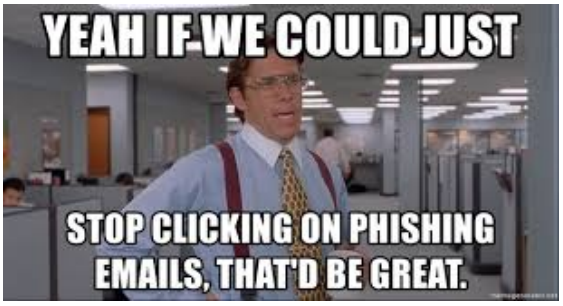
(Abwärts-)Trend Datensicherheit



Inhaltsverzeichnis

1. Einleitung

In diesem Trendbericht zur zwölften Ausschreibungsrunde des Prototype Fund beleuchten wir das Thema Datensicherheit. Die Ausschreibung, die am 1. Februar 2022 beginnt, ist allerdings themenoffen, so dass auch alle Public-Interest-Projekte, die sich nicht auf die in diesem Bericht skizzierten Fragestellungen beziehen, aber unter die Förderrichtlinie[1] fallen, eingereicht werden können. Datensicherheit[2] ist neben Civic Tech, Data Literacy und Infrastruktur eine der vier Grundsäulen, in denen wir Softwareprojekte fördern.[3]

Unter Datensicherheit verstehen wir im Rahmen dieses Berichts die (soziotechnische) Sicherung von Daten vor unzulässigen Eingriffen und Einsichten, um Datenschutz zu gewährleisten. Datensicherheit zielt damit auch auf Informationssicherheit ab. Unter dieser Definition steht das Thema in engem Bezug zu vergangenen Themenschwerpunkten, insbesondere der Betrachtung zur Stärkung von Nutzer:innen durch Open-Source-Software in Runde 4[4] und der Frage nach Vertrauensbildung im digitalen Kontext in Runde 7.[5]

Wie jedes Jahr ist der Jahreswechsel immer auch Anlass von Unternehmen, Beratungsagenturen und Anderen mit ihren Prognosen und Beobachtungen zu den vielversprechendsten und am prominentesten diskutierten Technologien für die nächsten zwölf Monate die Debatte um Technologieentwicklung zu besetzen.[6] Nur in wenigen dieser Berichte wurde explizit auf Datensicherheit eingegangen, wenn dann lediglich im Zusammenhang mit Quantencomputing. Das Thema Datensicherheit spielte aber in der medialen und zivilgesellschaftlichen Debatte eine merkliche Rolle. Denn (nicht nur) das Jahr 2021 fiel durch eine Vielzahl an Datenlecks, Angriffe mit Schadsoftware und Mängel in IT-Sicherheit allgemein auf. Diese Angriffe galten in der Mehrzahl Unternehmen und staatlichen Strukturen, auch die aufgedeckten Missstände sind dort zu verorten, wobei letzten Endes immer auch Privatpersonen, zivilgesellschaftliche Organisationen und generell Nutzer:innen der Angebote betroffen sind.

Während in einigen Fällen Schwachstellen in der Software für mangelnde Datensicherheit verantwortlich sind, spielen insbesondere bei gezielten Angriffen auch Fehler in der Nutzung von (Sicherheits-)Software, Unaufmerksamkeit oder Unwissen von Mitarbeitenden eine Rolle. Häufig aber nicht immer handelt es sich dabei um die Menschen, die lediglich Anwender:innen einer Technologie sind und diese nicht in ihren technischen Einzelheiten durchdringen. Aus diesem Grund gehen wir in diesem Bericht den Fragen nach, wie mit der Entwicklung von Public-Interest-Technologien Organisationen und Einzelpersonen bei der Ausübung und Umsetzung von Datensicherheit unterstützt werden können und welche Rolle Datensicherheit bei der Wahrung von Gemeinwohlinteressen spielt.

---

[1] Vgl. https://www.bmbf.de/bmbf/shareddocs/bekanntmachungen/de/2017/08/1395_aenderung-der-bekanntmachung.
[2] Vgl. https://prototypefund.de/kenne-deine-daten/.
[3] Vgl. https://prototypefund.de/about/public-interest-tech/.
[4] Vgl. https://prototypefund.de/wp-content/uploads/2021/01/Trendforschung-Runden-1-4.pdf.
[5] Vgl. https://prototypefund.de/wp-content/uploads/2020/03/Begleitforschung7.pdf.
[6] Vgl. Eine Zusammenfassung von 73 dieser Trendberichte findet sich z. B. hier: https://drive.google.com/file/d/1VoqmnamQLk1PRY3w70PklhgO6cKGy8Xh/view.

Dafür soll im Folgenden zunächst der “Trend” eingegrenzt und deutlich gemacht werden, welche Entwicklungen ausschlaggebend für die Wahl dieses Berichts waren und sind. Im Anschluss werden die Anforderungen an Datensicherheit skizziert, um darauf aufbauend den Zusammenhang zwischen Datensicherheit und Public-Interest-Technologien anhand ausgewählter Projektbeispiele aufzuzeigen. Abschließend werden offene Fragestellungen herausgearbeitet, die für die Open-Source-Software-Entwicklung unter der Förderung des Prototype Fund von Interesse sein können.

2. Status Daten(un-)sicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinem Lagebericht für 2021[7] zusammengefasst, wie es um Datensicherheit in Deutschland steht. Der Bericht, der noch vor der Aufdeckung der Log4Shell-Sicherheitslücke herausgegeben wurde, kam selbst ohne dieses Ereignis zu dem Schluss, dass angesichts von vielfältigen Bedrohungsszenarien gravierende Mängel in der Datensicherheit bestehen. So wird beispielsweise von einem neuen Höchstwert von Schadprogramm-Varianten gesprochen, die 2021 eingesetzt wurden, um an sensible Daten zu gelangen oder diese gegen den Willen der Nutzer:innen zu verschlüsseln, um Gelder von Betroffenen zu erpressen. Neben verschiedenen Angriffsszenarien (Ransomware, Spam, Botnetze, Phishing etc.) geht der Bericht auf menschliche Fehler und Unsicherheiten als Einfallstor für Angriffe ein. Nach einer repräsentativen Umfrage für das Digitalbarometer wird festgestellt:

> *“Rund zwei Drittel der Befragten (67 %) kennen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet (65 %). 37 Prozent der Befragten setzen solche Sicherheitsempfehlungen zum Teil um, gut jeder Zehnte vollständig (12 %). Wer Sicherheitsempfehlungen kennt, aber nicht umsetzt (12 %), begründet dies entweder durch den zu hohen Aufwand oder dadurch, dass die Empfehlungen zu kompliziert seien und nicht verstanden würden.”*[8]

Diese Ergebnisse sind für alle vom BSI aufgeworfenen Zielgruppen (Gesellschaft, Wirtschaft, Staat und Verwaltung, internationale Akteur:innen) von Relevanz, da ein Querschnitt der Befragten auch mit den IT-Systemen in den entsprechenden Bereichen arbeitet - und damit zu ihrer Schwachstelle wird. Das BSI hat zudem die digitalen Arbeitsbedingungen in der Corona-Pandemie zur weiteren Einordnung der Erkenntnisse herangeführt, da schlecht abgesicherte VPN-Server oder der Einsatz privater IT im beruflichen Kontext, z. B. unter Bedingungen im sog. agilen Arbeiten, zu Sicherheitsvorfällen führten.

Weitere Beobachter:innen der IT-Welt, wie das Future Today Institute nehmen eine Zunahme von IoT-Scams und Phishing während der Pandemie wahr, da Heimnetzwerke von Mitarbeitenden meist weniger sicher sind als die entsprechenden

[7] Vgl. BSI, Lagebericht, 2021, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.
[8] BSI, Lagebericht, 2021, S. 47.

Unternehmensumgebungen.[9] Die Firma Sophos hat in ihrem jährlichen Bedrohungsbericht zudem die Qualitätszunahme von Ransomware-Angriffen prognostiziert.[10]

2.1 Exemplarische Sicherheitsvorfälle in den Jahren 2020/2021

Der Analyse von Sophos ließe sich u. U. ein gewisser, durch ihr Security-Geschäftsmodell begründeter Bias unterstellen, doch sie deckt sich mit dem Eindruck, der aus Medienanalysen entsteht. In der Presse wurde eine Vielzahl von Sicherheitsvorfällen dokumentiert, darunter etliche Ransomware-Angriffe und Schwachstellen, die noch dazu führen können. Hierzu zählen:

- Schwachstellen in der Sicherheitsinfrastruktur von Daten:
    - Log4Shell ist eine Schwachstelle in der weltweit verbreiteten Java-Bibliothek und Open-Source-Komponente Log4j, durch die Apps, Server und Netzwerk-Bestandteile nicht mehr vor Eingriffen Unbefugter geschützt waren.[11] Diese Schwachstelle zieht sich durch zahlreiche Bereiche des öffentlichen und privaten Lebens.
    - Das Kollektiv Zerforschung[12] hat mehrfach Sicherheitslücken in der Software von Corona-Testzentren in Deutschland aufgedeckt.[13] Persönliche Daten und Testergebnisse von tausenden Menschen standen nahezu ungeschützt im Netz.
    - Das Kollektiv deckte auch gravierende Sicherheitsmängel in einer Lernapp für Schüler:innen auf. Durch die Mängel waren die personenbezogenen Daten von 500.000 Accounts öffentlich zugänglich.[14]
- (Ransomware-)Angriffe auf kritische Infrastruktur im medizinischen Bereich:
    - Der E-Mail-Server der bayerischen Krankenhausgesellschaft (BKG) wurde mit Schadsoftware infiziert.[15]
    - Das Klinikum Wolfenbüttel wurde nach einem Schadsoftwareangriff erpresst.[16]
    - Ein Angriff auf einen IT-Dienstleister, der weit verbreitete Software für Ärzt:innen anbietet, gefährdete die Datensicherheit in zahlreichen Praxen.[17]
    - Die AG KRITIS, eine Arbeitsgruppe aus Fachleuten, die in verschiedenen Bereichen und kritischen IT-Infrastrukturen tätig ist, fordert, dass in diesen Bereichen generell nur quelloffene Software zum Einsatz kommen sollte. “Dies sorgt dafür, dass ein Patch zur Behebung einer kritischen Sicherheitslücke auch

[9] Vgl. Future Today Institute, Tech Trends Reports, 2021, https://www.dropbox.com/s/y2kcsly3gl1z84k/FTI_2021_Tech_Trends_Volume_8_Privacy_Security.pdf?dl=0=.
[10] Vgl. Sophos Threat Report 2021, https://news.sophos.com/de-de/2021/11/09/sophos-threat-report-2022-im-sog-der-ransomware/.
[11] Vgl. https://t3n.de/news/extrem-kritisch-bsi-stuft-log4j-1436845/?utm_source=newsletter&utm_medium=entwicklung-design&utm_campaign=221221, https://t3n.de/news/angriffe-log4j-luecke-ransomware-wurm-1439317/?utm_source=newsletter&utm_medium=software-infrastruktur&utm_campaign=221221.
[12] Vgl. https://zerforschung.org/.
[13] Vgl. https://zerforschung.org/posts/eventus-testzentren/, https://zerforschung.org/posts/medicus/, https://zerforschung.org/posts/coronapoint/.
[14] Vgl. https://zerforschung.org/posts/learnu/.
[15] Vgl. https://www.heise.de/news/Hackerangriff-auf-Krankenhausgesellschaft-in-Bayern-6281905.html
[16] Vgl. https://www.heise.de/news/Cybercrime-Ransomware-legt-IT-des-Klinikums-Wolfenbuettel-lahm-6140048.html
[17] Vgl. https://www.heise.de/news/Ransomware-Attacke-auf-Medatixx-Grossalarm-im-Gesundheitswesen-6260613.html

dann noch erstellt werden kann, wenn der ursprüngliche Hersteller nicht mehr existiert oder eine Fehlerbehebung durch den Hersteller unwahrscheinlich ist."[18]

- (Ransomware-)Angriffe auf Organisationsstrukturen des Staates:
    - Kommunale Verwaltungen als wichtige Schnittstelle zwischen Bevölkerung und Staat wurden durch Angriffe mit Schadsoftware in ihrer Arbeit massiv eingeschränkt wie z. B. Schwerin[19], die Verwaltung Anhalt-Bitterfeld[20] oder die Stadtreinigung in Leipzig[21] erfahren mussten.
    - Die argentinische Migrationsbehörde wurde 2020 zeitweise lahmgelegt und erpresst.[22]
    - Nicht in allen Fällen wurde von den Angreifer:innen versucht, Lösegeld zu erpressen (oder dieses zumindest nicht öffentlich kommuniziert). Angesichts der großen Datenmengen, die bei diesen Angriffen erbeutet wurden und der Folgeschäden von Systemausfällen sind die wirtschaftlichen, sozialen und politischen Schäden aber enorm.
    - Im Vorfeld der Bundestagswahl 2021 wurde von den Verantwortlichen mit Angriffen gerechnet. In diesem Zusammenhang wurde auch vor Falschinformationen im Netz als massive Bedrohung des demokratischen Prozesses gewarnt.[23] Ein Aspekt, der verdeutlicht, dass Datensicherheit zwar eine eindeutig technische Komponente hat, aber nicht alleine auf diese reduziert werden sollte. Bildung, digitale Mündigkeit sowie Medienkompetenz können einen Einfluss darauf haben, ob und wie Sicherheitsvorfälle zustande kommen bzw. wie mit manipulierten Daten umgegangen wird und was deren gesellschaftliche Folgen sind.
- Kommerzialisierung von Angriffen:

  Es wurde eine Zunahme in der Kommerzialisierung von Ransomware-Angriffen beobachtet. Sogenannte Initial Access Broker verkaufen Zugänge zu Firmennetzen im Rahmen von Ransomware-as-a-Service. Gruppen wie DarkSide und REvil griffen den Pipeline-Betreiber Colonial und die Admin-Software Kaseya VSA an. Insbesondere die Kaseya-Angriffswelle von REvil hatte weitreichende Konsequenzen. Bis zu 1500 Unternehmen wurden erpresst.[24]
- Angriffe auf und Datendiebstahl bei Bildungseinrichtungen:

---

[18] Vgl. AG KRITIS, Politische Forderungen, https://ag.kritis.info/politische-forderungen/, abgerufen am 3. Januar 2022.
[19] Vgl. https://www.datensicherheit.de/deepbluemagic-ransomware-angriffe-kommunen, https://www.golem.de/news/ransomware-staatsanwaltschaft-ermittelt-nach-it-angriff-auf-schwerin-2111-161294.html.
[20] Vgl. https://www.golem.de/news/ransomware-angriff-anhalt-bitterfeld-will-weiter-nicht-auf-erpressung-eingehen-2108-158826.html.
[21] Vgl. https://www.mdr.de/nachrichten/sachsen/leipzig/leipzig-leipzig-land/hackerangriff-stadtreinigung-100.html.
[22] Vgl. https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million/.
[23] Vgl. https://www.mdr.de/nachrichten/deutschland/wahlen/bundestagswahl/cyberangriffe-zur-bundestagswahl-100.html.
[24] Vgl. https://www.heise.de/news/Massive-Cyber-Angriffswelle-auf-Behoerden-Onlineshops-Co-6278394.html.

> Forschung, Lehre und Studium an der TU Berlin wurden über Monate durch einen Hackerangriff stark eingeschränkt.[25] Bei dem Angriff sind viele personenbezogene Daten von Studierenden und Angestellten der Universität abgegriffen worden und konnten in Teilen auch nicht wieder hergestellt werden.[26]

Allein diese ausgewählten Beispiele belegen die Relevanz, die Datensicherheit für die Gesellschaft als Ganzes hat. In nahezu allen Bereichen des öffentlichen und privaten Lebens werden Daten gesammelt oder verarbeitet. Von Sicherheitsvorfällen wie Datenlecks sind u. a. besonders sensible Bereiche, wie der Gesundheitssektor, der Bildungsbereich, Verwaltungen und staatliche Dienstleistungen betroffen. Im Konsumbereich, in dem viele Zahlungsdaten anfallen, sind Unternehmen genauso wie Verbraucher:innen Zielscheibe von Erpressung oder Datenmissbrauch.

2.2 Der Faktor Mensch als Einfallstor

Ein scheinbar beliebter und vergleichsweise einfacher Weg, um in IT-Systeme einzudringen, scheint für Angreifer Scams zu sein, mit denen sie die Sicherheitsvorkehrungen eines Systems umgehen und sich durch Mitarbeitende eines Unternehmens, einer Institution oder auch Privatpersonen Zugang verschaffen.[27] Diese Schwachstelle wurde wissenschaftlich untersucht und belegt.[28] Hierfür versuchen die Angreifer:innen Routinen, Ängste, Gutgläubigkeit oder Lebensumstände von Personen auszunutzen und sie dazu zu bewegen, z. B. E-Mail Anhänge mit Schadsoftware zu öffnen, schädliche Dateien herunterzuladen oder zu installieren, auf Links zu klicken, die Schadsoftware aktivieren oder Nutzernamen und Passwörter preiszugeben. In einem Vortrag auf dem 36C3 stellt Linus Neumann, Sprecher des Chaos Computer Clubs (CCC) die These auf, dass “jedes praktisch relevante Problem der IT-Sicherheit [...] theoretisch gelöst” sei und die Praxis trotzdem ein “einziges Desaster” sei.[29] Dies führt er auf den Faktor Mensch zurück. In dem Vortrag zeigt er auf, wie mit Passwortmanagern (in der Regel) die Sicherheit von Passwörtern verbessert werden kann, Backups bei Datenverlust zumindest Abhilfe schaffen und dass sich mit Lernerfahrungen durch (simuliertes) Phishing psychologische Tricks von Phishing-Angriffen abfedern und geregelte Arbeitsprozesse wie Meldungen an die IT trainieren lassen. Für die bestmöglichen Effekte müssen diese Trainings aber häufig wiederholt und an aktuelle Gegebenheiten angepasst werden.

Christian Lölkes, ebenfalls vom CCC, argumentiert in einem Vortrag, dass es zur Erreichung (zumindest relativer) Datensicherheit wichtig sei, bei den Nutzer:innen Verständnis dafür zu wecken, wie Systeme funktionieren statt den Fokus lediglich auf einzelne Sicherheitstools zu

---

[25] Vgl. https://www.heise.de/news/Cyberangriff-TU-Berlin-rechnet-mit-monatelangen-IT-Einschraenkungen-6061688.html.
[26] Vgl. https://www.heise.de/news/Angriff-auf-IT-der-TU-Berlin-Daten-sind-abgeflossen-6050753.html.
[27] Vgl. https://www.itproportal.com/news/two-thirds-of-companies-have-experienced-an-insider-attack-this-year/.
[28] Vgl. z. B. DADA, O. S., Irunokhai, E.A., Shawulu, C. J, Nuhu, A. M., and Daniel, E.E. Information Security Awareness, a Tool to Mitigate Information Security Risk: a Literature Review. Innovative Journal of Science. Vol. 3, No. 3, 2021, pp. 29-54.
[29] Linus Neumann, Hirne hacken. Menschliche Faktoren der IT-Sicherheit, https://media.ccc.de/v/36c3-11175-hirne_hacken, 29.12.2019.

legen.[30] Er erläutert, dass bei dem Wissen um die gesamte Sicherheitskette (statt dem isolierten Fokus z. B. auf Passwörter als Schutzmaßnahme), Ängste im Gebrauch mit IT genommen werden können. Forscher:innen der La Trobe University in Australien unterstützen diese Ansicht. Sie haben gezeigt, dass auch theoretisch sichere Maßnahmen wie die Zwei-Faktor-Authentifizierung am menschlichen Umgang mit dieser Technologie scheitern können.[31]

Die European Union Agency for Cybersecurity (ENISA) setzt auch auf Bildungsmaßnahmen, um bei Nutzer:innen ein Bewusstsein für mögliche Angriffsszenarien und ein auf den Schutz von Daten gerichtetes Verhalten zu befördern.[32] Allerdings scheint dieses Vorhaben auf konzeptioneller statt praktischer Ebene angelegt zu sein.

Diese Praxiseinblicke in den Stand von Datensicherheit zeigen einen großen Bedarf in der Vereinfachung von technologischen Hilfsmitteln zum Schutz von Daten auf. Sie verdeutlichen die Notwendigkeit von unmittelbaren und individuellen Lernerfahrungen der Nutzer:innen sowie einer breiteren Bildung, wenn es um den Gebrauch von und das Verständnis für IT-Systeme geht. Technologische Hilfsmittel können demnach unter bestimmten Umständen für eine Verbesserung der Arbeitskultur im Umgang mit Datensicherheit sorgen. Allerdings ist ihre Wirkung eingeschränkt, wenn nicht gleichzeitig soziale Maßnahmen, wie eine wohlwollende Fehlerkultur umgesetzt werden, damit beispielsweise Sicherheitsvorfälle oder Bedenken schnellstmöglich an IT-Fachleute zur Schadensbegrenzung weitergegeben werden.

2.3 IT-Sicherheitspolitik auf Abwegen

Die Beobachtungen zu Sicherheitsvorfällen werden von politischen Maßnahmen begleitet, die nach Einschätzung von zivilgesellschaftlichen Akteur:innen wie dem CCC Datensicherheit eher erodieren als erhöhen. In seiner Stellungnahme zum Entwurf des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)[33] kritisiert der CCC die Anbindung des BSI an das Innenministerium, da diese Anbindung zu politischen Zielkonflikten führe. Zudem wird der Fokus auf große Unternehmen im Aufgabenbereich des BSI angeprangert. Diese solle sich stattdessen “auf die Förderung und Bereitstellung einer auf kompromisslose IT-Sicherheit ausgelegten Infrastruktur für Bürgerinnen und kleinere Unternehmen”[34] konzentrieren. Entwicklungen wie der Kauf einer IT-Sicherheitsfirma durch das Unternehmen Lidl[35] unterstreichen die Forderungen und Annahmen des CCC, dass Unternehmen ab einer bestimmten Größe selbst die Ressourcen besitzen, sich um ihre Datensicherheit zu kümmern und sich staatliche IT-Sicherheitseinrichtungen am Gemeinwohl orientieren sollen.

---

[30] Vgl. Christian Lölkes, Datensicherheit durch Verständnis, https://www.youtube.com/watch?v=_-hQuTi5uH4, 21.12.2018.
[31] Vgl. Watters/Scolyer-Gray/Kayes/Chowdhury, This would work perfectly if it weren’t for all the humans: Two factor authentication in late modern societies, 30.06.2019, https://journals.uic.edu/ojs/index.php/fm/article/view/10095.
[32] Vgl. https://www.enisa.europa.eu/topics/cybersecurity-education.
[33] Vgl. https://www.ccc.de/de/updates/2021/stellungnahme-zum-itsig2.
[34] Ebd.
[35] Vgl. https://www.handelsblatt.com/unternehmen/handel-konsumgueter/it-sicherheit-angst-vor-hackerangriffen-ehemalige-mossad-agenten-sollen-lidl-schuetzen/27825198.html.

Angesichts politischer Diskussionen rund um technische Hintertüren, um an verschlüsselte Daten und Informationen zu gelangen - vermeintlich zur Bekämpfung von Kriminalität - hat der CCC sich zudem gegen eine Schwächung von Verschlüsselungstechnologien und IT-Sicherheit im Allgemeinen ausgesprochen.[36] In einer Stellungnahme an den Ausschuss für Menschenrechte und humanitäre Hilfe des Deutschen Bundestages[37] hebt der CCC die Bedeutung von Verschlüsselung, anonymer digitaler Briefkästen und des Tor-Netzwerks[38] für die sichere Kommunikation und Arbeit u. a. von Journalist:innen, Aktivist:innen und Oppositionellen hervor. Datensammlungen und -auswertungen stuft der CCC außerdem als eine der größten menschenrechtlichen Bedrohungen ein. Viele Projekte, die sich mit Datensicherheit beschäftigen und die bisher bereits vom Prototype Fund gefördert wurden, bewegen sich daher auch in diesem Bereich und zielen häufig auf die oben aufgeführten, besonders bedrohten Gruppen ab.

Der Organisationszusammenschluss European Digital Rights (EDRi) ergänzt, dass die Schlüsselverwaltung für eine sichere Verschlüsselung eine bedeutende Rolle spielt und warnt vor Aussagen von Politiker:innen einen "zusätzlichen Schlüssel", gleichsam einen Generalschlüssel, einzuführen, da dieser Verschlüsselungssysteme insgesamt kompromittieren würde.[39]

Um diesen Bedrohungen der Datensicherheit zu begegnen, setzen zivilgesellschaftliche Organisationen und IT-Sicherheitsforscher:innen u. a. auf politische Arbeit für den gesetzlichen Schutz von Datensicherheit und die Umsetzung von Security by Design[40] in der Softwareentwicklung. Hier wird davon ausgegangen, dass Sicherheitsvorfälle zum Alltag gehören und die Software von Grund auf so aufgebaut, dass die Folgen eines Angriffs minimiert werden. Begleitend fordern Aktivist:innen für Datensicherheit die Schulung der betreffenden Personengruppen, eine Stärkung der wissenschaftlichen Forschung auf diesem Gebiet und die Förderung von Maßnahmen wie Auditierungen und Penetrationstests.[41] Mit Freier und Offener Software ist es zudem möglich, langfristig und unabhängig von unternehmerischen Interessen für Sicherheitsupdates von Software zu sorgen. Der Schutz von Daten liegt darüber hinaus im demokratischen Interesse, da dieses das Vertrauen in staatliche Institutionen und Abläufe befördert.

3. Dimensionen von Datensicherheit

Für die Bewertung der oben aufgeführten Sicherheitsvorfälle dienen zusätzlich Kriterien bzw. Ziele, die Anforderungen an Datensicherheit definieren. Hier werden in den Quellen zumeist drei Ziele von Datensicherheit angegeben, nämlich Vertraulichkeit, Verfügbarkeit und Integrität. Je nachdem, wie diese abgegrenzt sind, lassen sich zusätzliche Anforderungen wie Authentizität und Verbindlichkeit darunter fassen oder werden gesondert aufgeführt.

[36] Vgl. https://www.ccc.de/de/updates/2020/ccc-fordert-kompromissloses-recht-auf-verschlusselung.
[37] Vgl. https://www.ccc.de/system/uploads/302/original/CCC-Darknet_Stellungnahme.pdf.
[38] vgl. https://www.torproject.org/de/.
[39] Vgl. https://edri.org/our-work/tinkering-with-keys-weakens-encryption/.
[40] Vgl. https://en.wikipedia.org/wiki/Secure_by_design.
[41] Vgl. CCC, Stellungnahme Darknet, 2020, S. 8.

Mit Vertraulichkeit der Daten ist gemeint, dass nur die Personen, die dazu berechtigt sind, auf Daten zugreifen und diese einsehen können. Dies kann beispielsweise über Verschlüsselung oder andere Formen der Zugriffskontrolle gewährt werden. Verfügbarkeit bezieht sich darauf, dass alle Personen, die berechtigt sind, auf Daten zuzugreifen, dies auch tatsächlich wahrnehmen können, z. B. indem es Maßnahmen wie Redundanzen[42] gibt, die vor Systemausfall schützen. Integrität zielt auf die Unverfälschtheit der Daten ab. Das bedeutet, dass sie manipulationssicher sein sollen und dass Änderungen an den Daten nicht unbemerkt vorgenommen werden können.[43] Die Untersuchungen des Kollektivs Zerforschung belegen z. B. die Nichterreichung von Vertraulichkeit und Integrität bei den untersuchten Angeboten. Der Umgang mit Ransomware-Angriffen kann ein Beispiel für Schwächen in Bezug auf die Verfügbarkeit von Daten sein, wenn keine Backups vorliegen und sich Betroffene genötigt sehen, auf Erpressungsversuche einzugehen, um ihre Daten zurück zu erhalten.

Eng mit Integrität hängt der Faktor Authentizität zusammen, der gewährleisten soll, dass die Daten tatsächlich für das stehen, was sie abbilden, z. B. in Bezug auf ihre Quelle oder Verarbeitung. Auch Verbindlichkeit lässt sich unter Integrität subsumieren und ist von der Authentizität der Daten abhängig. Mit Verbindlichkeit wird ausgedrückt, dass eine Aktion, tatsächlich so stattgefunden hat wie vorgesehen, sie also nicht manipuliert wurde.[44] Nachhaltigkeit wird teilweise als Kriterium angeführt, ist in der Regel aber implizit in den vorherigen Faktoren enthalten, da alle oben aufgeführten Dimensionen replizierbar sein sowie dauerhaft überprüft, angepasst und umgesetzt werden müssen.

Die aufgeführten Faktoren sind mit Blick auf Datensicherheit einerseits technisch zu gewährleisten, z. B. durch automatische Zugriffskontrollen, Verschlüsselung, Versionsdokumentationen oder redundante Auslegungen von Systemen. Dies wird auch in internationalen Normen aufgeführt[45] oder im Bundesdatenschutzgesetz definiert.[46] Wie eingangs aufgeführt, haben sie aber zudem eine soziale Dimension, denn sie müssen in der Regel von Menschen korrekt ausgeführt, im besten Fall nachvollzogen und verstanden werden. Auch die beste Verschlüsselung ist kompromittiert, wenn durch Zeitdruck oder Unachtsamkeiten beispielsweise der private Schlüssel an Andere weitergegeben wird. Dass hiervon auch Sicherheitsexpert:innen nicht gefeit sind, zeigt ein solcher Vorfall aus dem BSI.[47]

4. Daten sichern mit Public Interest Tech

Im Projekt-Portfolio des Prototype Fund finden sich bereits einige Projekte, die sich explizit mit Datensicherheit beschäftigen. Sie stellen heraus, wie wichtig es für demokratische Kontrolle, Meinungsbildungsprozesse, aber auch für Geschäftsvorgänge und den Schutz der Privatsphäre ist, die eigenen Daten im Sinne von Vertraulichkeit, Verfügbarkeit und Integrität

[42] Vgl. https://de.wikipedia.org/wiki/Redundanz_(Technik).
[43] Vgl. z. B. https://www.fu-berlin.de/sites/it-sicherheit/grundwerte/vertraulichkeit/index.html, https://www.fu-berlin.de/sites/it-sicherheit/grundwerte/integritaet/index.html, https://www.fu-berlin.de/sites/it-sicherheit/grundwerte/verfuegbarkeit/index.html.
[44] Vgl. https://de.wikipedia.org/wiki/Informationssicherheit.
[45] Vgl. https://de.wikipedia.org/wiki/ISO/IEC-27000-Reihe.
[46] Vgl. https://www.datenschutz.org/bdsg/.
[47] Vgl. https://www.golem.de/news/verschluesselung-bsi-verschickt-privaten-pgp-schluessel-2111-161073.html.

zu schützen. Dabei nutzen sie verschiedene Ansätze wie Verschlüsselung oder maschinelles Lernen.

Das Projekt Cypherlock[48], das in Runde 5 des Prototype Fund gefördert wurde, möchte die Daten und Quellen von Journalist:innen (und damit auch ihre journalistische Integrität) in Bedrohungssituationen vor Zugriff schützen, indem eine Metaverschlüsselung des Festplattenschlüssels implementiert wird. Dafür werden mehrere Server eingesetzt, die nur gemeinsam den Schlüssel bereitstellen können.

Journalist:innen, Aktivist:innen und Oppositionspolitiker:innen adressiert das in Runde 6 geförderte Projekt Close Lid to Encrypt.[49] Auch hier geht es darum, Verschlüsselung zu verbessern. Konkret hat das Projekt die Festplattenverschlüsselung im Ruhezustand bei der Linux-Distribution Debian ermöglicht. Hier war es zuvor nur möglich, die Daten vor unerlaubten Zugriffen zu schützen, wenn der Rechner komplett heruntergefahren war, was sich bei vielen Arbeitsrechnern als wenig praktikabel erweist und zudem für die genannten Zielgruppen ein Risiko darstellt, wenn sie beispielsweise spontan durchsucht werden. Darüber hinaus profitieren auch alle anderen Nutzer:innen von dieser Entwicklung, da ihre Daten z. B. im Fall von Geräteverlust geschützt sind.

Ebenfalls im Bereich Verschlüsselungstechnologien setzt das Projekt Dark Crystal Social Key Recovery System[50] aus der Runde 6 an. Hier sollen Nutzer:innen befähigt werden, eine dezentrale Architektur für die Verwaltung von Passwörtern und Schlüsseln zu nutzen statt von zentralen Infrastrukturen abhängig zu sein. Mit der Förderung wurde die Widerrufsfunktion sowie die Neuausgabe von Schlüsseln bearbeitet.

Die in Kapitel 2 zitierte Studie des BSI zeigt, dass einer der Gründe, weshalb Personen auf empfohlene Sicherheitsmaßnahmen verzichten, im damit verbundenen Aufwand liegt. Diese Komplexität lässt sich z. B. auch auf den Umfang von Speicherplatz einer Sicherheitsanwendung herunterbrechen, die das Betriebssystem verlangsamt oder schlicht den vorhandenen Speicher besetzt. Das ebenfalls in Runde 5 geförderte Projekt Portable Firewall für QubesOS[51] setzt diesem Problem eine ressourcenschonende, alternative Firewall entgegen und adressiert damit die Bedürfnisse von Aktivist:innen, Journalist:innen und Hacker:innen, die dieses Betriebssystem vorwiegend nutzen.

Mit dem in Runde 5 geförderten Projekt Undo von Ransomware mittels Machine Learning[52] wird angestrebt, den Schaden nach einem Datenverlust durch einen Ransomware-Angriff einzudämmen, indem die Daten aus einem Cloudspeicher wiederhergestellt werden. Es wurde versucht, das Wiederherstellungstool um eine Komponente maschinellen Lernens zu ergänzen, die das Zugriffsverhalten bei Angriffen erfassen und die Daten anschließend zur Verfügung stellen sollte. Die Idee war, auf diesem Weg Modelle zur Prävention bzw. dem Erkennen von Ransomware-Angriffen zu trainieren.

[48] Vgl. https://prototypefund.de/project/cypherlock-coercion-resistant-storage/.
[49] Vgl. https://prototypefund.de/project/close-lid-to-encrypt/.
[50] Vgl. https://prototypefund.de/project/dark-crystal-social-key-recovery-system/.
[51] Vgl. https://prototypefund.de/project/portable-firewall-fuer-qubesos/.
[52] Vgl. https://prototypefund.de/project/undo-von-ransomware-mittels-machine-learning/.

Ein Szenario, das bei den aufgeführten Beispielen für Sicherheitsvorfälle nicht berücksichtigt wurde, aber massiv die Privatsphäre von Betroffenen bedroht, ist der Einsatz von Anwendungen zum digitalen Stalking. Das Projekt StalkerBuster[53] der Runde 4 bietet hierfür eine begleitende technische Unterstützung von Betroffenen an, mit der der ausgehende Netzwerkverkehr eines Geräts nach Autorisierung dokumentiert, aufbereitet und analysiert werden kann. So kann Gewissheit darüber erlangt werden, ob Stalkerware auf dem eigenen Gerät installiert ist. Das Projekt verdeutlicht, dass Datensicherheit auch an das Vertrauen in die Funktionalität und Integrität des eigenen Geräts geknüpft ist.

Weitere ausgewählte Projektbeispiele (auch außerhalb des Prototype Fund) sind:

- Das Projekt SugarCoat[54] von Brave Software und der Universität San Diego. SugarCoat ist ein Open-Source-Tool zur Vermeidung von Kompatibilitätsproblemen, die beim Blockieren bösartiger Skripte auf Websites entstehen können. SugarCoat erzeugt automatisch datenschutzfreundliche Versionen von Tracking-Skripten und bietet den Nutzer:innen dadurch mehr Anonymität im Netz.
- VeraCrypt[55] ist ein Verschlüsselungsprogramm, mit dem Dateien oder der ganze Rechner verschlüsselt werden können. Mit versteckten Tresoren lassen sich auch dann noch Dateien schützen, wenn eine Person z. B. genötigt wird, einen Schlüssel herauszugeben.
- Der Open-Source-Passwortmanager KeepassX, dessen Maintenance und Entwicklung inzwischen eingestellt wurde[56], stellte eine Alternative zu proprietären Passwortmanagern dar. Sie bieten automatisch generierte, sichere Passwörter an, die sich die Nutzer:innen nicht mehr selbst merken müssen, da sie lediglich ein Masterpasswort zur Verwaltung der Anwendung benötigen.
- Das Browser Add-on Privacy Badger[57] zielt darauf ab, Nutzer:innen mehr Kontrolle darüber zu geben, wo sie Spuren im Netz hinterlassen und lernt aus ihrem Verhalten, welche Tracker blockiert werden sollen und welche nicht.
- Tails[58] ist ein Betriebssystem, das von externen Datenträgern aus auf jedem Rechner gestartet werden kann und auf dem Rechner keine Spuren hinterlässt. Viele Anwendungen zur sicheren Kommunikation sind bereits vorinstalliert, um Anwendungsfehler zu vermeiden. Es wird das Tor-Netzwerk genutzt, um die Anonymität der Nutzer:innen zu schützen.
- Der Cyberkicker[59] des Fraunhofer Instituts und der DataRun[60] der Stiftung Deutsches Technikmuseum Berlin und des Vereins mediale pfade (beide Projekte wurden inzwischen eingestellt) setzen an dem Bedarf von aktiv zu erlebender und spielerischer Vermittlung von Datensicherheit an. Das Projekt Datenklaus[61] vom Prototype Fund

[53] Vgl. https://prototypefund.de/project/stalkerbuster/.
[54] Vgl. https://brave.com/privacy-updates/12-sugarcoat/.
[55] Vgl. https://veracrypt.fr/en/Home.html.
[56] Vgl. https://www.golem.de/news/passwortmanager-keepassx-offiziell-eingestellt-2112-161791.html.
[57] Vgl. https://privacybadger.org/.
[58] Vgl. https://tails.boum.org/index.de.html.
[59] Vgl. https://www.fraunhofer.de/en/press/research-news/2018/May/beating-trojans-and-viruses-at-the-football-table.html.
[60] Vgl. https://medialepfade.org/projekt/data-run/.
[61] Vgl. https://prototypefund.de/project/datenklaus/.

richtet sich mit ähnlichen Methoden an Schüler:innen und Lehrer:innen und schafft Bewusstsein für die Verarbeitung von Daten bei digitalen Diensten und lässt die Nutzer:innen verschiedene Auswirkungen ihres Umgangs mit Daten austesten.

Datensicherheit ist ein kontinuierlicher Prozess und wie alle Software brauchen auch Open-Source-Projekte ständige zeit- und ressourcenintensive Wartung, Aktualisierung und Überprüfung wie nicht zuletzt das Beispiel Log4j gezeigt hat.[62] Dies mit dem Prototype Fund zu unterstützen, ist nur sehr eingeschränkt möglich. Allerdings bietet er die Möglichkeit, kreative Ideen zu testen, damit Personen befähigt werden, ihre Daten besser zu schützen. Im Sinne der Public-Interest-Tech-Auslegung[63] des Prototype Fund sollen Projekte zum Thema Datensicherheit adaptierbar sein für verschiedene Kontexte und Zielgruppen. Der Fokus liegt auf den jeweiligen Nutzer:innen als Expert:innen dafür, was sie brauchen, um sicher mit ihren Daten umzugehen. Nach den hier zusammengefassten Erkenntnissen bedeutet dies, dass Anwendungen möglichst einfach und übersichtlich in der Nutzung sein sollten. Sie brauchen geeignete, leicht verständliche Erklärungen, Raum für Übung und müssen sich in gängige Arbeitsabläufe einfügen lassen.

5. Fragestellungen und Fazit

Maßnahmen zur Steigerung der Datensicherheit nehmen für Einzelnutzer:innen und Fachleute, die für Viele verantwortlich sind, verschiedene Formen an und nicht alle Probleme lassen sich überhaupt technisch lösen. Aus den aufgeführten Herausforderungen und Projektideen ergeben sich demnach folgende Themenfelder, die zur weiteren Betrachtung bei Public-Interest-Technologien von Interesse sein können: Die Erhöhung von Bewusstsein und das Aufzeigen von Handlungsoptionen für Maßnahmen der Datensicherheit, Tools zur Anwendungssicherheit bis hin zur Disaster Recovery sowie der Abbau von Barrieren in der Nutzung vorhandener Werkzeuge z. B. in Bezug auf Design, Sprache oder Anwendung.

Im Bereich Awareness kann ergründet werden, wie sich möglichst vielfältige bzw. unterschiedliche, realistische Angriffsszenarien oder der Umgang mit Sicherheitsproblemen simulieren lassen. Wie können in solchen Schulungen das soziale Umfeld berücksichtigt und verschiedene Kommunikationsstile und -arten integriert werden? Wie kann Software bei der Analyse von Datensicherheit unterstützen, auch bei unerfahrenen Anwender:innen, und auf geeignete Schutzmaßnahmen hinweisen? Wie kann das politische Ziel von Security by Design durch Kampagnen o. ä. befördert und technisch begleitet werden? Wie kann der Einsatz von Sicherheitsanwendungen beispielsweise durch Installationsassistenten, Dashboards, Löschhilfen etc. erleichtert und übersichtlicher gestaltet werden? Wie kann die Kontrolle der Funktionalität von Sicherheitsanwendungen auch für technisch weniger versierte Nutzer:innen gesichert werden?

Reduzierung von Komplexität, Verständlichkeit und Bedienbarkeit stehen bei all diesen Fragestellungen im Mittelpunkt. Zusätzlich sind Faktoren wie Energiesparsamkeit und

[62] Vgl. https://t3n.de/news/log4shell-problem-fuer-jahre-1437990/.
[63] Vgl. https://prototypefund.de/about/public-interest-tech/.

Ressourcenschonung allgemein von Interesse und müssen in der Software-Entwicklung mit dem Anspruch an Datensicherheit in Einklang gebracht werden.

In diesem Bericht sollte nachgewiesen werden, dass das Thema Datensicherheit aktuell, aber auch grundsätzlich, eine hohe Relevanz besitzt. Die Ziele von Datensicherheit sind der Schutz von Verfügbarkeit, Vertraulichkeit und Integrität der Daten. Diese können zwar niemals absolut erreicht, aber mit technologischen Hilfsmitteln befördert werden, indem z. B. Verschlüsselung eingesetzt, Verwaltungssoftware entwickelt, Analyse und Dokumentation von Sicherheitsvorfällen erleichtert werden. Open-Source-Software erzielt Vertrauen in diese Technologien und vermindert Abhängigkeiten z. B. in Bereichen kritischer Infrastruktur und in Krisensituationen. Aber auch in anderen Bereichen des öffentlichen Lebens, in Kultur, Politik, Verwaltung oder Gesundheit stellt verantwortungsbewusster Umgang mit Daten eine Komponente für gesellschaftliche Teilhabe dar.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
OPEN KNOWLEDGE FOUNDATION DEUTSCHLAND
Prototype Fund

Autorin: Claudia Jach | Prototype Fund
Vorgelegt im Januar 2022