Dialog für Cyber-Sicherheit

Ergebnisbericht des Workstreams BuntesBugBounty

Dialog für Cyber-Sicherheit

Ein Projekt im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Stand: September 2023

Informationen zum Produkt

Dieser Bericht dokumentiert den Workstream BuntesBugBounty, der von Dezember 2022 bis August 2023 im Rahmen des Projekts Dialog für Cyber-Sicherheit durchgeführt wurde. Das Ziel des Workstreams war die Unterstützung des gesamtgesellschaftlichen Dialogprozesses hinsichtlich eines bundesweiten Bug-Bounty-Programms für die IT-Systeme der öffentlichen Hand sowie Freie und Open-Source-Software (FOSS). Das BSI verfolgt mit dem Projekt das Ziel, einen offenen gesellschaftlichen Diskurs zum Thema IT-/Cyber-Sicherheit sowie damit verwandter gesellschaftlicher Themen zu ermöglichen. Das Projekt soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung an das Thema Cyber-Sicherheit aus Sicht der organisierten Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Ideengeber:innen des Workstreams waren: Gregor Bransky (Innovationsverbund Öffentliche Gesundheit e. V.) und Bianca Kastl (Innovationsverbund Öffentliche Gesundheit e. V.)

Mitwirkende Teilnehmer:innen des Workstreams waren: Lars Bartsch (BSI), Philipp Berg (Deutsche Stiftung für Ehrenamt und Engagement), Thomas Fricke (Innovationsverbund Öffentliche Gesundheit e. V.), Sabine Griebsch (GovThings), Helene Hahn (Report ohne Grenzen), Nora Kluger (BSI), Dr. Dennis Kügler (BSI), Claudius Link (Agile Security Consultant & Coach), Bernadette Längle (pep Stiftung), Alexander Sander (Free Software Foundation), Peter Schoo (Gesellschaft für Informatik), Ayten Öksüz (Verbraucherzentrale Nordrhein-Westfalen e. V.)

Beteiligte Mitarbeiter:innen der Geschäftsstelle des iRights.Lab waren: Marcel Schneuer, Jörg Rodermund, Wiebke Glässer, Georg Förster, Nikolai Horn, Lisa Schmechel sowie Jana Klawitter.

Der Dialog für Cyber-Sicherheit ist ein Projekt des Bundesamts für Sicherheit in der Informationstechnik (BSI), das vom Thinktank iRights.Lab und dem nexus Institut durchgeführt wird. Die Auftragnehmer haben dafür eine Geschäftsstelle eingerichtet.

Der Workstream BuntesBugBounty wurde im Rahmen eines partizipativen und offenen Austauschs von der Geschäftsstelle und den Teilnehmer:innen durchgeführt. Das genannte Thema des Workstreams aus dem Bereich Cyber-Sicherheit wurde von den Teilnehmer:innen des Dialogs für Cyber-Sicherheit eigenständig gewählt.

Der vorliegende Bericht wurde von der Geschäftsstelle erarbeitet und basiert auf der Dokumentation der Arbeit der Workstream-Teilnehmer:innen. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. aller Teilnehmenden wider.

Weitere Informationen zum Dialog für Cyber-Sicherheit:
http://www.dialog-cybersicherheit.de

Kontakt Geschäftsstelle (iRights.Lab und nexus Institut):
kontakt@dialog-cybersicherheit.de

Stand: August 2023

Inhaltsverzeichnis

1. Einleitung

Der vorliegende Abschlussbericht dokumentiert den Arbeitsprozess und die gewonnenen Erkenntnisse des Workstreams BuntesBugBounty. Dieser Bericht wurde aus der Perspektive der Geschäftsstelle verfasst, die den Workstream während seines gesamten Verlaufs organisatorisch und kommunikativ begleitet hat. Der Fokus liegt hierbei auf einer detaillierten prozessualen Beschreibung der Aktivitäten und Ergebnisse.

1.1 Hintergrund und Rahmen des Workstreams BuntesBugBounty

Der Workstream BuntesBugBounty wurde während der Denkwerkstatt „Sichere Informationsgesellschaft“ im September 2022 im Rahmen des Dialogs für Cyber-Sicherheit ins Leben gerufen. Ziel war es, die Grundlagen für ein mögliches staatliches Bug-Bounty-Programm in Deutschland zu erarbeiten. Durch eigene Dialogformate mit Expert:innen wurde der Fokus auf die Förderung der IT-Sicherheit im Bereich von Free and Open Source Software (FOSS) gelegt. Sicherheitslücken sollten durch das angestrebte Programm geschlossen werden, ebenso sollten rechtliche Hürden für IT-Sicherheitsforschende in Deutschland aufgearbeitet werden, die beispielsweise eine ehrenamtliche Analyse von Software oder die Meldung gefundener Sicherheitslücken an staatliche Stellen erschweren.

1.2 Ziele und Fragestellungen

Die in der Workstream-Skizze definierten Ziele konzentrieren sich auf zwei Punkte:

1. Die Schaffung eines partizipativen und diskursiven Rahmens zur Auseinandersetzung über die Hürden und Möglichkeiten eines Bug-Bounty-Programms.
2. Aktive Vermittlung und reger Austausch zwischen verschiedenen Akteur:innen und Stakeholder zur praxisnahen Gestaltung des Bug-Bounty-Ansatzes.

Die Stakeholder identifizierten dazu während der Denkwerkstatt 2022 einige Fragen, die sie innerhalb des Zyklus klären wollten:

1. **Arbeitsaufwand:** Nach dem Finden einer Sicherheitslücke liegen 60 bis 80 Prozent des Aufwands darin, diese so zu dokumentieren, dass die Sicherheitsforschenden juristisch nicht für einen unbefugten Datenzugriff belangt werden können. Kann dies einfacher gestaltet werden? Wie könnte ein guter Meldeprozess aussehen? Welche Minimalanforderungen werden an eine rechtssichere Dokumentation gestellt?
2. **Wertschätzung:** Wie können Anreize geschaffen und ausgestaltet werden, die die Sicherheitsforscher:innen verstärkt dazu motivieren, nach Schwachstellen zu suchen und diese zu melden? Wie werden diese Anreize finanziert? Welche formalen Hürden müssen berücksichtigt werden?
3. **Meldeprozess:** Wie kann sichergestellt werden, dass der Meldeprozess möglichst einfach und zuverlässig funktioniert, damit eine Sicherheitslücke schnell geschlossen wird?
4. **Öffentlichkeit:** Wie kann ein Bug-Bounty-Programm und dessen Wirkung für die Fachcommunity und betroffene öffentliche Stellen sichtbar gemacht werden?
5. **Akzeptanz:** Wie kann der gesellschaftliche Nutzen eines solchen Programms sowohl innerhalb der Bundesverwaltung als auch bei zivilgesellschaftlichen Akteur:innen verdeutlicht und die Akzeptanz gesteigert werden?

Diese Ziele wurden auf verschiedene Weisen verfolgt, die im folgenden Kapitel näher erläutert werden.

2. Methodisches Vorgehen

Der Schwerpunkt des Workstreams lag auf zwei festen Terminen: dem wöchentlichen Arbeitstreffen und der monatlichen Online-Veranstaltungsreihe B3 im Dialog. Die Veranstaltungsreihe B3 im Dialog war ein digitales Format, bei dem zunächst Expert:innen Impulse zum Thema des Abends gaben und dann innerhalb einer Fragerunde auf weitere Fragen eingingen. Die Veranstaltungen wurden aufgenommen und über den YouTube-Kanal des BSI veröffentlicht. Auf den Inhalt der Vorträge wird in Kapitel 3 eingegangen.

Vertreter:innen des Workstreams haben des Weiteren Vorträge bei verschiedenen relevanten Fachkonferenzen gehalten, um den Workstream und dessen Ziele in der breiten Öffentlichkeit bekannt zu machen und um weitere Perspektiven für den Workstream zu erhalten. Die gesammelten Erkenntnisse finden sich in Kapitel 4.

Ferner wurde die Geschäftsstelle beauftragt, Recherchen zu staatlichen Bug-Bounty-Programmen in der EU durchzuführen. Diese wurden parallel zu den Veranstaltungen erarbeitet und mit Workstream-Teilnehmer:innen besprochen. Die Erkenntnisse aus den Recherchen finden sich in Kapitel 5.

3. Ergebnisse der Veranstaltungsreihe B3 im Dialog

Die Veranstaltungsreihe B3 im Dialog entstand auf Vorschlag des Workstream-Sprechers Gregor Bransky und wurde von den Mitgliedern des Workstreams mitgetragen. Die monatliche Veranstaltungsreihe diente als Plattform zum Austausch zwischen den eingeladenen Expert:innen, der Zivilgesellschaft und den Mitgliedern des Workstreams. Die digitalen Veranstaltungen standen allen Interessierten innerhalb und außerhalb des Workstreams offen. Soweit möglich wurde die Veranstaltung aufgenommen und auf dem YouTube-Kanal des BSI veröffentlicht. Nach der Veranstaltung hatten die Teilnehmer:innen die Möglichkeit, sich im informellen Kontext weiter über das Thema auszutauschen.

Die Veranstaltungen wurden federführend von Gregor Bransky organisiert und durch die Teilnehmer:innen des Workstreams sowie die Geschäftsstelle unterstützt. Neben den geladenen Speaker:innen waren regelmäßig verschiedene Expert:innen aus Zivilgesellschaft, Wirtschaft, Forschung und Staat im Publikum, die sich an der Fragerunde und dem nachfolgenden Austausch beteiligten.

Im Folgenden werden die Inhalte einzelner Veranstaltungen zusammenfassend vorgestellt.

21.03.23 – B3 im Dialog: Log4Shell & Consequences

Thema des ersten Abends waren der Umgang mit und die Konsequenzen aus der Zero-Day-Sicherheitslücke Log4Shell[1] in der weitverbreiteten Software-Library Log4j.[2] Die im Dezember 2021 gefundene Sicherheitslücke führte dazu, dass fremder Code auf Servern, die die Bibliothek log4j nutzen, ausgeführt und auf sensible Daten von außen zugegriffen wurde, wovon schätzungsweise mehrere

[1] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4Shell_WarnstufeRot.html.
[2] https://github.com/apache/logging-log4j2/.

Millionen Produktivsysteme betroffen waren.[3] Die Lücke im Code existierte seit 2013 und es kann im Nachhinein nicht eingeschätzt werden, ob und auf welche Weise die Lücke vor dem offiziellen Fund ausgenutzt wurde.

Zu Gast waren Christian Grobmeier vom Log4j-Maintainer-Team und Brian Behlendorf von der Open Source Security Foundation (OpenSSF).[4] Behlendorf war Mitgründer des Apache-Webserver-Projekts und der Apache Foundation[5] und engagiert sich mit seiner Stiftung für die Verbesserung der Sicherheit in Open-Source-Software. Die Veranstaltung wurde von Isabel Drost-Fromm von der InnerSource Foundation[6] moderiert.

Christian Grobmeier sprach über die Auswirkungen der Sicherheitslücke Log4Shell auf die Gesellschaft und auf das Log4j-Team. Nach dem Vorfall gab es sehr eng getaktete Bemühungen, Log4j durch ehrenamtliche Programmierer, die ihren Weihnachtsurlaub kürzten oder komplett absagten, zu patchen. Obwohl alle ehrenamtlich an dem Projekt arbeiteten, war das Team starken Anfeindungen im Netz wegen der benötigten Zeit für den Patch ausgesetzt. Er sprach an, dass viele Unternehmen in einer großen Abhängigkeit von Open-Source-Software in ihren Projekten stehen und diese Softwarekomponenten nicht immer regelmäßig überprüfen und/oder updaten. So würden auch heute noch regelmäßig veraltete Versionen von Log4j heruntergeladen, die in alten Projekten nie upgedatet wurden. Grobmeier wies zudem darauf hin, dass die chinesische Firma Alibaba, die die Lücke meldete, im Anschluss von der eigenen Regierung mit wirtschaftlichen Sanktionen belegt wurde, da die Lücke rechtlich zunächst ihnen hätte gemeldet werden sollen.[7]

Brian Behlendorf stellte die Arbeit der Open Source Security Foundation vor, die 2020 von der Linux Foundation gegründet wurde und deren Ziel es ist, Open-Source-Entwickler:innen durch Weiterbildungen und Finanzierung zu unterstützen. Behlendorf stellte verschiedene Wege vor, dies zu realisieren. Erstens bräuchte es viel mehr Bildungsangebote zum Thema IT-Sicherheit für Entwickler:innen, und zwar bereits während ihrer Ausbildung. Zweitens könnten Security-Oriented Design Reviews und Security Audits dabei helfen, Sicherheitslücken zu entdecken. Open-Source-Projekten fehlen häufig die Ressourcen, diese

[3] https://www.washingtonpost.com/technology/2021/12/20/log4j-hack-vulnerability-java/.
[4] https://openssf.org/.
[5] https://www.apache.org/.
[6] https://innersourcecommons.org/.
[7] https://www.zdnet.com/article/log4j-chinese-regulators-suspend-alibaba-partnership-over-failure-to-report-vulnerability/.

Schritte zu gehen. OpenSSF hat verschiedene Angebote, um die Entwickler:innen in ihrer Arbeit unterstützen.

In der anschließenden Diskussionsrunde sprachen die Panel-Teilnehmer:innen über weitere Möglichkeiten der Unterstützung und Lösungen. Sie lobten die Gründung des SovereignTechFund[8], der Open-Source-Projekte in Deutschland finanziell unterstützt. Ein weiteres Thema war die Regulierung der Haftung für Schäden. Diese dürfe nicht auf die Entwickler:innen von Open-Source-Software verlagert werden, weil dies dazu führen würde, dass viele ihre Projekte nicht fortsetzen oder gar nicht erst anfangen. Ein letzter Punkt war die bessere Vernetzung zwischen Software-Communitys, die ihr Wissen strukturierter aufbauen sollen, um zügig auf Vorfälle wie Log4Shell reagieren zu können.

Die Aufnahme der Veranstaltung kann auf YouTube angeschaut werden: https://www.youtube.com/watch?v=rLYEwhCx8XY.

18.04.23 – B3 im Dialog: Meldeprozesse in Deutschland

In der zweiten Ausgabe von B3 im Dialog ging es um die existierenden staatlichen Meldewege in Deutschland für Sicherheitslücken in Software. Für den Meldeweg der eigentlichen Sicherheitslücke präsentierte Tassilo Thieme vom CERT-Bund[9] den CVD-Prozess des BSI. Für den Meldeweg von ungewollt abgeflossenen Daten präsentierte der Referent der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI)[10], Hinnerk van Bruinehsen, den Ansatz und Erfahrungen der Berliner Behörde. Ein Mitglied des Workstreams, Bianca Kastl, moderierte die Veranstaltung und das anschließende Q&A.

Nach einer kurzen Einführung, wie der CVD-Prozess[11] des BSI aufgebaut ist, zeigte Tassilo Thieme die verschiedenen Begleitangebote des BSI auf, etwa die CVD-Richtlinie[12] und die CVD-Leitlinie[13], die den Prozess im Detail erklären und verdeutlichen, was Sicherheitsforschende bei einer Meldung von Schwachstellen erwarten können. Ein Onlineformular ermöglicht, pseudonym oder anonym eine

[8] https://sovereigntechfund.de.
[9] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html.
[10] https://www.datenschutz-berlin.de/.
[11] https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Schwachstellenmeldungen/Schwachstellenmeldungen_node.html.
[12] https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html.
[13] https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Leitlinie/Leitlinie_node.html.

Meldung einzureichen. Das BSI tritt nach der Meldung als Vermittler zwischen Sicherheitsforschenden und Herstellern auf, an die die Schwachstellenmeldungen weitergegeben werden.

Hinnerk van Bruinehsen sprach im Anschluss über Meldungen an die BlnBDI zu Datenabflüssen wie Kund:innendaten durch Sicherheitslücken. Verantwortliche müssen Datenpannen innerhalb von 72 Stunden an ihre zuständige Aufsichtsbehörde melden. Neben Datenpannen können aber auch Datenfunde durch Dritte gemeldet werden. Er erklärte zudem die Rechtslage in Bezug auf § 202a StGB (Ausspähen von Daten), § 202b StGB (Abfangen von Daten), den sogenannten Hackerparagrafen, § 202c StGB (Vorbereitung des Ausspähens und Abfangen von Daten), sowie § 202d StGB (Datenhehlerei). Aufgrund der Formulierungen im StGB würde die BlnBDI nicht zu Meldungen aufrufen, da sich die Meldenden unter Umständen strafbar machen können. Daneben gibt es auch einige weitere Rechtsunsicherheiten, die durch unterschiedliche Regelungen und Auslegungen in den Bundesländern hervorgerufen werden.

Im anschließenden Gespräch ging es um Zuständigkeiten bei Meldungen und den Austausch zwischen den Aufsichtsbehörden und dem BSI, der bisher eher selten erfolgt, da sich die Hersteller bei Datenabflüssen als Verantwortliche an die zuständige Datenschutzbehörde (z. B. den BlnBDI) wenden müssen. Beide wiesen auf die Jahresberichte ihrer Behörden hin, die detailliert über die erfolgten Meldungen berichten. Als eine der größten Herausforderungen wurde von den Vortragenden einstimmig die Rechtsunsicherheit für Sicherheitsforschende genannt, die die Arbeit gerade für Personen im ehrenamtlichen Bereich erschweren würde.

Die Aufnahme der Veranstaltung kann auf YouTube angeschaut werden: https://www.youtube.com/watch?v=QxnL3Q9h0dU.

16.05.23 – B3 im Dialog: Bug-Bounty-Prozesse – Dos and Don'ts

Die dritte Ausgabe des Formats widmete sich Bug-Bounty-Programmen der Industrie aus der Perspektive von Sicherheitsforschenden. Zu Gast war Dr. Ralf-Philipp Weinmann[14], der sich sowohl als Gründer des The Research Institute OÜ für die ehrenamtliche IT-Sicherheitsforschung einsetzt als auch selbst an diversen Bug-Bounty-Programmen teilgenommen hat.

[14] https://ralf.coderpunks.org/.

Die Veranstaltung begann mit einem kurzen Vortrag von Dr. Weinmann über seine Erfahrungen mit Bug-Bounty-Programmen. Aus seiner Sicht zeichnen sich solche Programme durch die finanzielle Belohnung für gemeldete Sicherheitslücken sowie deren Schließung und Veröffentlichung aus. Allerdings erfüllen nicht alle Programme, auch solche von großen Unternehmen, diese Anforderungen. Es kommt immer wieder zu erheblichen Verzögerungen bei den Zahlungen, bis hin zum vollständigen Ausbleiben trotz angemessener Einstufung. Auch die Geschwindigkeit, mit der die Probleme behoben werden, ließe oft zu wünschen übrig. Überdies verpflichten einige Unternehmen Forscher:innen zur Verschwiegenheit, was gegen das Prinzip der Transparenz in der Sicherheitsforschung verstoße.

Im anschließenden Frage-und-Antwort-Teil ging der promovierte Kryptograf auf weitere Aspekte und die allgemeine Kultur rund um bestehende Bug-Bounty-Programme ein. Es sei etwa schon vorgekommen, dass Unternehmen versuchten, durch verpflichtende Verschwiegenheit in Bug-Bounty-Programmen Strafen von Datenschutzbehörden zu umgehen. In solchen Fällen seien die oft deutlich geringeren Belohnungen und der Erhalt des eigenen Rufs der eigentliche Anreiz für das Betreiben des Programms, nicht das Auffinden von Sicherheitslücken. Das führe in der Community oft zu Ablehnung.

Dr. Weinmann betrachtet auch aktuelle Programme kritisch, die zwar Belohnungen für das Auffinden von Schwachstellen in FOSS-Anwendungen anbieten, den betroffenen Entwickler:innen jedoch keine weiteren Ressourcen zur Verfügung stellen. Dadurch werden die Entwickler:innen oft überfordert, wodurch schnelle Updates für Anwender:innen sogar eher behindert würden. Seiner Meinung nach sollte ein gutes Bug-Bounty-Programm eine eindeutige und transparente Kommunikation über den Erhalt, die Bearbeitung und den Abschluss einer Meldung gewährleisten. Außerdem sollten die Bereiche, für die Belohnungen ausgezahlt werden, verständlich definiert werden. Als weiteren Wunsch äußerte der Sicherheitsforscher, dass bei der Einreichung einer bereits gemeldeten Sicherheitslücke deutlich angezeigt wird, dass es sich um ein Duplikat handelt.

Die Aufnahme der Veranstaltung kann auf YouTube angeschaut werden: https://www.youtube.com/watch?v=tb0rcdTi0Jc.

20.06.23 – B3 im Dialog: Diskussion des aktuellen Stands

Innerhalb der vierten Veranstaltung von B3 im Dialog wurde ein Zwischenfazit über die bisherigen Erkenntnisse des Workstreams gezogen und wie diese genutzt werden können, um die weitere Arbeit des Workstreams zu informieren. Als Diskussionsgrundlage präsentierte der Workstream-Sprecher Gregor Bransky den Entwurf eines möglichen Gutachtens, das die Stakeholder ausarbeiten könnten.

Die Diskussion drehte sich zunächst um die identifizierten Hürden in der deutschen IT-Rechtslage, die eine Suche und die Meldung von Sicherheitslücken in Software grundsätzlich erschweren. An dieser Stelle wurden vor allem der Hackerparagraf (§ StGB 202c) und die Paragrafen § StGB 202a und § StGB 202b genannt, auf die sich der Hackerparagraf bezieht. Weiterhin wurde Abschnitt 8 des Urheberrechtsgesetzes genannt, der die Analyse von Computercode von Herstellern ohne deren Zustimmung (z. B. durch eine Veröffentlichung im Open-Source-Rahmen) unterbindet.

In diesem Rechtsrahmen wurden Probleme für Sicherheitsforscher:innen, die Industrie, aber auch Ermittlungsbehörden identifiziert, die ein zivilgesellschaftliches Engagement in der IT-Sicherheitsforschung und auch denkbare staatliche Bug-Bounty-Programme in ihren Möglichkeiten einschränken. Sicherheitsforscher:innen würde die Gefahr drohen, bei der Meldung von Sicherheitslücken wegen der Überwindung von Sicherheits- oder Kopierschutzmechanismen angezeigt zu werden und somit einem Ermittlungs- und Gerichtsverfahren sowie einer eventuellen Verurteilung ausgesetzt zu sein.

Die Industrie kann für ihre eigene Software nur Penetrationstests beauftragen, die sich im Rahmen des eigenen Codes bewegen. Schnittstellen, die von anderen Diensten bereitgestellt werden, müssen aus Rechtsgründen außen vor bleiben. Dieser Umstand ist den Entwickler:innen meist bewusst, bedeutet aber, dass selbst nach Penetrationstest bekannte Unsicherheiten im Softwaredesign bleiben, die den Kund:innen nicht immer mitgeteilt werden. Schließlich könnten staatliche Einrichtungen wie die Datenschutz- oder Verbraucherschutzbehörden Hinweisen oft nicht nachgehen, da die Sicherheitsforscher:innen bei Meldungen aus Selbstschutz zu wenig Informationen für eine Ermittlung gegeben. Bis auf das BSI[15] kann keine staatliche Institution initiativ Penetrationstests für vermutete unsichere Produkte in Auftrag geben, ohne die Hersteller um Erlaubnis zu bitten. Ein solches Vorgehen ist in anderen physischen Produktkategorien, die der Verbraucherschutz testet, nicht nötig.

[15] Das BSI hat hier durch § 7a BSI-Gesetz eine Sonderrolle inne.

Für staatliche Bug-Bounty-Programme bedeutet die aktuelle Rechtslage, dass der Rahmen solcher Programme auf einige wenige Softwarekomponenten limitiert ist, um sich mit einem Aufruf zur Untersuchung fremder IT-Systeme nicht selbst rechtlich angreifbar zu machen. So muss auch bei selbst entwickelten Systemen darauf geachtet werden, dass Schnittstellen zu Dienstleistern im Rahmen einer Analyse nicht untersucht werden und Sicherheitsforscher:innen damit Rechtsbruch begehen.

Die Teilnehmer:innen der Veranstaltung einigten sich darauf, dass die Multidimensionalität der rechtlichen Hürden in der IT-Sicherheitsforschung bislang nicht in seiner Gesamtheit von den politischen Akteur:innen wahrgenommen wird. Es müssen daher Netzwerke mit der Industrie und Behörden ausgebaut werden, um gemeinsam anhand von Fallstudien darzustellen, wer von der aktuellen Regulierung betroffen ist und somit von einer Reform profitieren kann. Die Darstellung der Vorteile einer Reform des IT-Rechts für verschiedene Stakeholder, wie Industrie und Aufsichtsbehörden, könnte die Relevanz in den Augen politischer Akteure erhöhen und zu einem Fortschritt im Diskurs beitragen.

18.07.23 – B3 im Dialog: Staatliche Förderung von FOSS auf EU-Ebene

In der fünften Ausgabe der Veranstaltungsreihe ging es um die Förderung von FOSS auf Ebene der Europäischen Union. Als Gast teilte Saranjit Arora vom Open Source Programme Office der Europäischen Kommission (EC-OSPO)[16] einen Einblick in die Arbeit des Büros. Erneut moderierte Isabel Drost-Fromm von der InnerSource Foundation.

Das EC-OSPO wurde im Rahmen der Open Source Software Strategie 2020-2023[17] der Europäischen Kommission als einer der zehn Punkte des Aktionsplans gegründet und damit beauftragt, die weiteren neun Punkte des Plans umzusetzen bzw. zu fördern. Zu diesen Punkten gehören unter anderem die Förderung einer Open-Source-Kultur innerhalb der Entwicklungsteams der EU sowie die Öffnung der EU-Software-Projekte gegenüber der Öffentlichkeit. Andere Ziele sind der Kontakt zur Open-Source-Community und die Förderung der Sicherheit in FOSS-Projekten, die die EU für Staat und Bürger:innen als wichtig erachtet. Zu diesem

[16] https://joinup.ec.europa.eu/collection/ec-ospo.
[17] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/open-source-software-strategy_en.

Zweck wurden innerhalb des Strategie-Zeitraums Bug-Bounty-Programme für 28 verschiedene Projekte ausgeschrieben und 23 Hackathons durchgeführt.

Im Gespräch mit Saranjit Arora wurden weitere Aspekte der EU-Bestrebungen thematisiert. So wurde erläutert, dass bisher keine strukturierten Kriterien zur Erfolgsmessung von Hackathons und Bug-Bounty-Programmen genutzt werden. Arora sieht des Weiteren einen großen Nutzen darin, eine allgemeine Dokumentation der Förderung von FOSS-Projekten zu beginnen, kann jedoch zu diesem Zeitpunkt keine Ressourcen vonseiten der EU zusagen. Darüber hinaus erachtet er es als notwendig, dass eine Software Bill of Materials (SBoM) zum Standard bei staatlichen Vergaben wird, kann jedoch auch zu diesem Punkt keine Aussagen über Entwicklungen in diese Richtung auf EU-Ebene tätigen.

Die Aufnahme der Veranstaltung kann auf YouTube angeschaut werden: https://www.youtube.com/watch?v=bJeHBj90oRs.

15.08.23 – B3 im Dialog: Sicherheitsforschung im Verbraucher:innenschutz

In der letzten Veranstaltung der Reihe B3 im Dialog im Rahmen des Workstream-Zyklus 2022/2023 ging es um die Rolle des Hackerparagrafen beim Feststellen von Datenschutzverstößen aus der Perspektive des Verbraucher:innenschutzes. Den Impulsvortrag hielt Workstream-Mitglied Dr. Ayten Öksüz von der Verbraucherzentrale Nordrhein-Westfalen e.V.[18], die sich mit Datenschutz und Datensicherheit im digitalen Raum beschäftigt. Moderiert wurde die Veranstaltung vom Workstream-Sprecher Gregor Bransky.

Der Vortrag begann mit einer Erklärung, wie die Verbraucherzentrale NRW e. V. Datenschutzverstöße von Anbietern digital vernetzter Geräte und Dienste prüfen kann. Zum einen besteht die Möglichkeit der generellen Überprüfung der Datenschutzhinweise auf Legalität, zum anderen kann der Datenverkehr technisch überprüft werden. Dies geht jedoch potenziell mit Risiken einher. So sieht die Verbraucherzentrale NRW e. V. aktuell keine Möglichkeit, beispielsweise eine Transportverschlüsselung zu überwinden oder durch Reverse Engineering Einblick in besonders geschützten Datenverkehr zu erhalten, um etwaige Datenschutzverstöße der Anbieter zu überprüfen, ohne sich unter Umständen nach § 202 a StGB strafbar zu machen. Daher kann sie auch nur sehr begrenzt Aussagen zum Datensendeverhalten unabhängig von Herstelleraussagen überprüfen.

[18] https://www.verbraucherzentrale.nrw/.

Die Definition des Hackerparagrafen behindere somit nicht nur die Bestrebungen von ehrenamtlichen Sicherheitsforscher:innen, sondern erschwere auch die Arbeit von öffentlichen Stellen wie den Verbraucherzentralen, da der § 202 a StGB nicht nach Motiven unterscheidet (kriminelle vs. nicht kriminelle Absichten). Anbieter, die möglicherweise gegen geltende Datenschutzgesetze verstoßen oder unzureichende Sicherheitsmechanismen einbauen, könnten so ihre Praktiken hinter dem Hackerparagrafen verstecken. Aus Sicht von Dr. Öksüz besteht ein Bedarf an umfangreicher Rechtssicherheit, unter welchen Voraussetzungen IT-Sicherheitsforschung bzw. technische Prüfungen unter Umgehung von (Transport-)Verschlüsselungen zulässig sind. So wäre es etwa denkbar, derartige Prüfungen in einem verantwortungsvollen Verfahren auf berechtigte Stellen wie Aufsichtsbehörden im Datenschutz und Verbraucherschutzorganisationen und/ oder auf bestimmte Zwecke (z. B. Identifizieren von IT-Sicherheitslücken, Aufdecken von Datenschutzverstößen) zu beschränken.

Dabei müssten neben den betroffenen Paragrafen im Strafgesetzbuch (z.B. § 202 a StGB) ggf. auch andere Normen und Gesetze berücksichtigt werden, gegen die derartige Prüfungen verstoßen könnten (z. B. Urheberrecht bei Reverse Engineering). Der Koalitionsvertrag für die Legislaturperiode 2021 bis 2025 von SPD, Bündnis 90/Die Grünen und FDP sieht vor, dass das „Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z.B. in der IT-Sicherheitsforschung, […] legal durchführbar sein soll." Nach Ansicht von Dr. Öksüz wäre es für die Diskussionen über mögliche Gesetzesänderungen sinnvoll, in Erwägung zu ziehen, ob dazu auch das Feststellen von Datenschutzverstößen zählen soll.

Die anschließende Diskussionsrunde drehte sich größtenteils um mögliche Novellierungen der deutschen Rechtslage der IT-Sicherheitsforschung und mögliche Auswirkungen des Cyber Resilience Act (CRA) auf EU-Ebene. Die Abschaffung des Hackerparagrafen wird von großen Teilen der Teilnehmer:innen nicht unterstützt, da dieser eine wichtige Schutzfunktion für Hersteller:innen, aber auch Verbraucher:innen hat. Benötigt werden jedoch, wie im Impulsvortrag erwähnt, präzise Definitionen von Ausnahmen. Den Ausnahmen sollten enge Grenzen gesetzt werden, allerdings sollte sich die Benennung von befugten Stellen schon allein aus Kapazitätsgründen nicht nur auf eine:n Akteur:in beschränken.

Die Aufnahme der Veranstaltung kann auf YouTube angeschaut werden: https://www.youtube.com/watch?v=nfg-mCnME9w

4. Ergebnisse der externen Vorträge

Im Rahmen der Workstream-Skizze wurde festgelegt, dass der Workstream Vorträge und andere Veranstaltungsformate konzipiert und durchführt. Ziel dieser Bestrebung war es, ein möglichst breites Spektrum an Positionen in den Diskurs zu bringen, um ein staatliches Bug-Bounty-Programm und die Rechtslage in Deutschland zu erörtern. Zusätzlich zu der bereits dargestellten Online-Reihe B3 im Dialog wurden daher bei relevanten Veranstaltungsformaten Dritter Vorträge gehalten und Workshops durchgeführt. Die Veranstaltungen sowie das Feedback wurden in den Workstream-Treffen vor- und nachbereitet und in den darauffolgenden Veranstaltungsformaten aufgegriffen.

Neben den an dieser Stelle vorgestellten Vorträgen wurden weitere Präsentationen konzipiert und eingereicht, die jedoch im Auswahlverfahren des Programmkomitees nicht angenommen wurden oder aus Zeitgründen abgesagt werden mussten. Dazu gehören unter anderem Konzepte für die re:publica 23[19] und die TROOPERS23[20].

29.12.22 – Hacking in Parallel

Speaker: Gregor Bransky
Beschreibung: https://pretalx.c3voc.de/hip-berlin-2022/talk/CLCACQ/
Video: https://media.ccc.de/v/hip-berlin-2002-49277-b3-buntesbugbounty

Der Vortrag von Gregor Bransky setzte sich mit der aktuellen Lage in der deutschen Sicherheitsforschung auseinander und wies vorrangig auf die Problematik des Hackerparagrafen (2020a & 202c StGB) sowie verwandte Regelungen zu Geschäftsgeheimnissen hin. Diese Rechtsvorschriften könnten grundsätzlich dazu führen, so die These des Vortrags, dass das unbeauftragte Testen zugangsgeschützter Anwendungen auf Sicherheitslücken eine empfindliche Strafe nach sich zieht. Auch wenn der Hackerparagraf bislang nicht zu einer Verurteilung von Sicherheitsforscher:innen geführt hat, sind bereits mehrere Fälle einer Anklagedrohung auf dieser Rechtsgrundlage bekannt.

[19] https://re-publica.com.
[20] https://troopers.de/.

Ein weiterer zentraler Punkt des Vortrags war die bisher undurchsichtige Struktur für die Meldung von Sicherheitslücken durch Sicherheitsforscher:innen. So gäbe es mehrere Hundert Institutionen in Deutschland, die in die Cyber-Sicherheit öffentlicher Strukturen eingebunden sind.[21] Die richtige Ansprechperson für die Übermittlung einer Meldung zu finden, könne einen enormen Mehraufwand bedeuten. Es bestehe aber die Hoffnung, dass der in jüngster Vergangenheit aufgesetzte CVD-Prozess des BSI langfristig zu einer Vereinheitlichung von Meldeprozessen führen könne. In der zugehörigen CVD-Richtlinie des BSI sind jedoch das Zurückhalten und die Weitergabe von Sicherheitslücken an andere Behörden nicht explizit ausgeschlossen. Aktivist:innen kritisieren, dass dies dazu genutzt werden könnte, um gemeldete Sicherheitslücken zurückzuhalten und für die Weiterentwicklung von sogenannten Staatstrojanern zu nutzen.

Im Vortrag wurde schließlich eine mögliche Lösung in Form einer zentralen Meldestelle skizziert, deren Aufgabe es wäre, Meldungen an die relevanten Cyber-Sicherheits- und Datenschutzbehörden in Deutschland weiterzuleiten und so den Aufwand für Sicherheitsforscher:innen zu verringern. Es wurde außerdem die Abschaffung des genannten Hackerparagrafens in seiner jetzigen Form gefordert. Im Nachgang des Vortrags gab es mehrfach Interessenbekundung zum Fortgang des Projekts.

07.03.23 – 124. Netzpolitischer Abend

Speaker: Gregor Bransky
Beschreibung: https://digitalegesellschaft.de/2023/03/124-netzpolitischer-abend/
Video: https://www.youtube.com/watch?v=SvXRcoaAY7E

Beim 124. Netzpolitischen Abend wurde Gregor Bransky als Vertreter des Innovationsverbunds Öffentliche Gesundheit[22] eingeladen, um über die Ideen des Workstreams BuntesBugBounty zu sprechen. Neben ihm sprachen zum Thema „Responsible Disclosure“ der Sicherheitsforscher Matthias Marx (kantorkel) und die Journalistin Eva Wolfangel.

Ähnlich wie bei dem Vortrag auf der Hacking in Parallel wurden auch bei diesem Anlass die aktuellen Probleme der intransparenten Meldewege sowie die Gefahr

[21] Siehe dazu auch das Diagramm der Stiftung Neue Verantwortung: https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur.
[22] https://www.inoeg.de/.

für Sicherheitsforscher:innen durch den Hackerparagrafen erörtert. In einer anschließenden kurzen Fragerunde ging Gregor Bransky auf weitere Beispiele für Problematiken im Zusammenhang mit der aktuellen gesetzlichen Lage ein. So nannte er einen Fall aus dem Bereich des Verbraucher:innenschutzes, bei dem eine Behörde eine fahrlässige Lücke nicht weiterverfolgen konnte, da die Person, die die Lücke entdeckt hatte, rechtliche Konsequenzen durch den Hersteller fürchtete und somit keine weiteren Details preisgeben wollte.

Eva Wolfangel präsentierte in ihrem Vortrag einen zu diesem Zeitpunkt aktuellen Erfahrungsbericht zur Meldung von Sicherheitslücken in der Infrastruktur von Universitäten und hob unter anderem die fehlende Einheitlichkeit in Qualität und Struktur bei Meldewegen hervor. Matthias Marx stellte in seinem Vortrag einige Tipps für Sicherheitsforscher:innen aus der Praxisperspektive vor, wie Sicherheitslücken grundsätzlich am besten behandelt und gemeldet werden sollten. In einer anschließenden Podiumsdiskussion sprachen die Referent:innen über mögliche Vorschläge zur Verbesserung der Sicherheitsforschung in Deutschland. Diese Diskussion wurde nicht aufgezeichnet.

14.03.23 - FOSS Backstage

Speaker: Gregor Bransky
Beschreibung: https://program.foss-backstage.de/fossback23/talk/WEXPSB/
Video: https://www.youtube.com/watch?v=xDbbNm2_JLg

An einem offenen Panel zur Funktion von Sicherheit bei Free and Open Source Software nahm Gregor Bransky als Vertreter des Workstreams BuntesBugBounty teil. Zu den Teilnehmer:innen gehörten außerdem Isabel Drost-Fromm, Open-Source-Strategin, und Thomas Fricke, Sicherheitsarchitekt und FOSS-Aktivist. Des Weiteren konnten sich Personen aus dem Publikum auf die Bühne setzen, um Fragen zu stellen oder mitzudiskutieren.

Zu den besprochenen Themen gehörte unter anderem die Vereinfachung von Sicherheitslücken-Meldungen im FOSS-Bereich. Der Fokus lag dabei auf der Bekanntmachung von Lücken durch die Software-Supply-Chain hindurch. Im Idealfall sollte es einen einfachen Weg für Nutzer:innen und Entwickler:innen geben, zu erfahren, wenn kritische Sicherheitslücken in Software-Bibliotheken gefunden wurden, die wiederum in größeren Software-Projekten genutzt werden. Dies könne durch eine Software Bill of Materials (SBoM) realisiert werden.

Ferner wurden positive und negative Beispiele aus der Praxis vorgestellt und thematisiert, wie mit Sicherheitslücken in FOSS-Projekten bereits umgegangen wurde. Ergänzend wurden Ansätze diskutiert, wie die Resilienz von FOSS-Projekten gegenüber teilweise jahrealten Sicherheitslücken gestärkt werden kann.

Vor dem Panel gab Gregor Bransky einen kurzen Impuls zum Vorschlag einer security.txt. Hierbei handelt es sich um eine Datei in einem Git Repository oder auf einem Webserver (ähnlich wie die Datei robots.txt auf einem Webserver), über die die Forscher:innen schnell erfahren können, wie sie Lücken korrekt melden können.[23]

08.04.23 – easterhegg

Speaker: Gregor Bransky
Beschreibung: https://cfp.eh20.easterhegg.eu/eh20/talk/XEGM7H/ & https://cfp.eh20.easterhegg.eu/eh20/talk/ADNGMY/
Video: https://media.ccc.de/v/eh20-71-buntes-bug-bounty-teil-ii-update-aus-dem-cybersicherheitsdialog

Bei der easterhegg-Konferenz wurde ein Update zu den bisherigen Erkenntnissen aus dem Workstream BuntesBugBounty durch Gregor Bransky präsentiert. Die Erkenntnisse wurden im Rahmen der Arbeitstreffen und der bisherigen Vorträge gesammelt.

Unter anderem wurden als mögliche Lösungsansätze für transparente Meldewege die Software Bill of Materials sowie eine security.txt vorgestellt. Weitere Aspekte waren die zu beachtenden Punkte bei der Erstellung eines Bug-Bounty-Programms, inklusive der Finanzierung und der Besonderheiten bei FOSS-Software. Es wurde außerdem ein Schlaglicht auf die aktuellen Entwicklungen in nationalen und internationalen Regulierungsprozessen im Kontext der Sicherheitsforschung geworfen. Schließlich wurde auch die Rolle von NGOs bei der Wartung von FOSS-Software hervorgehoben.

In einer anschließenden Fragerunde wurden weitere Aspekte der Regulierung in Deutschland, die Ziele des Workstreams und die Erleichterungen für Sicherheitsforscher:innen thematisiert. Anschließend konnten Interessierte an

[23] https://program.foss-backstage.de/fossback23/talk/KEMRGG/.

einem Workshop teilnehmen, in dem mögliche Lösungswege und die nächsten Schritte für den Workstream konkretisiert wurden.

10.05.23 – 19. Deutscher IT-Sicherheitskongress

Speaker: Bianca Kastl & Sabine Griebsch
Link: https://www.bsi.bund.de/DE/Service-Navi/Veranstaltungen/Deutscher-IT-Sicherheitskongress/19-Dt-IT-Sicherheitskongress/19-dt-IT-Sicherheitskongress_node.html

Workstream-Stakeholderin Bianca Kastl stellte zusammen mit Sabine Griebsch vom Dialogkomitee beim 19. Deutschen IT-Sicherheitskongress des BSI sowohl den Dialog für Cyber-Sicherheit als auch die Workstreams „BuntesBugBounty“ und „UpSchooling“ vor. Zunächst ging es um die Entstehungsgeschichte des Dialogs, der 2016 als jährliche und in sich geschlossene Denkwerkstatt begann und 2021 um die Workstreams erweitert wurde, die jeweils ein im Rahmen der Denkwerkstatt festgelegtes Thema in einem Zeitraum von drei bis neun Monaten bearbeiten.

Nachdem Sabine Griebsch den Workstream „UpSchooling“ näher beleuchtet hatte, ging Bianca Kastl auf die Idee und den Verlauf den Workstreams „BuntesBugBounty“ ein. Kastl hob die Wichtigkeit einer einfachen und rechtssicheren Meldemöglichkeit für Sicherheitslücken hervor, die auf der einen Seite als Anlaufstelle für Lücken in Produkten aller Hersteller dienen und zum anderen die Meldung an alle relevanten Behörden weiterleiten soll, sodass die Sicherheitsforscher:innen entlastet werden.

Außerdem betonte sie, wie wichtig es ist, die ehrenamtlichen Sicherheitsforscher:innen (im FOSS-Bereich) wertzuschätzen, die Sicherheitslücken, die potenziell mehrere Tausend Nutzer:innen betreffen können, finden. Deswegen erörtere der Workstream die Möglichkeiten eines staatlichen Bug-Bounty-Programms, arbeite aber auch an den Hürden im deutschen Rechtssystem, die im Extremfall zu einer Freiheitsstrafe führen könnten.

5. Ergebnisse der Recherchen

Teil der Workstream-Skizze waren zudem Recherchen zum Thema Bug-Bounty-Programme in der EU, die federführend von der Geschäftsstelle durchgeführt und dem Workstream bereitgestellt wurden.

5.1 Recherche zu Bug-Bounty-Programmen

Als eine der Zielstellungen der Workstream-Skizze wurde festgelegt, dass eine Übersicht der existierenden staatlichen Bug-Bounty-Programme in der EU erstellt wird und weitere Beispiele aus dem internationalen Kontext hervorgehoben werden. Der Bericht findet sich in Anhang 1.

Zunächst erfolgte eine Materialrecherche zu öffentlich verfügbaren Informationen. Parallel wurden relevante Behörden innerhalb der Mitgliedsländer der EU kontaktiert. Es konnten öffentliche Informationen über sechs staatliche Bug-Bounty-Programme eingeholt werden, von denen zwei auf EU-Ebene stattfanden oder -finden. Des Weiteren wurden Informationen über neun weitere Programme aus Kanada, der Schweiz, den USA und Singapur dokumentiert.

Die Recherche zeigt, dass sich die meisten staatlichen Bug-Bounty-Programme auf einzelne staatliche Dienste beschränken, die bereits über eine öffentlich zugängliche Oberfläche für Bürger:innen verfügen. Ferner ist ein großer Teil der Programme zeitlich begrenzt, was sich durch die oft temporären Budgets in staatlichen Kontexten erklären lässt. Einzig die Niederlande verfügen über eine Art dauerhaftes staatliches Bug-Bounty-Programm, das jedoch in der Art und Höhe der Belohnungen für gemeldete Schwachstellen vage bleibt. In Hinblick auf FOSS-Anwendungen sind vorrangig das Projekt EU-FOSSA 2[24] und das EC-OSPO[25] hervorzuheben, zu denen jeweils ein temporäres Bug-Bounty-Programm für ausgewählte Open-Source-Software gehört (hat).

Bei der Recherche wurde durch Einschränkungen bei Antworten und Hinweise in Dokumenten deutlich, dass es mit großer Wahrscheinlichkeit weitere staatliche Bug-Bounty-Programme gibt oder gab, über die jedoch nicht öffentlich gesprochen wird. Über die Dimension dieser „verborgenen“ Programme konnten keine Informationen erlangt werden.

5.2 Recherche zu möglichen Kriterien

[24] https://joinup.ec.europa.eu/collection/eu-fossa-2/solution/eu-fossa-pilot/news/eu-fossa-project-submits-resu.
[25] https://joinup.ec.europa.eu/collection/ec-ospo.

Aus der genannten Recherche zu staatlichen Bug-Bounty-Programmen in der EU und weiteren Beispielen wurden mögliche Kriterien abgeleitet, nach denen ein weiteres staatliches Programm konzeptionell aufgebaut werden könnte. Die Auflistung dieser Kriterien findet sich in Anhang 2.

Mit der Erstellung des Kriterienkatalogs kam die Erkenntnis, dass eine effektive Abdeckung der Open-Source-Infrastruktur eines Staates nur möglich ist, wenn Auftragnehmer verpflichtet und FOSS-Projekte dabei unterstützt werden, eine Software Bill of Materials zu erstellen, die eine Auflistung der genutzten Softwareprojekte enthält. Zudem muss ein Staat eine Liste der genutzten High-Level-Anwendungen pflegen, um die Software-Landschaft im eigenen Land vollständig zu überblicken.[26] Nur so kann realistisch eine Übersicht geschaffen werden, welche Projekte in welcher Relevanz auftauchen und somit unterstützt werden sollten. Solange eine solche Übersicht jedoch nicht verpflichtend erstellt werden muss, können andere Prozesse, wie die Sicherheitsbewertung beispielsweise durch ein Expert:innengremium oder ein Abstimmungsverfahren, als Alternative dienen.

5.3 Recherche zu Richtlinie 2013/40/EU

Zu Beginn des Workstream-Zyklus wurde eine Recherche zur Richtlinie 2013/40/EU[27] des Europäischen Parlaments und des Europäischen Rates vom 12. August 2013 erwogen, die die Umsetzung in allen Mitgliedsstaaten der EU analysieren sollte. Diese Recherche wäre über den definierten Output der Workstream-Skizze hinaus gegangen. Es stellte sich jedoch heraus, dass die Workstream-Teilnehmer:innen und die Geschäftsstelle eine Recherche in dieser Dimension nicht im Rahmen des Projekts durchführen können. Sowohl die Rechtstexte in Originalsprache als auch die Eigenheiten der Rechtssysteme der Mitgliedsländer hätten individuelle Expertise für jedes Land im Bereich des IT-Rechts verlangt.

6. Erkenntnisse

Im Folgenden werden die Erkenntnisse aus dem Workstream-Zyklus zusammengefasst. Zunächst wird der inhaltliche Perspektivgewinn durch die Vorträge und Workshops dargestellt und darauffolgend die Erfahrungen der Gruppe mit dem Prozess an sich.

[26] Ein Ausgangspunkt könnte in Deutschland zum Beispiel die Open CoDE-Initiative sein: https://opencode.de/de.
[27] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32013L0040.

6.1 Erkenntnisse aus den Veranstaltungen

Ziel und Ergebnis der Veranstaltungen waren vor allem das Zusammenbringen von Positionen und Erkenntnissen aus verschiedenen Gruppen, die sich im weitesten Sinne mit dem Finden und Bearbeiten von Sicherheitslücken überwiegend in FOSS-Software befassen.

1. **Multidimensionalität des Problems:** Einer der Ausgangspunkte des Workstreams war die rechtliche Unsicherheit für ehrenamtliche Sicherheitsforscher:innen nach dem sogenannten Hackerparagrafen. Es zeigte sich jedoch, dass es deutlich mehr Gesetzestexte (z. B. zum Urheberrecht) gibt, die die Sicherheitsforschung betreffen und für die Rechtsunsicherheit sorgen. Zudem sind auch wesentlich mehr Stakeholder in ihrer Arbeit von den rechtlichen Einschränkungen betroffen. So haben etwa Verbraucher:innenschutzzentralen derzeit keine Handhabe, um Meldungen von Datenschutzverstößen in Software auf technischer Ebene nachzugehen. Auch professionelle Penetration-Tester können oftmals nicht das gesamte System testen, da die Schnittstellen zu anderer Software nicht Teil des Service-Vertrags sind und daher keine Rechtssicherheit besteht.
2. **Uneinigkeit in der Auslegung des gesetzlichen Rahmens:** Innerhalb des Diskurses zeichnete sich ab, dass es ein breites Spektrum an Einschätzungen der bestehenden Rechtslage gab. Während die einen betonten, dass es noch zu keinem Gerichtsverfahren für Sicherheitsforscher:innen etwa auf Basis des Hackerparagrafen gekommen ist, wiesen die anderen darauf hin, dass bereits ein Ermittlungsverfahren eine emotionale und/ oder finanzielle Belastung bedeuten kann. Des Weiteren würde die Judikative der Bundesländer die Gesetzeslage unterschiedlich auslegen, weshalb Sicherheitsforscher:innen rechtlich zusätzlich verunsichert sind.
3. **Unterfinanzierung von FOSS-Projekten:** Viele FOSS-Projekte, die in der staatlichen Infrastruktur Nutzung finden, werden weiterhin ehrenamtlich betreut, was dazu führen kann, dass Sicherheitsmeldungen lange unbearbeitet bleiben oder in besonders kritischen Fällen eine Lösung des Problems wegen fehlender Krisenmechanismen länger dauern kann, wie es bei Log4Shell der Fall war. Dieses Problem könnte dadurch gelöst werden, dass die Entwickler:innen finanziell so entlohnt werden, dass sie einen Teil ihrer Zeit dauerhaft für das Projekt aufwenden können. Die Finanzierung von Bug-Bounty-Programmen kann also nur ein erster Schritt sein und

muss von der Finanzierung der Lösung und Implementierung begleitet werden. Im Gegenzug sollten veraltete und mit Sicherheitslücken behaftete Versionen nicht mehr zum Download angeboten werden, um Sicherheitslücken nachhaltig zu schließen.

4. **Strukturierung der FOSS-Förderung:** Es gibt bisher keine gute Dokumentation der verschiedenen Fördermaßnahmen für FOSS-Software. Einzelne Fördertöpfe sind in der Community bekannt, jedoch müssen Akteur:innen, die ein neues Förderprogramm aufbauen möchten, erst eine Recherche durchführen, welche Projekte wann und wie bereits gefördert wurden. Den befragten Expert:innen sind auch keine Planungen eines solchen Projekts bekannt.
5. **Keine Absprache zwischen Behörden bei Meldungen:** Wenn die Meldung einer Sicherheitslücke entweder an eine Datenschutzbehörde oder das BSI geht, bedeutet das nicht, dass die andere Behörde automatisch darüber in Kenntnis gesetzt wird. Dies wird sowohl mit den bisher fehlenden Kommunikationskanälen als auch den Zuständigkeiten der Meldestellen begründet. Mehrfach wurde von Personen aus der Sicherheitsforschung betont, dass die Rationalisierung des Prozesses den Aufwand für die meldende Person deutlich verringern würde.

6.2 Erkenntnisse aus der Reflexion bzw. den Umfragen mit Mitgliedern

Eine Abfrage der Perspektiven wurde auf Wunsch der Teilnehmenden des Workstreams sowohl in der Mitte des Workstream-Zyklus als auch zum Ende als Teil der internen Evaluation durchgeführt. Ergänzend wurden Notizen aus den Arbeitstreffen herangezogen.

Ein Großteil der Antworten hob positiv hervor, dass der Schwerpunkt auf den Austausch verschiedener Perspektiven gelegt wurde. Auf diese Weise konnten die Dimensionen der im Workstream identifizierten Probleme erörtert und das Format zum Netzwerkaufbau für weiterführende Projekte genutzt werden. Die Gäste und die Impulsvorträge wurden gelobt. Die Aufnahmen der einzelnen Veranstaltungen der Reihe B3 im Dialog wurden auch im Nachhinein interessiert angeschaut und diskutiert. Durch die Veröffentlichungen auf YouTube wurden einzelne Personen überhaupt erst auf das Projekt Dialog für Cyber-Sicherheit aufmerksam.

Wiederholt kam jedoch die Kritik auf, dass eine tiefergehende inhaltliche Auseinandersetzung mit Teilaspekten im Rahmen des Formats nicht möglich war und

die zeitlich begrenzte Verfügbarkeit einiger Teilnehmer:innen eine intensivere Zusammenarbeit erschwerte. Kollaborationstools wie die Nextcloud und ein Git-Repository standen zur Verfügung, wurden jedoch kaum genutzt. Diskussionen außerhalb der Veranstaltungen fanden vor allem über den E-Mail-Verteiler statt.

7. Fazit und nächste Schritte

Der Workstream BuntesBugBounty hat es sich zur Aufgabe gemacht, eine diskursive Plattform zu schaffen, die sich mit der Rechtslage der IT-Sicherheitsforschung auseinandersetzt, Probleme identifiziert und mögliche Gegenmaßnahmen erarbeitet. Recht früh zeigte sich, dass einem staatlichen Bug-Bounty-Programm in Deutschland eine weitreichende Diskussion über die rechtlichen Rahmenbedingungen eines solchen Programms voransteht. In den sechs Veranstaltungen der Reihe „B3 im Dialog“ sowie den diversen Vorträgen auf externen Konferenzen konnte ein großes Spektrum an Perspektiven erhoben werden. So konnten weitere Gruppen von Stakeholder identifiziert werden, die in ihrer Arbeit durch das existierende IT-Recht behindert werden, wie z. B. IT-Sicherheitsforscher:innen, die bei Aufträgen nicht Schnittstellen zu anderen System testen können, und Aufsichtsbehörden, die in ihren Ermittlungsfähigkeiten limitiert sind. Außerdem wurde der Blick auf Teile des IT-Rechts außerhalb des Hackerparagrafen erweitert, wie dem Urheberrecht und das Gesetz zum Schutz von Geschäftsgeheimnissen.

Die Teilnehmenden des Workstreams werden die Erkenntnisse aus dem Zyklus bei der kommenden Denkwerkstatt des Dialogs für Cyber-Sicherheit im Oktober 2023 vorstellen. Einige Mitglieder des Workstreams beabsichtigen ihre Arbeit fortzuführen und planen bereits neue Veranstaltungen, um weitere Stakeholder in die Diskussion zu einem staatlichen Bug-Bounty-Programm und die Rechtslage der IT-Sicherheit in Deutschland einzubeziehen. Parallel dazu gibt es Bestrebungen innerhalb der Gruppe, das gesammelte Wissen in Textform zu bringen und Handlungsmaßnahmen zu formulieren. Das Produkt soll sich an politische Akteur:innen richten, die in einem nächsten Schritt ebenfalls in den Dialog eingebunden werden sollen, um konkrete Möglichkeiten auf legislativer Ebene zu besprechen.

Es hat sich gezeigt, dass von vielen Seiten großes Interesse an dem Thema staatliches Bug-Bounty-Programm sowie den rechtlichen Rahmenbedingungen besteht. Allerdings wurde auch deutlich, dass viele Aspekte nicht hinreichend beleuchtet sind, beispielsweise wie eine mögliche Änderung des Hackerparagrafen

aussehen könnte, um den dargestellten Problempunkten entgegenzuwirken. Die Mitglieder des Workstreams BuntesBugBounty bleiben hierzu im Dialog.

Anhang

Anhang 1 – Recherche zu internationalen Bug-Bounty-Programmen
Anhang 2 – Mögliche Kriterien eines Bug-Bounty-Programms

Dialog für Cyber-Sicherheit

Staatliche Bug-Bounty-Programme in der Übersicht

Recherche im Rahmen des Workstreams „BuntesBugBounty“

Dialog für Cyber-Sicherheit

Ein Projekt im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Stand: Juni 2023

1. Bug-Bounty-Programme - Definition

Im Rahmen von Bug-Bounty-Programmen werden externe Sicherheitsforscher:innen dazu eingeladen, nach Schwachstellen in einer Software oder IT-Infrastrukturen zu suchen. Es sind strukturierte Initiativen, bei denen finanzielle oder andere materielle Belohnungen (Bounties) für das Identifizieren und Melden von Sicherheitslücken in IT-Systemen angeboten werden. Die Initiativen werden entweder durch die Hersteller der Software oder Akteure, die direkt oder indirekt von Schwachstellen betroffen wären, durchgeführt. Diese Akteure können z. B. private Firmen, staatliche Institutionen, aber auch NGOs sein. Die Auszahlung der Belohnung erfolgt dabei häufig nach der Validierung und Behebung der gemeldeten Schwachstellen. Die Höhe der Belohnung variiert je nach Schweregrad der gemeldeten Schwachstelle und den Richtlinien der jeweiligen Institution.

Bug-Bounty-Programme können entweder intern verwaltet oder über externe Plattformen angeboten werden. Das Ziel dieses Verfahrens besteht dabei in der systematischen Einbeziehung externer IT-Sicherheitsspezialist:innen. Nach diesem Verständnis fallen somit unter den Begriff der Bug-Bounty keine Einzelfälle, in denen die materiellen Belohnungen ohne einen zuvor definierten Prozess einmalig ausgezahlt werden. Ausgeschlossen sind auch Programme, die einen *Coordinated Vulnerability Disclosure* (CVD) Prozess anbieten, jedoch keine materielle oder finanzielle Gegenleistung anbieten. Eine Nennung innerhalb einer „Wall of Fame“ ist somit keine „Bounty“.

2. Gegenstand der Programmübersicht

In der nachfolgenden Übersicht werden Bug-Bounty-Programme in der Europäischen Union und repräsentative Programme außerhalb der EU aufgezählt und erläutert. Der Fokus der vorangegangenen Recherche im Rahmen des Workstreams „BuntesBugBounty“ des Dialogs für Cyber-Sicherheit lag dabei auf den Programmen, die entweder durch staatliche Institutionen direkt oder durch staatliche Förderungen durchgeführt wurden oder werden. Neben einer eigenhändigen Recherche basierend auf öffentlich zugänglichen Dokumenten wie Info-Webseiten, Interviews, Pressemitteilungen und Abschlussberichten, wurden die mit der Cyber-Sicherheit beauftragten Behörden aller EU-Länder kontaktiert und um Informationen gebeten. Diese Anfragen wurden von ca. einem Drittel der Befragten beantwortet.

Sowohl in öffentlichen Quellen als auch in den oben erwähnten Antworten der Cyber-Sicherheit-Behörden wurde immer wieder erwähnt, dass auch Invite-Only-Programme existieren, die nicht öffentlich kommuniziert werden. Dementsprechend kann über Länder, die in diesem Bericht nicht genannt werden, nur die Aussage getroffen werden, dass keine öffentlich einsehbaren Bug-Bounty-Programme gefunden wurden (siehe dazu auch die Matrix im Anhang). Es ist weiterhin davon auszugehen, dass die im Bericht genannten Länder möglicherweise weitere Programme betreiben.

Details des Meldeprozesses, wie eine mögliche Verschwiegenheitserklärung als Gegenleistung für eine Belohnung, waren zum Zeitpunkt dieser Recherche teilweise nicht öffentlich zugänglich und konnten daher nur eingeschränkt eingesehen und berücksichtigt werden.

3. Programme in der Europäischen Union

Zusätzlich zu der eigenhändigen Recherche wurden alle zuständigen Institutionen der EU-Länder per E-Mail um weitere Informationen gebeten. Sofern sie mitgeteilt haben, dass kein Bug-Bounty-Programm existiert oder existiert hat, wurde dies in der Matrix im Anhang vermerkt. Fehlende Antworten sind dort ebenfalls dokumentiert.

3.1 Finnland: Ministry of Foreign Affair - Bug Bounty

Beginn: September 2020
Ende: -
Programm-Zugriff: Semi-Offen
Mögliche Höchstsumme: 3.000 EUR
Verantwortlich: Ministry of Foreign Affairs Finland

Das Bug-Bounty-Programm des finnischen Außenministeriums lief in einer Testphase von Dezember 2019 bis Mai 2020 und ist seit September 2020 als dauerhaftes Programm angelegt. Gegenstand des Programms sind insbesondere die öffentlich zugänglichen Webseiten des Ministeriums, darunter:

- um.fi – Die Informationsseite des Außenministeriums
- matkustusilmoitus.fi – Eine Seite zur Meldung von Reisen an das Ministerium
- vaarinkayttoilmoitus.fi – Eine Seite zur Missbrauchsmeldung von Entwicklungsgeldern

Die Webseiten werden in der Produktionsumgebung getestet. Forscher:innen bekommen keinen erweiterten Zugriff. Das Programm ist nach einer Registrierung im System ausschließlich für Personen mit einem finnischen Bankkonto offen.

In der Testphase haben 30 Personen aus Finnland, Argentinien und Indien 100 Schwachstellen gemeldet. Von diesen wurden 32 als kritisch eingestuft, bearbeitet und mit einer Bounty entlohnt. Die Gesamtsumme der Bounties betrug ca. 10.000 EUR, wobei die höchste ausgezahlte Summe für eine einzelne Meldung 3.000 EUR betrug. Es gibt keine Angaben dazu, inwieweit gelöste Meldungen bekannt gemacht wurden.

In der aktuellen Version des Programms werden für Bounties zwischen 100 EUR und 5.000 EUR ausgezahlt. Es sind keine weiteren Informationen zum aktuellen Stand des Programms verfügbar.

Links
https://um.fi/press-releases/-/asset_publisher/ued5t2wDmr1C/content/ulkoministeri-c3-b6n-yhteis-c3-b6llinen-tietoturvatestaus-onnistui-bug-bounty-ohjelmasta-pysyv-c3-a4-testausmuoto/35732
https://www.hackr.fi/ohjelmat/ulkoministerio.html

3.2 Finnland: Suomi.fi Bug Bounty

Beginn: Oktober 2022
Ende: April 2023
Programm-Zugriff: Geschlossen
Mögliche Höchstsumme: 30.000 EUR
Verantwortlich: Digital and Population Data Services Agency Finland

Im Oktober 2022 wurde ein Programm für das Digitale-Dienste-Portal Suomi.fi initiiert, welches Bürger:innen verschiedene Möglichkeiten gibt, Verwaltungsdienstleistungen digital in Anspruch zu nehmen. Das Programm lief bis April 2023 und wurde im November 2022 von einem Hack Day zu elektronischen Identifikationsdiensten begleitet. Forscher:innen konnten je nach Schweregrad zwischen 100 EUR und 30.000 EUR für eine Meldung erhalten. Forscher:innen mussten sich zuvor für das Programm bewerben. Die Systeme wurden in Produktionsumgebungen ohne erweiterten Zugriff getestet.

Es wurden bisher noch keine weiteren Aussagen zu den gemeldeten Schwachstellen oder anderen Metriken gemacht.

Links
https://www.hackr.fi/ohjelmat/DVV-BB.html
https://dvv.fi/en/-/the-digital-and-population-data-services-agency-s-bug-bounty-program-expands-to-suomi.fi-messages-
https://dvv.fi/en/-/ethical-hackers-are-looking-for-information-security-gaps-in-suomi.fi-services-the-digital-identity-application-also-under-testing

3.3 Frankreich: France Identité Private Bounty

Start: Juni 2022
Ende: -
Programm-Zugriff: Auf Einladung
Mögliche Höchstsumme: -
Verantwortlich: Französische Regierung (Zusammenschluss verschiedener Ministerien)

Die französische Regierung startete im Juni 2022 ein Bug-Bounty-Programm, welches sich nur spezifisch mit der Beta-Version der Identifikationsapp „France Identité“ beschäftigt. Nach aktuellen Informationen wurden ca. 30 ethische Hacker:innen eingeladen, um alle Aspekte der App zu überprüfen, vor allem jedoch die Verschlüsselung der Daten. Die App ist noch nicht für die breite Bevölkerung verfügbar.

In einem zweiten Schritt sollen weitere Forscher:innen eingeladen werden. Auf lange Sicht ist geplant, das Programm für alle Akteur:innen zu öffnen. Es wurden keine Aussagen über gefundene Lücken oder ausgezahlte Bounties gemacht.

Links
https://france-identite.gouv.fr/
https://portswigger.net/daily-swig/french-government-launches-private-bug-bounty-program-for-identity-authentication-app

3.4 Niederlande: Responsible Disclosure Policy

Start: ca. 2013
Ende: -
Programm-Zugriff: Offen
Mögliche Höchstsumme: -
Betreiber: National Cyber Security Center of the Netherlands

Der CVD-Prozess der niederländischen Regierung ist offen für alle zentralen Systeme der Regierung. Wenngleich als reguläre CVD-Meldestelle benannt, wird in den Richtlinien eine materielle und finanzielle Belohnung für relevante Sicherheitsmeldungen in Aussicht gestellt. Die Belohnung für eine gemeldete Schwachstelle richtet sich nach dem potenziellen Schaden und der Qualität der Meldung und wird in den öffentlich zugänglichen Unterlagen nicht explizit aufgeführt.

Ähnlich wie die CVD-Richtlinie des BSI erlaubt die niederländische Richtlinie ebenfalls die Meldung von Schwachstellen außerhalb der regierungseigenen Systeme. Es wird jedoch nicht weiter definiert, inwieweit diese Meldungen qualifiziert genug sind, um mit einer Belohnung honoriert zu werden. Weiterhin gibt es keine Angaben dazu, inwieweit gelöste Meldungen bekannt gemacht werden.

Links
https://english.ncsc.nl/contact/reporting-a-vulnerability-cvd

3.5. Europäische Union: EU Free and Open Source Software Auditing 2 (EU-FOSSA 2)

Start: Januar 2019
Ende: August 2022
Programm-Zugriff: Offen
Mögliche Höchstsumme: 25.000 EUR
Verantwortlich: Generaldirektion für Informatik der Europäischen Kommission

Nach einem ersten Zyklus des EU-FOSSA-Projekts zwischen 2014 und 2016, welches einen Security-Audit des Apache Servers und KeePass finanzierte[1], beschloss das EU-Parlament eine Erweiterung des Projekts um ein Bug-Bounty-Programm zwischen Januar 2019 und August 2022.

[1] https://joinup.ec.europa.eu/collection/eu-fossa-2/solution/eu-fossa-pilot/news/eu-fossa-project-submits-resu

Das Programm wurde mit 1,9 Millionen EUR gefördert und umfasste 15 FOSS-Programme[2], welche aus einer Liste von FOSS-Projekten[3] gewählt wurden, die in den EU-Strukturen selbst genutzt werden. Die Liste wurde im Rahmen des ersten Zyklus des Projekts erstellt und im zweiten erneuert. Teil des zweiten Zyklus waren außerdem die Veröffentlichung von Code von selbst entwickelten Anwendungen der EU-Kommission und drei Hackathons.

Die Bedingungen der Programme unterschieden sich in den Anwendungen hinsichtlich der Offenheit, ausgezahlten Beträgen und jeweiligen Dienstleistern, die das Programm durchführten. Eine Gemeinsamkeit war jedoch, dass den Meldeenden weitere 20 % auf die Bounty-Summe gezahlt wurden, wenn zusätzlich zur Meldung auch eine valide Lösung des gemeldeten Problems eingereicht wurde. Insgesamt wurden 213 relevante Bugs gefunden, wovon 70 als kritisch eingestuft wurden (einer davon existierte über 20 Jahre im Code der Anwendung).[4]

Es gibt bisher keine weiteren Informationen darüber, ob und auf welche Weise EU-FOSSA weitergeführt wird.

Links
https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/eu-fossa-2-free-and-open-source-software-auditing_en
https://joinup.ec.europa.eu/collection/eu-fossa-2/news/eu-fossa-2-project-close

3.6 Europäische Union: European Commission's Open Source Programme Office (EC-OPSO)

Start: Januar 2022
Ende: März 2022
Programm-Zugriff: Offen
Mögliche Höchstsumme: 5.000 EUR
Verantwortlich: Europäische Kommission

Das EC-OPSO entstand 2020 auf einer Initiative der Europäischen Kommission als Teil der „Open source software strategy 2020–2023“[5] zur Stärkung von Open-Source-Software im EU-Kontext. Im Januar 2022 wurde das Büro um ein Bug-Bounty Programm erweitert, welches ca. zwei Monate lief.

Das Programm umfasste fünf Anwendungen, die durch öffentliche Dienste der EU genutzt werden. Die Maximalsumme pro gemeldete Sicherheitsmeldung betrug 5.000 EUR. Wie innerhalb des EU-FOSSA Projekts können auch bei EU-OPSO weitere 20 % der Bounty ausgezahlt werden, wenn eine valide Lösung eingereicht wird.

[2] https://joinup.ec.europa.eu/collection/eu-fossa-2/news/eur-3000-eur-25000
[3] https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/2022-02/EC%20FOSS%20Inventory%20Methodology%20%28Revision%202021%29_0.pdf
[4] https://www.computerweekly.com/news/252473363/EU-patches-20-year-old-open-source-vulnerability
[5] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/open-source-software-strategy_en

Ein zusammenfassender Abschlussbericht zum Projekt wurde bisher nicht veröffentlicht, es wurde jedoch in einem Erfahrungsbericht für die Anwendung LEOS verkündet, dass in den zwei Monaten 18 relevante Sicherheitsmeldungen verarbeitet und 16.000 EUR ausgezahlt wurden.[6]

Links
https://joinup.ec.europa.eu/collection/ec-ospo
https://joinup.ec.europa.eu/collection/justice-law-and-security/solution/leos-open-source-software-editing-legislation/news/leos-and-bug-bounty

4. Programme außerhalb der EU

Die repräsentativen staatlichen Bug-Bounty-Programme außerhalb der EU wurden basierend auf Nennungen von Workstream-Mitgliedern und der Qualität der Quellen in englischer und deutscher Sprache ausgewählt. Zu den Programmen wurden nur öffentlich verfügbare Informationen herangezogen.

4.1 Kanada: Bug-Prämienprogramm der Regierung von Quebec

Start: 01.04.2022
Ende: -
Programm-Zugriff: Offen
Mögliche Höchstsumme: 7 500 USD
Verantwortlich: Ministère de la Cybersécurité et du Numérique

Das Ministerium für Cybersicherheit und Digitalisierung der Stadt Quebec hat im April 2022 ein Bug-Bounty-Programm für die eigenen Systeme ins Leben gerufen. Dabei handelt es sich um das erste Programm des Landes auf staatlicher Ebene. Ausgewählte Systeme der Regierung werden in einer Sandbox-Umgebung ohne personenbezogene Daten für Forscher:innen bereitgestellt. Darunter fallen:

- Das Authentifizierungssystem
- Kontaktmöglichkeiten mit der Regierung
- Terminbuchung-Systeme
- Corona-Testportale

Es gibt keine Angaben dazu, inwieweit gelöste Meldungen bekannt gemacht werden. Auch zu der Art der Meldungen oder ausgezahlten Summen waren keine Angaben auffindbar.

Links
https://yeswehack.com/programs/programmes-de-primes-aux-bogues-du-gouvernement-du-quebec-cgcd

[6] https://joinup.ec.europa.eu/collection/justice-law-and-security/solution/leos-open-source-software-editing-legislation/news/leos-and-bug-bounty

https://www.quebec.ca/nouvelles/actualites/details/un-pas-de-plus-pour-rehausser-la-securite-des-actifs-gouvernementaux-lancement-du-programme-de-prime-aux-bogues-40015

4.2 Schweiz: Bug Bounty Post

Start: April 2021
Ende: -
Programm-Zugriff: Offen
Mögliche Höchstsumme: 10 000 CHF
Verantwortlich: Schweizer Post

Als spezialgesetzliche Aktiengesellschaft ist die Schweizer Post im Besitz des Bundes in seiner Rolle als alleiniger Aktionär. Nach einem zunächst geschlossenen Programm mit Einladung im Jahr 2020, öffnete die Post im Mai 2021 die Möglichkeit der Schwachstellensuche und Meldung für alle. Das Bug-Bounty-Programm richtet sich an die meisten Online-Dienste der Post. Darunter fallen:

- Login & Registrierung im Portal
- Der Post-Shop
- Lieferungsverwaltung
- Adressen-Verwaltung / Umzugsanmeldung
- Umleitungsservices
- Die Apps der Post
- Die hauseigene Zahlungsdienstleistung Billing Online

Die Belohnung variiert je nach Dienstleistung und Art der Sicherheitslücke zwischen 100 und 10.000 CHF. Eine Gesamtsumme wird nicht genannt, jedoch zeigt das genutzte Portal zur Annahme von Meldungen, dass (Stand Mai 2023) bereits 560 Meldungen eingegangen sind. Es gibt keine Angaben dazu, inwieweit gelöste Meldungen bekannt gemacht werden.

Links
https://yeswehack.com/programs/swiss-post
https://www.post.ch/en/about-us/responsibility/swiss-post-bug-bounty

4.3 Schweiz: e-Voting Bug Bounty

Start: 02.09.2021
Ende: -
Programm-Zugriff: Offen
Mögliche Höchstsumme: 230 000 CHF
Verantwortlich: Schweizer Post

Als verantwortliche Institution für das e-Voting-Verfahren in der Schweiz organisiert die Schweizer Post ein separates Bug-Bounty-Programm für das dahinterstehende System. Der Quellcode ist schrittweise öffentlich gemacht worden und kann somit auf Schwachstellen überprüft werden. Das Programm folgte einem größeren Testlauf 2019, in dem eine Test-Wahl[7] durchgeführt wurde.

Die Meldungen werden nach erfolgreicher Behebung innerhalb des GIT Repositories in regelmäßigen Statusberichten dokumentiert. Laut Statistik der Plattform wurden bisher 168 Meldungen eingereicht.

Links
https://yeswehack.com/programs/swiss-post-evoting
https://gitlab.com/swisspost-evoting
https://www.evoting-blog.ch/de/pages/2021/der-quellcode-des-zukuenftigen-e-voting-systems-ist-veroeffentlicht

4.4 Singapur: Vulnerability Rewards Programme

Start: 31.08.2021
Ende: -
Programm-Zugriff: Geschlossen
Mögliche Höchstsumme: 150 000 USD (Regulär bis zu 5 000 USD)
Verantwortlich: GOVTECH Singapur

Das *Vulnerability Rewards Programme* ist neben dem *Government Bug Bounty Programme*[8] und dem *Vulnerability Disclosure Programme*[9] eine der Initiativen, welche die digitale Sicherheit des Landes stärken soll. VRP fokussiert sich auf essenzielle Digitale Dienste für die Bürgerinnen des Landes. Dazu gehören:

- Account-Management für Individuen und Unternehmen
- Digitale Identifikationslösungen für Individuen und Unternehmen
- Digitale Dienste für Krankenversicherung und Rente
- Digitale Dienste für Leute mit Visa

Laut eigener Aussage sollen weitere Systeme des Landes folgen. Die Teilnahme am Programm muss durch den Dienstleister HackerOne genehmigt werden, bevor eine Meldung möglich ist. Genehmigte Forscher:innen bekommen einen VPN-Zugang, um das legale Testen der Systeme zu ermöglichen. Dies ermöglicht gleichzeitig dem Dienstleister, die Einhaltung der Richtlinien beim Testen zu kontrollieren.

Weitere Informationen, wie die konkreten Richtlinien oder wie sich Forscher:innen registrieren können, sind nicht öffentlich einsehbar.

[7] https://www.theverge.com/2019/2/12/18221570/swiss-e-electronic-voting-public-intrusion-test-hacking-white-hack-bug-bounties
[8] Siehe weiter unten.
[9] https://www.tech.gov.sg/report_vulnerability

Links
https://hackerone.com/govtech-vrp
https://www.tech.gov.sg/media/media-releases/2021-08-31-new-vulnerability-rewards-programme

4.5 Singapur: Government Bug Bounty Programme

Anfang: 27.12.2018
Ende: Nicht bekannt
Programm-Zugriff: Geschlossen
Mögliche Höchstsumme: 10 000 USD
Verantwortlich: GOVTECH Singapur

Das *Government Bug Bounty Programme* ist eine laufende Reihe von Challenges, die Sicherheitsforscher:innen aufrufen, in einem gewissen Zeitraum Teile der digitalen Infrastruktur des Landes zu testen.

Laut Factsheet[10] wurden vier Iterationen des Programms durchgeführt. Es konnten jedoch nur Informationen über drei Iterationen ausfindig gemacht werden. Forscher:innen mussten sich zuvor als „ethische Hacker:innen" registrieren lassen. Die Belohnungen rangierten zwischen 250 USD und 10.000 USD. Die Programm-Iterationen werden im Folgenden erläutert.

27.12.2018 bis 16.01.2019 // Erstes Government Bug Bounty Programm

Die erste Iteration des Programms umfasste fünf Webseiten der Regierung, die an die Zivilgesellschaft des Landes gerichtet sind.

Es wurden insgesamt 26 relevante Schwachstellen gefunden und 12 000 USD ausgezahlt[11]. Die Belohnungen rangierten zwischen 250 USD und 10 000 USD.

Link: https://www.tech.gov.sg/media/media-releases/govtech-and-csa-partner-cybersecurity-community-on-government-bug-bounty-programme

08.08.2019 bis 28.07.2019 // Zweites Government Bug Bounty Programm

Das zweite Bug-Bounty-Programm der Reihe beschäftigte sich mit neun digitalen Diensten und mobilen Apps, die „higher user touchpoints" hatten.

[10] https://www.tech.gov.sg/files/media/media-releases/Factsheet%20on%20Government%20Crowdsourced%20Vulnerability%20Discovery%20Programmes%20(Updated%20Aug%202021).pdf
[11] https://www.tech.gov.sg/media/media-releases/second-government-bug-bounty-programme-expanded-to-cover-more-systems-and-digital-services?utm_medium=recommender_0

Es wurden insgesamt 31 relevante Schwachstellen innerhalb des Zeitraumes gemeldet und insgesamt 25.950 USD ausgezahlt.

Link: https://www.tech.gov.sg/media/media-releases/31-vulnerabilities-remediated-in-second-government-bug-bounty-programme

18.11.2019 bis 08.12.2019 // Drittes Government Bug Bounty Programm

Das dritte Bug-Bounty-Programm der Reihe beschäftigte sich mit 13 digitalen Diensten und mobilen Apps, die „higher user touchpoints" hatten.

Die Belohnungen rangierten zwischen 250 USD und 10.000 USD, mit weiteren Boni im Wert von 500 EUR, wenn Fehler spezifisch in der mobilen Nutzung der Dienste gefunden wurden. Es wurden 33 relevante Sicherheitslücken gemeldet und insgesamt 30.800 USD ausgezahlt.

Link: https://www.tech.gov.sg/media/media-releases/third-govt-bug-bounty-programme-offers-bonus-payouts-for-mobile-applications

4.6 USA: Hack The Pentagon

Start: April 2016
Ende: Nicht bekannt
Programm-Zugriff: Offen / Geschlossen
Mögliche Höchstsumme: 15 000 USD
Verantwortlich: Department of Defense

"Hack The Pentagon" lief von April bis Mai 2016 und war das erste Programm auf staatlicher Ebene in den USA. Der Aufruf umfasste die Open-Source-Webseiten des *Department of Defense.* Insgesamt registrierten sich 1410 Hacker und es wurden 138 relevante Sicherheitslücken über den Verlauf der Testphase gemeldet. Belohnungen variierten zwischen 100 USD und 15.000 USD, insgesamt wurden 75.000 USD ausgezahlt. Es konnten keine Informationen über die Bekanntmachung der Lücken an die Öffentlichkeit gefunden werden.

Im Anschluss an das Projekt ließ der *Defense Secretary* Ashton Carter verlauten, dass das Ministerium weitere Projekte dieser Art plante. Es ist bekannt, dass mindestens zwei weitere Iterationen des Programms durchgeführt wurden, jedoch ist die Informationslage über den Rahmen und Erfolg für die Öffentlichkeit eingeschränkt.[12]

Das hinter dem Programm stehende *Directorate for Digital Services* verkündete in einer Presseerklärung im März 2023,[13] dass es seit Beginn von „Hack The Pentagon" über 40 weitere

[12] Die Berichterstattung limitierte sich hier nur noch auf die Ausschreibungen, wie z. B. https://www.defense.gov/News/News-Stories/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative/ und https://www.cybercareers.blog/2023/01/hack-the-pentagon-3-0-bug-bounty-announced/

[13] https://www.defense.gov/News/Releases/Release/Article/3346188/dod-chief-digital-and-artificial-intelligence-office-launches-hack-the-pentagon/

Bug-Bounty-Programme durchgeführt hat, jedoch gibt es über die meisten dieser Programme keine öffentlichen Informationen.

Links
www.hackthepentagon.mil
https://www.defense.gov/News/News-Stories/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative/
https://www.usds.gov/projects/hack-the-pentagon

4.7 USA: Hack The Army

Start: November 2017
Ende: Anfang 2021
Programm-Zugriff: Offen / Geschlossen
Mögliche Höchstsumme: 15 000 USD
Verantwortlich: Department of Defense

"Hack the Army" war eine direkte Weiterentwicklung des "Hack The Pentagon", die sich auf die öffentlichen Webseiten der U.S. Armee konzentrierte. Die erste Iteration im November 2017 führte zu 118 relevanten Sicherheitsmeldungen und Belohnungen im Wert von insgesamt 100.000 USD.

Die zweite Iteration fand im vierten Quartal 2019 statt, in der 146 valide Schwachstellenmeldungen dokumentiert und 275.000 USD ausgezahlt wurden. Die dritte Iteration fand zwischen Ende 2020 und Anfang 2021 statt und fokussierte sich ebenfalls auf öffentliche Systeme der Armee. Neben zivilen Sicherheitsforscher:innen wurden diesmal auch Forscher:innen aus dem Militärkontext zur Teilnahme eingeladen. Hier wurden 238 relevante Meldungen gefunden, wovon 102 als hoch eingestuft wurden. An zivile Akteur:innen wurden ca. 150.000 USD ausgezahlt. Es konnten keine Informationen über die Bekanntmachung der Lücken an die Öffentlichkeit gefunden werden.

Links
https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/3106335/hack-the-army/

4.8 USA: Hack U.S.

Start: 04.06.2022
Ende: 11.06.2022
Programm-Zugriff: Offen
Mögliche Höchstsumme: -
Verantwortlich: Department of Defense

Das Programm "Hack U.S." war eine Sonderaktion des *Department of Defense*, welche einen finanziellen Anreiz für die Meldung von Sicherheitslücken bot, die im Rahmen des *DoD*

Vulnerability Disclosure Programm[14] als kritisch oder hoch eingestuft wurden und öffentliche Systeme betraf. Die Aktion lief eine Woche und führte zu 648 Meldungen.

Insgesamt wurden 349 relevante Meldungen eingesendet und ca. 75.000 USD ausgezahlt. Weitere 35.000 USD wurden in nicht weiter definierten Boni vergeben. Es konnten keine Informationen über die Bekanntmachung der Lücken an die Öffentlichkeit gefunden werden.

Links
https://www.hackerone.com/bounty/announcing-results-hack-us
https://hackerone.com/hack-us-h1c?type=team
https://therecord.media/pentagon-bug-bounty-program-turns-up-nearly-350-vulnerabilities

4.9 Vereinigtes Königreich: MoD Bug Bounty Challenge

Start: 01.07.2021
Ende: 03.08.2021
Programm-Zugriff: Geschlossen
Mögliche Höchstsumme: -
Verantwortlich: Ministry of Defense

Das Verteidigungsministerium in Großbritannien führte 2021 eine 30-tägige Challenge durch, in der Sicherheitsforscher:innen eingeladen waren, die Systeme der Behörde zu testen. Am Wettbewerb nahmen 26 eingeladene Forscher:innen teil, die autorisierten Zugriff auf die interne digitale Infrastruktur erhielten.

Die Pressemitteilungen präsentieren keine genaueren Informationen über den Rahmen der Challenge und wie die Belohnungen aussahen. Jedoch wurde in der Erklärung betont, dass das Ministerium die Arbeit mit den Sicherheitsforscher:innen ausbauen möchte, wobei jedoch nicht näher erläutert wurde, in welcher Weise dies geplant ist. Das Ministerium verfügt seit Dezember 2020 über eine eigene CVD-Richtlinie.[15]

Links
https://www.hackerone.com/press-release/uk-ministry-defence-embraces-hackers-secure-digital-assets
https://www.gov.uk/government/news/ethical-hackers-collaborate-with-defence-to-strengthen-cyber-security

[14] https://www.dc3.mil/Missions/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/
[15] https://www.gov.uk/guidance/report-a-vulnerability-on-an-mod-system

5. Fazit

Als Zielstellungen der Recherche wurde definiert, eine Übersicht über die existierenden staatlichen Bug-Bounty-Programme in der Europäischen Union zu erstellen und weitere Beispiele aus dem internationalen Kontext hervorzuheben. Das Vorgehen bestand aus einer Materialrecherche zu öffentlich verfügbaren Informationen sowie dem Kontaktieren von relevanten Behörden innerhalb der Mitgliedsländer. Es konnten Informationen zu sechs staatlichen Bug-Bounty-Programmen in der EU ermittelt werden, von denen vier auf nationaler und zwei auf überstaatlicher Ebene durchgeführt wurden oder noch durchgeführt werden. Ferner wurden Informationen zu neun weiteren Programmen aus Kanada, der Schweiz, den USA und Singapur dokumentiert.

Die Ergebnisse der Recherche verdeutlichen, dass die meisten öffentlichen staatlichen Bug-Bounty-Programme sich auf einzelne staatliche Dienste konzentrieren, die bereits über eine öffentlich zugängliche Benutzeroberfläche für die Bürger:innen verfügen. Hingegen sind Programme, die sich auf die interne staatliche Infrastruktur beziehen, ausschließlich für eingeladene Forscher zugänglich. Des Weiteren sind viele der Programme zeitlich begrenzt, was mit dem einmalig genehmigten Budget erklärt werden kann. Lediglich die Niederlande verfügen über ein dauerhaftes und weitreichendes staatliches Bug-Bounty-Programm, dessen Belohnungssystem für gemeldete Schwachstellen jedoch vage gehalten ist. Im Hinblick auf FOSS-Anwendungen sind insbesondere die Projekte EU-FOSSA 2[16] und EC-OSPO[17] zu erwähnen, die jeweils ein temporäres Bug-Bounty-Programm für ausgewählte Open-Source-Software beinhalten bzw. beinhaltet haben.

Während der Recherche wurde wiederholt festgestellt, dass potenziell weitere staatliche Bug-Bounty-Programme existieren oder existierten, über die jedoch keine öffentliche Kommunikation erfolgt. Informationen über den Umfang dieser „verborgenen“ Programme konnten nicht erlangt werden. Dies verdeutlicht jedoch auch, dass eine tiefergehende und mit rechtlichen Schritten verbundene Recherche zu weiteren Erkenntnissen führen könnte.

Es gibt verschiedene Ansätze, um die vorliegende Recherche fortzusetzen. Nicht beantwortete Kontaktanfragen im EU-Raum könnten erneut gestellt werden, gegebenenfalls auch an andere nationale Institutionen. Sofern eine rechtliche Grundlage besteht, könnten auch formale Informationsanfragen an die zuständigen Behörden gerichtet werden. Obwohl die Kenntnis der Landessprachen der untersuchten Länder potenziell zu zusätzlichen Erkenntnissen führen könnte, lässt die vorliegende Untersuchung vermuten, dass die untersuchten englischsprachigen Materialien bereits einen umfassenden Überblick über den Rahmen der Programme bieten, da sich die Programme in der Regel an ein internationales Publikum richten.

[16] https://joinup.ec.europa.eu/collection/eu-fossa-2/solution/eu-fossa-pilot/news/eu-fossa-project-submits-resu
[17] https://joinup.ec.europa.eu/collection/ec-ospo

Anhang: Matrix

Land / Verbund	Titel	Verantwortlich	Scope	Maximale Bounty	Teilnahme	Aktiv
Belgien	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Bulgarien	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Dänemark	Laut E-Mail-Antwort vom 16.05.2023 gibt und gab es kein staatliches Bug-Bounty-Programm.					
Deutschland	Es ist bisher nicht bekannt, dass ein Programm durchgeführt wurde.					
EU	EU Free and Open Source Software Auditing 2	Generaldirektion für Informatik der Europäischen Kommission	15 FOSS-Programme	25 000 EUR		Nein
EU	European Commission's Open Source Programme Office (EC-OPSO)	Europäische Kommission	Fünf Open-Source Anwendungen des EU Public Services	5 000 EUR		Nein
Estland	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Finnland	Ministry of Foreign Affair Bug Bounty	Ministry of Foreign Affairs Finland	Öffentlich zugängliche Webseiten des Ministeriums	3 000 EUR	Semi-Offen	Ja
Finnland	Suomi.fi Bug Bounty	Digital and Population Data Services Agency Finland	Dienste der Webseite	30 000 EUR	Geschlossen	Nein
Frankreich	France Identité Private Bounty	Regierung Frankreichs	Francé Identité App	-		Ja
Griechenland	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Irland	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Italien	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Kanada (Stadt Quebec)	Programme de prime aux bogues du Gouvernement du Québec	Ministère de la Cybersécurité et du Numérique	Ausgewählte Systeme der Regierung	7 500 USD	-	Ja
Schweiz	Bug Bounty Post	Schweizer Post	Online-Dienste der Post	10 000 CHF	Offen	Ja

Schweiz	e-Voting Bug Bounty	Schweizer Post	System des e-Voting-Systems	230 000 CHF	Offen	Ja
Singapur	Vulnerability Rewards Programme	GOVTECH Singapur	Digitale Dienste für Bürger:innen	150 000 USD	Geschlossen	Ja
Singapur	Government Bug Bounty Programme	GOVTECH Singapur	„Higher User Touchpoints“ der Regierung	10 000 USD	Geschlossen	Nein
Kroatien	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Lettland	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Litauen	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Luxemburg	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Malta	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Niederlande	Responsible Disclosure Policy	National Cyber Security Center of the Netherlands	Alle zentralen Systeme der Landesregierung	-		Ja
Österreich	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Polen	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Portugal	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Rumänien	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Schweden	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Slowakei	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Slowenien	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Spanien	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Tschechische Republik	Keine öffentlichen Informationen gefunden und keine Antwort auf eine E-Mail-Anfrage vom 10.05.23 erhalten.					
Ungarn	Laut E-Mail-Antwort vom 09.05.2023 gibt und gab es kein staatliches Bug-Bounty-Programm.					
USA	Hack The Army	Department of Defense	Öffentliche Systeme der Armee	15 000 USD	Offen / Geschlossen	Nein
USA	Hack The Pentagon	Department of Defense	Öffentliche Webseiten des DoD	15 000 USD	Offen/ Geschlossen	Nein

USA	Hack U.S.	Department of Defense	Scope des VDP Programms des Ministerium	-	Offen	Nein
Vereinigtes Königreich	MoD Bug Bounty Challenge	Ministry of Defense	Interne digitale Infrastruktur des Ministeriums	-	Auf Einladung	Nein
Zypern	Laut E-Mail-Antwort vom 12.05.2023 gibt und gab es kein staatliches Bug-Bounty-Programm. Eine mögliche Initiative wird jedoch untersucht.					

Dialog für Cyber-Sicherheit

Mögliche Auswahlprozesse und -kriterien zur Eingrenzung von Komponenten für ein staatliches Bug-Bounty-Programm

Recherche im Rahmen des Workstreams „BuntesBugBounty“

Dialog für Cyber-Sicherheit

Ein Projekt im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Stand: Juni 2023

1. Einleitung

Im vorliegenden Abschnitt werden potenzielle Prozesse und Kriterien präsentiert, die als Leitlinien für die Auswahl eines Software-Pools für ein staatliches Bug-Bounty-Programm dienen können. Diese Kriterien basieren sowohl auf dem Erfahrungsaustausch innerhalb des Workstreams als auch auf bestehenden staatlichen Bug-Bounty-Programmen. Im Einklang mit den Zielen des Workstreams konzentrieren sich die vorgeschlagenen Ansätze auf *Free and Open-Source-Software* (FOSS), also Programme und Komponenten, die der Öffentlichkeit frei zugänglich sind, aber selten über eine kontinuierliche Finanzierung verfügen. Bei allen vorgeschlagenen Kriterien muss die Nachhaltigkeit des Prozesses berücksichtigt werden, da sich durch stetige Software-Weiterentwicklung und Änderungen in der Lieferkette auch der Anwendungsbereich des Programms verändern kann.

Die Auflistung befasst sich nicht mit den Möglichkeiten und Herausforderungen der Meldung von Sicherheitslücken innerhalb solcher Programme. Eine umfassende Diskussion und Ausarbeitung dieser und anderer Aspekte eines staatlichen Bug-Bounty-Programms ist Bestandteil des Workstreams und seiner Veranstaltungsreihe "B3 im Dialog".

2. Mögliche Auswahlprozesse für Softwarekomponenten

In diesem Kapitel werden mögliche Auswahlprozesse für Softwarekomponenten in ihrer Reinform vorgestellt. Möglich wäre auch eine Kombination der Prozesse, wie eine Vorauswahl von Komponenten (siehe Abschnitt 2.1), die dann in eine Abstimmung (siehe Abschnitt 2.3) kommen.

2.1 Komponenten, die direkt oder indirekt durch staatliche Institutionen genutzt werden.

Um die Notwendigkeit eines staatlichen Bug-Bounty-Programms für die Öffentlichkeit besser zu vermitteln, empfiehlt es sich, Programm auf Softwarekomponenten auszurichten, die von staatlichen Institutionen verwendet werden. Bei der Analyse der direkten Nutzung könnten etwa das *OpenOffice*-Paket, welches zunehmend von Behörden eingesetzt wird, und bei der Analyse der indirekten Nutzung der Paketmanager *conda*, der auch in vielen kommerziellen Softwareentwicklungsprozessen verwendet wird, einbezogen werden.

Eine Schwierigkeit könnte hier der dauerhafte Arbeitsaufwand sein. Oft ist eine leicht auffindbare Auflistung aller FOSS-Komponenten pro Software nicht verfügbar und muss zunächst angefragt oder erstellt werden. Auch existiert bei der Softwareentwicklung das klassische Problem der Versorgungskette, sodass zwar die direkt genutzten Komponenten dokumentiert werden, jedoch nicht die Komponenten der Software, die im Entwicklungsverlauf Anwendung

finden. Jedoch sind es gerade diese Komponenten, die von Angreifer:innen gerne genutzt werden, da sie oft im Sicherheitskonzept von Akteuren nicht genug Beachtung finden.[1]

Eine mögliche Lösung besteht darin, bei staatlichen Aufträgen eine verpflichtende *Software Bill of Materials (*SBOM)[2] einzuführen. Wenn es sich um kostenlose Software handelt, liegt die Recherche nach den Komponenten in der Verantwortung der staatlichen Stelle und muss regelmäßig aktualisiert werden. Bis zu Einführung einer solchen Verpflichtung könnte man entweder auf die Selbstauskunft der Hersteller vertrauen oder eine sich wiederholende Recherche durch das ausführende Organ des Bug-Bounty-Programms durchgeführt werden.

2.2 Expert:innengremium

Eine Gruppe von Expert:innen aus der Sicherheitsforschung eruiert FOSS-Komponenten, die ihrer Meinung nach essenziell für das bestehenden der globalen Software-Infrastruktur sind. Ein potenzieller Vorteil dieses Ansatzes besteht darin, dass Komponenten identifiziert werden können, die in anderen Programmen bisher vernachlässigt wurden, wodurch eine gerechtere Verteilung der finanziellen Ressourcen ermöglicht wird.

Allerdings birgt dieses Programm auch potenzielle Nachteile. Zum einen könnte es zu einer geringeren Vielfalt an abgedeckten Komponenten führen und eine Situation schaffen, in der Komponenten gefördert werden, die zwar allgemein gesellschaftlich relevant sind, jedoch in staatlichen Organisationen wenig oder gar keine Anwendung finden. Ebenso besteht die Möglichkeit, dass die Auswahl der Komponenten aufgrund subjektiver Kriterien erfolgt, je nachdem, wie die Gruppe zusammengesetzt ist.

2.3 Abstimmung / Petitionsverfahren

Im Rahmen dieses Verfahrens besteht die Möglichkeit einer breiten öffentlichen Beteiligung bei der Auswahl der Komponenten. Das Hauptziel sollte darin bestehen, diese Abstimmung in erster Linie an Programmierer:innen und aktive Nutzer:innen zu richten, um sicherzustellen, dass nicht nur Komponenten mit hoher Bekanntheit wie VLC oder GIMP in das Programm aufgenommen werden. Dadurch kann eine breite Akzeptanz für das Programm geschaffen werden, und die aktive Teilnahme ermöglicht zudem ein besseres Verständnis für die Rolle von FOSS. Bereits ähnliches wurde innerhalb des EU-FOSSA-Verfahren[3] durchgeführt.

1 https://en.wikipedia.org/wiki/Supply_chain_attack
2 https://www.cisa.gov/sbom
3 https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/informatics/eu-fossa-2-free-and-open-source-software-auditing_en

3. Mögliche Kriterien für die Auswahlprozesse

Die in Kapitel 2 dargestellten Auswahlprozesse können durch Kriterien informiert werden, die die Priorisierung von Softwarekomponenten erleichtert. Diese werden im Folgenden vorgestellt.

3.1 Nutzungszahl basierend auf Downloads in Paketmanagern/Repositories

Um die Downloadzahlen als Kriterium heranzuziehen, müssen die Zahlen aus verschiedenen Download-Angeboten aggregiert werden. Bei Software, die direkt über die offizielle Webseite des Projekts heruntergeladen wird, muss entweder den selbstberichteten Zahlen vertraut oder ein unabhängiger Prozess definiert werden, der eine Verifizierung der Zahlen ermöglicht. Insbesondere bei grundlegenden Komponenten entspricht die Anzahl der Downloads nicht zwangsläufig der tatsächlichen Nutzung.

3.2 Nutzung innerhalb der staatlichen Infrastruktur

Wie bereits in Abschnitt 1.1 erläutert, gestaltet sich eine vollständige Erfassung aller genutzten Komponenten momentan schwierig, wenngleich nicht unmöglich. Es ist jedoch möglich, Komponenten daraufhin zu überprüfen, ob sie in der staatlichen digitalen Infrastruktur verwendet werden, sofern sie auf anderem Wege vorgeschlagen wurden.

3.3 Finanzierungsmodell des Projekts

Einige FOSS-Projekte gehören teilweise oder vollständig kommerziellen Anbietern, wie npm (Microsoft) oder React (Meta). In diesem Zusammenhang sollte geklärt werden, ob die finanziellen Möglichkeiten des Mutterkonzerns eine Teilnahme an staatlichen Bug-Bounty-Programmen ausschließen. Falls dies der Fall ist, müssten Projekte generell im Umkehrschluss nachweisen, dass sie nicht über ausreichende finanzielle Mittel verfügen, um ein eigenes Bug-Bounty-Programm zu organisieren und zu finanzieren.

3.4 Aufgabenbereich der Komponenten

Es könnten Kategorien geschaffen werden, die vom Projekt abgedeckt werden, wie „Verschlüsselung“, „Programmiersprache“ oder „Datenbank-Management“. So könnte gewährleistet werden, dass sich die Förderung, wenn gewünscht, auf sicherheitskritische Projekte beschränkt. Dadurch könnte sichergestellt werden, dass eine Förderung, falls gewünscht, auf sicherheitskritische Projekte beschränkt wird. Allerdings könnte die Definition dieser Kategorien auch dazu führen, dass es Projekte gibt, die zwar für die Sicherheit der staatlichen Infrastruktur wichtig sind, aber keiner der vorhandenen Kategorien zugeordnet werden können.

4. Fazit

Die vorgestellte Zusammenstellung von Auswahlprozessen und -kriterien bietet einen Überblick über mögliche Ansätze für den Aufbau eines staatlichen Bug-Bounty-Programms. Jeder dieser Ansätze weist seine eigenen Vor- und Nachteile auf, die einander beeinflussen können, wenn mehrere der vorgeschlagenen Optionen kombiniert werden. Für ein Bug-Bounty-Programm, das hauptsächlich auf die Sicherheit staatlicher Infrastruktur abzielt, ist jedoch nur die Analyse der direkt und indirekt verwendeten Software-Komponenten (siehe Abschnitt 2.1) geeignet, um eine möglichst umfassende Abdeckung zu gewährleisten. Eine solche Analyse kann nur durch eine zuvor erwähnte Software Bill of Materials erfolgen. Die verbindliche Erstellung solcher Listen wird beispielsweise im aktuellen Gesetzesentwurf des Cyber Resilience Acts[4] diskutiert.

4 Siehe zum Beispiel Seite 11 des aktuellen Entwurfs:
https://ec.europa.eu/newsroom/dae/redirection/document/89543