Dialog für Cyber-Sicherheit

Empfehlungen für eine wertegeleitete Messenger-Entwicklung:

Leitfaden des Workstreams „Dos and Don’ts für nachhaltig sichere Produkte“ im Projekt „Dialog für Cyber-Sicherheit“

Inhaltsverzeichnis

Einleitung – Ziel des Leitfadens

Dieser Leitfaden ist das Ergebnis des Workstreams 3 „Dos and Don'ts für nachhaltig sichere Produkte", der im Rahmen des Projekts „Dialog für Cyber-Sicherheit" des Bundesamts für Sicherheit in der Informationstechnik (BSI) entstanden ist. Die Umsetzung des Workstreams wurde durch den ThinkTank iRights.Lab begleitet.

Der Leitfaden soll Hersteller:innen und Entwickler:innen wesentliche Kriterien für eine werteorientierte Gestaltung sicherer digitaler Produkte an die Hand geben. Die Auswahl der Kriterien ist angesichts der Breite der Themen- und Produktfelder subjektiv.

Die Autor:innen wollen Hersteller:innen und Entwickler:innen mit diesem Werk dabei unterstützen, strukturiert Anforderungen an nachhaltig sichere digitale Produkte zu definieren und ihnen gerecht zu werden – also gegenwärtige und zukünftige Gefahrensituationen früh zu identifizieren und ihnen vorzubeugen. Dabei handelt es sich um eine Orientierungshilfe zur Umsetzung der Anforderungen an die Gestaltung nachhaltig sicherer IT-Produkte für alle Personen (z. B. Entwickler:innen, Programmierer:innen und Designer:innen), die einen signifikanten Einfluss auf die Entwicklung und den Einsatz dieser Produkte haben. Mit dem Leitfaden soll ein interdisziplinärer Austausch über die potenziellen Auswirkungen der Technologie gefördert und der Aufbau von Fachkompetenzen ermöglicht werden. Zudem sollen damit Entwicklungsteams bei der Umsetzung erforderlicher Maßnahmen unterstützt werden. Nicht zuletzt stellt der Leitfaden eine Einladung zum Nachdenken und Diskutieren dar. Er liefert absichtlich keinen exakten und detaillierten Umsetzungspfad für die Gestaltung nachhaltig sicherer IT-Produkte, sondern stellt wichtige grundsätzliche Aspekte und Fragen zusammen.

Auch sensibilisiert dieser Leitfaden für die mit Informationssicherheit zusammenhängenden übergeordneten Herausforderungen. Zudem zielt er darauf ab, Transparenz und Partizipationsmöglichkeiten für potenzielle Nutzer:innen zu schaffen. Darum berücksichtigt dieser Text ebenfalls gesellschaftliche Dimensionen der Informationssicherheit, etwa „Vertrauensbildung", „Partizipation" und „selbstbestimmte Nutzung von IT-Produkten" im Sinne von „Security by Default". Der Fokus der vorliegenden Veröffentlichung liegt exemplarisch auf Messengerdiensten als digitalen Kommunikationsmitteln. Dahinter steht die Absicht, das insgesamt sehr umfangreiche Thema transparent und verständlich eingegrenzt darzustellen. Die Empfehlungen können jedoch auch auf andere digitale Produkte übertragen werden.

Der hier genutzte Begriff der nachhaltigen Sicherheit ist deutlich breiter gefasst als das, was man üblicherweise unter Informationssicherheit versteht. Er soll also über den Schutz von IT-Systemen (Computer, Programme, Netzwerke, Cloud-Dienste etc.) vor Schäden und Risiken aller Art (unberechtigte Zugriffe, Cyber-Angriffe, Zerstörung durch fahrlässiges Handeln, physikalische Ereignisse etc.) hinausgehen.

Informationssicherheit kann mit organisatorischen (wie Managementsystemen) und technischen Maßnahmen sowie dem IT-Grundschutz-Standard nach ISO 27001[1] des BSI angestrebt werden. Bei dem üblichen Verständnis von Informationssicherheit geht es vor allem um die Gewährleistung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sowie um Werkzeuge zur dauerhaften Abwehr von Angriffen und Bedrohungen. Eine Herleitung von Grundsätzen und Maßstäben für die Entwicklung von nachhaltig sicheren IT-Produkten ist dagegen auch mit Aspekten verbunden, die über die konventionellen Schutzziele hinausführen: „… die ethische und rechtliche Relevanz von Sicherheit besteht in ihrer Funktion, hochrangige Güter zu schützen".[2] Dieser Leitfaden verfolgt daher nicht das Ziel, die in vielen Arbeitshilfen (wie dem BSI-Grundschutz) verankerten technisch-organisatorischen Maßnahmen für die funktionale Gewährleistung der Informationssicherheit „neu zu erfinden", vielmehr soll er helfen, die Herausforderungen für Informationssicherheit aus einer normativen, also werteorientierten Perspektive zu betrachten.

Der Leitfaden ist modular aufgebaut und besteht aus vier übergeordneten werteorientierten Grundsätzen, die ihrerseits durch einzelne Teilaspekte konkretisiert werden. Die einzelnen Teilaspekte beinhalten Hinweise in Form von Orientierungsfragen, die beachtet werden müssen, um eine werteorientierte Gestaltung nach-

1 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (letzter Aufruf: 17.03.2022).
2 Datenethikkommission der Bundesregierung (2019): Gutachten der Datenethikkommission der Bundesregierung. Berlin. S. 45, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 (letzter Aufruf: 17.03.2022).

haltig sicherer IT-Produkte zu ermöglichen und zu erleichtern. Die Umsetzung einzelner, durch Orientierungsfragen adressierten Aspekte und ihre Relevanz hängt vom jeweiligen Fall ab: von den beteiligten Personen, vom Einsatzkontext und -ziel sowie von den verfügbaren Ressourcen und Kompetenzen. Der Leitfaden ist somit auch eine Einladung, Denkanstöße und Ideen für eigene Entwicklungsprozesse zu sammeln. Des Weiteren soll er anregen zu überlegen, welcher Weg mit Blick auf Umfang und Orientierungsfragen bei der Gestaltung nachhaltig sicherer IT-Produkte passend ist.

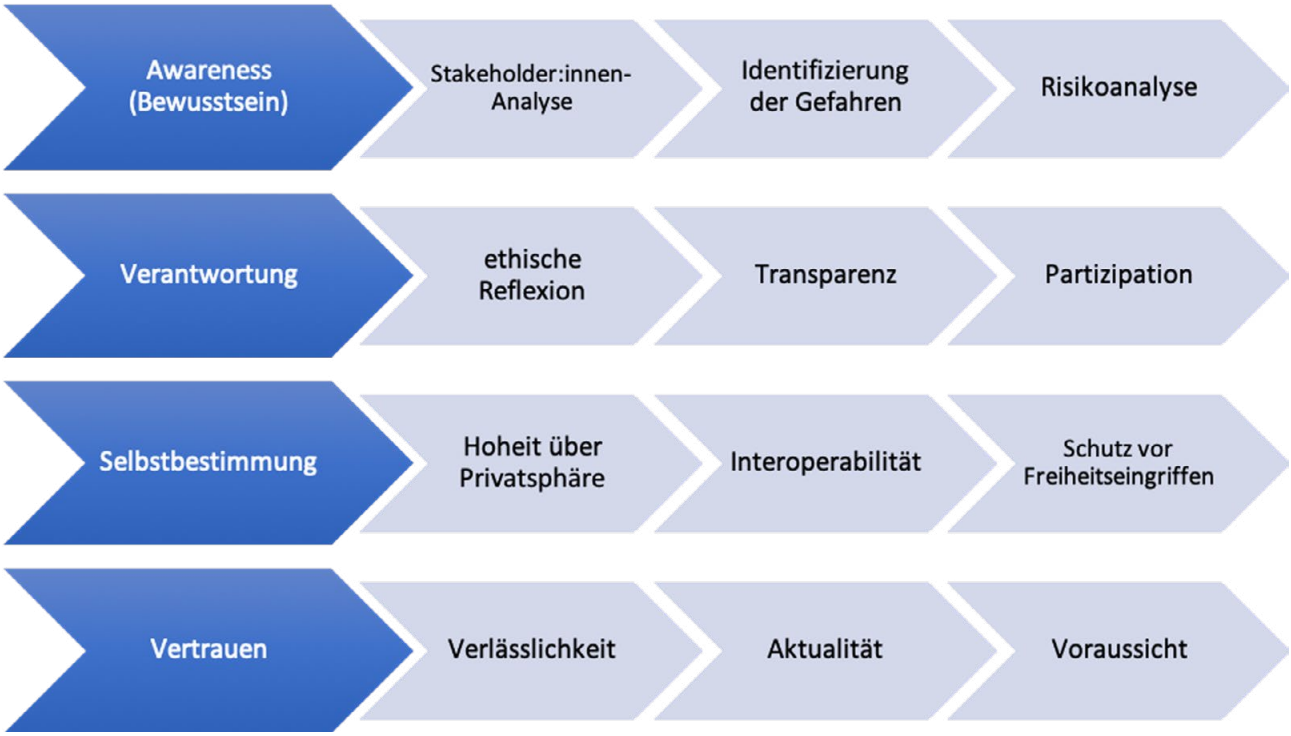

Abb. 1: Der Leitfaden mit seinen vier Grundsätzen und untergeordneten Teilaspekten.

Der Leitfaden

1. Awareness – Bewusstsein für die Beurteilung der Gefahrenlage schaffen

Voraussetzung für die Ausgestaltung von Informationssicherheit ist, sich des breiten Spektrums potenzieller Gefahren und Risiken, die mit dem Internet und dem Umgang mit IT-Produkten einhergehen können, für die zu entwickelnde Anwendung bewusst zu sein, somit eine Risikoanalyse zu vollziehen.

Dabei geht es nicht allein um die Identifizierung von Gefahren und Risiken, sondern vor allem um Sicherheit mit Augenmaß: Eine bewusste Beurteilung der Gefahrenlage ist die erste Voraussetzung dafür, dass die Risiken gesehen und richtig eingeschätzt werden. Bewusstsein ist die Basis für Orientierungskompetenzen in Sicherheitsfragen, für einen aufgeklärten und souveränen Umgang mit IT-Systemen sowie für Selbstentfaltungschancen von Nutzer:innen im digitalen und im analogen Raum.

1.1. Stakeholder:innen-Analyse – wer soll involviert werden?

Um der Vielfalt der Perspektiven möglichst gerecht zu werden, ist es vor der Betrachtung von konkreten Gefahrenpotenzialen, Befähigungsstrategien für Betroffene und weiteren Ansätzen zur Gestaltung nachhaltiger Informationssicherheit wichtig, zu überlegen und festzuhalten, an welcher Stelle und bei welchen Themen Stakeholder:innen und Nutzer:innen in die Produktentwicklung einbezogen werden sollen:

Entwickler:innen, Anwender:innen, Informationssicherheitsexpert:innen, Vertreter:innen diverser beruflicher und gesellschaftlicher Gruppen – alle haben ihren eigenen Blickwinkel auf die mit der Nutzung von IT-Produkten und -Diensten verbundenen Risiken und Bedürfnisse, die durch das Produkt erfüllt werden sollen. Je nach Anwendungsbereich sollten zur Risikobewertung daher bereits in der Entwicklungsphase (aber auch im weiteren Lebenszyklus – vgl. Punkt 4. „Vertrauen“) Vertreter:innen aller genannten Gruppen einbezogen werden. Hat man die jeweiligen Bedarfe festgelegt und die Einschätzungen relevanter Stakeholder:innen eingeholt, ist der Rahmen für den weiteren Prozess gesteckt. An dieser Stelle kann man nun die Entwicklung entscheidend ausrichten:

Zielgruppen identifizieren, deren Bedürfnisse adressiert werden:

- Wer gehört zur typischen Nutzendengruppe und welche besonderen Anforderungen (z. B. Bedienung, Anonymität, Barrierefreiheit) sollen berücksichtigt werden?
- Welche Zielländer sind in Betracht zu ziehen? Gibt es länderspezifische Unterschiede in der Nutzungspraxis und im rechtlichen Rahmen?
- Welche weiteren spezifischen Gruppen (z. B. öffentlicher Dienst, bestimmte Berufe, vulnerable Gruppen) sollen erreicht werden?
- Welche Nutzer:innengruppen müssen Ihr Produkt verwenden, weil es für sie keine wirkliche Alternative gibt? Ist das Produkt darauf eingerichtet?
- Welche spezifischen Bedarfe zeichnen die jeweilige Gruppe aus?
- Welche Personengruppen können von dem Ansatz direkt und indirekt betroffen sein?

Externe Stakeholder:innen einbeziehen:

- Welche Stellen und Organisationen mit Fachwissen sollen für die zielgruppenorientierte Bedarfsermittlung einbezogen werden?
- Welche Expert:innen werden für die Erfüllung zielgruppenspezifischer Anforderungen an Ihr IT-System angehört, um eventuelle Wissenslücken zu schließen?
- Wie werden Stakeholder:innen in Planung und Entwicklung (z. B. Entscheidungsprozesse, Entwicklungsschritte, Austauschformate) eingebunden?[3]

3 Siehe auch: Puntschuh, Michael / Fetic, Lajla (2020): Praxisleitfaden zu den Algo.Rules. Berlin, abrufbar unter: https://algorules.org/fileadmin/files/alg/Algo.Rules_Praxisleitfaden.pdf (letzter Aufruf: 17.03.2022).

Rahmenbedingungen festlegen, die das Produkt erfüllen soll:

- Welchem Zweck dient Ihr Produkt für welche Nutzer:innengruppe?
- Welche Seiteneffekte (Nicht-Ziele) sollten innerhalb des Produkts vermieden werden?

Wie sieht ein Beispiel aus?

> **DO:** *Die Entwickler:innen eines Messengers entschieden sich, beim Öffnen der App ein Pop-up-Fenster einzublenden, das zur Teilnahme an einer Umfrage aufrief. Wurde dieses weggeklickt, tauchte es nicht mehr auf. So konnte eine möglichst breite Masse der tatsächlichen Nutzer:innen erreicht werden.*

> **DON'T:** *Insbesondere in der Anfangsphase von Messengerdiensten wurde auf Menschen mit Seh- und Höreinschränkungen kaum oder gar nicht Rücksicht genommen, sodass ihnen eine vollumfängliche Nutzung nicht möglich war und sie auf Software von Drittanbieter:innen zurückgreifen mussten, dessen Praktiken zur Datenverarbeitung teils undurchsichtig waren.*

1.2. Identifizierung der Gefahrenmomente – welche Szenarien sind möglich?

Je nach Zielgruppe und spezifischem Einsatzbereich können bei der Nutzung eines digitalen Produkts unterschiedliche Gefahrenmomente entstehen. Die Wahrnehmung dessen, was als Risiko gilt, kann sich allerdings je nach Perspektive stark unterscheiden. Hierbei sollte der Fokus nicht nur auf der digitalen Gefahrenlage (z. B. Hacker-Angriffen), sondern auch auf analogen Gefahren (z. B. Mobbing) liegen. Aus diesem Grund sollten bei der Ermittlung der Gefahrenlage die im Schritt 1.1. identifizierten Stakeholder:innen einbezogen werden.

Identifikation potenzieller Gefahren für verschiedene Nutzer:innengruppen (Technikfolgenabschätzung) seitens der Hersteller:innen und Entwickler:innen gemeinsam mit den Stakeholder:innen:

- Welche Grundrechte oder -werte könnten von dem Einsatz Ihres Produkts durch Gefährder:innen potenziell berührt sein?
- Welche spezifischen Gefahrenszenarien können bei unterschiedlichen Nutzungsgruppen durch Ihr Produkt auftreten?
- Welche Gefahren drohen Nutzer:innen im analogen Raum, dadurch dass andere Nutzer:innen Ihr Produkt verwenden? Wie können diese abgemildert werden?
- Welche analogen Gefahren können sich durch Ihr Produkt verstärken (beispielsweise Mobbing, Ausschluss von der digitalen Teilhabe im Alter)?
- Welche Gefahren könnten durch neue Technologien entstehen, die momentan noch nicht marktreif sind?
- Wie kann die vollumfängliche Nutzung des Dienstes gefährdet werden (z. B. durch Barrieren[4])?

Wie sieht ein Beispiel aus?

> **DO:** *Ein Messengerdienst führte im Zuge der Black-Lives-Matter-Proteste 2020 ein Feature ein, mit dem man Gesichter und Objekte auf Fotos direkt auf dem Gerät verschleiern kann, bevor man die Fotos verschickt. Die Entwickler:innen erkannten, dass viele demonstrierende Nutzer:innen die Verschleierung bereits in Apps von Drittanbieter:innen vornahmen, da sonst die Gefahr bestand, dass Personen und Orte auf den Bildern hätten identifiziert werden können, wodurch sie zum Angriffsziel geworden wären. Die direkte Einbindung des Features in den Messenger ermöglichte eine schnellere Kommunikation in Gruppen und machte die Nutzung von Foto-Apps mit undurchsichtigen Verarbeitungspraktiken auf ihren Servern unnötig.*

> **DON'T:** *In den frühen Jahren der Social-Media-Plattformen sind Nutzer:innen der Dienste Hassrede und anderen Angriffen fast ungeschützt ausgesetzt gewesen. Gerade über Direkt-*

4 Das W3C-Konsortium bietet hier Ansätze, wie der eigene Dienst zugänglicher gemacht werden kann: https://www.w3.org/WAI/media/av/ (letzter Aufruf: 17.03.2022).

nachrichten konnten toxische Botschaften eine Person ungefiltert erreichen. Amnesty International veröffentliche 2018 eine Studie, nach der vor allem weiblich gelesene Personen Ziel von solchen Attacken waren, und baute darauf eine breit angelegte Kampagne auf, die eine der am stärksten betroffenen Plattformen zum Handeln bewegen sollte.[5] Auch wenn es gerade in den letzten Jahren deutliche Verbesserungen in der Abwehr solcher Angriffe gab, brauchte es immer wieder Druck von außen und durch nationale Gesetze, um diese Entwicklungen zu beschleunigen. Eine stärkere Einbindung der Betroffenen hätte Angriffe und die damit verbundenen Traumata verhindern können.

1.3. Risikoanalyse – Einschätzung möglicher Risiken

Basierend auf den Ergebnissen von Punkt 1.1. und 1.2. ermittelt man nun, wie hoch das Risiko und die Eintrittswahrscheinlichkeit der dokumentierten Gefahren sind und wie man beides minimieren kann. Entwickler:innen und Expert:innen analysieren mögliche Risiken, stufen diese ein und bestimmen technisch-organisatorische Maßnahmen zur Eindämmung „by design". Dabei sind die folgenden Fragen essenziell.

Durchführung einer Risikoanalyse von Entwickler:innen und Stakeholder:innen:

- Wie können Risiken aussehen, die aus den von Ihnen im Schritt 1.2. identifizierten Gefahrenmomenten entspringen?
- Wer oder was ist eine mögliche Risikoquelle für die Nutzer:innen?
- Welcher physische, materielle oder immaterielle Schaden kann durch den Einsatz Ihres Produkts entstehen (sowie indirekt bei Personen, die es nicht nutzen)?
- Wie hoch ist die Wahrscheinlichkeit (vernachlässigbar/ begrenzt/ wesentlich/ maximal), dass der von Ihnen als möglich eingestufte Schaden eintritt?
- Wie schwerwiegend ist der von Ihnen vermutete mögliche Schaden für die jeweils Betroffenen (vernachlässigbar/ begrenzt/ wesentlich/ maximal)? Welche Metrik ergibt hierbei Sinn und wie kann diese gemessen werden?
- Wie werden die einzelnen identifizierten Risiken im Hinblick auf die Eintrittswahrscheinlichkeit und Schwere möglicher Schäden insgesamt eingestuft?
- Mit welchen technisch-organisatorischen Maßnahmen wird das Risiko minimiert?
- Wie können die Risikoanalyse und der Erstellungsprozess für die Nutzer:innen transparent gemacht werden?

Wie sieht ein Beispiel aus?

DO: *Mehrere Messengersysteme erlauben, in ihren Code-Repositories[6] für die Einführung bestimmter Features oder Änderungen zu argumentieren. Zwar trägt eine mehrheitlich gewollte Änderung nicht unbedingt zur Sicherheit bei, jedoch können derartige Partizipationsmöglichkeiten – in Kombination mit einer Einschätzung des Entwicklungsteams – den Prozess der Risikopriorisierung für ein breites Spektrum an Akteur:innen öffnen.*

DON'T: *Einige Messengerdienste erzwingen beim Erstellen eines Accounts die Weitergabe der eigenen Telefonnummer. Während dies ein funktionierender Mechanismus ist, um Nutzer:innen einen erneuten Zugang zu der Plattform zu erschweren, falls sie blockiert werden, führt dies auch dazu, dass alle Nutzer:innen eindeutig identifizierbar sind. Dies kann beispielsweise für Aktivist:innen in autokratischen Staaten problematisch sein. Hinweise auf dieses Problem wurden laut Kritiker:innen nicht genug beachtet bzw. wurde durch die Reaktionen der Entwicklungsteams nicht deutlich, inwieweit sie sich mit diesem Risikopotenzial beschäftigt haben.*

5 Siehe: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ (letzter Aufruf: 17.03.2022).
6 Repositories werden die Strukturen genannt, in der Programmiercode und dessen Weiterentwicklung organisiert werden. Auf Webseiten verschiedener Anbieter kann man diese hochladen und mit Entwickler:innen oder anderen Interessierten teilen.

2. Verantwortung – Verpflichtung zu user:innen-fokussierter Produktgestaltung

Verantwortung zu übernehmen bedeutet, Rechenschaft über das eigene Tun und dessen Folgen ablegen zu können. Verantwortungsbewusstes Handeln heißt, Fragen nach dem „Wie und Warum" sowie der eigenen Haltung zum Ergebnis beantworten zu können.

Verantwortung setzt Handlungsfreiheit im Sinne einer moralischen Selbstverpflichtung voraus. Sie unterscheidet sich von gesetzlichen Verpflichtungen, da sie freiwillig und selbst auferlegt ist. Verantwortung ist vor allem auf die Zukunft gerichtet, da Folgen des Handelns oft erst spät ihre Wirkung entfalten.

Im Kontext nachhaltig sicherer IT geht es darum, dass Entwickler:innen anwendende Personen und Institutionen befähigen, Sicherheitseinschätzungen und darauf basierende Maßnahmen zu verstehen, die intrinsische Logik des Produktangebots (z. B. das Finanzierungsmodell) nachzuvollziehen und sich auch in Entwicklungs- und Optimierungsprozesse aktiv einbringen zu können.

Verantwortung heißt an dieser Stelle auch, einen Beitrag dazu zu leisten, dass Bürger:innen hinsichtlich Sicherheitsthemen und Nutzung digitaler Dienste in ihrer Mündigkeit gefördert werden, dabei ihre Selbstentfaltung schützen und gleichzeitig andere nicht gefährden. Verantwortungsübernahme durch Entwickler:innen und Produktbetreiber:innen ist keine Einbahnstraße: Antizipation von Meinungen und Erfahrungen der Nutzer:innen sowie ihre aktive Einbindung in die Produktoptimierung gehören dazu.

2.1. Ethische Reflexion – unterschiedliche Perspektiven auf ethische Fragen betrachten

Oft führt die Etablierung von digitalen Produkten zu großen Veränderungen, mit zum Teil weitreichenden Folgen für Einzelne und das Gemeinwohl. Um ethische Herausforderungen im digitalen Zeitalter frühzeitig erkennen und darauf eine Antwort geben zu können, sollten Entwicker:innen und Hersteller:innen unterschiedliche Perspektiven zu übergeordneten ethischen Fragen betrachten. Das Ziel einer ethischen Reflexion ist, dass das Entwicklungsteam ein gemeinsames Verständnis der ethischen Herausforderungen entwickelt und darauf aufbauend Handlungsbedarfe und mögliche Wertekonflikte identifiziert. Eine ethische Reflexion kann auch als Reaktion auf das Nutzer:innen-Feedback aus Punkt 4.3. durchgeführt werden, um Anregungen aufzunehmen und mögliche neue Problemfelder aufzugreifen. Im Idealfall begleitet der ethische Reflexionsprozess die Produktentwicklung und den Austausch mit Stakeholder:innen sowie Nutzer:innen fortlaufend. Dabei ist zu beachten:

Identifizierung ethischer Herausforderungen:

- Welche Chancen und Herausforderungen werden mit dem Einsatz Ihres Produkts aus ethischer Sicht verbunden?
- Welche Werte oder legitimen Bedürfnisse können aus den genannten Chancen und Herausforderungen geschlossen werden?

Beurteilung ethischer Herausforderungen:

- Welche Begriffe aus den herausgearbeiteten Chancen und Herausforderungen empfinden Sie als zentral? Welche unterschiedlichen Deutungen sind möglich?
- Welche Auswirkungen auf welche Werte oder Bedürfnisse können Sie vom Produkteinsatz erwarten?
- Welche Ziele und Werte können Ihrer Meinung nach miteinander in Konflikt geraten (z. B. Freiheit vs. Sicherheit, Individualvorteil vs. Gemeinwohl)? Wie geht man damit um?

Umgang mit identifizierten Herausforderungen:

- Welche Anschlussfragen ergeben sich für Sie aus den identifizierten ethischen Herausforderungen? Was sind die nächsten Klärungsschritte?
- Welche Stakeholder:innen (z. B. aus Schritt 1.1.) und Fachexpert:innen sollten Ihrer Meinung nach in die Abwägung möglicher Handlungsoptionen einbezogen werden?

Wie sieht ein Beispiel aus?

> **DO:** *Das Bundesfamilienministerium bietet eine Anleitung[7] zum ethischen Reflexionsprozess für digitale Projekte, um diese verantwortungsvoll und gemeinwohlorientiert umzusetzen. Die Durchführung eines solchen Prozesses kann Ihrem Team helfen, Aspekte Ihres Produkts auf die Vereinbarkeit mit Ihren eigenen ethischen Grundsätzen zu überprüfen.*

> **DON'T:** *Eine Messengerapp kündigte 2021 ein eigenes Bezahlsystem innerhalb der App an, das einen anonymen Geldtransfer ermöglichen soll. Das Feature wird seit Januar 2022 ausgerollt, stößt jedoch sowohl bei Beobachter:innen als auch intern auf große Skepsis. Kritiker:innen fürchten, anonyme Zahlungen könnten zu einem Vorwand für Strafbehörden werden, um die Entwickler:innen rechtlich zur Aufhebung der Verschlüsselung zu zwingen. Der CEO des Unternehmens trieb die Entwicklung des Features persönlich voran und blockt Diskussionen über die Gefahren für die sichere Kommunikation ab.*

2.2. Transparenz – Nachvollziehbarkeit der Funktionsweisen der IT-Systeme herstellen

Mit Transparenz ist an dieser Stelle nicht der entsprechende Datenschutzgrundsatz (Art. 5 Abs. 1. lit. a DSGVO) gemeint, sondern vielmehr nachvollziehbare Funktionsweisen der IT-Systeme, soweit die Entwickler:innen hierüber Kontrolle und Wissen haben.[8] Nutzende können nur dann Vertrauen in das Produkt aufbauen, wenn sie wissen, in welchem Kontext der Messenger entwickelt wird. Transparenz über die Geschäftsmodelle, Sicherheitsvorkehrungen, Datenverarbeitungen und Gefahrenhinweise eines digitalen Produkts sind notwendige Bedingungen für einen souveränen Umgang und somit erstrebenswert. Gleichzeitig sollten Nutzer:innen nicht durch einer Informationsflut überfordert und die Transparenz über Geschäftsprozesse nicht zu einer Angriffsfläche an sich werden. Transparenz sollte also nicht Selbstzweck sein, sondern sich nach den Bedürfnissen der Nutzer:innen richten und gleichzeitig den Betrieb nicht gefährden.

Hersteller:innen allein können diese Form von Transparenz nur bedingt erzielen. Sie wird erst durch Einbeziehung Dritter möglich. Eine externe Zertifizierung durch eine neutrale Institution kann auch Lai:innen einen besseren Einblick in die Qualität einzelner Produktaspekte geben. Zu beachten ist dabei:

Transparente Definition und Kommunikation von Zielen und dem Geschäftsmodell:

- Wie werden Nutzer:innen transparent und verständlich informiert? Wie könnte ein Projektleitbild lauten?
- Wie transparent kann das Geschäftsmodell für Nutzer:innen sein?
- Welche Zusatzinformationen fördern das Vertrauen der Nutzer:innen in das Produkt?
- Welche Medien können genutzt werden, um Nutzer:innen zu informieren (z. B. soziale Medien, Blogs, Chat-Gruppen oder Newsletter)?

Die Logik der Systemfunktionalität verständlich darstellen und dokumentieren:

- Wie lässt sich die Funktionalität des Produkts verständlich beschreiben?
- Wie lässt sich der Zugang zu diesen Informationen erleichtern?
- Welche Elemente gehören in eine umfassende Dokumentation? Welche Strukturen können Sie aufbauen, damit diese aktuell gehalten werden kann?

Sicherheitsvorkehrungen darstellen und dokumentieren:

- Wie können Schwachstellen schnell und verständlich kommuniziert werden?
- Wie lässt sich einfach erklären, welche Faktoren in die Risikobewertung einfließen?

Wie sieht ein Beispiel aus?

> **DO:** *Über einen Support-Account innerhalb eines Messengerdienstes werden Nutzer:innen*

7 Siehe: https://www.bmfsfj.de/anleitung-digitale-ethik (letzter Aufruf: 17.03.2022).
8 Zwar sollte das Entwicklungsteam idealerweise einen vollumfänglichen Blick auf die Funktionsweisen aller genutzten Schnittstellen und Bibliotheken haben, jedoch wäre es zu viel erwartet, dass sie deren Dokumentation ebenfalls übernehmen. Vielmehr ist an dieser Stelle die Transparenz des eigenen Produkts gemeint.

standardmäßig über die Veränderungen in der App informiert. Diese Informationen erscheinen wie eine normale Nachricht und können stummgeschaltet werden.

DON'T: *Der Unternehmenssitz eines viel genutzten Messengers wurde immer wieder durch die Führungsebene verlegt, nachdem verschiedene Ermittlungsbehörden um Hilfe bei der Ergreifung von Nutzer:innen gebeten hatten. Zuletzt verlegte das Unternehmen seinen Standort in ein Land, das dafür bekannt ist, nur in geringem Maße mit internationalen Ermittlungsbehörden zusammenzuarbeiten, während in der Regierung autokratische Strukturen vorherrschen. Weiterhin existieren kaum Informationen zum Geschäftsmodell und den Vereinbarungen mit dem Staat, in dem das Unternehmen aktuell sitzt. Die spärlichen öffentlichen Informationen sind durch Medienrecherchen ans Licht gekommen und wurden nicht vom Unternehmen veröffentlicht.*

2.3. Partizipation – relevante Akteur:innen und Nutzer:innen einbinden

Um die Aspekte nachhaltiger Sicherheit möglichst umfänglich berücksichtigen zu können, ist es notwendig, alle relevanten Akteur:innen in den Prozess der Produktentstehung und -weiterentwicklung einzubeziehen. Ziel ist nicht ein Mehrheitswille, sondern die Teilhabe sowie die gleichen Informationsgrundlagen für Entscheidungen.

Im besten Fall stellt man Nutzer:innen Kanäle zur Verfügung, über die sie dem Entwicklungsteam sowohl Ideen als auch Kritik mitteilen können. Hierbei sollten Ansprechpartner:innen in Schnittstellenfunktion agieren und die entsprechenden Nachrichten vertrauenswürdig behandeln, damit diese in den Entwicklungsprozess einbezogen werden können. Essenziell ist bei diesem Punkt:

Möglichkeiten für Nutzer:innen schaffen, Entwicklungsprozesse konstruktiv zu begleiten:

- Wie kann ein Alpha-/ Beta-Programm aufgebaut werden, das wertvolles Feedback für den Entwicklungsprozess liefert?
- Wie sieht eine Struktur aus, mit der sich das Feedback der Nutzer:innen bewältigen lässt?
- Über welche Kanäle können Nutzer:innen mit dem Entwicklungsteam und auch miteinander kommunizieren? Haben Sie die Ressourcen, um ein Forum zu pflegen?

Möglichkeiten schaffen, um das Spektrum an Perspektiven für Ihr Feedback stetig zu erweitern:

- Welche Gruppen sind bei den bisher befragten Stakeholder:innen unterrepräsentiert? Wie können Sie dies (datenschutzkonform) ermitteln?
- Welche Möglichkeiten und Veranstaltungen bieten sich an, um neue Perspektiven auf Ihr Produkt zu gewinnen?

Interne Teams in Strategien und Entscheidungsprozesse einbeziehen:

- Welches Medium ist für das Team sinnvoll, um eine regelmäßige Beteiligung zu ermöglichen?
- Welche Entscheidungsprozesse sollen durch das Team begleitet werden? Welche Begründung gibt es, Entscheidungen allein zu treffen?
- Sind atmosphärische Veränderungen notwendig, damit sich Mitglieder des Teams vertrauenswürdig an leitende Personen wenden können?

Wie sieht ein Beispiel aus?

DO: *Einige Messenger beziehen Nutzer:innen über ein offizielles Forum regelmäßig in den Entwicklungsprozess ihrer Dienste ein. Dort können diese aktuelle Entwicklungen diskutieren, Fehler melden, aber auch einen Einblick in den längerfristigen Plan der Entwickler:innen erhalten und diesen gegebenenfalls kommentieren.*

DON'T: *Ein Messenger kündigte 2021 an, Nutzer:innen bei Ablehnung der Änderung der Allgemeinen Geschäftsbedingungen vom Dienst auszuschließen. Viele Nutzer:innen interpretierten die Änderung als einen starken Eingriff in die eigene Privatsphäre. Der Hersteller korrigierte daraufhin die Änderung. Der enorme Imageschaden und die abgewanderten Nutzer:innen hätten jedoch verhindert werden können, wenn im Vorfeld mehr Ressourcen in die Aufklärung der Nutzer:innen gesteckt worden wären.*

3. Selbstbestimmung – Technologie selbstbestimmt nutzen

Im Kontext von Informationssicherheit bedeutet Selbstbestimmung, digitale Technologien in einem Handlungsspielraum zu nutzen, der seine Grenze in den Freiheitsrechten anderer hat. Selbstbestimmung kann man auch als Hoheit über und Verantwortung für die Nutzung von Technologie, das eigene digitale Abbild und die eigenen „digitalen Spuren" verstehen.[9]

Dabei geht es um mehr als um die Einhaltung der Datenschutzvorschriften. Zentrales Interesse ist, Nutzer:innen einerseits mit Instrumenten wie Migrationstools und differenzierten Privatsphäre-Einstellungen in einem *Privacy-by-Default*-Ansatz eine größtmögliche Standardsicherheit („Security by Default") zu ermöglichen und andererseits zum eigenverantwortlichen Umgang mit Risiken zu befähigen. Ergänzend soll es den Nutzer:innen ermöglicht werden, das Produkt an das persönliche digitale und analoge Sicherheitsbedürfnis anzupassen.

3.1. Hoheit über Privatsphäre – selbstbestimmt über Datennutzung entscheiden

Zu den primären Datenschutz-Themen gehören die Hoheit über die Privatsphäre ebenso wie die Gewährleistung informationeller Selbstbestimmung – beides setzen wir als Einhaltung der DSGVO voraus. Im Fokus stehen an dieser Stelle die nicht-obligatorischen Funktionen eines IT-Produkts, die Nutzer:innen einen differenzierten Umgang mit ihrer eigenen sowie fremder Privatsphäre und eine selbstbestimmte praktische Datensparsamkeit ermöglichen. Als Ausdruck der Selbstbestimmung verstehen wir etwa ein klares UI- und UX-Design, das Nutzer:innen in die Lage versetzt, über die Verwendung ihrer Daten unkompliziert selbst zu entscheiden. Essenziell ist dabei:

Differenzierte Privatsphäre-Einstellungen implementieren:

- Können die Privatsphäre-Einstellungen Ihres Produkts zu Verarbeitungszwecken je nach individuellen Präferenzen der Nutzer:innen dynamisch angepasst werden?
- Können Datenzugriffe durch Dritte innerhalb des Produkts nachvollzogen werden (z. B. durch Logging der Zugriffe, Datenaustausch und Zugriff-Visualisierungen in einer Art „Privacy-Cockpit")? Können diese eingegrenzt werden?
- Können Betroffenenrechte (Auskunft, Berichtigung, Widerspruch) einfach und ohne Medienbrüche durchgesetzt und gewährleistet werden?
- Kann Ihr Produkt ohne Daten, die sich eindeutig einer Person zuordnen lassen, und ohne Identitäts-Freigabe verwendet werden? Wenn nein, wie kann die Speicherung solcher Daten minimiert werden?

Wie sieht ein Beispiel aus?

> ***DO:*** *Mehrere Messengerdienste ermöglichen mittlerweile die Einstellung, alle Nachrichten mit einer Person nach einem gewissen Zeitraum automatisch sowohl von den Geräten als auch von den Servern zu löschen.*

> ***DON'T:*** *Einige Messenger verfügen über die Funktion, eine Ende-zu-Ende-Verschlüsselung zwischen Kontakten herzustellen, haben diese aber nicht standardmäßig aktiviert. Die Entwickler:innen teilen dies nicht eindeutig in der App mit, sodass dieser Umstand Nutzer:innen meist nicht bewusst ist und sie somit keine informierte Entscheidung über ihre Kommunikation treffen können.*

3.2. Interoperabilität – über Service-Nutzung selbstbestimmt entscheiden

Durch „Lock-in-Effekte" bei der Nutzung digitaler Produkte entstehen Asymmetrien, die Kund:innen daran hindern, Anbieter:innen – ohne Nachteile im Komfort – zu wechseln. Die Monopolstellung einiger Plattformen schränkt auf diese Weise die Wahlfreiheit zwischen unterschiedlichen Dienstanbieter:innen ein.

Um dem entgegenzuwirken, kann die Entwicklung von dokumentierten und vollumfänglichen Standards bezüglich Interoperabilität in der jeweiligen Branche dabei helfen, die Kompatibilität zwischen digitalen Diensten sicherzustellen. Nur ein ausgereifter Standard kann dafür

9 Horn, Nikolai / Stecher, Björn (2019): Denkimpuls Innovativer Staat: Datensouveränität – Datenschutz neu verstehen. Initiative D21 (Hg.). Berlin, abrufbar unter: https://initiatived21.de/app/uploads/2019/05/denkimpuls_datenschutz-neu-verstehen_20190528.pdf (letzter Aufruf: 17.03.2022).

sorgen, dass Entwickler:innen nicht bei kleinsten Meinungsverschiedenheiten zu Spezifikationen von diesen abweichen. Um dies zu gewährleisten, sollte man den Entwicklungsprozess der Standards an sich offen gestalten, damit diese eine breitflächige Nutzung erfahren.[10]

Nutzer:innen profitieren von offenen interoperablen Systemen, da sie an Entscheidungsfreiheit, Autonomie und Komfort gewinnen.[11]

Dies funktioniert im Großen, wenn Nutzer:innen entscheiden, welches System sie einsetzen, ebenso wie im Kleinen, wenn es um die Möglichkeit geht, bestimmte Daten über ein System hinaus zu nutzen: etwa Kalendereinträge, die sich in verschiedene Systeme übertragen lassen. Darauf kommt es an:

Wahrscheinlichkeit der Entstehung von Interoperabilitätsbarrieren möglichst reduzieren:

- Wird auf proprietäre Formate bei der Speicherung von Text, Bild und anderen Medien innerhalb Ihres Produkts verzichtet?
- Kann die Nutzung Ihres Produkts und seiner einzelnen Komponenten mit der Nutzung der Systeme, Produkte und Dienstleistungen anderer Anbieter:innen kombiniert werden?
- Werden interoperable Standards und Formate innerhalb Ihres Produkts verwendet, sodass die generierten Daten bei Bedarf in einem strukturierten, gängigen und maschinenlesbaren Format zu anderen Dienstanbieter:innen übertragen werden können?

Wie sieht ein Beispiel aus?

> **DO:** *Ein Open-Source-Messenger hat es sich zur Aufgabe gemacht, zu möglichst vielen anderen Diensten Softwarebrücken zu bauen, sodass Nutzer:innen dieses Messengers mit Nutzer:innen anderer Dienste einfach kommunizieren können.*

> **DON'T:** *Viele Messengerdienste erlauben es, einzelne oder mehrere Unterhaltungen als Text-Dateien zu exportieren. Die Art der Formatierung unterscheidet sich allerdings von Messenger zu Messenger, sodass solche Dateien nicht einfach übertragen werden können.*

3.3. Schutz vor Freiheitseingriffen – physische und psychische Integrität absichern

Ob Menschen sich in ihrer psychischen und physischen Integrität, in ihrer Freiheit zur Selbstentfaltung geschützt fühlen, beruht auf subjektiver Wahrnehmung. Dennoch gibt es Eingriffe in die individuelle Freiheit, die durch einen großen Teil der Gesellschaft als solche anerkannt werden. Dies kann beispielsweise direkt durch digitale Dienste oder indirekt durch Desinformationen und Hassrede zur Mobilisierung gegen Gruppierungen oder Individuen geschehen und in analoge Gewalt umschlagen. Um solche Verläufe zu verhindern, ist essenziell:

Mechanismen im System integrieren, die die Verbreitung von Hassrede, Desinformationen, Trolling, Grooming, Doxxing etc. unterbinden:

- Können Nutzer:innen für sie gefährliches Verhalten einfach und sicher melden?
- Haben Nutzer:innen einfachen Zugang zu Informationen, die sie darüber aufklären, wie sie gegen gefährdendes Verhalten gegen sich selbst oder andere außerhalb des Dienstes vorgehen können?
- Haben Sie Ressourcen, um gegen gefährdende Inhalte in Ihrem Dienst vorzugehen? Könnten Sie mit anderen Organisationen zusammenarbeiten, beispielsweise für einen Faktencheck?
- Wie lassen sich Kontrollmechanismen automatisieren, ohne dass es zu einer Zensur von legitimem Verhalten kommt? Wie kann dies geschehen, ohne z. B. die Verschlüsselung von Informationen unsicher zu machen?
- Wie werden Nutzer:innen bei dauerhaftem Fehlverhalten ausgeschlossen?

10 Ein Beispiel aus der Vergangenheit ist zum Beispiel das XMPP-Protokoll, auf das Anfang des 21. Jahrhunderts sehr viele Messenger setzten, bevor es zu einer Fragmentierung aus zumeist geschäftlichen Interessen kam.
11 Horn, Nikolai / Riechert, Anne (2018): Recht auf Datenübertragbarkeit. Rechtliche, technische und verbraucherbezogene Implikationen. Stiftung Datenschutz (Hg.). Leipzig. S. 30, abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/kurzversion_studie_datenportabilitaet.pdf (zuletzt abgerufen am 17.03.2022).

- Wie wird eine Verbreitung/ Weiterleitung von gefährdenden Inhalten eingeschränkt?

Infrastruktur schaffen, die es ermöglicht, gefährdendes Verhalten nachzuverfolgen:

- Wie lassen sich Urheber:innen von unerwünschtem Verhalten identifizieren, ohne die Privatsphäre zu stark einzuschränken?

- Wie kann ein Zugang zu Ihrer Infrastruktur für Wissenschaftler:innen ermöglicht werden, ohne die Prinzipien des Datenschutzes zu verletzen?

Wie sieht ein Beispiel aus?

> **DO:** *Nach ungebremster Weiterleitung von Falsch-Informationen und – infolgedessen – physischen Angriffen auf Personen und Einrichtungen haben mehrere Messengerdienste die freie Nachrichten-Weiterleitung eingeschränkt und machen nun derlei Mitteilungen grafisch kenntlich. So können Empfänger:innen eindeutig erkennen, wenn es sich um eine weitergeleitete Nachricht handelt.*

> **DON'T:** *Anhänger:innen von Verschwörungsideologien und Rechtsextreme haben sich in den letzten Jahren auf einer Messenger-Plattform versammelt. In dieser App können sich Menschen mit extremen Ansichten frei und in öffentlichen Gruppen austauschen und zur Zerstörung von Gebäuden und zu Morden aufrufen. Expert:innen warnen seit Langem, dies könne zur Radikalisierung von Einzelpersonen führen. Das Unternehmen hinter dem Messenger verfolgt bisher jedoch keine kohärente Strategie, um diese Entwicklung zu unterbinden.*

4. Vertrauen – Verlässlichkeit, Aktualität und Voraussicht

Unter Vertrauen versteht man eine positive Erwartung in Bezug auf eine handelnde Person oder Institution als eine „Hypothese künftigen Verhaltens“.[12] Vertrauen ist zukunftsbezogen und beinhaltet darum den Gedanken der Nachhaltigkeit. Im Kontext der Sicherheit der IT-Systeme und -Produkte beinhaltet Vertrauen beispielsweise die Annahme, dass die Funktionsfähigkeit des Systems und seine Resistenz gegen mögliche Gefahren und Risiken zukünftig aufrechterhalten werden können. Zur Natur des Vertrauens gehört, dass es leicht entzogen werden kann.[13] Um Vertrauen in die nachhaltige Gewährleistung der Sicherheit aufzubauen, muss man Maßnahmen implementieren und diese eindeutig kommunizieren: Dazu zählen die Sicherstellung der Verlässlichkeit, Aktualität und Voraussicht bei der Ausgestaltung des Systems sowie ständige Anpassungen an die technologischen Entwicklungen und sich verändernden Gefahrenlagen. Wollen wir Nachhaltigkeit gewährleisten, müssen wir präventiv nicht nur mögliche technologische Entwicklungen, sondern auch gesetzliche Vorhaben und mögliche sozialpsychologische Verhaltensänderungen in der Gesellschaft antizipieren.

4.1. Verlässlichkeit – durchgehende Funktionsfähigkeit des Systems sicherstellen

Funktioniert ein System zu jeder Zeit wie erwartet, baut dies Vertrauen bei den Nutzer:innen auf und vermittelt Verlässlichkeit. Dazu gehört ebenfalls, Unerwartetes zu verhindern, beispielsweise durch eindeutige und rechtzeitige Kommunikation bei Veränderungen (siehe „Transparenz“ und „Partizipation“). Dafür ist wichtig:

Ausfallsichere, redundante Infrastruktur schaffen, nach möglichen Alternativen suchen:

- Welche Komponenten Ihres Systems sind für den Kernbetrieb notwendig? Wie können diese notfalls ersetzt werden?
- Bestehen Abhängigkeiten von Orten oder Unternehmen, die die Wahrscheinlichkeit eines Komplettausfalls Ihres Systems erhöhen? Wie wirken Sie Monopol-Tendenzen entgegen?
- Wie wird mit Nutzer:innen kommuniziert, wenn die eigene Infrastruktur ausfällt?
- Werden regelmäßig Testverfahren zur Sicherstellung der Funktionalität von Prozessen und zur Identifikation von Risiken in Ihrem Entwicklungsprozess durchgeführt?

Wie sieht ein Beispiel aus?

> **DO:** *Ein experimenteller Messenger erlaubt eine direkte Verbindung zwischen zwei Geräten und ermöglicht dabei das Teilen von Nachrichten über Wi-Fi, Bluetooth und das Internet ohne zentralen Server. Die Wahrscheinlichkeit, dass Nutzer:innen gänzlich von der Kommunikation miteinander durch externe Eingriffe abgehalten werden, ist dadurch sehr gering, solange eine Art der genannten Verbindungen besteht.*

> **DON’T:** *Diverse Messengerdienste setzen für ihre Server-Infrastruktur zu großen Teilen oder komplett auf einen der großen Cloud-Anbieter. Kommt es zu einem Fehler im System des Cloud-Anbieters, werden die Dienste, die von diesem Anbieter abhängig sind, ebenfalls lahmgelegt.*

4.2. Aktualität – am Puls der Zeit bleiben

Anpassungen des Produkts an äußere Gegebenheiten gewährleisten Aktualität – dieser Anspruch gilt auf allen Ebenen. Gemeint ist hierbei nicht nur die Suche nach Sicherheitslücken im Programmcode, sondern auch die Aktualität von UI und UX. Durch stetige Anpassungen an den Kontext, in dem das Produkt genutzt wird, bleibt es attraktiv und kann seinen Status als beliebte und sichere Option im Produktangebot

12 Simmel, Georg (1908): Soziologie. Untersuchungen über die Formen der Vergesellschaftung. Duncker & Humblot. Leipzig.
13 Horn, Nikolai (2021): Vertrauen, das Handlungsoptionen schafft, ohne naiv zu sein, in: CDR-Online-Magazin. Berlin, abrufbar unter: https://corporate-digital-responsibility.de/article/philosophischer-zwischenruf-vertrauen/ (letzter Aufruf: 17.03.2022).

aufrechterhalten. Eine hohe Popularität unter Nutzer:innen sollte sich in einer Erhöhung der Entwicklungsressourcen widerspiegeln[14] und somit die Wahrscheinlichkeit steigern, dass Fehler innerhalb der Anwendung gefunden werden. Das Bestreben, am Puls der Zeit zu sein, sollte man allerdings nicht überstrapazieren, da eine übereilte Adaption ohne Beachtung der anderen hier vorgestellten Aspekte zu neuen Gefahren führen kann. Beachtet werden sollte:

Liste von genutzten Bibliotheken und anderen Technologien aktuell vorhalten und Informationen über Änderungen einholen:

- Wie erfahren Sie von neuen Sicherheitslücken in Ihren genutzten Code-Bibliotheken?
- Wie bleibt Ihre Technologie-Infrastruktur aktuell, ohne die Sicherheit zu verringern?

Produkt für Nutzer:innen attraktiv halten:

- Welche Features der Mitbewerber:innen, die Ihr Produkt nicht hat, sind besonders attraktiv für Nutzer:innen? Gibt es eine sichere Implementation, die Sie übernehmen können?
- Welche Features bzw. Änderungswünsche haben Ihre Nutzer:innen? (siehe „Stakeholder:innenanalyse“ und „Partizipation“)
- Welche existierenden Einsatzmöglichkeiten Ihres Produkts könnten durch weitere Sicherheitsfeatures gestärkt werden?

Wie sieht ein Beispiel aus?

> **DO:** *Aktuelle Verschlüsselungen in Messengern könnten durch die Weiterentwicklung von Quantencomputern ausgehebelt werden. Projekte zur Post-Quanten-Kryptografie[15] treiben die Forschung zu Verschlüsselungen voran, die mit den neuen Kapazitäten mithalten können. Entwicklungen in diesem Feld sollten beobachtet werden.[16]*

> **DON’T:** *Einige Messengerentwickler:innen setzen für die Verschlüsselung ihrer Nachrichten auf selbstentwickelte Protokolle, teils ohne einen starken Hintergrund in Kryptografie zu haben. Durch fehlende Transparenz und/ oder Ressourcen kann dies dazu führen, dass der Verschlüsselungsalgorithmus gar nicht oder nur schleppend weiterentwickelt wird. Dadurch können länger Schwachstellen ausgenutzt werden, die bei Protokollen, die offen und breiter adaptiert wurden, in dieser Art und Dauer nicht existieren.*

4.3. Voraussicht – sicherheitsrelevante Tendenzen antizipieren

Stetige Antizipation der sich verändernden sicherheitsrelevanten Gegebenheiten ist unverzichtbar: Verhaltensmuster der User:innen, gesellschaftliche Stimmungen, rechtliche Gegebenheiten. Entwickler:innen sollten nicht nur auf Veränderungen reagieren (siehe „Aktualität“), sondern auch proaktiv sicherheitsrelevante Tendenzen (im Sinne von Freiheitseingriffen) antizipieren, um die Produktentwicklung vorausschauend daran anzupassen. Zu beachten ist hierbei:

Produkt an Veränderungen im Nutzer:innenverhalten und UI/UX-Entwicklungen anpassen:

- Wie informieren Sie sich über potenzielle Entwicklungen in der UI/UX-Entwicklung?
- Inwieweit können Sie datenschutzkonforme Nutzungsstatistiken verwenden, um Verhaltensänderungen der Nutzer:innen zu antizipieren?

Veränderungen im rechtlichen Kontext antizipieren:

- Wie informieren Sie sich über aktuelle Gesetzesvorhaben, die Ihr Produkt und Ihren Entwicklungsprozess beeinflussen könnten?

14 Voraussetzung ist, dass die Ressourcen tatsächlich zur Fehlersuche eingesetzt werden und nicht nur zur Entwicklung neuer Features.
15 Siehe dazu zum Beispiel die Bestrebung einer Standardisierung durch das amerikanische NIST: https://csrc.nist.gov/Projects/post-quantum-cryptography (letzter Aufruf: 17.03.2022).
16 Das BSI hat hier bereits Handlungsempfehlungen zur Migration veröffentlicht: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html (letzter Aufruf: 17.03.2022) und eine erste technische Richtlinie: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html (letzter Aufruf: 17.03.2022).

Veränderungen im gesellschaftlichen Kontext antizipieren:

- Wie verfolgen Sie den gesellschaftlichen Diskurs, der für Ihr Produkt relevant ist?
- Welche „Schwelle“ muss erreicht werden, damit der Entwicklungsprozess beeinflusst wird?

Ungewollte Auswirkungen von Systemarchitektur, UI und UX auf die Nutzer:innen antizipieren:

- Wie bleiben Sie über wissenschaftliche Erkenntnisse zu UI/UX-Design und Algorithmendesign auf dem aktuellen Stand?
- Wie werden Entwicklungsteams aufgestellt, um eine eventuelle „Betriebsblindheit“ auszugleichen?

Wie sieht ein Beispiel aus?

> **DO:** *Bilder haben einen großen Einfluss auf Menschen. Darum zeigt einer der größeren Messenger mittlerweile keine Profilbilder mehr bei Nachrichtenanfragen von Personen, die nicht in der eigenen Kontaktliste sind, damit User:innen sich auf (potenziell schädliche) Inhalte konzentrieren können.*

> **DON’T:** *Jede größere Kommunikationsplattform erlaubt es, Nutzer:innen zu blockieren. In der Vergangenheit ist es jedoch passiert, dass mehrere dieser Plattformen es zuließen, dass eine dritte Person (unwissend) die blockende und die blockierte Person in einen Gruppenchat einladen konnte, was wiederum eine direkte Kommunikation erlaubte. Dies hätte durch tieferes Durchdringen der Kontaktpunkte innerhalb der Plattform verhindert werden können.*

Informationen zum Produkt

Dieser Leitfaden wurde im Rahmen des Projekts „Dialog für Cyber-Sicherheit“ von Juli 2021 bis März 2022 erarbeitet.

Ideengeber:innen des Workstreams waren:
Lisa Dittmer, Reporter ohne Grenzen
Vivian Simon, Autorin/ Dozentin

Mitwirkende Teilnehmer:innen des Workstreams waren:
Christian Niemitz-Rossant, Infobrett.net
Philipp Berg, Deutsche Stiftung für Engagement und Ehrenamt (DSEE)

Wir danken des Weiteren folgenden Personen für ihre Unterstützung:
Christian Paul
Eva Scheid
Dagmar Hirche
Victor Kommerell
Sascha Fahl

Beteiligte Mitarbeiter:innen der Geschäftsstelle (iRights.Lab) waren:
Nikolai Horn
Marcel Schneuer
Vera Dünninger
Viktar Vasileuski
Wiebke Glässer

Lektorat:
Mario Sixtus
Hannah Willing (text | struktur)

Satz:
Christoph Löffler

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

Der Workstream „Dos and Don‘ts für nachhaltig sichere Produkte“, in dem der Leitfaden entstanden ist, wurde im Rahmen eines partizipativen und offenen Austauschs von der Geschäftsstelle (iRights.Lab) und interessierten Dialogpartner:innen (s. Ideengeber:innen und mitwirkende Teilnehmer:innen) durchgeführt. Die Dialogpartner:innen haben das Thema aus dem Bereich Cyber-Sicherheit für den Workstream selbst gewählt.
Der vorliegende Leitfaden wurde von der Geschäftsstelle und den Workstream-Teilnehmer:innen eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. jedes einzelnen Teilnehmenden wider. 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 Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Weitere Informationen zum „Dialog für Cyber-Sicherheit“:
www.dialog-cybersicherheit.de

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

Stand: Juni 2022

Ein Projekt im Auftrag des:

Bundesamt
für Sicherheit in der
Informationstechnik

nexus

iRights.Lab
Think Tank für die
digitale Welt