

Open-Source-Software

Steuermillionen für Hobbyprojekte

Ohne Freiwillige würden weder unser Navi noch unser Smartphone laufen. Der Staat unterstützt sie nun über den Sovereign Tech Fund mit Geld. Reicht das?

Von **Inga Pötting**

30. Dezember 2022, 17:59 Uhr / [155 Kommentare](#) /



Kleine Softwarebausteine, die kaum jemand kennt, sind das Fundament vieler wichtiger digitaler Anwendungen. © Karl Abuid/Shutterstock [https://unsplash.com/@spongzy]

Das Programm, das in Millionen von internetfähigen Geräten steckt, in Fernsehern, Druckern, Smartphones, Navigationssystemen, würde es ohne Daniel Stenberg nicht geben. Seit 25 Jahren kümmert er sich um einen kleinen Programmcode namens Curl. Wie viel Zeit er seit den Neunzigerjahren in seine Software gesteckt hat, kann er heute nicht mehr sagen. Pro Woche investiert er momentan 25 bis 30 Stunden in die Instandhaltung, schätzt er. In dieser Zeit stopft der schwedische Programmierer ehrenamtlich Sicherheitslücken, beantwortet Fragen anderer zum Programm, bessert die Software aus, damit sie weiter funktioniert. Einfach, weil ihm diese Software wichtig ist. Auch wenn er sich nicht komplett allein darum kümmert, könnte man sagen: Damit mein Navigationssystem im Auto und Ihr Smartphone läuft, sitzt Stenberg am Rechner. Und das in seiner Freizeit.

Erst jetzt, nach 25 Jahren, bekommt er erstmals Geld für die Pflege seiner Software. Aus Deutschland.

INGA PÖTING

Freie Autorin bei ZEIT
ONLINE

Curl ist eines von neun Open-Source-Projekten [<https://sovereigntechfund.de/>], die seit Oktober dieses Jahres [[https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2022/10/20221018-der-sovereign-tech-fund-](https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2022/10/20221018-der-sovereign-tech-fund-startet-die-forderung-eine-investition-in-die-digitale-souveranitat-europas.html)

[startet-die-forderung-eine-investition-in-die-digitale-souveranitat-europas.html](https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2022/10/20221018-der-sovereign-tech-fund-startet-die-forderung-eine-investition-in-die-digitale-souveranitat-europas.html)] vom Sovereign Tech Fund gefördert werden. Das Berliner Projekt bekommt bis Ende 2023 rund 13 Millionen Euro vom Bundesministerium für Wirtschaft und Klimaschutz, um quelloffene Software zu fördern, die ersten 1,3 Millionen wurden dieses Jahr an Projekte ausgezahlt. Diese auch als Open Source bezeichneten Komponenten sind so etwas wie das Fundament des Digitalen: Sie sind in unzähligen Anwendungen und Programmen verbaut und stehen offen zugänglich im Internet, sodass jede und jeder sie verwenden, überprüfen oder ausbauen kann.

Sie bringen aber kein oder zu wenig Geld ein, als dass sich professionell um ihre Pflege, das Ausputzen von Fehlern oder die Weiterentwicklung gekümmert wird. Deshalb hängt das reibungslose Funktionieren dieser Softwarekomponenten – und damit auch aller weitverbreiteten Programme und Anwendungen, die auf sie setzen – am Engagement weniger Freiwilliger. Freiwillige wie Daniel Stenberg.

Open-Source-Software steckt in vielen Systemen

Der Ansatz, den der Sovereign Tech Fund verfolgt, ist daher mehr als ungewöhnlich. Gerne fördert die öffentliche Hand Schaufensterprojekte: alles, was neu ist, nach außen sichtbar und worauf man in Großbuchstaben "INNOVATION" schreiben kann. IT-Sicherheitsexpertinnen dagegen fordern schon lange, dass digitale Infrastruktur, die von öffentlichem Interesse ist, besser unterstützt werden soll, auch mit öffentlichem Geld.

Das klingt so dröge, als wäre der Satz frisch aus einem Admin-Handbuch. Dabei sei die digitale Infrastruktur ähnlich existenziell wie die analoge, sagt Adriana Groh. Sie hat den Sovereign Tech Fund gemeinsam mit Fiona Krakenbürger gegründet. Ohne Software funktioniere kein Flughafen, kein Krankenhaus, keine Telekommunikation, sagt Groh. Und sehr oft seien dort Open-Source-Bausteine verbaut. "Wir alle nutzen jeden Tag quelloffene Systeme", sagt Groh. "Also ist es auch eine gesellschaftliche Aufgabe, sie zu stärken und instand zu halten. Es erwartet ja auch niemand, dass unsere Straßen von Ehrenamtlichen gebaut und ausgebessert werden."

Damit spricht sie ein Problem an, das sich seit vielen Jahren aufbaut und verschärft: Für Entwicklerinnen und Entwickler werden ihre Schöpfungen nämlich mit der Zeit manchmal zu einer Bürde.

Das Fundament, auf dem Ihr Smartphone gebaut ist

Das kann man gut am Beispiel von Softwareentwickler Stenberg erzählen. Anfang der Neunziger war es, da programmierte er eine Chatsoftware, die ein kleines Tool enthalten sollte, das automatisch Währungen umrechnete. Der Einfachheit halber verwendete der schwedische Programmierer für das Währungstool einige Zeilen quelloffenen Code, die jemand anderes geschrieben hatte. Stenberg ergänzte den Ursprungscode für seinen Währungsrechner an einigen Stellen, informierte den Autor, veröffentlichte das, was er programmiert hatte, ebenfalls wieder als Open-Source-Software und entwickelte sie anschließend über Jahre hinweg gemeinsam mit anderen Entwicklerinnen und Entwicklern weiter. So entstand die Software Curl.

Heute kann sie sehr viel mehr als schwedische Kronen in US-Dollar umrechnen. Sie fungiert als Transportmittel für Daten, die zwischen Geräten und Servern hin- und hergeschickt werden. Weil der Code Open Source ist, haben in den vergangenen Jahrzehnten viele andere Softwareprojekte ihn genutzt und als Fundament tief in ihre Programme eingegraben. Denn so funktioniert das Entwickeln großer wie kleiner Systeme heute: Statt alles von Grund auf selbst zu coden, bedienen sich die Verantwortlichen kleiner Softwarebausteine wie Curl und bauen ihre Anwendungen darauf auf.

So steckt Curl heute in unzähligen Geräten, die Informationen aus dem Internet laden. Man könnte sagen: Der kleine Baustein zählt zu den Fundamenten vieler Anwendungen. Ohne ihn würden zum Beispiel weder Kartenmaterial auf dem Navi noch Streamingdaten auf dem Fernseher ankommen. Aber: Die Verantwortung dafür, dass Curl läuft, hat kein professionelles Unternehmen mit Dutzenden Festangestellten übernommen. Sondern bis heute kümmert sich Stenberg darum – vom Service bis zur Fehlerbehebung. "Von denjenigen, die mit dem System zufrieden sind, höre ich so gut wie nie. Wer mir schreibt, braucht meistens Hilfe bei irgendwas", sagt Stenberg im Videocall mit ZEIT ONLINE.

Das Problem daran: Hören Menschen wie Stenberg auf, ihre Open-Source-Bausteine zu pflegen, würde vieles im Digitalen wohl störanfälliger und unsicherer. Mein Smartphone. Ihre E-Mail-Verschlüsselung. Das IT-System des Krankenhauses um die Ecke.

Wenn zahllose Geräte plötzlich angreifbar werden

Das mag in den Ohren mancher überdramatisch klingen. Im vergangenen Jahr hat sich aber gezeigt, was passiert, wenn eine nicht reparierte Sicherheitslücke eines Open-Source-Bausteins zu Ausfällen führt. Im Dezember 2021 wurde in der quelloffenen Java-Bibliothek Log4J eine Schwachstelle entdeckt, über die sich zahllose Geräte, von privaten Laptops bis zu Unternehmensrechnern,

angreifen und lahmlegen ließen. Die Open-Source-Community reagierte schnell und stellte ein Update bereit. Doch ein solcher Flicker bringt nur dann etwas, wenn er auch wirklich festgenäht wird. Institutionen, die die Java-Bibliothek nutzen, das Update aber bis jetzt nicht in ihre Systeme eingespielt haben, weil sie von dem Problem nichts mitbekommen oder seine Tragweite nicht begriffen haben, sind weiterhin angreifbar [<https://www.nuernbergmesse.de/en/magazine/connecting-people/the-worst-case-it-security-vulnerability-log4shell>]. Ihre Systeme könnten beispielsweise von Cyberkriminellen lahmgelegt und nur nach Zahlung eines Lösegelds wieder freigegeben werden.

Thema

Open-Source-Software

Log4j-Sicherheitslücke

"Wir rasen an metertiefen Schlaglöchern vorbei, ohne es zu merken"

[<https://www.zeit.de/digital/2021-12/log4j-sicherheitsluecke-adriana-groh-open-knowledge-foundation>]

Log4j-Sicherheitslücke

Ungeschützt

[<https://www.zeit.de/digital/2021-12/log4j-sicherheitsluecke-software-log4shell-it>]

Das alles heißt nicht, dass Open-Source-Bausteine unsicherer sind als geschlossene Systeme. Sicherheitslücken entstehen in allen komplexen Softwares. Öffentlich einsehbarer Code hat dabei den Vorteil, dass er jederzeit von Unabhängigen überprüft werden kann. Unerwünschtes Verhalten kann also theoretisch leichter entdeckt werden. Wenn aber am Ende doch nur wenige genau hinschauen, weil es weder Geld noch öffentliche Anerkennung für diese Arbeit gibt, steigt die Gefahr, dass Schwachstellen übersehen oder aus praktischen Gründen wie Zeitmangel nicht effektiv gestopft werden.

Auch bei Curl seien 124 bekannte Fehler in dem System aufgelaufen, als er das letzte Mal geschaut hätte, sagt Stenberg im Gespräch. Fehler, um die er sich jetzt, dank der Förderung durch den Sovereign Tech Fund, kümmern kann. Er sei ziemlich überrascht gewesen, als das Angebot aus Deutschland kam: "Dass es Unterstützung für die Ausbesserung eines bereits lange bestehenden Systems gibt, habe ich noch nicht erlebt – und ich mache diese Arbeit schon eine ganze Weile."

Digitale Infrastruktur so zugänglich machen wie Wasser und Strom

Die Gründerinnen Groh und Krakenbürger treibt der Wunsch nach einer gerechteren digitalen Welt an, einer Welt, die nicht in erster Linie großen

Konzernen, sondern allen gehört. Der Name Sovereign Tech Fund für eine staatlich geförderte Initiative klingt deshalb vielleicht etwas verwirrend. Gemeint ist keine wirtschaftliche oder politische Souveränität, sondern die Möglichkeit digitaler Selbstbestimmung für jede und jeden.

Eine echte Wahlfreiheit bei der Nutzung von Technik sei erst durch ein florierendes Open-Source-Ökosystem wirklich gegeben, sagt Krakenbürger. Denn quelloffene Systeme seien nicht nur transparent und überprüfbar, sondern sie stünden auch allen zur Verfügung. Also auch anderen Open-Source-Entwicklerinnen, die damit Neues schaffen und die Auswahl der Programme für Nutzerinnen vergrößern können.

Wie haben sie die Bundesregierung überzeugt, für ein solches Vorhaben Millionen locker zu machen? "Open Source ist den meisten Menschen, die mit Technik nichts zu tun haben, überhaupt kein Begriff", sagt Groh. "Wir haben deshalb immer wieder erklärt, dass wir im Prinzip etwas ganz Einfaches vorhaben: Wir möchten die Infrastruktur im Digitalen stärken, damit Grundlagensysteme für alle, die sie brauchen, zugänglich sind – so ähnlich wie Wasser und Strom."

Groh und Krakenbürger kennen sich von früheren Jobs, zuletzt arbeiteten beide für ein Technikprojekt der Open Knowledge Foundation, die sich für den freien Zugang zu Wissen einsetzt. Mit Unterstützung der Organisation führten sie für den Sovereign Tech Fund zunächst eine Machbarkeitsstudie ([PDF](https://sovereigntechfund.de/SovereignTechFund_Machbarkeitsstudie.pdf) [https://sovereigntechfund.de/SovereignTechFund_Machbarkeitsstudie.pdf]) durch, die genau aufdröselte, warum die Pflege von digitaler Infrastruktur von öffentlichem Interesse ist.

Eine wichtige Vermittlungsrolle nahm außerdem die Bundesagentur für Sprunginnovationen (SPRIND) ein. Sie unterstützte die Gründerinnen dabei, den Sovereign Tech Fund aufzubauen, und finanziert ihre Stellen. Die Agentur wird von mehreren Bundesministerien betrieben und ist eigentlich dafür da, Innovationen zu begleiten und zu unterstützen. "Die SPRIND hat schnell verstanden, warum unser Anliegen wichtig ist – obwohl wir nichts Neues erfinden, sondern etwas Bestehendes stärken wollen", sagt Groh. "Schließlich kann man Glasschlösser nicht auf Sand bauen, sondern auch Innovationen brauchen ein sicheres Fundament."

Kaum mehr als ein Taschengeld

Mit dem Steuergeld gefördert werden neben Curl mehrere Projekte, die mehr Selbstbestimmung im Internet ermöglichen, zum Beispiel die Verschlüsselungsstandards OpenPGP und OpenMLS sowie die VPN-Technik WireGuard. OpenPGP verschlüsselt E-Mails, OpenMLS Chatnachrichten Ende-

zu-Ende, das bedeutet, dass niemand außer dem Sender und der Empfängerin den Inhalt lesen kann. Ein Virtual Private Network (VPN) sorgt dafür, dass eine Person beim Surfen anonym bleibt, indem ihre IP-Adresse verschleiert wird.

Dass die jeweilige Technik im Hintergrund quelloffen ist, also transparent und überprüfbar, ist bei privatsphärekritischen Systemen wie diesen besonders wichtig. Denn schleicht sich dort ein Fehler ein, könnte die Kommunikation aller, die die Systeme nutzen, womöglich für andere einsehbar werden – also genau das ermöglichen, was die Systeme eigentlich verhindern wollen.

Nun könnte man sagen: 1,3 Millionen Euro für digitale Infrastruktur sind, unter mehreren Projekten aufgeteilt, kaum mehr als ein Taschengeld für die Entwicklerinnen und Entwickler. Selbst die 11,5 Millionen Euro, die kommendes Jahr zur Unterstützung weiterer Projekte an den Sovereign Tech Fund gehen sollen, sind angesichts der unzähligen Open-Source-Systeme, die unseren digitalen Alltag am Laufen halten, eigentlich noch viel zu wenig.

Ist digitale Infrastruktur Aufgabe des Staates?

Man kann aber natürlich auch fragen: Ist die Förderung mit Steuergeld überhaupt der richtige Ansatz? Ist es Aufgabe des Staates, quelloffene Software zu unterstützen? Schließlich geht es dem Sovereign Tech Fund nicht darum, eine ganz bestimmte Software für einen klaren öffentlichen Zweck zu entwickeln. Sondern im Fall von Curl wird beispielsweise ein schwedischer Entwickler für die Pflege von Software bezahlt, die nicht nur der Bundesrepublik nützt, sondern auch privaten Unternehmen aus der ganzen Welt. Und die wiederum verdienen Geld mit der jetzt auch aus Steuergeldern finanzierten Arbeit der Entwicklerinnen.

Aus Sicht von Indra Spiecker gen. Döhm, die an der Goethe-Universität in Frankfurt am Main einen Lehrstuhl für Informationsrecht innehat, ist diese Unkontrollierbarkeit durchaus ein Problem. Begreife man die öffentliche digitale Infrastruktur als direkte Aufgabe des Staates, müsse man sicherstellen, dass das staatliche Handeln erwünschte und messbare Ergebnisse bringt – und dass es dauerhaft wirkt. "Die Förderung bestehender Open-Source-Systeme ist ein sehr guter erster Schritt. Aber um das Ganze wirklich nachhaltig zu gestalten, müsste die Bundesregierung selbst Entwicklerinnen und Entwickler beschäftigen."

Denn: Jede Förderung läuft irgendwann aus, während Software aber konstant gepflegt und weiterentwickelt werden muss. Würde der Staat aber selbst Mitarbeiter anstellen, um Software zu eigenen Konditionen zu entwickeln – Software, die nicht von anderen zu unerwünschten Zwecken verwendet

werden kann –, dann würde das zwangsläufig bedeuten, dass der Programmcode geheim bleiben müsste. So betrachtet wäre ein Staat, der quelloffene Software unterstützt, ein unauflösbarer Widerspruch.

Sieht man den Staat aber als eine Instanz, die jeder Person digitale Selbstbestimmung und freien Zugang zu Technik ermöglichen soll, wäre die Förderung von Open-Source-Systemen genau der richtige Ansatz. Für Groh und Krakenbürger ergeben staatliche Grenzen beim Thema Open Source ohnehin keinen Sinn, da diese Software auf freien Zugang und freie Mitgestaltung ausgelegt sei. "Die Open-Source-Community ist über die ganze Welt verteilt. Es wäre gar nicht möglich, nur Personen aus einem Land zu fördern", sagt Krakenbürger.

Eine freiwillige Feuerwehr fürs Digitale

Und dennoch bleibt die Frage: Wie geht es weiter, wenn die Bundesregierung irgendwann kein Geld mehr nachschießt? Das Bundesministerium für Wirtschaft und Klimaschutz strebt eine längerfristige Förderung des Sovereign Tech Funds über 2023 hinaus immerhin an, wie in der Antwort auf eine schriftliche Frage der Bundestagsabgeordneten Petra Sitte (Die Linke) vom 24. Oktober 2022 nachzulesen ist ([PDF](https://dserver.bundestag.de/btd/20/042/2004209.pdf) [<https://dserver.bundestag.de/btd/20/042/2004209.pdf>]).

Doch was danach konkret passiert – die Gründerinnen wissen es noch nicht. Die Suche nach Antworten sei ein wichtiger Teil ihres Projekts, sagt Groh: "Wir möchten nach und nach herausfinden, ob staatliche Förderung die gewünschten Ergebnisse bringt und welche anderen Strukturen wir noch brauchen."

Was außer Geld sonst noch helfen könnte? Die vielen existierenden Open-Source-Projekte würden zeigen, dass im Engagement Freiwilliger eine Kraft stecke, die nicht zu unterschätzen sei, sagt Groh. "Wenn die Bedingungen stimmen, kann ehrenamtliche Entwicklung durchaus eine langfristige Lösung sein."

Schon heute gibt es bei der analogen Infrastruktur Bedingungen, die ehrenamtliches Engagement unterstützen. Bei der freiwilligen Feuerwehr etwa: Deren Ehrenamtliche dürfen, wenn es brennt, bei voller Bezahlung ihren Arbeitsplatz verlassen, das ist gesetzlich so geregelt [https://www.fuk-mitte.de/sites/default/files/media_files/brschg_st_2017_1.pdf]. Dass Arbeitgeber eines Tages einmal – wenn die digitale Infrastruktur durch Initiativen wie den Sovereign Tech Fund als öffentliche Aufgabe etabliert ist – auch das Stopfen kritischer Sicherheitslücken zur Arbeitszeit erlauben müssen, scheint da gar nicht so weit hergeholt.

