ein Drittel der Unternehmen (100 bis 199 Beschäftigte: 33 Prozent; 200 bis 499 Beschäftigte: 35 Prozent).

Bei Großunternehmen mit 500 bis 1.999 Beschäftigten haben vier von zehn (39 Prozent) Unternehmen eine Strategie für das Thema OSS. In Großunternehmen mit 2.000 und mehr Beschäftigten sind es sogar rund die Hälfte (49 Prozent) der Unternehmen.

Gibt es in Ihrem Unternehmen eine Strategie zur Verwendung bzw. zur Beteiligung an OSS?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Quelle: Bitkom Research 2023

Abbildung 11 – Open-Source-Software-Strategie nach Unternehmensgrößenklasse

Stay Open. OX

Unsichtbare Helfer: Wie Open-Source-Software die digitale Souveränität stärkt

Studien zeigen es längst: Die Verbreitung und der Nutzen von Open-Source-Lösungen schreitet voran. Doch dieses Wachstum wird in der öffentlichen Wahrnehmung allzu oft übersehen.

Studie
Eine Umfrage von Open Email ergab 2020, dass 76,93 Prozent aller in Deutschland erreichbaren E-Mail-Systeme auf Open-Source-Technologien wie Open-Xchange setzen.

Ohne es zu wissen, greifen demnach hierzulande Millionen von Nutzern täglich auf Open-Source-Lösungen zu. Und zwar immer dann, wenn sie sich bei ihren privat genutzten E-Mail-Anbietern einloggen.

Die Vorteile in der öffentlichen Verwaltung nutzen

Für die öffentliche Verwaltung spielen Open-Source-Lösungen eine entscheidende Rolle, wenn es darum geht, echte digitale Souveränität zu erreichen.

Deshalb wächst die **politische Unterstützung** für Open-Source-Lösungen kontinuierlich. Verschiedene Bundesländer haben bereits Beschlüsse zur Förderung der digitalen Souveränität gefasst und auch das bundesweit agierende Zentrum für Digitale Souveränität (ZenDis) hat seine Arbeit aufgenommen.

Ein besonderes Augenmerk wird auf einen **stabilen und sicheren Betrieb** der E-Mail- und Collaboration-Plattformen gelegt. Viele Behörden bevorzugen dafür spezialisierte Service-Provider und setzen auf bewährte Open-Source-Lösungen. Diese Anbieter sind in der Lage, effektiven Schutz vor Spam, Malware und Botnetzen zu bieten.

Open-Source-Lösungen sind außerdem deutlich benutzerfreundlicher geworden und es haben sich Standards etabliert. Bemerkenswert ist, dass sich **bereits sieben von 16 Bundesländern dazu entschieden** haben, im Bildungs- bzw. Verwaltungsbereich landesweit eingesetzte E-Mail- und Kollaboration-Plattformen auf Lösungen wie Open-Xchange und Univention aufzusetzen.

Vier Prinzipien für Digitale Souveränität

Die Vorteile können am gewinnbringendsten genutzt werden, wenn es sich um echte Open-Source-Software handelt. Durch vier einfache Prinzipien lässt sich bei jeder Software und jeder Cloud-Lösung erkennen, ob es sich tatsächlich um Open Source handelt.

1. **Die Verfügbarkeit bei mehreren Anbietern** sichert Herstellerunabhängigkeit.
2. **Der flexible Betrieb der Software** gewährleistet Unabhängigkeit.
3. **Flexible Datenmigration** ermöglicht eine flexible und freie Nutzung.
4. **Kontrolle durch Offenheit:** transparente Software ermöglicht gemeinsame Weiterentwicklung und Kontrolle.

Wenn Behörden ihre digitale Souveränität zurückerlangen wollen, führt kein Weg an echter Open-Source-Software vorbei. Das liefert die Voraussetzungen dafür, dass die öffentliche Hand ihre rechtlichen Anforderungen **herstellerunabhängig** technisch umsetzen kann.

Open-Source-basierter Web-Arbeitsplatz für den öffentlichen Sektor

Digital souverän arbeiten mit der dPhoenixSuite

Die digitale Transformation im öffentlichen Sektor erfordert vermehrt digitale Zusammenarbeit und flexible Videokonferenzen. Dies macht die Verwaltung abhängiger von Herstellern digitaler Lösungen. Ohne Zugriff auf IT und Daten ist der Staat nicht mehr handlungsfähig, da die Verarbeitung von Bürger- und Unternehmensdaten ohne digitale Lösungen unmöglich ist. Digitale Souveränität der Verwaltung, also unabhängige IT- und Datenkontrolle, ist entscheidend für den digitalen Staat.

Wie kann die Verwaltung moderne digitale Lösungen nutzen, ohne in technische Abhängigkeiten zu geraten? Dataport bietet die Antwort: die dPhoenixSuite, einen open-source-basierten Web-Arbeitsplatz für den öffentlichen Sektor. Diese Suite vereint E-Mail, Kalender, Kontakte, Textverarbeitung, Chat, Videokonferenzen und Zusammenarbeit in virtuellen Räumen. Sie ist modular aufgebaut und beinhaltet leistungsstarke Open-Source-Anwendungen verschiedener deutscher und europäischer Hersteller.

Dataport hat die dPhoenixSuite in Zusammenarbeit mit Partnern aus Wirtschaft und Verwaltung im Projekt Phoenix entwickelt. Durch dieses Netzwerk wird der Web-Arbeitsplatz mit Service Level Agreements und Support ausgestattet und kontinuierlich verbessert. Die einzelnen Open-Source-Module der dPhoenixSuite werden in gesicherten deutschen Clouds und auf deutschen Servern betrieben, wodurch der Staat die volle Kontrolle über alle Daten hat, die den Datenschutzrichtlinien der EU unterliegen.

Die dPhoenixSuite ist eine echte, digitale Alternative zu traditionellen Office-Paketen. Sie ist ohne Installation über einen Webbrowser oder mobil zugänglich und bietet eine benutzerfreundliche Oberfläche mit »Single-Sign-On«-Modus an. Nutzerinnen und Nutzer von klassischen Office-Anwendungen werden sich schnell zurechtfinden.

Die Module der dPhoenixSuite im Einzelnen:

dPhoenixMail

- Per E-Mail kommunizieren
- Termine organisieren
- Kontakte verwalten
- Aufgaben planen

dPhoenixOffice & FileShare

- Texte, Tabellen und Präsentationen erstellen und mit mehreren Personen gleichzeitig bearbeiten (kompatibel zu Microsoft-Office-Produkten und dem Open-Document-Format)
- Dateien teilen und in Ordnern organisieren

dOnlineZusammenarbeit 2.0

- Audio- und Videokonferenzen durchführen
- Chatten
- Parallel in Kleingruppen arbeiten (Breakoutsessions)
- Am Whiteboard zusammenarbeiten
- Notizen anfertigen
- Abstimmungen durchführen

Derzeit liegt die dPhoenixSuite in der Version 3.0 vor. Das Upgrade auf Version 4.0, die unter anderem eine Anbindung an die E-Akte ermöglicht, ist für das Frühjahr 2024 geplant.

© @freepik

Rund 200.000 Personen in verschiedenen Verwaltungen im Bundesgebiet arbeiten mit der dPhoenixSuite, mit verschiedenen Modulen der Suite oder werden dies zeitnah tun. Dazu gehören unter anderem die Landesverwaltung und das Bildungsministerium Schleswig-Holstein, das Ministerium für Infrastruktur und Digitales Sachsen-Anhalt, das Ministerium der Justiz des Landes Nordrhein-Westfalen und das Robert Koch-Institut.

↗ dPhoenixSuite.de

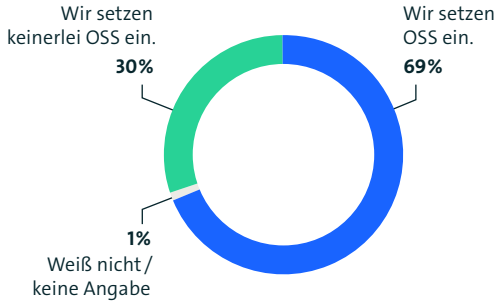
1.3 Einsatz von Open-Source-Software

Die vorhergehenden zwei Kapitel zeigen, dass knapp jedes zweite (53 Prozent) Unternehmen generell aufgeschlossen gegenüber dem Thema OSS ist (↗ Kapitel 1.1, Abbildung 5), während ein Drittel (32 Prozent) der Unternehmen eine niedergeschriebene Strategie für die Verwendung oder Beteiligung an OSS hat (↗ Kapitel 1.2, Abbildung 9). Die überwiegend positive Grundeinstellung in der deutschen Wirtschaft spiegelt sich aktuell also noch nicht eins zu eins in der strategischen Einbettung von OSS wider. In diesem Kontext eröffnen sich zwei weitere Fragen, die für diese Studie eine zentrale Rolle spielen:

- Wie steht es aktuell um den Einsatz von OSS in den Unternehmen?
- Welche Faktoren beeinflussen maßgeblich die Auswahl von eingesetzter OSS in Unternehmen?

Unter den deutschen Unternehmen ab 20 Beschäftigten zeigt sich, verglichen zur Grundeinstellung sowie zu den OSS-Strategien, dass der Einsatz von OSS weitaus mehr verbreitet ist. Rund sieben von zehn Unternehmen (69 Prozent) setzen OSS in ihrem Unternehmen ein (siehe Abbildung 12). 30 Prozent der Unternehmen geben an, keinerlei OSS einzusetzen.

Setzt Ihr Unternehmen OSS ein?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155)
Quelle: Bitkom Research 2023

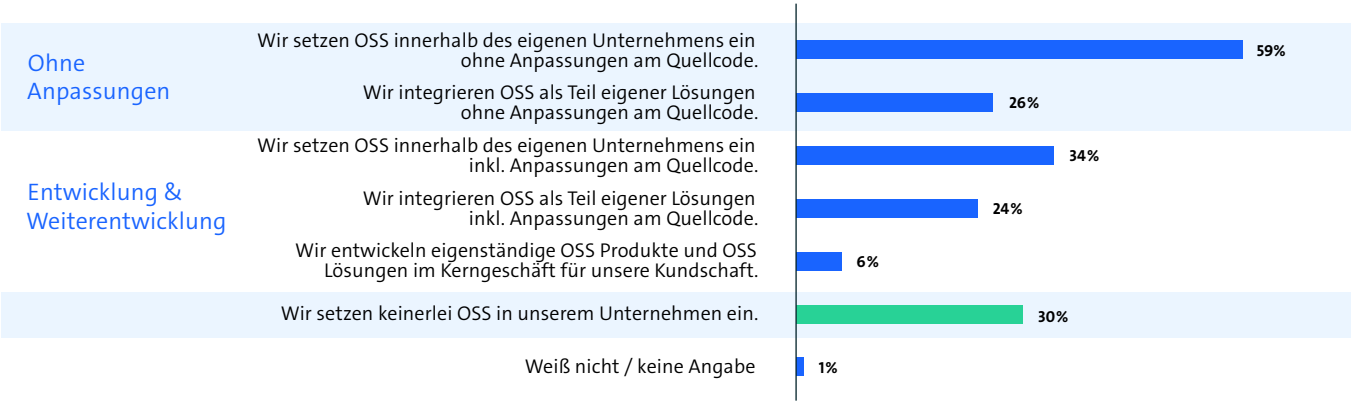
Abbildung 12 – Einsatz von Open-Source-Software

Betrachtet man die Art des Einsatzes, ist zu sehen, dass die Mehrheit (59 Prozent) der Unternehmen OSS für einen Anwenderkreis innerhalb des eigenen Unternehmens einsetzt, ohne dabei Anpassungen am Quellcode vorzunehmen (siehe Abbildung 13). Diese Erkenntnis brachte auch die Befragung aus dem Jahr 2021, wobei die spezifische Einsatzart in den letzten zwei Jahren um 7 Prozentpunkte gestiegen ist (2021: 51 Prozent Verwendung im Unternehmen, ohne Anpassung). Des Weiteren integriert ein Viertel (26 Prozent) der Unternehmen OSS als Bestandteil eigener Produkte und Lösungen für ihre Kundschaft, ohne dabei Anpassungen am Quellcode vorzunehmen.

Ein Drittel (34 Prozent) der Unternehmen gibt an, OSS innerhalb des Unternehmens einzusetzen und dafür Anpassungen am Quellcode vorzunehmen. Ein Viertel (24 Prozent) nimmt Anpassungen am Quellcode vor und integriert OSS dabei als Lösungsbestandteil für die Kundschaft. Nur 6 Prozent der Unternehmen entwickelt eigenständige OSS-Produkte und Lösungen im Kerngeschäft der Unternehmenstätigkeiten.

Der Blick auf die Unternehmensgrößenklassen zeigt erneut eine Zunahme beim Einsatz von OSS entlang der Beschäftigtenzahl (siehe Abbildung 14). Während rund sieben von zehn Kleinunternehmen (20 bis 99 Beschäftigte: 68 Prozent) OSS einsetzen, sind es bei den Großunternehmen (ab 2.000 Beschäftigen) schon 85 Prozent. In der Unternehmensgrößenklassen von 100 bis 199 Beschäftigten liegt der Einsatz von OSS bei 73 Prozent. Bei Unternehmen mit 200 bis 1.999 Beschäftigten sind es 8 von 10 (78 Prozent) Unternehmen, die OSS einsetzen.

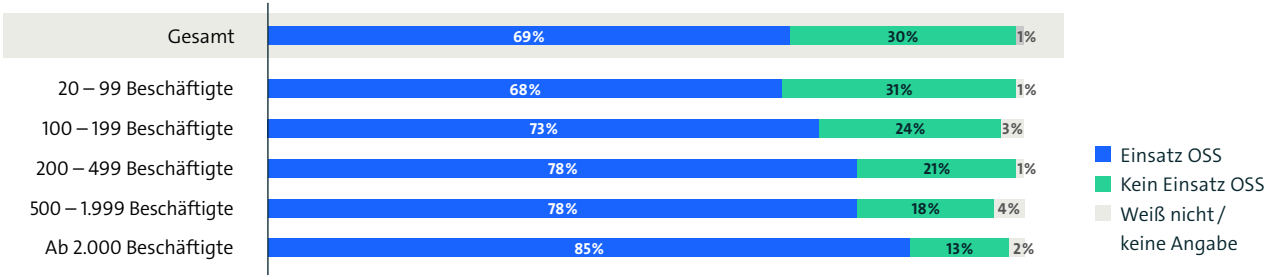
Welche der folgenden Aussagen treffen auf den Einsatz von OSS in Ihrem Unternehmen zu?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2023

Abbildung 13 – Einsatz von Open-Source-Software nach Art

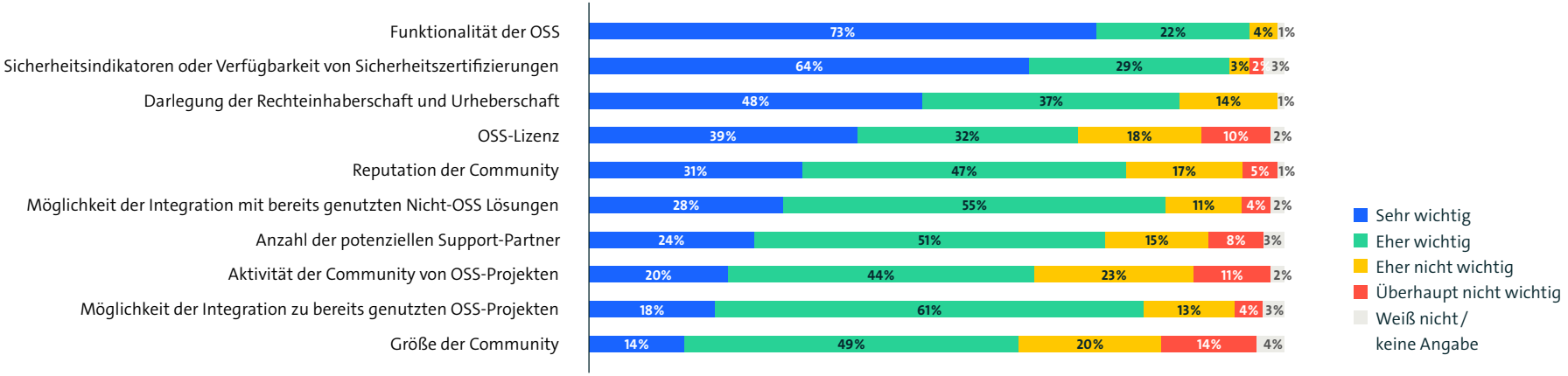
Setzt Ihr Unternehmen OSS ein?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Quelle: Bitkom Research 2023

Abbildung 14 – Einsatz von Open-Source-Software nach Unternehmensgrößenklassen

Wie wichtig sind die folgenden Kriterien bei der Auswahl von OSS-Projekten in Ihrem Unternehmen?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln (n=801) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen
Quelle: Bitkom Research 2023

Abbildung 15 – Auswahlkriterien Open-Source-Software-Projekte

Nachdem der Einsatz von OSS beleuchtet wurde, stellt sich die Frage nach den Faktoren, die Unternehmen, welche OSS nutzen (also verwenden, integrieren oder (weiter-) entwickeln) bei der Auswahl von OSS in Betracht ziehen. Abbildung 15 zeigt, dass die Funktionalität der OSS als wichtigstes Kriterium gilt und von 73 Prozent der befragten Unternehmen als »sehr wichtig« eingestuft wird.

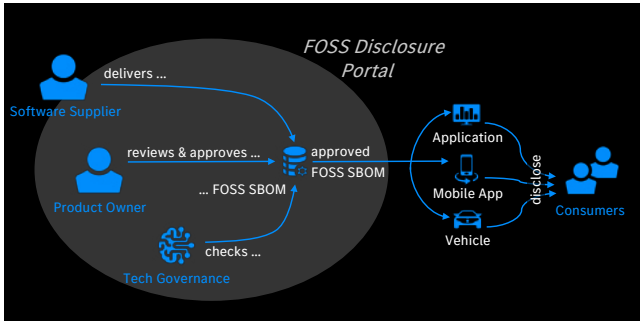
Darüber hinaus bewerten weitere 22 Prozent der Unternehmen die Funktionalität mit »eher wichtig«. Neben dieser grundlegenden Voraussetzung wird deutlich, dass durchaus mehr als die Funktionalität der OSS von Bedeutung für die Unternehmen ist. Neun von zehn (93 Prozent) Unternehmen sehen Sicherheitsindikatoren, wie z. B. die CVE-Meldungsanzahl, oder die Verfügbarkeit von Sicherheitszertifizierungen, wie z. B. NIST-Zertifizierungen oder Common Criteria, als ein wichtiges Kriterium an. Dabei ist dieser Aspekt für zwei Drittel (64 Prozent) »sehr wichtig« und für 29 Prozent »eher wichtig«. Neben der Funktionalität und den Sicherheitsaspekten haben für die Unternehmen außerdem die rechtlichen Rahmenbedingungen einen hohen Stellenwert. Somit folgt mit 85 Prozent, an dritter Stelle der Auswahlkriterien, die Darlegung der Rechteinhaberschaft sowie der Urheberschaft der OSS. Für knapp die Hälfte (48 Prozent) der Unternehmen ist dieser Faktor »sehr wichtig«, für 37 Prozent »eher wichtig«.

SBOM Management at Mercedes-Benz

With our published **Mercedes-Benz Free & Open Source Software (FOSS) Manifesto**, we demonstrate that we want to facilitate the cultural change in Mercedes-Benz and our subsidiaries towards Inner Source and FOSS. While **FOSS** brings innovation, efficiency, and speed, we need to make sure to play it safe. Therefore, opening to the worldwide FOSS community must also go along with the responsibility in a highly regulated industry to have clear internal rules and processes for FOSS. Furthermore, **digital standards** need to be established within the supply chain. We envision this and can already demonstrate it with several company activities. Overall, we strive to foster a secure and standardized data exchange for all **participants in our automotive value chain**.

With the development of a **FOSS Disclosure Portal**, we are continuing to build a more efficient, transparent, and digital supply chain. By digitizing and automating our FOSS disclosure process with our internal and external partners, we want to further increase transparency regarding the FOSS components we use, for better licence compliance and security. FOSS information is handled in **Software Bills of Materials (SBOM) with SPDX from the OpenChain Project** (ISO / IEC standard for Open Source licence compliance programs) as the defined format for our SBOM exchange.

We recognized the need to introduce a FOSS Disclosure Portal to manage our FOSS SBOMs at scale, together with our partners.



FOSS SBOM in the Software Supply Chain

The purpose is to facilitate the exchange FOSS information directly & frequently from the CI/CD pipeline for developers, product & application owners, and suppliers. That way, our software guidelines, especially for FOSS compliance and security, can be followed. We want to provide more automated guidance with respect to checking licence conformance (e. g. allow and deny list information for licences defined in respective software development use case policies) and obligation management (quality checks on relevant SBOM details based on our licence database).

As a result, a central worldwide inventory of FOSS SBOMs from all companies within the Mercedes-Benz Group AG will be created. This inventory can be analysed e. g. for identified security issues.

Our partners and suppliers in the supply chain should benefit from the introduction of the FOSS Disclosure Portal in the following ways: By connecting to the portal's API, FOSS information can be submitted directly instead of filling out specific disclosure documents. The resulting information in the portal provides transparency and allows for earlier and more frequent alignments between all parties in the development process in order to meet our defined FOSS quality standards.

The development of our FOSS Disclosure Portal is based on current technologies. Our vision is to drive the development of this product together with the Open Source Community and our partners. To allow the optimization to exchange FOSS information on both sides, an initial component of the FOSS Disclosure Portal (our Command Line Interface, CLI) has already been published under Open Source. Based on these learnings we would like to plan further steps in driving this initiative together with motivated FOSS experts.

References

↗ Mercedes-Benz FOSS Manifesto

↗ Disclosure CLI on Github

Sonatype

So wichtig Open Source für die Entwicklung von Software in der heutigen Welt ist, so groß ist auch die Gefahr von Schwachstellen, wenn sie nicht richtig verwaltet werden. Open Source hat die Art und Weise, wie die Welt heute Innovationen hervorbringt, verändert, und wird dies auch weiterhin tun. Aber nicht alle Komponenten können als gleichwertig betrachtet werden. Der jährlich von Sonatype herausgebrachte Bericht zum State of the Software Supply Chain zeigt in seiner aktuellen achten Fassung, dass Unternehmen im letzten Jahr mehr als 3,5 Billionen Open-Source-Komponenten heruntergeladen haben, dies allein in den vier wichtigsten Programmiersprachen. Diese Komponenten machen 80–90 Prozent einer durchschnittlichen Anwendung aus.

Außerdem zeigt sich, dass etwa eine aus zehn heruntergeladenen Komponenten eine bekannte Sicherheitslücke enthält. Dabei sind die böswilligen Angriffe auf Open Source (die in den letzten drei Jahren jährlich um mehr als 700 Prozent zugenommen haben) noch nicht berücksichtigt. Hierbei handelt es sich aber nur um bekannte Sicherheitslücken. Diese Realität ist auf dem Markt nicht unbekannt. Man denke nur an das berüchtigte Log4j-Projekt aus dem Jahr 2021, welches die inzwischen berühmte Log4Shell-Sicherheitslücke enthielt.

Es ist wichtig, dies alles zu verstehen, wenn man sich die sehr interessanten Daten aus der aktuellen Bitkom-Studie Open Source Monitor 2023 zum Thema Sicherung von Open Source ansieht. Dem Bericht zufolge versuchen 40 Prozent der kommerziellen und 33 Prozent der öffentlichen Unternehmen, all dies manuell zu bewältigen. Während es ermutigend ist, dass fast ein Drittel der Unternehmen ein Analysetool einsetzt, ist der Prozentsatz derjenigen, die die Sicherheit von Open Source-Komponenten manuell oder überhaupt nicht überwachen, besorgniserregend. Ein weiteres Drittel der Befragten, sowohl aus dem privaten als auch aus dem öffentlichen Sektor, gab an, dass sie darauf vertrauen, dass der Open Source-Anbieter sie informiert, sollten sie Kenntnis über ein Sicherheitsproblem in einer ihrer Komponenten erlangen.

Wenn man sich das Ausmaß der Nutzung von Open Source vergegenwärtigt, wird die harte Realität deutlich: Sich ausschließlich auf manuelle Überprüfungen zu verlassen, ist vergleichbar mit dem vergeblichen Versuch, den Ozean mit einem Teelöffel leer zu löffeln, und damit praktisch erfolglos. Die Bemühungen der Open Source Maintainer-Gemeinde sind uns bekannt, und wir betrachten und schätzen sie als Verbündete von ganzem Herzen an. Aber es ist wichtig, die Schwachstellen der Maintainer anzuerkennen und sich nicht ausschließlich auf diese zu verlassen, wenn es um eine primäre Open Source-Cybersicherheitsstrategie geht.

Bei näherer Betrachtung der diesjährigen Ergebnisse wird deutlich, dass nur 21 Prozent der Nutzer von Analysewerkzeugen diese wie vorgesehen im Rahmen der Softwareentwicklung einsetzen. Die überwiegende Mehrheit sowohl der privaten Unternehmen (63 Prozent) als auch der öffentlichen Unternehmen (53 Prozent) setzt diese Tools manuell ein, das heißt immer dann, wenn sie benötigt werden. Leider ist es die harte Realität, dass ein Unternehmen, das sich dafür entscheidet, eine Analyse nur »bei Bedarf« durchzuführen, wahrscheinlich bereits im Rückstand ist.

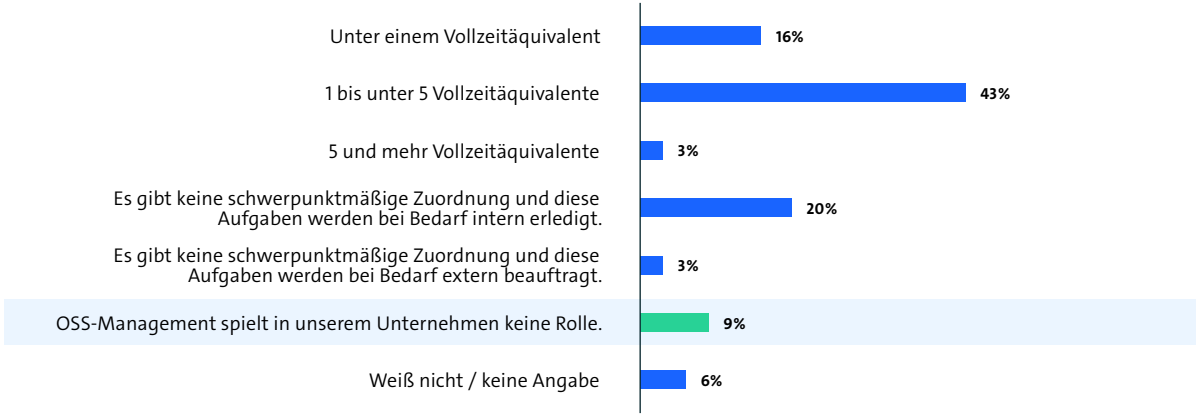
Mit der jüngsten Verabschiedung des Cyber Resilience Act (CRA) werden die Daten für die Mitgliedsländer der Europäischen Union noch alarmierender und erfordern eine gründliche Analyse. Mit dem CRA soll den wachsenden Bedrohungen im Zusammenhang mit digitalen Produkten begegnet werden, indem die Entwicklungs- und Lieferstandards gestärkt werden. Sie nimmt die Produktentwickler in die Pflicht und stellt sicher, dass die Sicherheit während des gesamten Produktlebenszyklus ernst genommen wird. Die Einhaltung der CRA erfordert von deutschen Unternehmen den Aufbau eines skalierbaren Betriebs. Die Antworten auf die Bitkom-Studie zeigen jedoch, dass noch ein weiter Weg zurückzulegen ist.

1.4 Open-Source-Software-Management und Umgang mit Sicherheitsprüfungen

Das vorherige Kapitel zeigt, dass die Mehrheit (69 Prozent) der Unternehmen ab 20 Beschäftigten in Deutschland angeben OSS einzusetzen. Um einen detaillierteren Einblick in den Einsatz und Umgang mit OSS innerhalb der Unternehmen zu erhalten, werden in diesem Kapitel Fragen rund um das Management von OSS behandelt. OSS-Management wurde in diesem Kontext wie folgt definiert: Praktiken und Prozesse, die verwendet werden, um die Entwicklung und den Einsatz von OSS innerhalb der Unternehmen zu steuern und zu koordinieren. Neben der Anzahl an Beschäftigten, die von Unternehmen für das Management von OSS eingesetzt werden, sind auch die Fragen nach einer Organisationseinheit für OSS, sowie der Umgang mit Sicherheitsprüfungen, die im Rahmen von OSS-Management durchgeführt werden, wesentliche Aspekte, die betrachtet werden.

Rund sechs von zehn (62 Prozent) Unternehmen, die OSS nutzen, geben an, dass es eine dedizierte Anzahl von Personen gibt, die sich schwerpunktmäßig mit dem Management von OSS im Unternehmen befassen (siehe Abbildung 16). Für ein Fünftel (20 Prozent) der Unternehmen werden die Aufgaben bei Bedarf intern geregelt, 3 Prozent der Unternehmen beauftragen bei Bedarf externe Dienstleister für das OSS-Management. Nur ein Zehntel (9 Prozent) der Unternehmen geben an, dass OSS-Management in ihrem Unternehmen keine Rolle spielt.

Wie viele Beschäftigte befassen sich schwerpunktmäßig mit OSS-Management?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln (n=801) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen | Quelle: Bitkom Research 2023

Abbildung 16 – Open-Source-Software-Management

Wie viele Beschäftigte befassen sich schwerpunktmäßig mit OSS-Management?

Größenklassen	Ø Beschäftigte
20 – 99 MA	1,2
100 – 199 MA	2,9
200 – 499 MA	2,8
500 – 1.999 MA	6,1
2.000+ MA	6,7
Gesamt	1,7

Einsatzebene	Ø Beschäftigte
Verwendung ohne Weiterentwicklung	1,7
Integration ohne Weiterentwicklung	1,8
Entwicklung und Weiterentwicklung	1,8
Gesamt	1,7

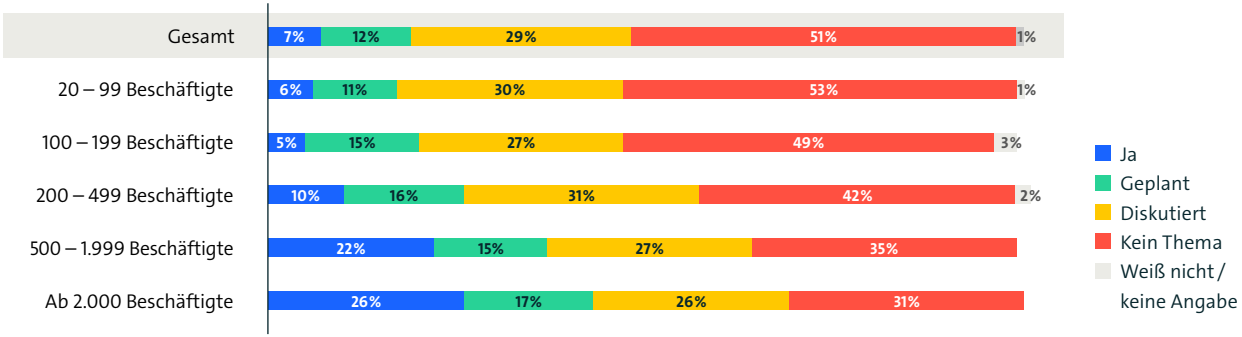
Basis: Alle Unternehmen ab 20 Beschäftigten, die eine schwerpunktmäßige Zuordnung von OSS-Management haben (n=504)
Quelle: Bitkom Research 2023

Abbildung 17 – Beschäftigte Open-Source-Software-Management

Abbildung 17 zeigt, dass Unternehmen, die eine schwerpunktmäßige Zuordnung von Beschäftigen für das OSS-Management vornehmen, im Durchschnitt 1,7 Vollzeitäquivalente für diese Aufgabe beschäftigen. Die Anzahl der Beschäftigten steigt, wie zu erwarten, mit der Größe der Unternehmen. Mit Blick auf die Einsatzebenen von OSS (Verwendung, Integration und (Weiter-) Entwicklung) sind keine Unterschiede bei der durchschnittlichen Beschäftigungszahl zu erkennen.

Bei der Frage nach einem Open Source Program Office (OSPO) – also einer zentralen Organisationseinheit, die sich übergreifend um Open-Source-Software-Belange kümmert – geben 7 Prozent der Unternehmen, die OSS verwenden, integrieren oder (weiter-)entwickeln, an, eine solche Organisationseinheit eingerichtet zu haben (siehe Abbildung 18). Rund ein Zehntel (12 Prozent) gibt an, die Einrichtung konkret zu planen. Knapp ein Drittel (30 Prozent) diskutiert die Einrichtung einer solchen Organisationseinheit. Für die Hälfte (51 Prozent) der Unternehmen ist diese Überlegung momentan kein Thema.

Haben Sie ein Open Source Program Office eingerichtet?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln (n=801) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen | Quelle: Bitkom Research 2023

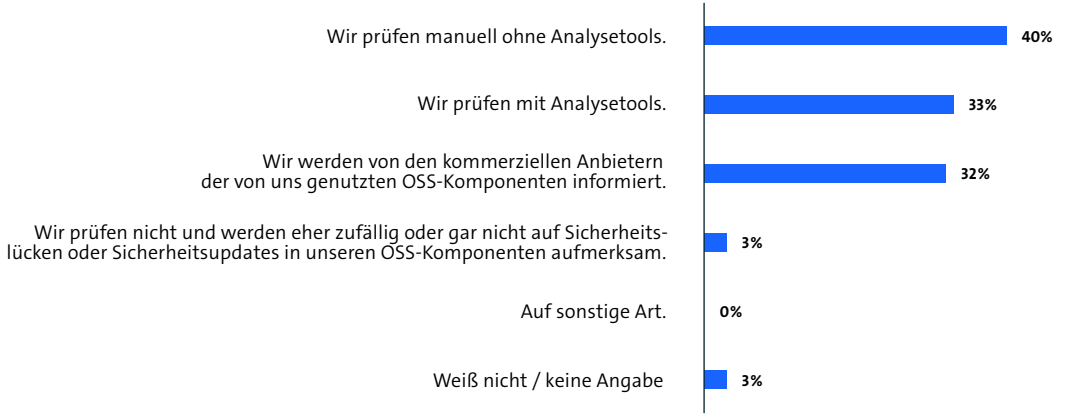
Abbildung 18 – Einrichtung Open Source Program Office nach Unternehmensgrößenklassen

Der Blick auf die Einrichtung eines OSPO entlang der Unternehmensgrößenklassen zeigt einen größeren Sprung für Unternehmen ab 500 Beschäftigten. Unter den Unternehmen mit 500 bis 1.999 Beschäftigten haben bereits ein Fünftel (22 Prozent) ein OSPO eingerichtet. Bei den Unternehmen ab 2.000 Beschäftigten sind es sogar schon ein Viertel (26 Prozent). Entsprechend geringer fällt bei größeren Unternehmen auch der Anteil der Unternehmen aus, für die eine OSPO-Einrichtung derzeit kein Thema ist (500 bis 1.999 Beschäftigte: 35 Prozent; ab 2.000 Beschäftigten: 31 Prozent).

↗ Kapitel 1.1 zeigte, dass Aspekte rund um die IT-Sicherheit von OSS, verglichen mit den größten Vorteilen, überwiegend als Nachteil von OSS genannt wurden (Nachteil: 19 Prozent, Vorteil: 4 Prozent). Der Umgang mit der Prüfung auf Sicherheit von OSS-Komponenten, die von Unternehmen eingesetzt, integriert oder (weiter-)entwickelt werden, ist daher ein weiterer zentraler Aspekt dieses Kapitels.

Während 40 Prozent der Unternehmen angeben, manuell ohne Analysetools zu prüfen, geben ein Drittel (33 Prozent) an, mit Analysetools zu prüfen (siehe Abbildung 19). Ein weiteres Drittel (32 Prozent) wird außerdem von kommerziellen Anbietern, der von ihnen genutzten OSS-Komponenten, über Sicherheitslücken informiert.

Welchen Ansatz verfolgen Sie in Ihrem Unternehmen bei der Prüfung auf Sicherheit der von Ihnen eingesetzten OSS-Komponenten?



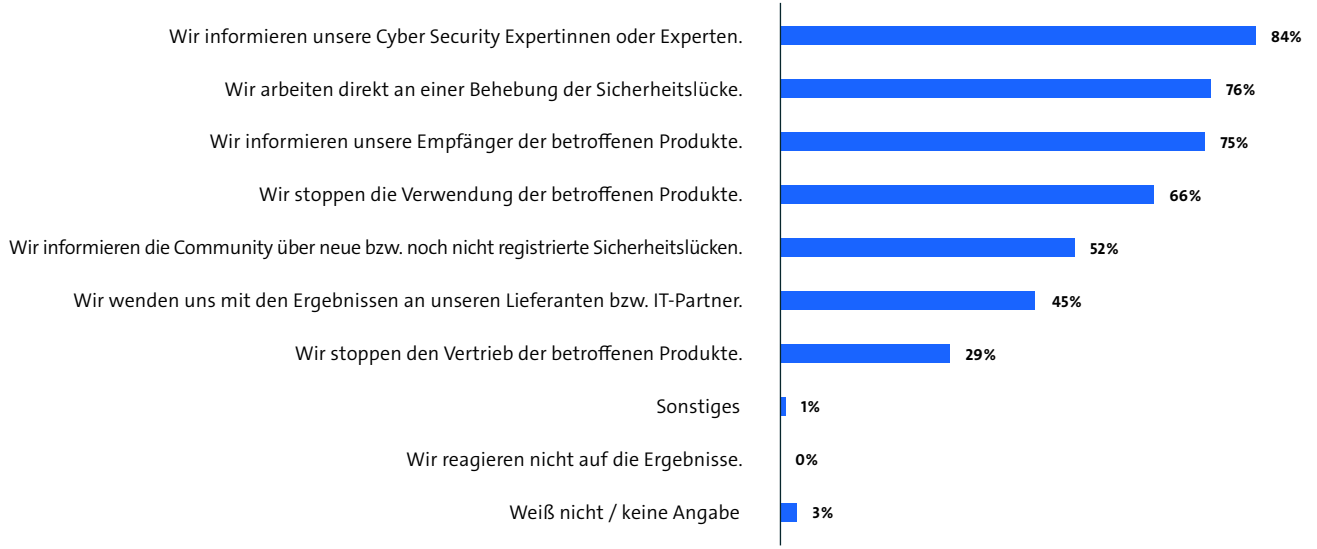
Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln (n=801) | Mehrfachnennung möglich
Quelle: Bitkom Research 2023

Abbildung 19 – Open-Source-Software-Sicherheitsprüfung

Nur 3 Prozent der Unternehmen geben an, nicht gezielt auf Sicherheitslücken oder Sicherheitsupdates zu prüfen, im Jahr 2021 waren es noch 23 Prozent. Der Rückgang um 20 Prozentpunkte zeigt deutlich, dass die Sicherheit der eingesetzten OSS in den letzten zwei Jahren stark an Bedeutung gewonnen hat.

Unter den Unternehmen, die einen Prozess für die Prüfung auf Sicherheit von eingesetzten OSS-Komponenten haben, gibt, wie zu erwarten, niemand (0 Prozent) an, nicht auf die Ergebnisse zu reagieren (siehe Abbildung 20). Acht von zehn (84 Prozent) der Unternehmen informieren bei Sicherheitsschwachstellen ihre Cyber Security Expertinnen oder Experten. Jeweils drei Viertel (76 Prozent) der Unternehmen arbeiten direkt an der Behebung von Schwachstellen und informieren die Personen, welche betroffene OSS-Produkte nutzen (75 Prozent). Zwei Drittel (66 Prozent) der Unternehmen stoppen außerdem die Verwendung der betroffenen Produkte. Falls die Sicherheitslücken noch nicht registriert sind, geben die Hälfte (52 Prozent) der Unternehmen an, die OSS-Community zu informieren. 45 Prozent der Unternehmen wenden sich mit den Erkenntnissen an Lieferanten, beziehungsweise an IT-Partner. Drei von zehn (29 Prozent) Unternehmen geben an, den Vertrieb der betroffenen Produkte zu stoppen.

Wie gehen Sie mit Erkenntnissen über Sicherheitsschwachstellen aus der Analyse um?



Basis: Alle Unternehmen ab 20 Beschäftigten, die generell auf Sicherheitsschwachstellen prüfen (n=753) | Mehrfachnennung möglich
Quelle: Bitkom Research 2023

Abbildung 20 – Umgang mit Sicherheitsschwachstellen der Open-Source-Software

NORDEMANN

Open-Source-Software und Patentportfolios

Rechtliche und organisatorische Herausforderung bei Open-Source-Contributions

Die erfreuliche Entwicklung zunehmender Open-Source-Contributions ruft vermehrt auch die Frage nach Patentklauseln und deren »Gefährdung« für das IP-Portfolio auf den Plan. Tatsächlich enthalten zahlreiche Open-Source-Lizenzen Regelungen über die Lizenzierung von Patenten und auch ohne solche Regelungen kann eine implizite Lizenzierung angenommen werden. In unserer Praxis sind uns bereits Fälle begegnet, bei denen Patentinhaber durch eine unbedachte und unzureichend organisierte Open-Source-Auslizenzierung eine Patentfamilie nahezu vollständig unentgeltlich potenziell an jedermann lizenziert haben.

Gerade in größeren Technologieunternehmen, die regelmäßig auch Patentportfolios verwalten, ist dieses Thema von besonderer Relevanz. Hier ist dann eine funktionierende Abstimmung zwischen tendenziell »IT-nahen« Open-Source-Teams (OSPOs) und traditionell Patent-zentrierten IP-Abteilungen erforderlich. An dieser Schnittstelle entstehen durch Open-Source-Contributions neue zentrale Rechtsfragen und ein entsprechender organisatorischer Gestaltungsbedarf.

Denn in rechtlicher Hinsicht ist zunächst zu prüfen, welche Patente möglicherweise von einer Auslizenzierung im Wege einer Open-Source-Contribution erfasst sein könnten. Dazu muss einerseits die entsprechende Patentklausel ausgelegt werden, was nach unserer Erfahrung für Rechtsabteilungen und Open-Source-Teams bereits eine erste Herausforderung darstellen kann. Für die Patentabteilung gilt es dann, das Schutzrechtsportfolio vor diesem Hintergrund zu untersuchen, was ebenfalls eine Herausforderung darstellen kann. Insbesondere die »Subsumtion« einer konkreten Softwarekomponente unter den Anwendungsbereich einer Patentklausel und die anschließende Identifizierung der entsprechenden Schutzrechte kann – wenn dies im Detail geprüft werden muss – komplex werden.

Diese im Ausgangspunkt rechtlich Frage schlägt sich auch auf organisatorische Aspekte und Prozesse innerhalb des Unternehmens nieder. Zunächst muss sichergestellt sein, dass im Unternehmen entsprechende Regelungen für Open-Source-Contributions vorliegen und Open-Source-Contributions in Begleitung durch das Open-Source-Team erfolgen können. Anschließend muss sichergestellt werden, dass das Open-Source-Team gemeinsam mit der IP-Abteilung die relevanten Schutzrechte identifiziert, ein etwaiges Risiko bewertet und bei Bedarf risikominimierende Gestaltungsmöglichkeiten aufzeigt.

NORDEMANN bietet umfangreiche Beratung im Bereich des IP/IT- und Open-Source-Rechts an. Christian Czychowski und Sebastian Dworschak stehen für Anfragen gerne zur Verfügung.

Prof. Dr. Christian Czychowski

Sebastian Dworschak

↗ www.nordemann.de
↗ info@nordemann.de

Sichere Open Source

Vom Uni-Projekt zur Plattform für Geheimhaltungsgrad GEHEIM zugelassene Produkte bis zum EAL4+ zertifizierten Separation Kernel – Am Beispiel des Open-Source Betriebssystems »L4Re«

Katrin Kahle
Head of Product, Kernkonzept GmbH

Entstehung des FOSS-Betriebssystemkerns an der TU Dresden

Das L4Re Operating System Framework ist Ergebnis der Entwicklung einer Gruppe von Betriebssystem-Wissenschaftlern an der TU Dresden, die seit Mitte der 90er an real-time-fähigen und sicheren L4-Mikrokernen forsch(t)en. Aufgrund der damaligen Bedingungen spielten die heutigen Anforderungen an Sicherheit oder Zertifizierung noch keine Rolle.

Dank des hohen Anspruchs der Gruppe an qualitative Softwareentwicklung entstand jedoch das Fundament von L4Re. Inzwischen wird L4Re als Betriebssystem oder Hypervisor in vielen, bis Geheimhaltungsgrad GEHEIM zugelassenen Produkten genutzt.

Umsetzung mit Shift-Left seit den 90ern

Der hohe Anspruch wurde frühzeitig durch eine ausgeprägte Shift-Left-Orientierung umgesetzt, um Fehler frühestmöglich zu entdecken. So wurde ein Prozess mit sechs zu durchlaufenden Quality Gates vor einem Release etabliert.

Quality Gate 1: Integrierte Entwicklungsumgebung der Entwicklerin oder des Entwicklers: Die Wahl einer guten IDE unterstützt bei der Navigation durch den Code, dem Bereitstellen der Dokumentation und Code-Vervollständigungen.

Quality Gate 2: Automatisierte Build-Checks nach jeder Änderung über alle Prozessorarchitekturen, für alle relevanten Konfigurationen

Quality Gate 3: Code Review im Vier-Augen-Prinzip, mit Audit Logs für die Dokumentation schwieriger Design-Entscheidungen, Verhinderung des Einschleusens von Backdoors und hohe Nachvollziehbarkeit

Quality Gate 4: Automatisiertes Testen mit Low-Level-API-Tests, Integrationstest, Regressionstests

Quality Gate 5: Versionierung für hohe Nachvollziehbarkeit, Integritätsschutz, Verfügbarkeit und gemeinsame Entwicklung

Quality Gate 6: Automatisierte Security Checks mittels formaler Methoden, erweitertem Testing und Schwerpunkt-Tests

Shift-Left Quality Gates bei Kernkonzept

Weitere Schritte für Sicherheit nach CC EAL4+

Gründung der Kernkonzept GmbH 2012 als einziger Betreuer zur Sicherstellung der Qualitätsansprüche von Kundschaft und Zertifizierung

Evaluierung und Testing durch ein unabhängiges Evaluationsbüro

Massiver Ausbau der Dokumentation: Prozessdokumentation und Lebenszyklus, Erstellung von Security Advisories

Einführung von SBOM im SPDX-Format 2017 (Open Chain Project)

Ergebnis

Ein zertifiziert sicheres Open-Source-Betriebssystem für sichere vernetzte Geräte und ein digital souveränes Europa

↗ contact@kernkonzept.com / kernkonzept.com

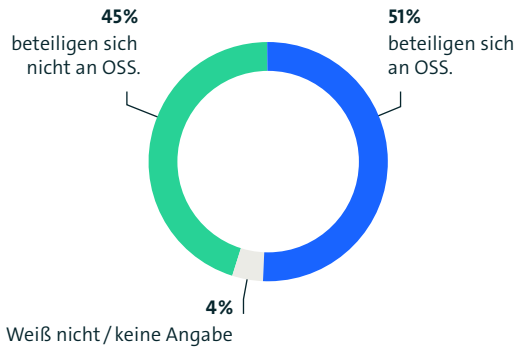
1.5 Beteiligung an Open-Source-Software

Die Stärke von Open-Source-Software liegt in der engagierten Teilnahme der Nutzerinnen und Nutzer an der stetigen Verbesserung der Software. Eine aktive OSS-Community, mit einer hohen Beteiligung an der Entwicklung oder Weiterentwicklung der Software, ist somit das Fundament eines erfolgreichen OSS-Projekts. Die Hälfte (51 Prozent) der Unternehmen ab 20 Beschäftigten in Deutschland beteiligt sich aktiv an der Entwicklung beziehungsweise Weiterentwicklung von OSS (siehe Abbildung 21).

Im Detail gestaltet sich die Beteiligung an OSS-Projekten dabei wie folgt: 4 von 10 (41 Prozent) Unternehmen unterstützen durch den Kauf von Support-Leistungen oder Subskriptionen für entsprechende Enterprise Editionen von OSS (siehe Abbildung 22). Ein Viertel (25 Prozent) der Unternehmen gibt einzelnen Beschäftigten oder Teams die Erlaubnis, sich im Rahmen ihrer Arbeit an OSS-Projekten zu beteiligen.

Ein Siebtel (15 Prozent) beteiligt sich durch die Bereitstellung von weiterentwickeltem OSS-Quellcode. 12 Prozent initiieren und beteiligen sich aus der eigenen Unternehmenstätigkeit heraus an Projekten. Weitere 8 Prozent geben an, zahlendes Mitglied von OSS-Foundations zu sein, während sich lediglich 3 Prozent der Unternehmen durch das Sponsoring von OSS-Veranstaltungen an OSS beteiligen.

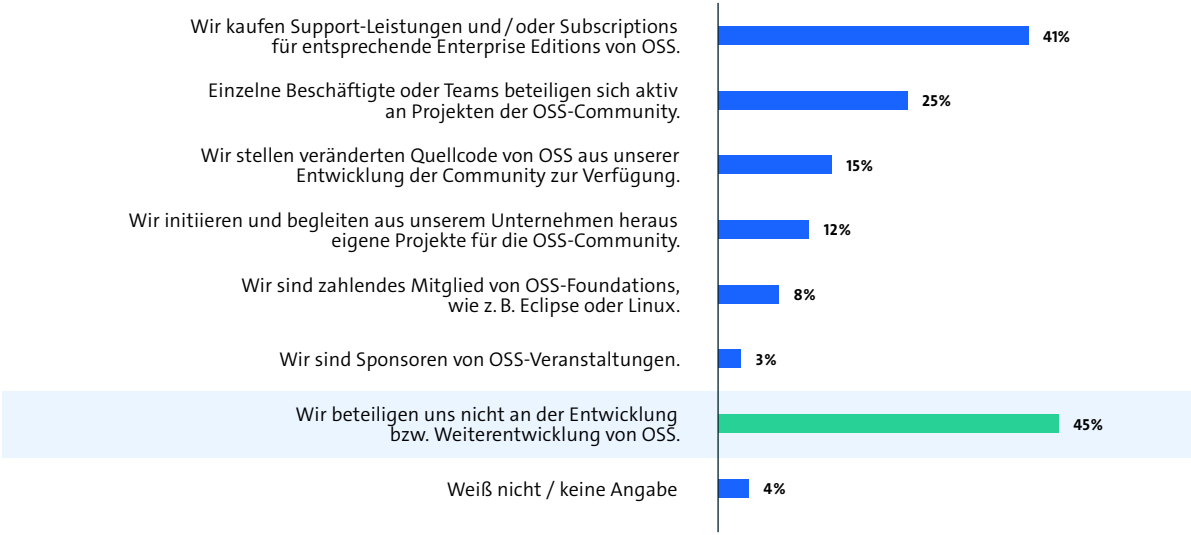
Beteiligen Sie sich an der Entwicklung bzw. Weiterentwicklung von OSS?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155)
Quelle: Bitkom Research 2023

Abbildung 21 – Beteiligung an Open-Source-Software

Inwiefern beteiligt sich Ihr Unternehmen an der Entwicklung bzw. Weiterentwicklung von OSS?

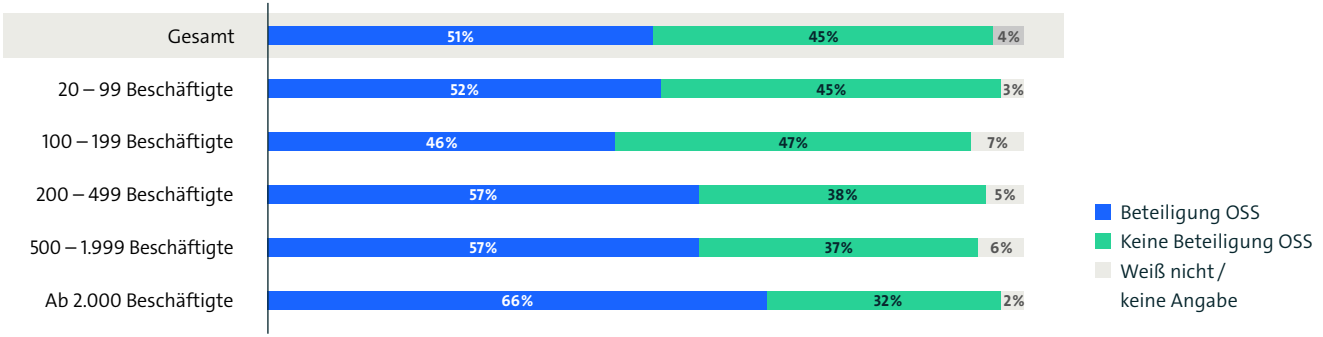


Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2023

Abbildung 22 – Beteiligung an Open-Source-Software nach Art

Die Beteiligung an der Entwicklung beziehungsweise Weiterentwicklung von OSS ist wiederum abhängig von den Unternehmensgrößenklassen (siehe Abbildung 23) und steigt mit der Größe der Unternehmen. Die Hälfte (52 Prozent) der Unternehmen mit 20 bis 99 Beschäftigten beteiligt sich an OSS. Bei den Unternehmen mit 100 bis 199 Beschäftigten nimmt die Beteiligung mit 46 Prozent leicht ab. Die Beteiligung steigt wiederum bei Unternehmen mit 200 bis 1.999 Beschäftigten: hier beteiligen sich rund sechs von zehn (57 Prozent) Unternehmen. Mit 66 Prozent ist die ausgeprägteste Beteiligung bei Großunternehmen ab 2.000 Beschäftigten vorhanden. Hier zeigen sich Parallelen zu Anzahl der Personen, die sich schwerpunktmäßig mit OSS beschäftigen, welche ebenfalls mit zunehmender Unternehmensgröße steigt (↗ Kapitel 1.4., Abbildung 17).

Beteiligen Sie sich an der Entwicklung bzw. Weiterentwicklung von OSS?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Quelle: Bitkom Research 2023

Abbildung 23 – Beteiligung an Open-Source-Software nach Unternehmensgrößenklassen

Open Source Compliance? Aber bitte effizienter!

Open-Source-Software (OSS) ist überall und ist für die moderne Software-Entwicklung unverzichtbar geworden. Ein typisches Softwareprodukt enthält heute oft mehr als 90 Prozent Open Source.

Alarmiert durch spektakuläre Cyberangriffe auf die Software-Lieferkette wurden in den USA Vorgaben wie die »Executive Order on Improving the Nation's Cybersecurity« erstellt und in der EU entsteht gerade der europäische Cyber Resilience Act (CRA). Für eine rechtssichere Verwendung müssen daher alle Open Source Bestandteile bekannt und benannt sein.

Die Erstellung einer kompletten Software Bill of Materials (SBOM) mit korrekter Bezeichnung von Bestandteilen und Urheberrechten kann jedoch sehr aufwändig und teuer sein. Beispielsweise kommen für eine komplette Analyse eines auf Android aufbauenden Produktes schnell sechsstellige Summen für die Prüfung zustande. Gerade für mittelständische Unternehmen sind diese Kosten oft ungeplant und in der Regel eine immense Herausforderung.

Alle Marktakteure sind sich daher weitgehend einig, dass die Effizienz in der Erstellung einer rechtssicheren SBOM gesteigert werden muss. Hierbei werden verschiedene Ansätze verfolgt: Mit dem ISO-Standard 5230 der OpenChain wurde eine wichtige **Standardisierung** des Compliance-Prozesses durchgeführt. Weiterhin wurden mit SPDX und CycloneDX Vereinheitlichungen zur Beschreibung der relevanten Daten ins Leben gerufen, so dass ein Austausch innerhalb der Supply-Chain effizienter bewerkstelligt werden kann.

Da die meisten **Scanner** heute noch mit Texterkennung oder kuratierten Datenbanken arbeiten, gibt es mittlerweile Forschungsprojekte, mittels KI die Effizienz in der SBOM-Erstellung zu erhöhen. Erste Tests lassen aber noch auf einen gehörigen Entwicklungs- und Forschungsaufwand schließen.

Eine andere Idee ist es, schon **kuratierte Lizenzinformationen bereitzustellen**. Repositorien wie »GitHub« oder »Maven« stellen diese neuerdings bereit, und Werkzeuge verfolgen Abhängigkeiten nach um die Lizenzzusammenstellung zu erleichtern. Die Zuverlässigkeit der bereitgestellten Informationen entspricht jedoch nicht immer den rechtlichen Anforderungen. Projekte wie »OSSelot« oder »ClearlyDefined« erlauben die Wiederverwertung von SBOMs schon auditierter Open-Source-Pakte, und bieten nach eigener Darstellung besser kuratierte Daten.

Die Vorgehensweise von SW360 und SBOM Insight erlauben den Aufbau eines eigenen **Kataloges** auditierter Komponenten entlang der Supply Chain, und machen auch die Wiederverwendung vertrauenswürdiger (eigener) Daten zwischen Projekten möglich. Um die Erkennung zu erleichtern, verfolgen einige Projekte den Ansatz, den Code selbst **umzustrukturieren** und mit weiteren Informationen zu versehen.

»REUSESOFTWARE« gibt Empfehlungen, wie vollständige Lizenzinformationen automatisch direkt im Code verankert werden können. Auch die Linux-Clean-up-Aktivität 2017 hatte zum Ziel, alle Dateien des Kernels mit einer eindeutigen SPDX-Kennung zu versehen.

Oft wird versucht, die Lizenzerkennung schon direkt in den Entwicklungsprozess in eine CI / CD Pipeline einzubinden und **kontinuierlich** die SBOM auf einem aktuellen Stand zu halten.

Es bleibt festzuhalten, dass momentan mehrere Ansätze verfolgt werden, um die Erstellung einer SBOM wirtschaftlich effizienter abzubilden, aber die Frage nach der Haftung bei Fehlern in den Listen wird nicht abschließend geklärt.

Bitsea berät bezüglich nachhaltiger Nutzung und Compliance von Open Source Software. Zu unseren Kunden zählen namhafte Konzerne aller Branchen. Bitsea ist Partner von OpenChain.

↗ www.bitsea.de

{metæffekt}

Einordnung des EU Cyber Resilience Act zum OSM#23

Bezug

Mit dem Cyber Resilience Act (CRA) [1] strebt die EU die Harmonisierung der Sicherheitsanforderungen von Produkten mit digitalen Elementen im Binnenmarkt an. Der CRA beabsichtigt, das Maß an Cybersicherheit dieser Produkte zu erhöhen und Schwachstellen entgegenzutreten.
Der derzeitige Entwurf beinhaltet grundlegende und nachvollziehbare Forderungen zu folgenden Themen:

- Erstellung von Software Bill of Materials (SBOM)
- Evaluation und Verwaltung von Sicherheitsaspekten
- Konformitätsnachweise der Hersteller in der Lieferkette
- Verifikation und Validierung von SBOM-Inhalten

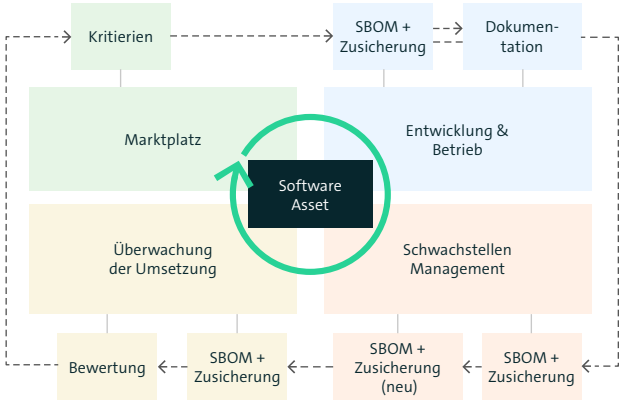
Open-Source-Software (OSS), sofern im kommerziellen Kontext genutzt, wird von der zukünftigen Verordnung eingeschlossen. Insofern finden sich zentrale Aspekte des CRA im Open Source Monitor 2023 (OSM#23) des Bitkom wieder.

Status Quo

Im CRA ausformulierte Maßnahmen und Anforderungen sind bereits heute Treiber für Industrie und Verwaltung. Dies wird an den Kennzahlen des OSM#23 deutlich. So erstellen 38,5 Prozent in der Verwaltung und 31,7 Prozent der befragten Unternehmen eine SBOM. Bei der Verwendung von OSS prüfen 64,3 Prozent in der Verwaltung und 72,8 Prozent in der Industrie die eingesetzten Komponenten auf ihre Sicherheit. Allerdings erfolgt bei nur 13,7 Prozent in der Industrie und 23,5 Prozent in der Verwaltung die Prüfung automatisiert in festgelegten Zeitabständen.

Ableitung aus dem CRA

Nachfolgend wird der Blick auf das Software-Asset als Bestandteil eines Produkts mit digitalen Elementen und die vier Regulierungsbereiche des CRA gerichtet:



Software-Asset Lebenszyklus

Für ein Software-Asset leiten sich aus dem Markt und dem CRA diverse Kriterien ab, die in Entwicklung und Betrieb zu berücksichtigen sind. Zur Erfassung eines Software-Assets wird eine SBOM verlangt, um individuelle Eigenschaften der detaillierten Bestandteile zuzusichern. Die SBOM wird zur Erzeugung von Dokumentation und zum Management von Schwachstellen herangezogen. Der CRA stellt konkrete Anforderungen an die Regelmäßigkeit von Analyse und Kommunikation der Schwachstellen an die Empfänger des Software-Assets. Die SBOM mit ihren Zusicherungen wird zur Bewertung und Überwachung der Kriterien genutzt.

Open Source in Industrie und Verwaltung

OSS ist zentraler Baustein der modernen Softwareentwicklung und bietet ein kollaboratives Ökosystem. Im OSM#23 wird deutlich, welche Aspekte von OSS für Industrie und Verwaltung eine besondere Rolle spielen. Um OSS in diesem Umfeld voranzutreiben, ist es erforderlich, die Verbindlichkeit in Gestaltung und Nutzung zu gewährleisten sowie das Maß an Sicherheit zu erhöhen. Der CRA kann genügen, die Akteure im Ökosystem auf ein neues Niveau an Sicherheit und Professionalität zu heben. Allerdings erfordert dies eine Mitwirkung aller beteiligten Freiwilligen und Unternehmen.

Fazit

Aus dem OSM#23 lässt sich die Hypothese ableiten, dass die Verwaltung zumindest formal besser aufgestellt ist als die Industrie. Um der Forderung des CRA nach einer unverzüglichen Reaktion auf Schwachstellen nachzukommen, reicht der aktuelle Automatisierungsgrad beider Sektoren jedoch noch nicht aus. Die Qualität der zugrundeliegenden SBOMs steht dabei zunächst noch außer Frage.

Die {metæffekt} GmbH [2] bietet Konzepte, Werkzeuge und Dienstleistungen zur Umsetzung von automatisierten Prozessen im Lebenszyklus von Software-Assets. Sie ist verbindlicher Partner einer maßgeschneiderten Umsetzung.

[1] ↗ https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[2] ↗ https://metaeffekt.com

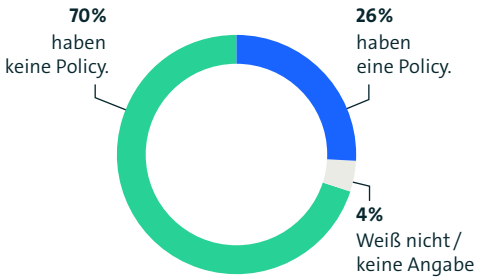
1.6 Open-Source-Software: Policy und Compliance

Open-Source-Software zeichnet sich dadurch aus, dass Anwender sie frei ausführen, den Quellcode einsehen und anpassen dürfen und sie in ihrer ursprünglichen oder veränderten Form weitergeben können. Es ist jedoch wichtig zu betonen, dass Open-Source-Software keineswegs in einem rechtsfreien Raum existiert. Die Freiheiten, die OSS bietet, sind häufig an spezifische Verpflichtungen oder Bedingungen gebunden, die in den entsprechenden Lizenzen festgelegt sind. Die Nichtbeachtung dieser Lizenzbedingungen kann zu Abmahnungen, Unterlassungsverpflichtungen oder Schadensersatzforderungen führen, die für Unternehmen erhebliche Kosten verursachen können.

Um in diesem Kontext potenzielle Probleme zu vermeiden, ist es ratsam, dass Unternehmen, die OSS nutzen oder sich an OSS-Projekten beteiligen, gleichzeitig über ein angemessenes OSS-Compliance-Management verfügen. Ein erster Schritt in diesem Managementprozess kann eine OSS-Policy sein. Dabei handelt es sich um ein schriftliches Dokument, das die Richtlinien und Regeln für den Umgang mit OSS im Unternehmen festlegt. Eine entsprechende OSS-Policy sollte zur Standard-Lektüre der Beschäftigten gehören, die mit OSS arbeiten.

Abbildung 24 zeigt, dass erst rund jedes vierte (26 Prozent) Unternehmen, welches OSS verwendet, integriert, (weiter-) entwickelt oder sich an OSS beteiligt, eine OSS-Policy hat. Die weite Mehrheit (70 Prozent) gibt an, keine niedergeschriebene OSS-Policy zu haben.

Gibt es in Ihrem Unternehmen eine OSS-Policy, d. h. ein Dokument, in dem Richtlinien und Regeln zum Umgang mit OSS in Ihrem Unternehmen niedergeschrieben sind?



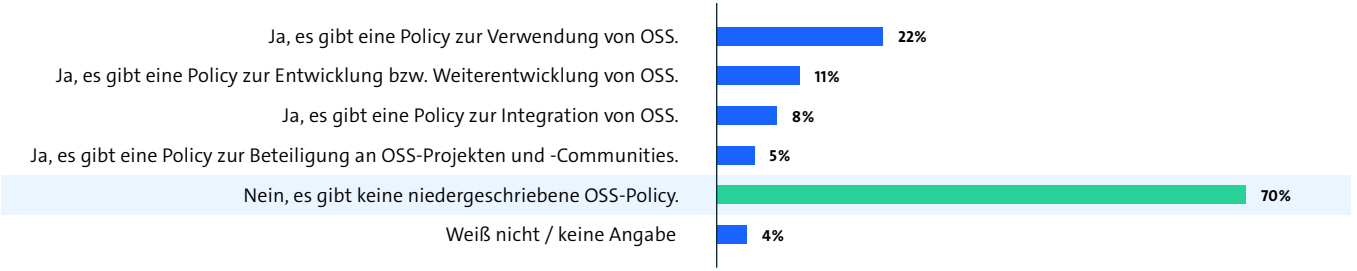
Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (n=809)
Quelle: Bitkom Research 2023

Abbildung 24 – Open-Source-Software-Policy

Die Aufschlüsselung nach Art der OSS-Policy zeigt, dass die meisten Unternehmen eine Policy zur Verwendung von OSS haben (22 Prozent), gefolgt von einer Policy zur Entwicklung beziehungsweise Weiterentwicklung (11 Prozent), einer Policy zur Integration von OSS (8 Prozent) und zum Schluss einer Policy zur Beteiligung an OSS (5 Prozent) (siehe Abbildung 25).

Die Aufschlüsselung nach Unternehmensgröße verdeutlicht, dass vor allem kleinere Unternehmen oft noch keine OSS-Policy definiert haben (25 Prozent mit Policy bei 20 bis 99 Beschäftigten sowie 26 Prozent bei 100 bis 199 Beschäftigten) (siehe Abbildung 26).

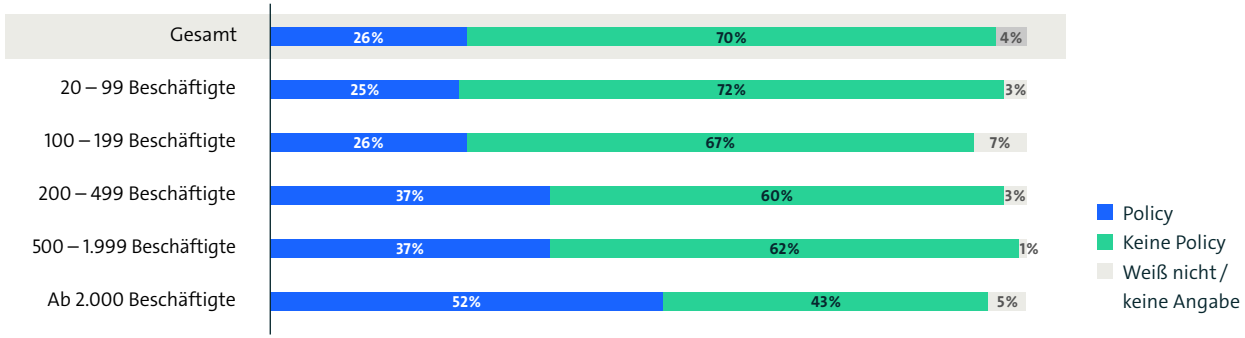
Gibt es in Ihrem Unternehmen eine OSS-Policy, d. h. ein Dokument, in dem Richtlinien und Regeln zum Umgang mit OSS in Ihrem Unternehmen niedergeschrieben sind?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (n=809)
Mehrfachnennung möglich | Quelle: Bitkom Research 2023

Abbildung 25 – Open-Source-Software-Policy nach Art

Gibt es in Ihrem Unternehmen eine OSS-Policy, d. h. ein Dokument, in dem Richtlinien und Regeln zum Umgang mit OSS in Ihrem Unternehmen niedergeschrieben sind?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (n=809)
Quelle: Bitkom Research 2023

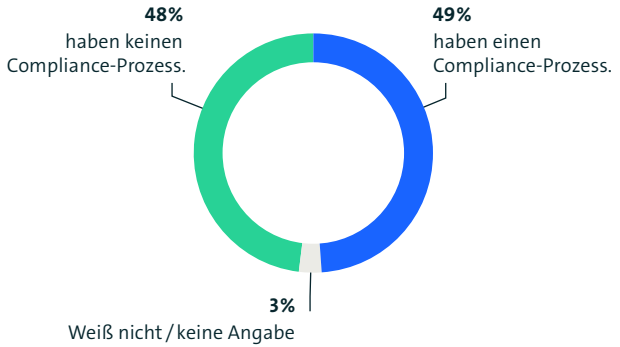
Abbildung 26 – Open-Source-Software-Policy nach Unternehmensgrößenklassen

Fast vier von zehn (37 Prozent) Unternehmen mit 200 bis 1.999 Beschäftigten haben eine OSS-Policy, bei Großunternehmen ab 2.000 Beschäftigten sind bereits mehr als die Hälfte (52 Prozent) mit einer OSS-Policy ausgestattet.

Die Ergebnisse bezüglich des Vorhandenseins von Compliance-Prozessen innerhalb der Unternehmen, die OSS nutzen oder sich an OSS-Projekten beteiligen, fallen verglichen zum Vorhandensein einer OSS-Policy anders aus (siehe Abbildung 27).

Rund die Hälfte (49 Prozent) der Unternehmen hat einen niedergeschriebenen Compliance-Prozess. Das bedeutet, dass im Vergleich zur OSS-Policy fast doppelt so viele Unternehmen über in einer Richtlinie dokumentierte Compliance-Prozesse verfügen – also über standardisierte Vorgehensweisen, welche die OSS-Strategie sowie die Richtlinien und Regeln für Mitarbeitende verbindlich vorschreibt. Tiefere Einblicke bezüglich einer vorhandenen OSS-Strategie und eines vorhandenen Compliance-Prozesses bietet ↗Kapitel 2. Dort werden zusätzlich die Zeitreihen der beiden Fragen betrachtet.

Gibt es in Ihrem Unternehmen einen niedergeschriebenen Compliance-Prozess zum Umgang mit OSS?



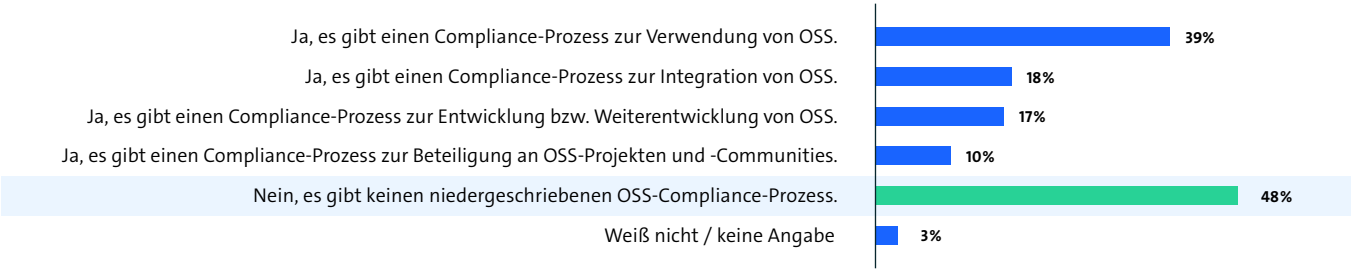
Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (n=809)
Quelle: Bitkom Research 2023

Abbildung 27 – Open-Source-Software-Compliance-Prozess

Der Blick auf die Tätigkeitsfelder, in denen Compliance-Prozesse existieren, zeigt: zwei Fünftel (39 Prozent) der Unternehmen hat einen Compliance-Prozess zur Verwendung von OSS (Abbildung 28). 18 Prozent haben einen Compliance-Prozess zur Integration von OSS. 17 Prozent zur Entwicklung oder Weiterentwicklung von OSS. Nur ein Zehntel (10 Prozent) der Unternehmen hat einen Compliance-Prozess zur Beteiligung an OSS-Projekten und Communitys.

Abbildung 29 zeigt hinsichtlich der Unternehmensgrößenklassen bis zu 1.999 Beschäftigten keine großen Veränderungen bei dem Anteil derjenigen Unternehmen, die einen Compliance-Prozess haben (20 bis 99 Beschäftigte: 49 Prozent; 100 bis 199 Beschäftigte: 52 Prozent; 200 bis 499 Beschäftigte: 46 Prozent; 500 bis 1.999 Beschäftigte: 51 Prozent). Erst bei Großunternehmen ab 2.000 Beschäftigten erhöht sich der Anteil deutlich. In dieser Unternehmensgrößenklasse haben zwei Drittel (67 Prozent) der Unternehmen eine standardisierte Vorgehensweise in Form von niedergeschriebenen Compliance-Prozessen.

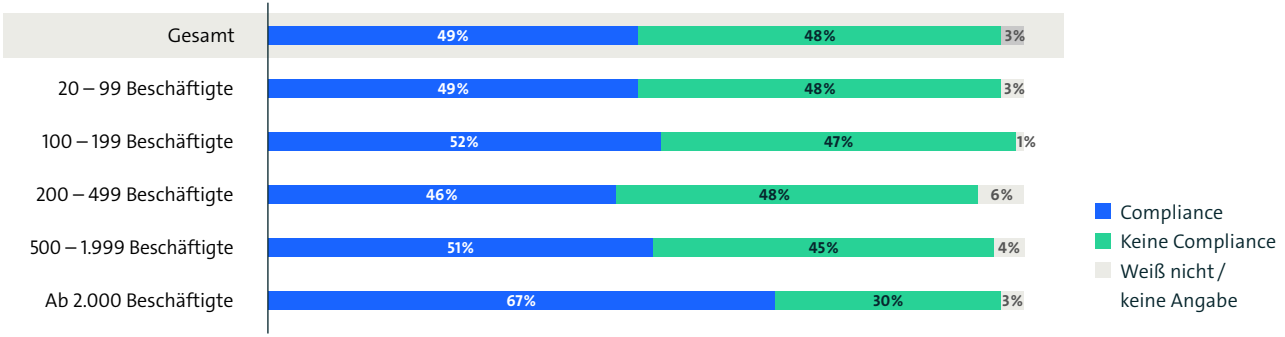
Gibt es in Ihrem Unternehmen einen niedergeschriebenen Compliance-Prozess zum Umgang mit OSS?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (n=809)
Mehrfachnennung möglich | Quelle: Bitkom Research 2023

Abbildung 28 – Open-Source-Software-Compliance-Prozess nach Art

Gibt es in Ihrem Unternehmen einen niedergeschriebenen Compliance-Prozess zum Umgang mit OSS?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (n=809)
Quelle: Bitkom Research 2023

Abbildung 29 – Open-Source-Software-Compliance-Prozess nach Unternehmensgrößenklassen

2 Unternehmens-Einsatz Fokusthema: Policy und Compliance

Die ersten Kapitel haben einen repräsentativen Überblick über die Verwendung von OSS in den Unternehmen ab 20 Beschäftigten in Deutschland gegeben. In diesem Kapitel soll der Fokus auf Fragen rund um die Standardisierung von Prozessen im Bereich Open Source liegen. Obwohl die Standardisierung von Prozessen im Bereich Open Source je nach Projekt und Community variiert, gibt es eine grundsätzliche Bestrebung, gewisse Standardisierungen zu etablieren, um die Zusammenarbeit, Interoperabilität und Wiederverwendbarkeit von Open-Source-Software zu verbessern.

Um dieses Thema in einen zeitlichen Kontext zu setzen, werden zunächst Zeitreihen der Fragen nach einer Policy und einem Compliance-Prozess für OSS gezeigt. Danach liegt der Fokus auf dem Compliance-Management von OSS in der Supply Chain. Hierfür wird untersucht:

- Kennen Unternehmen den OpenChain-Standard für OSS-Compliance, beziehungsweise die ISO 5230?
- Und stellen Unternehmen ein Dokument aller verwendeten OSS-Komponenen und derer Lizenzen, auch bekannt als Software Bill of Materials (SBOM), bereit oder fordern dies ein?

Der internationale Standard ISO 5230 definiert die Anforderungen für ein effektives Open-Source-Compliance-Programm, während die Erstellung eines Dokuments mit Lizenztexten hierbei ein wichtiger Bestandteil ist.

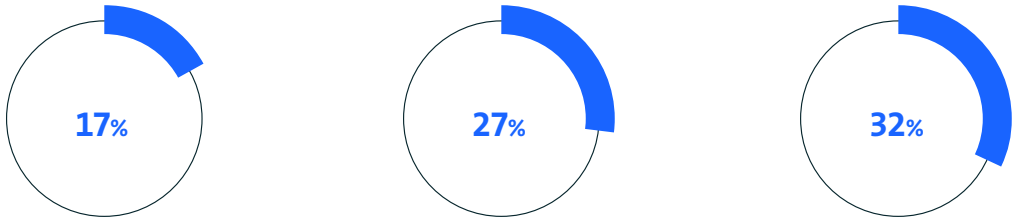
Die Ergebnisse sollen helfen zu verstehen, wie weit Unternehmen, die OSS verwenden, integrieren oder (weiter-) entwickeln, in puncto Standardisierung von OSS-Prozessen derzeit sind.

Wie im Abschnitt der Methodik erwähnt, wurden im Jahr 2019 nur Unternehmen ab 100 Beschäftigten befragt. Die ausgewählten Zeitreihen ab 2019 wurden somit über die Jahre für Unternehmen ab 100 Beschäftigten, die OSS nutzen oder sich an OSS-Projekten beteiligen, ausgewertet.

Der Jahresvergleich von 2021 zu 2023 wurde für diese Unternehmen zusätzlich ab 20 Beschäftigten ausgewertet.

Ein Blick auf die Verfügbarkeit einer OSS-Policy zeigt einen Anstieg um 10 Prozentpunkte vom Jahr 2019 (17 Prozent) zum Jahr 2021 (27 Prozent) (siehe Abbildung 30). Der Anstieg vom Jahr 2021 zum Jahr 2023 flacht jedoch sowohl für Unternehmen ab 100 Beschäftigten (2021: 27 Prozent; 2023: 32 Prozent; siehe Abbildung 30) als auch für Unternehmen ab 20 Beschäftigten (2021: 22 Prozent; 2023: 26 Prozent; siehe Abbildung 31) ab.

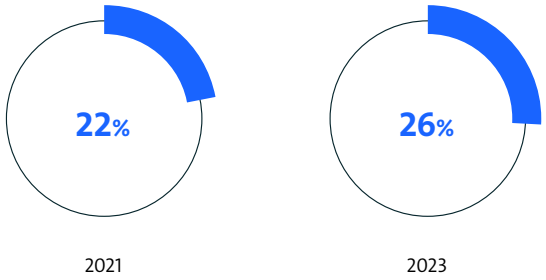
Gibt es in Ihrem Unternehmen eine OSS-Policy, d. h. ein Dokument, in dem Richtlinien und Regeln zum Umgang mit OSS in Ihrem Unternehmen niedergeschrieben sind?



Basis: Alle Unternehmen ab 100 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (2023:n=616 | 2021:n=629 | 2019: n=593) |Quelle: Bitkom Research 2023

Abbildung 30 – Open-Source-Software-Policy im Jahresvergleich seit 2019

Gibt es in Ihrem Unternehmen eine OSS-Policy, d. h. ein Dokument, in dem Richtlinien und Regeln zum Umgang mit OSS in Ihrem Unternehmen niedergeschrieben sind?

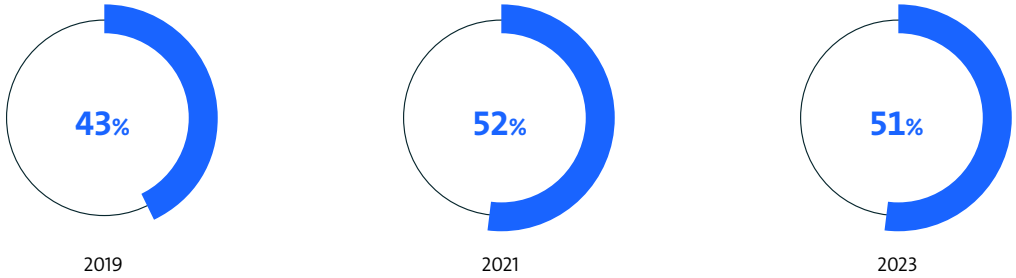


Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (2023:n=809 | 2021:n=843) | Quelle: Bitkom Research 2023

Abbildung 31 – Open-Source-Software-Policy im Jahresvergleich seit 2021

Eine ähnliche Beobachtung ist angesichts der Frage nach einem niedergeschriebenen Compliance-Prozess zu machen. Der Prozentsatz der Unternehmen, die einen Compliance-Prozess für OSS haben, steigt von 43 Prozent im Jahr 2019 auf 52 Prozent im Jahr 2021 (siehe Abbildung 32). Im Jahr 2023 sind im Falle der Compliance-Prozesse allerdings keine Änderungen festzustellen. Die Anteile stagnieren sowohl für Unternehmen ab 100 Beschäftigten (2021: 52 Prozent; 2023: 51 Prozent; siehe Abbildung 32) als auch für Unternehmen ab 20 Beschäftigten (2021: 48 Prozent; 2023: 49 Prozent; siehe Abbildung 33).

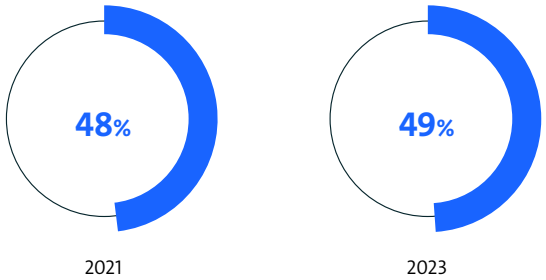
Gibt es in Ihrem Unternehmen einen niedergeschriebenen Compliance-Prozess zum Umgang mit OSS?



Basis: Alle Unternehmen ab 100 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (2023:n=616 | 2021:n=629 | 2019: n=593) | Quelle: Bitkom Research 2023

Abbildung 32 – Open-Source-Software-Compliance-Prozess im Jahresvergleich seit 2019

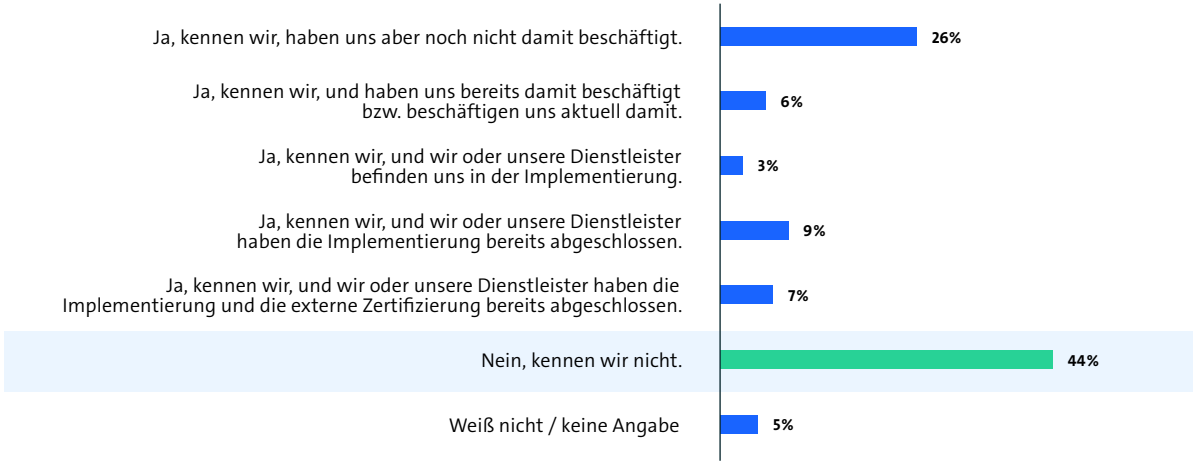
Gibt es in Ihrem Unternehmen einen niedergeschriebenen Compliance-Prozess zum Umgang mit OSS?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln oder sich an OSS beteiligen (2023:n=809 | 2021:n=843) | Quelle: Bitkom Research 2023

Abbildung 33 – Open-Source-Software-Compliance-Prozess im Jahresvergleich seit 2021

Kennen Sie den OpenChain-Standard für OSS-Compliance bzw. die ISO 5230?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln (n=801) | Quelle: Bitkom Research 2023

Abbildung 34 – Bekanntheit OpenChain Standard ISO 5230

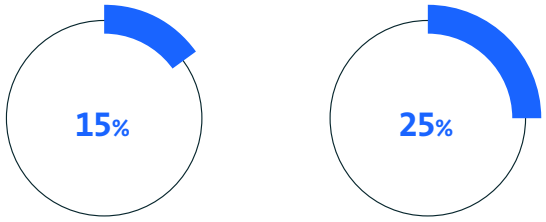
Eine erhöhte Standardisierung durch einen Anstieg an niedergeschriebenen firmeninternen OSS-Policies oder OSS-Compliance-Prozessen ist also seit dem Jahr 2021 nicht zu beobachten. Um ein besseres Bild zum Thema Standardisierung zu erhalten, wurden die Unternehmen mit mindestens 20 Beschäftigten, die OSS verwenden, integrieren oder (weiter-)entwickeln, außerdem zu Standardisierungsmaßnahmen rund um das Compliance-Management von OSS in der Supply Chain befragt.

Um bewährte Compliance-Verfahren für den Einsatz von Open-Source-Software in Unternehmen zu fördern, entwickelte das OpenChain Projekt der Linux Foundation einen Industriestandard für Open-Source-Lizenz-Compliance. Dieser wurde Ende 2020 als internationaler Standard ISO 5230 veröffentlicht. Unter den Unternehmen, die OSS nutzen, kennen die Hälfte (51 Prozent) den OpenChain Standard (siehe Abbildung 34). Allerdings ist zu beachten, dass rund ein Viertel (26 Prozent) der Unternehmen den Standard kennt, sich aber noch nicht weiter damit beschäftigt hat.

6 Prozent haben sich bereits näher damit beschäftigt, beziehungsweise beschäftigen sich aktuell damit. 3 Prozent geben an, dass sie oder ihre Dienstleister sich aktuell in der Implementierungsphase der ISO 5230 befinden. Rund ein Zehntel (9 Prozent) haben die Implementierung des Standards bereits abgeschlossen. Nur 7 Prozent der Unternehmen haben neben der Implementierung auch die externe Zertifizierung abgeschlossen.

Ein wichtiger Bestandteil eines Compliance-Programms ist die vollständige und richtige Identifikation aller OSS-Komponenten und entsprechende Erstellung einer Software Bill of Materials (SBOM). Eine SBOM listet alle Open-Source-Komponenten auf, die in einem Produkt oder einer Software verwendet werden, zusammen mit den dazugehörigen Lizenzinformationen. Die Erstellung einer SBOM ist ein entscheidender Schritt, um Transparenz und Nachvollziehbarkeit bezüglich der verwendeten Open-Source-Komponenten zu gewährleisten.

Welche der folgenden Maßnahmen und Instrumente kommen in Ihrem Unternehmen beim Compliance Management von OSS in der Supply Chain zum Einsatz?



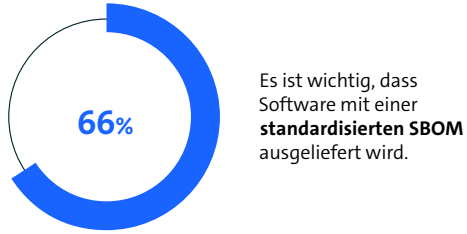
Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln (n=801)
Quelle: Bitkom Research 2023

Abbildung 35 – Einsatz SBOM beim Compliance Management von OSS

Dadurch können Unternehmen leichter erkennen, welche Lizenzen in ihrer Software enthalten sind, welche Lizenzobligationen sie zu erfüllen haben und ob die Verwendung dieser Lizenzen mit den unternehmensinternen Richtlinien und den Lizenzbedingungen der jeweiligen Open-Source-Komponenten in Einklang steht. Unter den Unternehmen, die OSS verwenden, integrieren oder (weiter-) entwickeln, fordern nur 15 Prozent eine SBOM bei eingehenden Software- oder Produktlieferungen (siehe Abbildung 35) ein. Ein Viertel (25 Prozent) der Unternehmen stellen eine SBOM bei allen Produkten bereit.

Standardisierte Compliance Prozesse sind mit Blick auf diese Ergebnisse also nicht mehrheitlich in der Praxis angekommen. Spannend ist allerdings, dass zwei Drittel (66 Prozent) der Unternehmen, die OSS nutzen, aussagen, dass es wichtig wäre, dass OSS mit einer standardisierten SBOM ausgeliefert wird (siehe Abbildung 36). Dies zeigt deutlich, dass der Handlungsbedarf hin zu mehr Standardisierung vom Markt erkannt wird – auch wenn die Umsetzung noch hinterherhängt. Diese Annahme wird dadurch gestützt, dass sich nur knapp die Hälfte (47 Prozent) der Unternehmen gut aufgestellt fühlt, um OSS sicher und bewusst einzusetzen (siehe Abbildung 37).

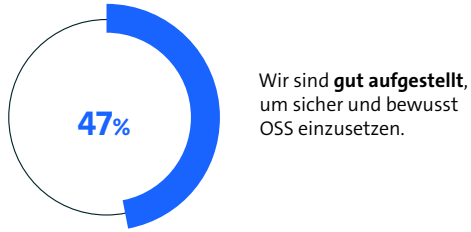
Trifft die folgende Aussage auf Ihr Unternehmen bzw. Ihrer Meinung nach zu?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln (n=801) | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2023

Abbildung 36 – Aussage: SBOM

Trifft die folgende Aussage auf Ihr Unternehmen bzw. Ihrer Meinung nach zu?



Basis: Alle Unternehmen ab 20 Beschäftigten, die OSS verwenden oder integrieren oder (weiter-)entwickeln (n=801) | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2023

Abbildung 37 – Aussage: Bewusster Einsatz OSS

Kooperativer Wettbewerb statt Einzelkämpfertum

Der Mehrwert eines Ökosystems wird umso deutlicher, je detaillierter man das Zusammenspiel aller Komponenten betrachtet. Wie von einer unsichtbaren Hand gesteuert, werden die Interessen und Bedürfnisse unzähliger Akteure in Einklang gebracht und innovative Ideen entwickelt. Open Source ist ein solches Ökosystem, das Entwicklerinnen und Entwickler, Dienstleister und Berater in ihren Projekten dazu befähigt, gemeinsam an neuen Lösungen zu arbeiten. Es erfordert ein offenes und transparentes Mindset, das Einzelkämpfertum durch kollaborative Leistung ersetzt. Dadurch wird es nicht zum Weichspüler für den Unternehmenserfolg, sondern vielmehr zum Beschleuniger des kulturellen Wandels, der Unternehmen zu disruptiven Innovationen befähigt.

Einer der zentralen Vorteile von Open Source ist die effiziente und vor allem unternehmensübergreifende Nutzung von Ressourcen. Er hebelt damit die Grundannahme in der Produktionstheorie aus, mit den im Unternehmen vorhandenen Ressourcen einen maximalen Output erzielen zu müssen. Durch Open Source sind nicht länger die internen Ressourcen der limitierende Faktor, da Unternehmen auf ein ganzes Ökosystem von Innovationen und Lösungen zurückgreifen können.

Dies ermöglicht es, interne Pfadabhängigkeiten aufzulösen, Entwicklungsschritte zu überspringen und an den internationalen Status quo anzudocken. Neben diesem ökonomischen Mehrwert ist es auch aus ökologischer Perspektive sinnvoll, auf Open Source zu setzen: In Zeiten von Ressourcenknappheit und Regulierungsdruck können Unternehmen so nachhaltiger mit Arbeitskräften und Umweltressourcen umgehen.

In der Praxis ist ein transparentes und offenes System oft die Grundvoraussetzung dafür, dass Unternehmen, trotz begrenzter Budgets, komplexe und disruptive IT-Lösungen in ihre Prozesse integrieren können. Das Beispiel Künstliche Intelligenz (KI) zeigt das deutlich. Schon heute sind intelligente Dialogsysteme in der Kundenkommunikation und KI-Systeme in der Industrie zur Automatisierung und Vernetzung von Anlagen im Einsatz. Beide Beispiele erfordern jedoch Lösungen, die mit riesigen Datenmengen umgehen können und sich in die Bestandssoftware und -infrastruktur integrieren lassen. Mit Open Source können Unternehmen hier über Firmengrenzen hinweg von Hochtechnologie profitieren, ohne dass Return on Investment-Berechnungen oder Quick Wins die Rechnung sprengen. Damit wird ein langfristiger Entwicklungsansatz möglich, der nicht auf kurzfristigen Return on Investment angewiesen ist, sondern das große Ganze im Blick hat.

So tragen Ressourceneffizienz und Hochtechnologie zu einem dritten Erfolgsfaktor bei: Innovation im Tagesgeschäft. In der komplexen digitalen Produktion, die heute in vielen Märkten Realität ist, wird es zunehmend schwieriger, innovative Produkte oder Prozesse zu entwickeln und umzusetzen. Eine Neuentwicklung von heute auf morgen zu etablieren, wird den wenigsten Verantwortlichen gelingen. Mit Open Source kann diese Innovationsschwelle deutlich gesenkt werden: Verantwortliche können auf ein ausgereiftes Produkt- und Lösungsportfolio zurückgreifen, anstatt dieses selbst entwickeln zu müssen. So muss niemand das Rad neu erfinden, das andere bereits zur Perfektion gebracht haben. Gemeinsam profitiert man von einem technologischen Status quo, der den nächsten Schritt nach oben in greifbare Nähe rückt.

Dinko Eror
Vice President EMEA Central Europe, Red Hat

OpenSource »Ende-zu-Ende«

Digitalisierung mit Low-Code

Die publicplan GmbH, mit Sitz in Düsseldorf, Berlin und Málaga, realisiert seit 2010 zukunftsfähiges E-Government für die öffentliche Verwaltung. Das Leistungsportfolio reicht dabei von der E-Government-Beratung und Projektbegleitung über die (Weiter-)Entwicklung von Softwarelösungen bis hin zur langfristigen Pflege und Wartung sowie dem Support.
Das Team aus mehr als 200 Expert:innen entwickelt Open-Source-Lösungen mit dem Ziel, Bürgern die Leistungen der Verwaltung zugänglich zu machen – jederzeit, überall und auf jedem Endgerät.

Die Herausforderung
Die »end-to-end«-Digitalisierung ist nach wie vor eine der größten Herausforderungen im öffentlichen Sektor. Viele Verfahren bieten zwar von der Bürger- und Unternehmensseite aus einen digitalen Zugang, wenn man aber denkt, dass nach Absenden des Antrages alles nahtlos digital weiterverarbeitet wird, so ist man auf dem »Holzweg« – und dies im wortwörtlichen Sinne. Viele Anträge werden auf Papier ausgedruckt und gehen dann per Umlaufmappe weiter in den alten, etablierten Geschäftsgang. Dies kostet unnötig viel Zeit und Ressourcen, sowohl beim Antragsteller, aber vor allem bei den Institutionen des öffentlichen Sektors. Digitalisierung sieht anders aus.

Die Lösung
Genau hier setzt die von publicplan eingesetzte Open-Source-Lösung »formsflow.ai« an, die von der Antragsstellung bis hin zur Bescheiderstellung, Rückfragen zum Antragsteller oder auch Ablehnung alles in einem Software-Produkt liefert und dies vollumfänglich auf Low-Code-Basis.

Möglich ist dies durch den Einsatz und der intelligenten Orchestrierung gängiger Open-Source-Softwarekomponenten, die individuell für die jeweiligen Bedarfe von Behörden (oder auch für Kunden aus der Wirtschaft) schnell und modular angepasst werden können – von der Erstellung von Online-Formularen, über Workflows bis hin zur Anbindung von Drittsystemen.

Ganz im Sinne der Low-Code-Philosophie können einfache Anpassungen und Erweiterungen von Administratoren, aber auch von Sachbearbeitern in den einsetzenden Institutionen, nach nur kurzem Einweisen in das System, selbständig umgesetzt werden.

publicplan setzt die Low-Code-Software »formsflow.ai« bereits für Projekte in verschiedenen Bundesländern sowohl für die Digitalisierung interner Prozesse als auch für Förderantragsverfahren und deren interne Weiterverarbeitung erfolgreich ein.

»formsflow.ai« selbst hat eine breite Nutzerbasis in der öffentlichen Verwaltung in Kanada und in anderen Ländern auf dem amerikanischen Kontinent. Die eingesetzten OSS-Komponenten sind bspw. form.io, Camunda, reDash, Robocorp und Keycloack. Die Anbindung von Drittsystemen und das Verknüpfen von Schnittstellen ist durch diesen modularen Aufbau der publicplan Low-Code Lösung auf Open-Source-Basis, abgestimmt auf die individuellen Use-Cases, einfach und flexibel möglich.

publicplan ist Partner für den DACH-Raum
des formsflow.ai-Main-Contributors AOT.

↗ https://www.publicplan.de/loesungen/low-code-loesungen

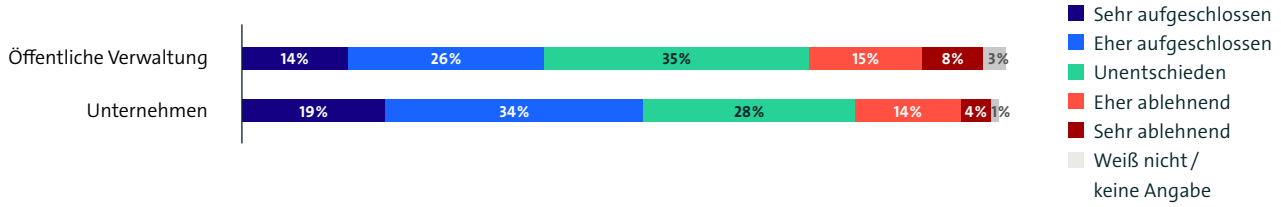
Dr. Christian Knebel
Geschäftsführer, publicplan GmbH

3 Open-Source-Software in der Öffentlichen Verwaltung

Neben Unternehmen der Wirtschaft wurden im Rahmen dieser Studie auch Organisationen der Öffentlichen Verwaltung befragt, um herauszufinden, wie OSS im öffentlichen Sektor genutzt wird. Wie in der Methodik erwähnt, sind die Ergebnisse der Öffentlichen Verwaltung nicht repräsentativ, geben aber ein aufschlussreiches Stimmungsbild. Im Vergleich zur Wirtschaft zeigt sich ein geringeres Interesse an OSS in der Öffentlichen Verwaltung (siehe Abbildung 38).

Nur zwei Fünftel (40 Prozent) der Verwaltungsorganisationen zeigen sich aufgeschlossen für den Einsatz von OSS, während dies für die Hälfte (53 Prozent) der Unternehmen gilt. Ein Drittel (35 Prozent) der Verwaltungsorganisationen ist unentschieden, knapp jede vierte (23 Prozent) Organisation hat eine ablehnende Haltung gegenüber OSS.

Wie steht Ihre Organisation / Ihr Unternehmen generell zum Thema OSS?

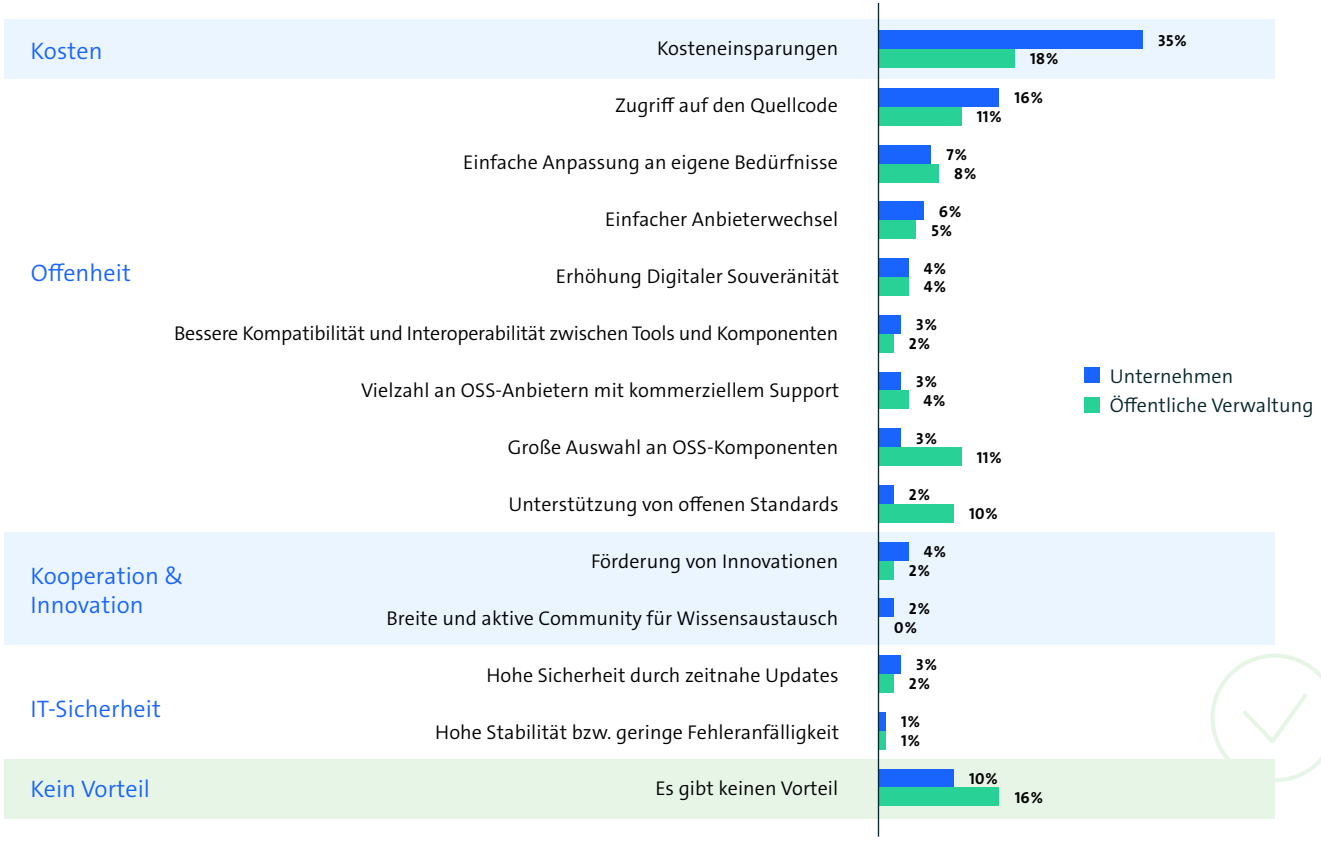


Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) sowie alle Befragten der Öffentlichen Verwaltung (n=102) | rundungsbedingt kann die Summe der Prozentwerte von 100 abweichen | Quelle: Bitkom Research 2023

Abbildung 38 – Einstellung zu Open-Source-Software in der Öffentlichen Verwaltung

Bei Betrachtung der offenen Frage nach dem größten Vorteil für den Einsatz von OSS, stechen die große Auswahl an OSS-Komponenten (11 Prozent) sowie die Unterstützung von offenen Standards (10 Prozent), im Vergleich zu der Wirtschaft heraus (siehe Abbildung 39). Die gesparten Kosten durch die Verwendung von OSS werden zwar insgesamt auch am häufigsten genannt, allerdings liegt der Anteil bei den Verwaltungsorganisationen mit 18 Prozent deutlich unter dem der Wirtschaft (35 Prozent). Gleichzeitig sieht ein größerer Anteil der Organisationen der Öffentlichen Verwaltung explizit keinen Vorteil von OSS (16 Prozent) im Vergleich zur Wirtschaft (10 Prozent).

Was ist aus Ihrer Sicht der größte Vorteil, der für den Einsatz von OSS in Ihrer Organisation / Ihrem Unternehmen spricht?

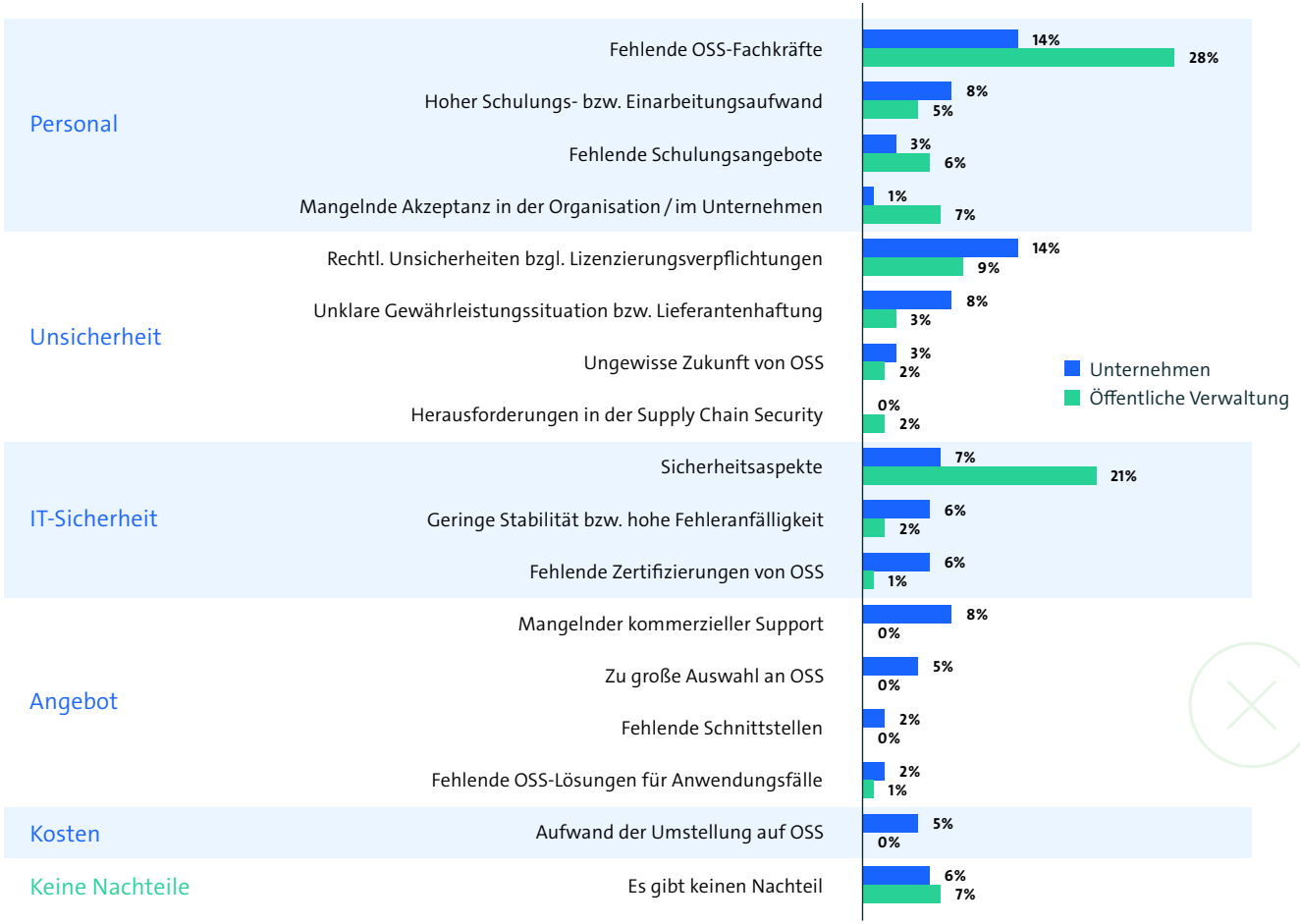


Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) | Offene Abfrage, nur eine Antwort möglich | fehlende Werte: »Weiß nicht / k. A.«
Quelle: Bitkom Research 2023

Abbildung 39 – Vorteile von Open-Source-Software aus Sicht der Öffentlichen Verwaltung

Hinsichtlich des größten Nachteils sind ebenfalls einige Unterschiede zwischen der Wirtschaft und der Öffentlichen Verwaltung zu sehen (siehe Abbildung 40). Mit deutlichem Abstand nennen die Organisationen der Öffentlichen Verwaltung die fehlenden OSS-Fachkräfte (28 Prozent) als Nachteil. Bei den Unternehmen wird dieser Nachteil nur halb so oft (14 Prozent) genannt. Im Vergleich zu Unternehmen der Wirtschaft sticht für Organisationen der Öffentlichen Verwaltung ein weiterer Nachteil besonders hervor: die Sicherheitsaspekte. Ein Fünftel (21 Prozent) der Organisationen der Öffentlichen Verwaltung nennt diesen Nachteil, bei der Wirtschaft sind es nur 7 Prozent.

Was ist aus Ihrer Sicht der größte Nachteil, der gegen den Einsatz von OSS in Ihrer Organisation / Ihrem Unternehmen spricht?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) sowie alle Befragten der Öffentlichen Verwaltung (n=102) | Offene Abfrage, nur eine Antwort möglich | fehlende Werte: »Weiß nicht / k. A.« | Quelle: Bitkom Research 2023

Abbildung 40 – Nachteile von Open-Source-Software aus Sicht der Öffentlichen Verwaltung

Auf der Ebene der OSS-Strategie ist die Öffentliche Verwaltung auf einem ähnlichen Stand wie die Wirtschaft (siehe Abbildung 41). 29 Prozent der Öffentlichen Verwaltungen haben eine OSS-Strategie, bei den Unternehmen sind es 32 Prozent.

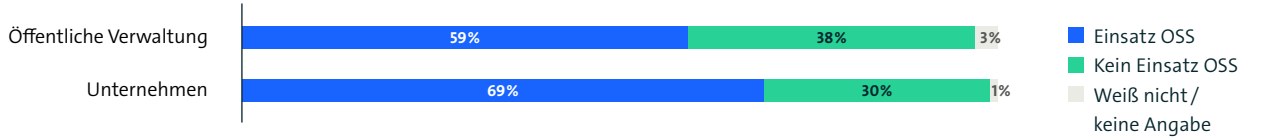
Beim Einsatz von OSS verdoppelt sich diese Zahl – rund sechs von zehn (59 Prozent) der Verwaltungsorganisationen setzen OSS ein (siehe Abbildung 42). Damit liegt die Nutzung von OSS bei den Organisationen 10 Prozentpunkte unter der Nutzung der Unternehmen.

Gibt es in Ihrer Organisation / Ihrem Unternehmen eine Strategie zur Verwendung bzw. zur Beteiligung an OSS?

Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) sowie alle Befragten der Öffentlichen Verwaltung (n=102) | Quelle: Bitkom Research 2023

Abbildung 41 – Open-Source-Software-Strategie in der Öffentlichen Verwaltung

Setzt Ihre Organisation / Ihr Unternehmen OSS ein?



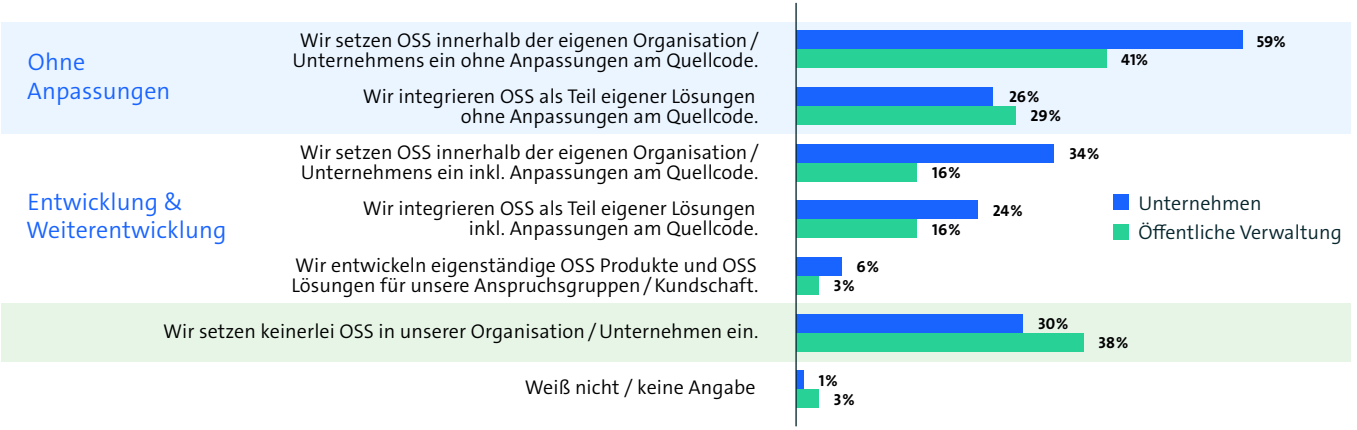
Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) sowie alle Befragten der Öffentlichen Verwaltung (n=102) | Quelle: Bitkom Research 2023

Abbildung 42 – Einsatz Open-Source-Software in der Öffentlichen Verwaltung

In den meisten Fällen wird OSS in der Öffentlichen Verwaltung ohne Anpassungen am Quellcode verwendet (siehe Abbildung 43). Dabei setzen etwa vier von zehn (41 Prozent) Organisationen OSS für die interne Nutzung ein, drei von zehn (29 Prozent) integrieren OSS als Teil eigener Lösungen. Im Vergleich dazu verwenden jeweils 16 Prozent der Verwaltungsorganisationen OSS mit angepasstem Quellcode für interne Zwecke und integrieren sie als Teil eigener Lösungen. Nur 3 Prozent der Organisationen entwickeln eigenständige OSS-Produkte und -Lösungen für ihre Anspruchsgruppen.

6 von 10 (60 Prozent) der Organisationen beteiligen sich an der Entwicklung oder Weiterentwicklung von OSS (siehe Abbildung 44). Im Vergleich zu Unternehmen fällt die Beteiligung etwas höher aus, da sich hier die Hälfte (51 Prozent) an OSS-Projekten beteiligt.

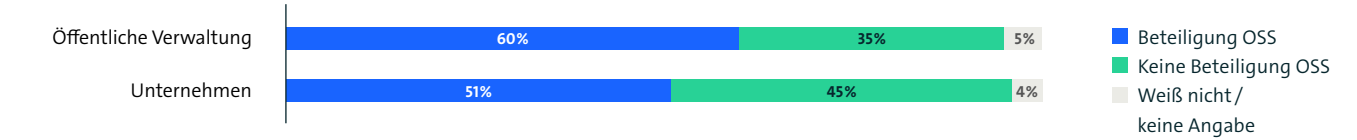
Welche der folgenden Aussagen treffen auf den Einsatz von OSS in Ihrer Organisation / Ihrem Unternehmen zu?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) sowie alle Befragten der Öffentlichen Verwaltung (n=102) | Mehrfachnennungen möglich
Quelle: Bitkom Research 2023

Abbildung 43 – Einsatz von Open-Source-Software nach Art in der Öffentlichen Verwaltung

Beteiligen Sie sich an der Entwicklung bzw. Weiterentwicklung von OSS?

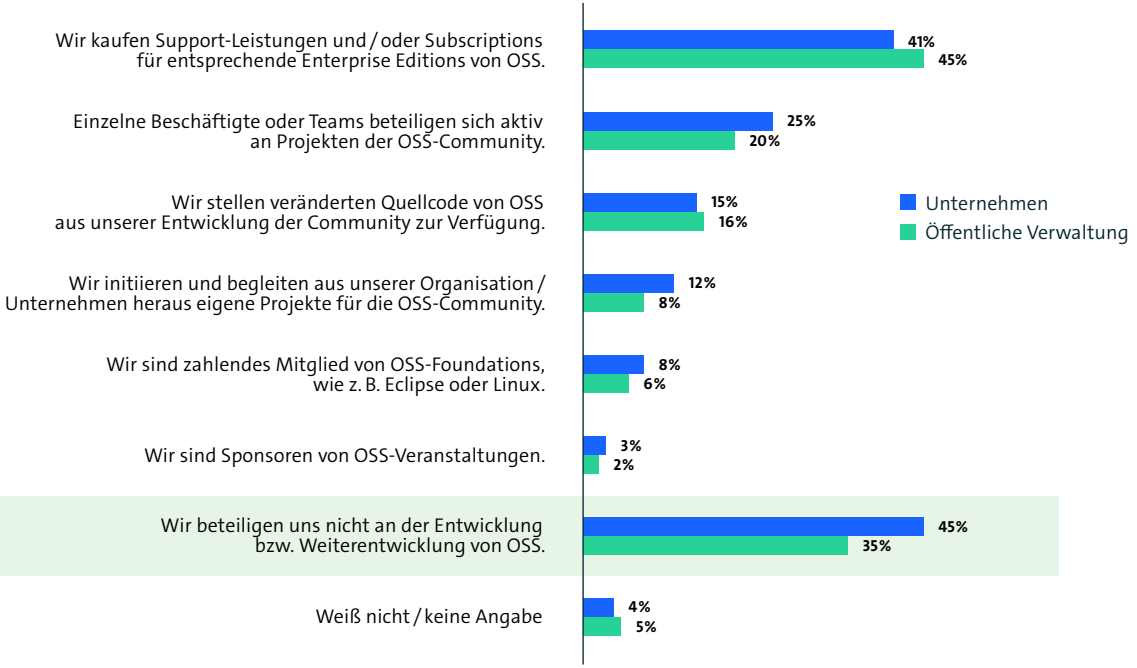


Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) sowie alle Befragten der Öffentlichen Verwaltung (n=102) | Quelle: Bitkom Research 2023

Abbildung 44 – Beteiligung an Open-Source-Software in der Öffentlichen Verwaltung

Ähnlich wie in der Wirtschaft besteht die verbreitetste Art der Beteiligung darin, dass Öffentliche Verwaltungen Support-Leistungen oder Subskriptionen für OSS erwerben (45 Prozent, siehe Abbildung 45).

Inwiefern beteiligt sich Ihre Organisation / Ihr Unternehmen an der Entwicklung bzw. Weiterentwicklung von OSS?

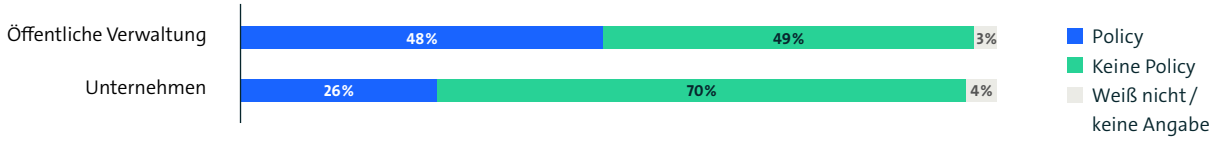


Basis: Alle Unternehmen ab 20 Beschäftigten (n=1.155) sowie alle Befragten der Öffentlichen Verwaltung (n=102) | Mehrfachnennungen möglich
Quelle: Bitkom Research 2023

Abbildung 45 – Beteiligung an Open-Source-Software nach Art in der Öffentlichen Verwaltung

Ein Blick auf die Fragen nach dem Vorhandensein einer niedergeschriebenen OSS-Policy und eines OSS-Compliance-Prozesses zeigt, dass Verwaltungsorganisationen, die OSS nutzen oder sich an OSS-Projekten beteiligen, der Wirtschaft hier etwas voraus sind (siehe Abbildung 46 und Abbildung 47). Während jedes vierte (26 Prozent) Unternehmen eine OSS-Policy hat, sind es bei den Organisationen der Öffentlichen Verwaltung knapp die Hälfte (48 Prozent). Bei den Compliance-Prozessen ist der Abstand nicht ganz so groß. Trotzdem liegen die Verwaltungen hier mit 56 Prozent 7 Prozentpunkte vor der Wirtschaft.

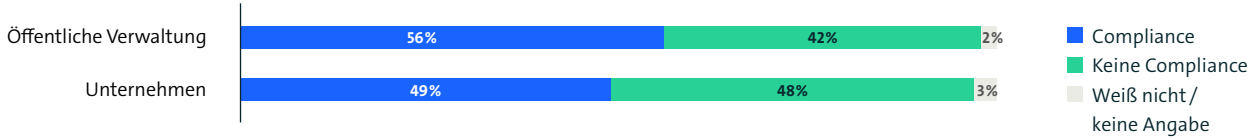
Gibt es in Ihrer Organisation / Ihrem Unternehmen eine OSS-Policy, d. h. ein Dokument, in dem Richtlinien und Regeln zum Umgang mit OSS in Ihrem Unternehmen niedergeschrieben sind?



Basis: Alle Unternehmen ab 20 Beschäftigten (n=809) sowie alle Befragten der Öffentlichen Verwaltung (n=65), die OSS verwenden oder integrieren oder (weiter-) entwickeln oder sich an OSS beteiligen | Quelle: Bitkom Research 2023

Abbildung 46 – Open-Source-Software-Policy in der Öffentlichen Verwaltung

Gibt es in Ihrer Organisation / Ihrem Unternehmen einen niedergeschriebenen Compliance-Prozess zum Umgang mit OSS?



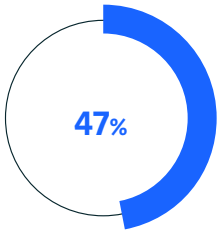
Basis: Alle Unternehmen ab 20 Beschäftigten (n=809) sowie alle Befragten der Öffentlichen Verwaltung (n=65), die OSS verwenden oder integrieren oder (weiter-) entwickeln oder sich an OSS beteiligen | Quelle: Bitkom Research 2023

Abbildung 47 – Open-Source-Software-Compliance-Prozess in der Öffentlichen Verwaltung

Unter den Organisationen, die OSS verwenden, integrieren oder (weiter-)entwickeln, liegt der Anteil der Organisationen, die sich gut aufgestellt fühlen, um sicher und bewusst OSS einzusetzen, mit 47 Prozent exakt so hoch wie bei der Wirtschaft (siehe Abbildung 48).

Allerdings zeigt sich bei den Aussagen erneut ein deutlicher Unterschied beim Thema Compliance. Neun von zehn (90 Prozent) der Organisationen finden es wichtig, dass OSS mit einer standardisierten SBOM ausgeliefert wird. Unter den Unternehmen waren es nur zwei Drittel (66 Prozent, siehe Abbildung 49).

Welche der folgenden Aussagen treffen auf Ihre Organisation / Ihr Unternehmen bzw. Ihrer Meinung nach zu?



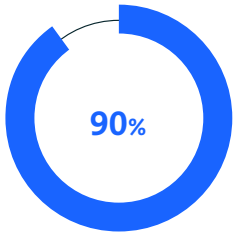
Wir sind **gut aufgestellt**, um sicher und bewusst **OSS einzusetzen**.

(Wirtschaft: 47%)

Basis: Alle Unternehmen ab 20 Beschäftigten (n=801) sowie alle Befragten der Öffentlichen Verwaltung (n=60), die OSS verwenden oder integrieren oder (weiter-)entwickeln | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2023

Abbildung 48 – Aussagen: Bewusster Einsatz OSS Öffentliche Verwaltung

Welche der folgenden Aussagen treffen auf Ihre Organisation / Ihr Unternehmen bzw. Ihrer Meinung nach zu?



Es ist wichtig, dass Software mit einer **standardisierten SBOM** ausgeliefert wird.

(Wirtschaft: 66%)

Basis: Alle Unternehmen ab 20 Beschäftigten (n=801) sowie alle Befragten der Öffentlichen Verwaltung (n=60), die OSS verwenden oder integrieren oder (weiter-)entwickeln | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2023

Abbildung 49 – Aussagen: SBOM Öffentliche Verwaltung

Vorreiter für Open Source

Das IT-Dienstleistungszentrum Berlin (ITDZ Berlin) als zentraler IT-Dienstleister des Landes Berlin forciert den Einsatz von Open-Source-Software (OSS). Drei Viertel der Server- und Datenbankinfrastruktur des ITDZ Berlin sind inzwischen Open Source. Die strategische Ausrichtung auf OSS bildet eine wichtige Grundlage für den sicheren und stabilen Betrieb der Infrastruktur und ermöglicht so den Einsatz moderner Informations- und Kommunikationstechnologien in der Berliner Verwaltung.

Mehr Open Source wagen

OSS hat das Potenzial, die Art und Weise, wie die öffentliche Verwaltung arbeitet und mit den Bürgerinnen und Bürgern interagiert, grundlegend zu verbessern.

Für eine digital souveräne Stadt sind Open Source und offene Standards unverzichtbar. Das Land Berlin verfolgt daher den Ansatz »Public Money for Public Code« und stellt Open Source in den Mittelpunkt seiner IT-Lösungen.

Durch die hohe Anpassungsfähigkeit von OSS können Anforderungen der Verwaltung schneller und flexibler umgesetzt werden, was zu einer effizienteren Verwaltungsarbeit führt. Gleichzeitig basiert der Open-Source-Ansatz auf Transparenz und Mitgestaltung und stärkt damit das Vertrauen der Bürgerinnen und Bürger in Staat und Verwaltung.

- Digitale Souveränität dank offener Standards und Interoperabilität
- Erhöhung der Transparenz und des Vertrauens in Staat und Verwaltung
- Schnellere und effizientere Erstellung von Verwaltungsanwendungen

Die Zukunft

Laut Open Source Monitor setzt nicht nur die Mehrheit der Verwaltungen in Deutschland bereits OSS ein, sondern beteiligt sich auch an der Weiterentwicklung. Häufig fehlt es jedoch noch an Ressourcen, um die vorhandenen Potenziale voll auszuschöpfen und den Anteil der OSS-Nutzung weiter zu erhöhen.

Hier setzt das ITDZ Berlin an: Um das Know-how von wirtschaftlichen, zivilgesellschaftlichen und wissenschaftlichen Akteuren zu bündeln und der Berliner Verwaltung zentral zur Verfügung zu stellen, baut das ITDZ Berlin in seiner Verantwortung ein Open-Source-Kompetenzzentrum auf. Dieses ermöglicht als Teil eines Open-Source-Ökosystems die effiziente Nutzung von Ressourcen, die Förderung von Innovationen und die effektive Nachnutzung vorhandener Lösungen.

Die Bereitstellung von Quellcode auf »Open CoDE«, der gemeinsamen Plattform der öffentlichen Verwaltung, fördert dabei die Nachnutzung und das gemeinsame Arbeiten an Softwarelösungen der öffentlichen Verwaltung.

Digitalisierung souverän und sicher gestalten

Torsten Hallmann
Head of Public Affairs
SUSE

Bundes-CIO Dr. Markus Richter brachte es vor wenigen Monaten auf den Punkt: »Gerade vor dem Hintergrund der aktuellen geopolitischen Lage ist die Förderung von Open-Source-Software und die Stärkung der Digitalen Souveränität wichtiger denn je«, sagte er anlässlich der Gründung des Zentrums für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS).

Das ZenDiS ist als Plattform, Impulsgeber und Innovationstreiber für eine technologisch unabhängige Verwaltung in Deutschland zu sehen. Die Ergebnisse des aktuellen Open-Source-Monitors zeigen, dass es durchaus Bedarf für eine zentrale Anlaufstelle gibt, die die öffentliche Verwaltung bei der Umsetzung von Open Source-Strategien unterstützt. So stehen derzeit nur 40 Prozent der Befragten in Verwaltungseinrichtungen dem Thema Open Source aufgeschlossen gegenüber.

Aufklärung und Sensibilisierung für das Thema Open Source dürften daher in Zukunft zu den wichtigsten Aufgaben des ZenDiS gehören.

Erfolgreich vorantreiben lassen sich Open-Source-Strategien in der Verwaltung aber nur, wenn es intern klare Zuständigkeiten gibt. Auch hier weist der Open-Source-Monitor auf großen Nachholbedarf hin: In 70 Prozent der befragten Einrichtungen gibt es keinen Verantwortlichen für das Thema Open Source. In den übrigen Organisationen werden Open-Source-Initiativen oft eher informell von der IT-Leitung mitbetreut.

Die mangelnde Zuständigkeit spiegelt sich auch im Nichtvorhandensein einer Strategie wider: Knapp 69 Prozent der öffentlichen Verwaltungseinrichtungen haben derzeit überhaupt keine Open-Source-Strategie. Nicht einmal jede siebte Organisation (14 Prozent) verfügt über eine bereichsübergreifende Strategie zum Einsatz von Open-Source-Software (OSS). Andererseits sind Open-Source-Lösungen aus dem Alltag vieler Verwaltungseinrichtungen nicht mehr wegzudenken: 59 Prozent der Befragten gaben an, bereits heute Open- Source-Software einzusetzen. Die größten Hürden für einen weiteren Ausbau von Open-Source-Initiativen sind aus Sicht der öffentlichen Verwaltung die fehlenden Fachkräfte (28 Prozent) und Sicherheitsaspekte (21 Prozent).

Um Sicherheitsbedenken im öffentlichen Sektor auszuräumen und das Vertrauen in OSS zu stärken, sind transparente und sichere Softwarelieferketten unerlässlich. Die US-Regierung verlangt von ihren Lieferanten bereits seit 2021 eine Software Bill of Materials (SBOM). Diese Inventarliste gibt an, welche Komponenten und Bibliotheken in eine Software eingeflossen sind. In Deutschland dürften vor allem im KRITIS -Sektor schon bald SBOMs für alle eingesetzte Softwareprodukte verpflichtend sein.

Darüber hinaus werden auch durch das BSI ausgestellte Sicherheitszertifizierungen wie Common Criteria EAL4+ als Nachweis der Standardkonformität an Bedeutung gewinnen. Dabei sollten Einrichtungen immer darauf achten, dass der gesamte Entwicklungsprozess eines Softwareprodukts inkl. Fehlerbeseitigung bei der Zertifizierung berücksichtigt wird.

Im aktuellen Open-Source-Monitor sehen nur 4 Prozent der Befragten die digitale Souveränität als größten Vorteil von OSS. Jedoch kann die Verwaltung nur mit Open-Source-Initiativen wie Open CoDE und dem Souveränen Arbeitsplatz die Abhängigkeit von einzelnen Technologieanbietern reduzieren und mehr Handlungsfähigkeit zurückgewinnen. Entscheidend ist dabei, dass sich die Einrichtungen auf die Sicherheit der OSS verlassen können und diese flexibel und unter eigener Kontrolle an jedem Ort einsetzen können.

4 Zukunfts-perspektiven für Open-Source-Software

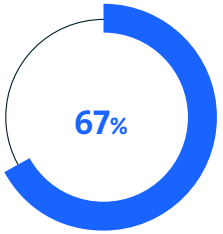
Dr. Frank Termer
Bereichsleiter Software Bitkom

Die Zukunftsperspektiven von OSS in Deutschland sind vielversprechend. Immer mehr Unternehmen und Organisationen erkennen die Vorteile von OSS-Lösungen und wissen diese zu nutzen. Dabei agieren sie nicht nur als reine »Konsumenten« von OSS, sondern erkennen ihre Verantwortung für das Open-Source-Ökosystem und bringen sich durch aktive Mitarbeit und inhaltliche Beiträge in die Open-Source-Community ein. Insbesondere die öffentliche Hand hat diesen Weg eingeschlagen und bekennt sich zunehmend zu ihrer Verantwortung, aktiver Teil der OSS-Community zu sein, um diese weiterzuentwickeln und eigene Vorteile zu realisieren. Damit trägt OSS auch zur Stärkung der digitalen Souveränität bei, da europäische Unternehmen und Institutionen die Kontrolle über ihre digitalen Infrastrukturen behalten oder wiedererlangen wollen. Sie ermöglicht kleinen und mittleren Unternehmen den Einsatz kostengünstiger und dennoch leistungsfähiger Lösungen und stärkt damit ihre Wettbewerbsfähigkeit. Diese Entwicklung wird sich mit Sicherheit weiter fortsetzen.

Europa ist Teil einer weltweiten Bewegung, die Open-Source-Software als Katalysator für digitale Innovation und Zusammenarbeit betrachtet. Die Zusammenarbeit zwischen europäischen und internationalen Akteuren im Bereich Open Source stärkt die globale Vernetzung und ermöglicht einen effizienten Austausch von Wissen und Ressourcen.

Open Source und OSS werden daher wichtige Bausteine sein, um die vielversprechenden Transformationspotenziale z. B. in den Bereichen Bildung, Gesundheit oder Verwaltung, aber auch bei sozialen Innovationen zu nutzen. Beim Blick in die Zukunft zeigt der Open Source Monitor, dass rund zwei Drittel (67 Prozent) der OSS-nutzenden Organisationen der öffentlichen Hand davon ausgehen, dass die Bedeutung von OSS für ihre Organisation zunehmen wird. Bei den OSS-nutzenden Unternehmen ist es nur knapp die Hälfte (47 Prozent) (siehe Abbildung 50).

Welche der folgenden Aussagen treffen auf Ihre Organisation / Ihr Unternehmen bzw. Ihrer Meinung nach zu?



Die **Bedeutung von OSS** wird in unserer Organisation / unserem Unternehmen zunehmen.

(Wirtschaft: 47%)

Basis: Alle Unternehmen ab 20 Beschäftigten (n=801) sowie alle Befragten der Öffentlichen Verwaltung (n=60), die OSS verwenden oder integrieren oder (weiter-)entwickeln | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2023

Abbildung 50 – Aussagen: Bedeutung von OSS Öffentliche Verwaltung

Diese Diskrepanz ist vermutlich darauf zurückzuführen, dass viele Unternehmen Open Source bereits heute eine hohe Bedeutung beimessen, die nicht weiter gesteigert werden kann. Im Bereich des Public Sector ist zu vermuten, dass dieser Reifegrad in Sachen Open Source noch nicht erreicht ist und daher noch ein entsprechender Auf- und Nachholbedarf besteht. Hier wird es spannend sein, die weitere Entwicklung zu beobachten.

Obwohl die Zukunft vielversprechend aussieht, gibt es noch viele Herausforderungen für den Einsatz und die Entwicklung von OSS. Eine der wichtigsten ist die Sicherstellung einer ausreichenden Finanzierung und Unterstützung von Open-Source-Projekten. Initiativen wie der Sovereign Tech Fund sind ein Schritt in die richtige Richtung, aber es bedarf weiterer Anstrengungen, um OSS als festen Bestandteil unserer digitalen Landschaft zu etablieren. Europa muss sicherstellen, dass es bestehende Abhängigkeiten von außereuropäischen Technologieanbietern reduziert und in der Lage ist, eigene digitale Infrastrukturen zu entwickeln, zu pflegen und zu sichern. Dies erfordert nicht zuletzt gezielte Investitionen in Open-Source-Lösungen und eine enge Zusammenarbeit zwischen öffentlichem Sektor, Industrie und Forschung.

Die Debatten der letzten Jahre zeigen, dass wir in der Diskussion um Open Source an einem neuen Punkt angelangt sind. Ging es in der Vergangenheit darum, dass sich Unternehmen gezielt von oder zu Open Source abgrenzten oder sich umgekehrt sehr stark zu Open Source bekannten, geht es heute nicht mehr um die Frage, ob Open Source besser, sicherer oder kostengünstiger als proprietäre Software ist, sondern es wird diskutiert, welche Rolle OSS in der digitalen Transformation spielt und welchen Stellenwert sie einnehmen kann. Folglich müssen sich alle Unternehmen mit der Frage auseinandersetzen, wie der individuelle Beitrag zum Gelingen der Digitalen Transformation als gesellschaftliche Aufgabe aussieht. Die Chancen von OSS stehen dabei klar im Vordergrund. Ob Staaten, Unternehmen oder Individuen: Gemeinsam müssen wir die Chancen von OSS erkennen und nutzen. Es liegt an jedem Einzelnen von uns, OSS zu unterstützen, zu nutzen und sich aktiv an der Weiterentwicklung der OSS-Community zu beteiligen. Indem wir Open Source als wichtigen Motor für Innovation und Fortschritt fördern, können wir eine starke und nachhaltige digitale Zukunft für Deutschland, Europa und die Welt gestalten.

Impressum

Herausgeber
Bitkom e.V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner
Greta Schnaack
Senior Research Consultant Bitkom Research
T 030 27576-194 | g.schnaack@bitkom-research.de

Dr. Frank Termer
Bereichsleiter Software Bitkom
T 030 27576-232 | f.termer@bitkom.org

Gestaltung
Sabrina Flemming | Bitkom

Bildnachweis
Titelbild © Umberto – unsplash.com

Autorenschaft
Greta Schnaack | Bitkom Research
Dr. Frank Termer | Bitkom

Redaktion
Greta Schnaack | Bitkom Research
Dr. Frank Termer | Bitkom

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Bitkom e.V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom