Newsletter für Engagement und Partizipation in Deutschland
11/2021

Hendrik vom Lehn

Digitale Infrastruktur für die Zivilgesellschaft – Gedanken zur Rolle von Open-Source-Software und Datenschutz

Die unsichtbare Infrastruktur

Die Zivilgesellschaft ist im Digitalen angekommen. Auch schon vor der COVID-19-Pandemie war es für viele Vereine und anderweitig organisierte Gruppen Alltag, sich über digitale Kanäle auszutauschen und zu organisieren. Aber spätestens seit letztem Jahr führt kaum noch ein Weg hieran vorbei und vormals rein zusätzliche, digitale Kommunikationsmöglichkeiten sind derzeit Standard.

Da vieles von dem, was wir im Digitalen tun, alltäglich ist, kann man leicht vergessen, welcher Hilfsmittel wir uns hierzu bedienen. Webseiten, E-Mail, eine gemeinsame Dateiablage, die digitale Vereinsverwaltung, E-Mail-Newsletter, Videokonferenztools oder geteilte Whiteboards zur gleichzeitigen Zusammenarbeit. All das kommt nicht aus einfach aus »der Cloud«, sondern ist eine Form von Infrastruktur, dessen Existenz wir uns verdeutlichen sollten.

Beim Begriff der digitalen Infrastruktur liegt der Gedanke an Glasfaserkabel nahe. In diesem Beitrag ist mit digitaler Infrastruktur jedoch nicht die Ebene des Netzzugangs gemeint. Hier gemeint sind vor allem webbasierte Dienste, welche einzeln oder im Zusammenspiel die von uns allen täglich genutzten Internetdienste bilden.

Unter dem Titel »Digitale Souveränität – Ein Plädoyer für die Open-Source-Gesellschaft« hat Teresa Staiger, Referentin im Projekt »Forum Digitalisierung und Engagement« des BBE, vor wenigen Monaten in diesem Newsletter auf die Vorteile von Open-Source-Software für den Aufbau einer solchen Infrastruktur hingewiesen. Dabei geht es vor allem um die digitale Souveränität, sodass Abhängigkeiten von einigen wenigen Akteur:innen vermieden werden.

Open Source und Datenschutz – untrennbar verbunden?

Ein Aspekt der im Zusammenhang mit Open-Source-Software immer wieder genannt wird, sind Vorteile im Hinblick auf Datenschutz. Während Anbieter proprietärer Software-Lösungen oftmals ein starkes Interesse an datengetriebener Nutzungsanalyse ihrer Software haben oder sogar detaillierte Nutzerprofile erstellen, um mittels Werbung ein Einkommen für ihren Dienst zu generieren, benötigen die Entwickler:innen von Open-Source-Software solche Daten in der Regel nicht. Hinzu kommt, dass die Nutzer:innendaten bei proprietären Cloud-Diensten auf den Servern der Anbieter liegen, wohingegen Open-Source-Software eine freie Wahl des Server-Standortes und auch der Softwarekonfiguration ermöglicht.

Neben den Eigenschaften durch technische und wirtschaftliche Rahmenbedingungen, ist Entwickler:innen von Open-Source-Software Datenschutz oftmals auch persönlich ein wichtiges Anliegen. Daher wird in entsprechenden Communities Open Source für gewöhnlich als besonders datenschutzfreundlich betrachtet.

Solche Zuschreibungen finden auch durch die Datenschutzaufsichtsbehörden statt. Ein Beispiel hierfür sind die immer wiederkehrenden Diskussionen rund um Plattformen für Videokonferenzdienste, die wir wohl alle im Laufe des letzten Jahres führen durften. So schreibt der baden-württembergische Landesdatenschutzbeauftragte Dr. Stefan Brink in einer Pressemitteilung, dass Lösungen auf Basis von Open-Source-Software es ermöglichen, die Datenflüsse von Videokonferenzsystemen selbst zu kontrollieren [2].

Gleichzeitig findet man in einer fortlaufend aktualisierten Liste der Berliner Landesdatenschutzbeauftragten mit einem Ampelsystem für Videokonferenzsysteme den Hinweis, dass »frei verfügbare Jitsi-Angebote in der Regel rot [seien], da in der Regel kein Auftragsverarbeitungsvertrag [abgeschlossen werden kann]« [3]. Aber wie kommt es dann, dass Open Source und Datenschutz vielfach als untrennbar verbunden wahrgenommen werden und Open-Source-Lösungen für Videokonferenzsysteme von einem Landesdatenschutzbeauftragten ausdrücklich empfohlen werden, aber die Videokonferenzangebote auf Basis einer eigentlich datenschutzkonformen Software in der Prüfung einer anderen Datenschutzaufsichtsbehörde durchfallen? Sind Open Source und Datenschutz doch nicht so untrennbar verbunden wie es auf den ersten Blick scheint?

Datenschutz ist mehr als Datensparsamkeit

Die Antwort hierauf ist natürlich komplexer. Open-Source-Software kann frei konfiguriert und auf einem Server der Wahl betrieben werden. Dazu kommt, dass Open Source meist keine Anreize für zweckfremde Sammlung personenbezogener Daten setzt und daher in der Regel datensparsam programmiert ist. Die Kerneigenschaft von Open-Source-Software, die freie Verfügbarkeit des Quellcodes, ermöglich darüber hinaus ein besonders hohes Maß an Transparenz.

All dies begünstigt einen datenschutzkonformen Betrieb von Diensten, aber ist nicht ausreichend. Zum einen muss auch Open-Source-Software im Hinblick auf Datenschutz korrekt konfiguriert werden. So verwenden auch selbst betriebene Jitsi-Server standardmäßig einen Server von Google, um Videoverbindungen unter den Teilnehmer:innen herzustellen [4]. Und bei der ebenfalls beliebten Videokonferenzsoftware Big Blue Button gibt es einige Fallstricke in Bezug auf unwissentliche Aufnahmen der Sitzungen [5]. Diese beiden Beispiele zeigen, dass es eine gewisse Detailkenntnis braucht, um die Dienste datenschutzkonform zu konfigurieren.

Neben der technischen Konfiguration der Software gibt es im Datenschutz auch einige formelle Aspekte zu beachten. So muss im Rahmen von Datenschutzhinweisen über die Datenverarbeitung informiert werden, wobei auch Pflichtangaben in Bezug auf die verantwortliche

Stelle oder gesetzliche Rechte gemacht werden müssen. Entsprechende Textvorlagen sind leider nur selten Bestandteil von Open-Source-Softwarepaketen. Bei einigen webbasierten Diensten bedarf es teilweise sogar technischer Anpassungen, um passende Texte überhaupt in die Software mit einbinden zu können.

Werden keine eigenen, sondern fremde Server genutzt, wird das Konstrukt der sogenannten Auftragsverarbeitung relevant. Datenverarbeitung, für die man eigentlich selbst verantwortlich ist, überträgt man einem technischen Dienstleister, den man hierzu vertraglich binden muss. Dies war auch schon nach altem Datenschutzrecht vor Inkrafttreten der Datenschutzgrundverordnung (DSGVO) so, aber wird zunehmend relevanter, da immer mehr Datenverarbeitung in Form von Cloud-Diensten ausgelagert wird. Dies ist auch der Punkt, aufgrund dessen die meisten frei verfügbaren Jitsi-Server in der Anbieterliste der Berliner Landesdatenschutzbeauftragten durchfallen. Relevant ist diese Thematik aber nicht nur bei Videokonferenzdiensten, sondern bei allen Arten von Cloud-Speichern, Webseiten, Datenbanken und so weiter.

Wer einen eigenen Dienst basierend auf einer Open-Source-Software datenschutzkonform betreiben will, muss man also auf mehreren Ebenen aktiv werden. Hierzu braucht es sowohl technisches, als auch datenschutzrechtliches Wissen. Dass ein kleiner Verein, für den Datenverarbeitung nur Mittel zum Zweck ist, dies leisten kann, ist illusorisch.

Die digitale Zivilgesellschaft als Bindeglied

Eine kleinere Organisation hat nun mehrere Möglichkeiten. Sie könnte sich Expertise für den Betrieb des Dienstes hinzukaufen. Dies ist jedoch allein aus Kostengründen für die meisten Organisationen kein gangbarer Ansatz und bei standardisierten Diensten auch aus wirtschaftlicher Sicht nicht sinnvoll. Ohne Kenntnis der möglichen Alternativen könnte für kleinere Organisationen so jedoch der Eindruck entstehen, dass Ihnen eine praxistaugliche und datenschutzkonforme Nutzung von Open-Source Software verwehrt bleibt. Hinweise von Datenschutzaufsichtsbehörden, entsprechende Dienste selbst zu betreiben, sind im Kontext kleinerer zivilgesellschaftlicher Organisationen jedenfalls nicht sonderlich hilfreich.

Es gibt jedoch auch kommerzielle Dienstleister, die bekannte Open-Source-Software als fertig konfiguriertes Paket anbieten. Anstatt sich also selbst um den Betrieb eines Servers zu kümmern oder dies einzeln zu beauftragen, kauft man es als Komplettpaket ein. So bieten die meisten Webhoster nicht nur das Betreiben einfacher Webseiten an, sondern erlauben es auch, Open-Source Cloud-Tools wie die beliebte Dateiablage und Groupware Nextcloud zu installieren. Im Bereich technisch komplexerer Anwendungen, wie beispielsweise Videokonferenzsysteme, muss man jedoch auf spezialisierte Anbieter mit speziell konfigurierten Servern zurückgreifen. Aber auch in diesem Bereich gibt es Möglichkeiten, Open-Source-Software als fertige Lösung einzukaufen, wie die Anbieterliste der Berliner Landesdatenschutzbeauftragten zeigt [3].

Häufig ist jedoch auch bei der Nutzung solcher Anbieter eine gewisse Kenntnis der dahinterliegenden Technik notwendig. So stehen auf den Webseiten der einschlägigen Anbieter häufig eher die Softwarefunktionalitäten im Vordergrund und man muss sich selbst erarbeiten, ob die angebotenen Produkte eine taugliche Lösung für die eigene Organisation darstellen. Kommerzielle Anbieter proprietärer – also nicht auf Open Source basierender – Software, sind in dieser Hinsicht meist besser aufgestellt. Sie haben Endanwender:innen und nicht Techniker:innen als Zielgruppe und beschäftigen dementsprechend ganze Marketing- und Vertriebsabteilungen, die herausarbeiten, welche Probleme welche Zielgruppen mit ihrer Software lösen kann.

Anbieter proprietärer Software sind auch ansonsten deutlich umtriebiger, was ihre Marketingaktivitäten und Außendarstellung betrifft. Daher sind die proprietären Cloud-Tools vielen bereits bekannt, wohingegen man für die Nutzung von Open-Source-Software erst einmal recherchieren muss. Daher kommt vielen Engagierten wohl zumeist proprietäre Software in den Sinn, wenn sie eine bestimmte Problemstellung in ihrem zivilgesellschaftlichen Engagement angehen wollen. Portale wie Stifter-helfen [6], auf denen Softwareanbieter ihre Dienste gemeinnützigen Organisationen zu vergünstigten Konditionen anbieten, verstärken die Sichtbarkeit proprietärer Cloud-Dienste noch weiter.

Um die Sichtbarkeit von Open-Source-Software in der Zivilgesellschaft weiter zu erhöhen, ist es daher wichtig, bei den konkreten Problemen und Fragestellungen zivilgesellschaftlicher Organisationen anzuknüpfen. Im Fall der Vereinssoftware CiviCRM bietet der deutsche Verein Software für Engagierte e.V. genau dies [7]. Durch solche Modelle kann die Zivilgesellschaft dafür sorgen, dass Open Source auch in der Zivilgesellschaft besser genutzt werden kann.

Digitale Infrastruktur durch die Zivilgesellschaft

Neben der besseren Auffindbarkeit und Nutzbarkeit von Open Source kann die Zivilgesellschaft natürlich auch den eigentlichen Betrieb von Cloud-Diensten übernehmen. Entsprechende Angebote stellen somit eine Alternative zu den oben erwähnten kommerziellen Hostern für Open-Source-Software dar. Hierzu zählen beispielsweise genossenschaftlich organisierte Anbieter wie Hostsharing [6] oder weChange [7], aber auch lose organisierte Gruppen (sogenannte Techkollektive) oder Einzelpersonen, die ehrenamtlich frei zugängliche Server anbieten.

Teilweise sind es auch eigens hierfür gegründete Vereine, die digitale Infrastruktur auf Basis von Open-Source-Software zur Verfügung stellen. Dies scheint aktuell aber eher selten der Fall zu sein und zumeist sind es etablierte Vereine, die neben ihrer eigentlichen Haupttätigkeit entsprechende Dienste anbieten. Ein Beispiel hierfür ist der Computerwerk Darmstadt e.V., welcher neben der wohltätigen Weitergabe gebrauchter Computer auch den relativ bekannten Videokonferenzdienst Senfcall betreibt [10].

Ein Grund dafür, dass es aktuell noch recht wenige Vereine gibt, die sich dezidiert dem Betrieb digitaler Infrastruktur widmen, ist sicherlich die fehlende Gemeinnützigkeit. Hierfür müsste

ein passender Zweck in den Katalog gemeinnütziger Zwecke nach § 52 Abgabenordnung aufgenommen werden. Dieser wurde zum Jahresanfang um den Betrieb von Freifunk-Netzen erweitert. Diese Regelung ist aber speziell auf Freifunk zugeschnitten und somit auf der Ebene des Netzzugangs angesiedelt. Initiativen, welche gemeinwohlorientierte Cloud-Dienste für die Allgemeinheit zur Verfügung stellen, fallen hier durchs Raster und sind nach aktueller Rechtslage nicht steuerbegünstigt. Daher arbeiten solche Gruppen oftmals eher lose organisiert, rein ehrenamtlich und finanzieren ihre Serverkosten über Spenden.

Eine öffentliche Förderung zivilgesellschaftlicher Initiativen wäre eine weitere Möglichkeit, den Aufbau einer gemeinwohlorientierten Infrastruktur auf Basis von Open Source voran zu treiben. Mit dem Prototype Fund [11] gibt es ein eigenes Förderprogramm des Bundes für die Entwicklung von gemeinwohlorientierter Open-Software (sogenanntes Public Interest Tech). Die Förderung endet leider mit der Erstellung der Quellcodes. Wenn sich nicht andere Player dem Betrieb entsprechender Dienste und damit einer Verstetigung annehmen, bleibt die hierdurch geförderte Software somit für große Teile der Zivilgesellschaft unzugänglich.

Wenn eine datenschutzkonforme, digitale Infrastruktur auf Basis von Open Source für die Zivilgesellschaft politisch gewollt ist, gäbe es durch eine Erweiterung des Katalogs gemeinnütziger Zwecke oder eine Förderung zum Betrieb von Software durchaus Möglichkeiten, die momentan eher lose organisierten Aktivitäten verschiedener Gruppen zu begünstigen und damit zu einer Verstetigung beizutragen.

Fazit

Open-Source-Software hat das Potential, die Basis einer datenschutzkonformen, digitalen Infrastruktur für die Zivilgesellschaft zu werden. Entsprechende Dienste sicher und datenschutzkonform zu betreiben, ist für die meisten zivilgesellschaftlichen Gruppen jedoch nicht möglich. Der Markt von Anbietern, die solche Dienste kommerziell anbieten, ist recht unübersichtlich und teilweise auch im Hinblick auf die Kosten für die Zivilgesellschaft unzugänglich.

Es gibt einige Initiativen aus der Zivilgesellschaft, eine Infrastruktur für die Zivilgesellschaft aufzubauen. Damit sich diese Initiativen professionalisieren und verstetigen können, braucht es jedoch die passenden Rahmenbedingungen. Eine Aufnahme des Betriebs digitaler Infrastruktur in den Katalog gemeinnütziger Zwecke und Förderprogramme zur Verstetigung von prototypisch entwickelten Lösungen können hierzu beitragen.

Unter den derzeitigen Rahmenbedingungen ist es für zivilgesellschaftliche Akteure in der Regel einfacher, zu den bunt angepriesenen und teils kostenlosen Angeboten proprietärer Cloud-Anbieter zu greifen. Aufgrund deren Geschäftsinteressen und datengetriebenen Geschäftsmodellen sind Konflikte im Hinblick auf Datenschutz jedoch vorprogrammiert. Hinzu kommt, dass nach dem Schrems II-Urteil des Europäischen Gerichtshofs aus dem letzten Jahr aktuell keine ausreichenden Rechtsgrundlagen für die Nutzung amerikanischer Cloud-Dienste bestehen.

Die Potentiale, die Open Source im Hinblick auf Datenschutz und den Aufbau einer souveränen, digitalen Infrastruktur bietet, kommen somit für die Zivilgesellschaft aktuell nicht zum Tragen. Durch passende politische Rahmenbedingungen könnte die Lücke zwischen der Erstellung von Open-Source-Programmcodes und der Nutzbarkeit der Software durch die Zivilgesellschaft geschlossen werden.

Quellen

[1] BBE Newsletter Nr. 2 vom 21.1.2021, https://www.b-b-e.de/bbe-newsletter/newsletter-nr-2-vom-2112021/staiger-digitale-souveraenitaet-open-source-gesellschaft/

[2] Pressemitteilung des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg vom 17. April 2020, https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

[3] Anbieterliste von Videokonferenzdiensten der Berliner Beauftragten für Datenschutz und Informationsfreiheit in der Version vom 18. Februar 2021, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

[4] https://www.kuketz-blog.de/jitsi-meet-datenschutzfreundlich-ohne-google-stun-server/

[5] https://bbb-hilfe.de/docs/aufnahme-funktion-in-bigbluebutton-technische-datenschutz-information/

[6] https://www.stifter-helfen.de/it-produkte

[7] https://sfe-ev.org/

[8] https://www.hostsharing.net/

[9] https://wechange.de/

[10] https://senfcall.de/

[11] https://prototypefund.de/

Autor

Hendrik vom Lehn *ist Berater für Datenschutz und Informationssicherheit. Er berät zivilgesellschaftliche Organisationen und baut bei der Stiftung Datenschutz den Bereich Datenschutz im Ehrenamt auf. Privat bloggt er unter vereint.digital rund um Digitalisierung im Vereinsumfeld.*

Website Stiftung Datenschutz

Twitter: @hendrikvomlehn

E-Mail: h.vomlehn@stiftungdatenschutz.org

Redaktion

BBE-Newsletter für Engagement und Partizipation in Deutschland

Bundesnetzwerk Bürgerschaftliches Engagement (BBE)

Michaelkirchstr. 17/18

10179 Berlin

Tel: +49 30 62980-115

newsletter@b-b-e.de

www.b-b-e.de