Die Trittbrettfahrer

Wie Behörden und ihre Auftragnehmer Open-Source-Software ausbeuten

Immer mehr Behörden setzen auf freie Software. Doch häufig beauftragen sie Dumpinganbieter, die dem Open-Source-Ökosystem schaden. Auch der Steuerzahler zahlt am Ende oft drauf.

Von Christian Wölbert

Man könnte meinen, in Deutschland herrschen goldene Zeiten für Open-Source-Entwicklerfirmen, wütet doch Donald Trump im Weißen Haus schlimmer denn je. Immer mehr Behörden erwägen deshalb, ihre Abhängigkeit von US-Konzernen wie Microsoft und Cisco zu verringern und auf Open-Source-Software umzusteigen.

Doch paradoxerweise profitieren die Unternehmen, die Open-Source-Software entwickeln, nur selten vom Trend zu „digitaler Souveränität“ im öffentlichen Sektor. Es komme immer wieder vor, dass Trittbrettfahrer ihre Software übernehmen und dann „mithilfe von Dumpingangeboten eine Ausschreibung gewinnen“, beklagte Mitte Februar die Open Source Business Alliance (OSBA), ein Verband von Open-Source-Firmen.

Den OSBA-Mitgliedern geht es dabei nicht nur um den entgangenen Umsatz. Die Dumpinganbieter kalkulierten „häufig keinen ausreichenden Support und keine ausreichenden Aufwände für Weiterentwicklung, Pflege oder Upstream-Veröffentlichung der Software ein“, warnt der Verband. Wenn die Projekte scheitern, müssten die etablierten Open-Source-Firmen das Problem ausbaden. Die Misserfolge schadeten dem „Ruf der gesamten Open-Source-Community“.

Das HessenConnect-Debakel

Manchmal werden die Entwicklerfirmen von den Trittbrettfahrern sogar mit „parasitären Supportfragen“ überhäuft, wie der Open-Source-Unternehmer Peer Heinlein es in einer Präsentation formuliert. Er spricht vom „Kuckuck im Bieterverfahren“, der die Software der Entwicklerfirmen zu einem „Kampfpreis unter den echten Herstellungskosten“ anbiete, ohne diese als Partner für Wartung, Weiterentwicklung oder Support zu beteiligen. Das sei zwar legal, widerspreche aber den Gepflogenheiten der Branche und gefährde letztlich die Existenz der Entwicklerfirmen und ihrer Software.

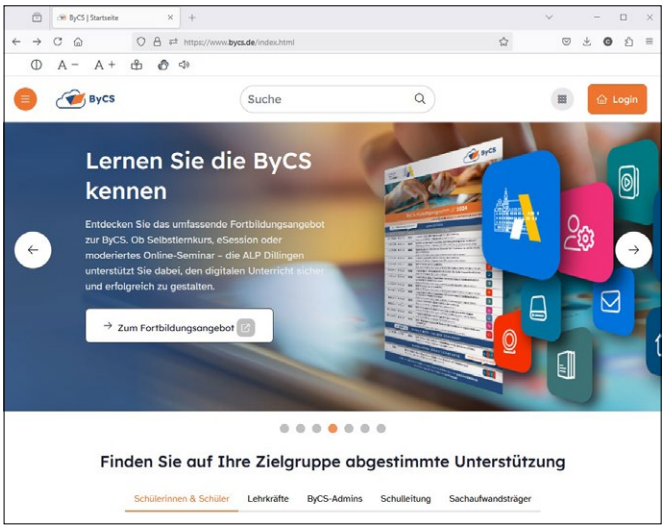
Eine Ursache des Problems liegt darin, dass viele Politiker sich zwar als Open-Source-Verfechter sehen, die Branche jedoch kaum kennen. Gegenüber der OSBA berichtete ein Open-Source-Hersteller anonym von einem bizarren Gespräch: „Vor anderthalb Jahren hat mir der CIO eines Bundeslandes zum Deal für die Videoarbeitsplätze mit unserer Software gratuliert und geschwärmt, dass er ein großer Open-Source-Verfechter sei. Ich wusste zuerst nicht, wovon er sprach, und dann stellte sich heraus, dass das Unternehmen xyz mit unserer Software eine Ausschreibung gewonnen hat.“

Doch bei dem Thema geht es nicht nur um die Interessen der Open-Source-Lobby. Auch die Steuerzahler sind am Ende oft die Dummen.

Beobachten ließ sich das zum Beispiel in Hessen. 2022 kündigte das Bundesland an, von Microsofts Skype for Business auf „Open-Source-Lösungen von Element/Matrix und Jitsi unter einer einheitlichen Oberfläche“ umzusteigen. Die Pressemitteilung las sich so, als sei an dem Projekt namens „HessenConnect 2.0“ auch die Element Software GmbH beteiligt. Das ist die deutsche Niederlassung der Firma, die Matrix-Software wie den Chatserver Synapse und die Element-Clients maßgeblich entwickelt.

Die Ausschreibung hatte jedoch die Telekom-Tochter T-Systems gewonnen. Diese arbeitete im Rahmen des Projektes nicht mit Element zusammen, sondern mit anderen Unternehmen. Die T-Systems und ihre Partner bedienten sich am Open-Source-Code und begannen mit der Entwicklung zahlreicher Zusatzfunktionen und Optimierungen, die das Land Hessen forderte. Spätestens am 1. Januar 2025 sollte HessenConnect 2.0 auf 35.000 IT-Arbeitsplätzen der hessischen Behörden eingeführt werden, denn zu diesem Zeitpunkt liefen die Skype-Lizenzen aus.

Doch kurz vor Weihnachten 2024 teilte das hessische Digitalministerium überraschend mit, HessenConnect 2.0 sei „zum aktuellen Zeitpunkt nicht einsatzbereit“. Daher führe man nun Webex von Cisco als „Übergangslösung“ ein. Auf Nachfrage von c’t erläuterte das Ministerium, T-Systems habe die Anforderung der Anwenderfreundlichkeit „nicht überzeugend und umfassend erfüllt“. T-Systems und einer der beteiligten Sub-Auftragnehmer wollten sich auf Anfrage von c’t nicht öffentlich zu dem Thema äußern.



Zur „BayernCloud Schule“ gehört ein Messenger auf Matrix-Basis. Bayern nutzt allerdings eine seit Ende 2023 veraltete Version des Chatservers.

Der Steuerzahler zahlt also nun doppelt: erstens für das HessenConnect-2.0-Projekt, zweitens für die ungeplanten Webex-Lizenzen. Und nicht nur das: Die zahlreichen Optimierungen, die die Telekom und ihre Subunternehmen entwickelt haben, flossen nicht „upstream" in den Code der Element-Clients und der Serversoftware Synapse ein. Die Wahrscheinlichkeit ist deshalb groß, dass dieselben oder ähnliche Features im Auftrag anderer Behörden noch einmal entwickelt werden. Der Steuerzahler würde also auch für die Optimierungen doppelt zahlen.

Trittbrettfahrer als Sicherheitsrisiko

Ein ähnlicher Fall spielt in Bayern. Als das Bundesland eine Messenger-Anwendung für seine „BayernCloud Schule" (ByCS) ausschrieb, setzte sich ein Tandem aus dem IT-Konzern Fujitsu und dem Koblenzer Unternehmen Sdui durch. Sdui übernahm den Quellcode der Element-Clients und des Synapse-Servers und entwickelte im Auftrag Bayerns Anpassungen. Die Quelltexte dieser Anpassungen wurden ebenfalls nicht der Matrix-Community übergeben.

Die Anpassungen seien „speziell auf die Bedürfnisse der bayerischen Schulen zugeschnitten", eine Bereitstellung ergäbe deshalb „keinen konkreten Nutzen für Produkte außerhalb der ByCS", rechtfertigte sich das bayerische Kultusministerium auf Anfrage. Diese Argumentation kann man hinterfragen, denn zu den Anpassungen gehörte laut Ministerium beispielsweise auch eine „PIN-Sperre für einzelne Räume zur Erhöhung der Sicherheit".

Sogar zu Sicherheitsrisiken kann die Trittbrettfahrerei führen. Denn wenn Dumpinganbieter bekannte Lücken nicht schnell genug schließen oder die Software ungeschickt konfigurieren, steigt die Gefahr von Datenlecks und Hackerangriffen.

Im Fall des bayerischen Schul-Messengers fällt auf, dass der dort verwendete Chatserver noch bei Redaktionsschluss auf Version 1.97.0 von Synapse basierte, die seit Dezember 2023 veraltet ist. Im Hauptzweig von Synapse hat Element seitdem zahlreiche Sicherheitslücken geschlossen, darunter zwei als schwerwiegend eingestufte.

Das Kultusministerium sieht dennoch kein Problem darin, die alte Version einzusetzen. Dies sei „Teil einer bewussten Strategie". Die Sicherheitslücken beträfen die bayerische Konfiguration nicht oder es seien keine Auswirkungen zu erwarten. Updates würden aber kontinuierlich evaluiert, obendrein habe das Landesamt für Sicherheit in der Informationstechnik das System getestet und freigegeben.

Bei Forks wie in Bayern oder Hessen gilt jedoch grundsätzlich: Je tiefgehender und umfangreicher die Anpassungen, desto aufwendiger wird es, Sicherheitspatches und andere Updates aus der Community einzubauen.

Patrick Alberts, der Produktchef der Entwicklerfirma Element, sorgt sich deshalb, dass die Strategie des Ministeriums „nicht nachhaltig ist und irgendwann zu einem Cybervorfall in den Schulen führen könnte". Darunter würde dann auch die Marke Matrix leiden und „Open Source insgesamt als mal wieder nicht so sicher abgestempelt", sagte er im Gespräch mit c't.

Sdui antwortete auf die Frage von c't nach konkreten Beispielen für Vertragsbeziehungen zu Open-Source-Herstellern nur ausweichend. Man gehe auf Anforderungen der Bundesländer ein und richte sich nach den entsprechenden öffentlichen Ausschreibungen, erklärte das Unternehmen.

Die c't-Recherchen scheinen nun ein Umdenken in Bayern ausgelöst zu haben. Das Kultusministerium teilte mit, dass der beauftragte Dienstleister – gemeint ist Sdui – sich mit der Element Software GmbH in Gesprächen über eine mögliche Zusammenarbeit befinde. „Dies ist insbesondere aufgrund der Größe und Bedeutung des Projekts erforderlich, um langfristige Wartung und Weiterentwicklung zu gewährleisten." Ob Sdui und Element künftig tatsächlich kooperieren, war bis Redaktionsschluss nicht absehbar.

Sdui ist auch bei weiteren Ausschreibungen von Behörden zum Zug gekommen. Zum Beispiel stellt das Unternehmen für das Land Berlin eine Videokonferenzlösung auf Basis der Open-Source-Anwendung BigBlueButton bereit.

Die OSBA hofft nun, dass Behörden ihre Ausschreibungen künftig so gestalten, dass Dumpinganbieter nicht mehr im Vorteil sind. In einem Positionspapier (ct.de/yb76) schlägt der Verband Kriterien für die „nachhaltige Beschaffung von Open-Source-Software" vor. Die Behörden sollen künftig zum Beispiel prüfen, ob der Anbieter eine Geschäftsbeziehung zum Softwarehersteller hat, ob er Änderungen an der Software im Sinne des Grundsatzes „Public Money, Public Code" für die Allgemeinheit verfügbar macht und ob er einen hochwertigen Support leisten kann.

Manche Behörden setzen solche Kriterien bereits heute um. Als Positivbeispiel gilt in der Open-Source-Community etwa das Zentrum für digitale Souveränität (ZenDiS), das bei der Entwicklung seiner Web-Office-Suite mit Entwicklern wie Nextcloud, Univention und Open-X-Change zusammenarbeitet. Aber auch die Bundesländer Schleswig-Holstein und Thüringen werden von Entwicklern häufig als Positivbeispiele genannt. *(cwo@ct.de)* c't

OSBA-Forderungen: ***ct.de/yb76***