jugendschutz net

Perspektiven des technischen Jugendschutzes

Aktuelle Herausforderungen und zukunftsfähige Konzepte

Juni 2016

jugendschutz net

Autoren:
Andreas Marx, Mark Bootz, Friedemann Schindler

unter Mitarbeit des Teams von jugendschutz.net

Mainz, den 30.06.16

Inhalt

1 Zeitgemäße und handhabbare Schutzfunktionen

Wie die jährlichen Filtertests von jugendschutz.net zeigen, genügen Jugendschutzprogramme für klassische Websites nicht mehr den Anforderungen eines zeitgemäßen Schutzes von Kindern und Jugendlichen im Internet. Junge User bewegen sich vor allem im Social Web und nutzen Soziale Netzwerke, Video- und Fotodienste. Dies geschieht vor allem über Apps auf mobilen Endgeräten und weniger am PC über den Browser. Auch Smart-TVs, Set-Top-Boxen, Spielekonsolen oder Smart-Watches verfügen inzwischen über Betriebssysteme, mit denen der Zugriff auf das Internet möglich ist. Das sogenannte „Internet der Dinge" vernetzt zunehmend alle Gegenstände des täglichen Gebrauchs – auch Spielzeug – mit dem Internet.

Heute verfügen die meisten Haushalte über mehrere onlinefähige Endgeräte wie PC, Laptop, Smart-TV, Smartphone oder Spielkonsole.[1] Vor der Etablierung mobiler Endgeräte war die Internetnutzung von Kindern und Jugendlichen meist auf den heimischen Desktop-PC beschränkt. Häufig war dies ein für Eltern verhältnismäßig leicht einsehbarer Familien-PC, welcher sich durch ein Jugendschutzprogramm schützen ließ. Die mobile Nutzung des Internets stellt dagegen neue Anforderungen an den technischen Jugendmedienschutz: Kinder und Jugendliche verfügen über eigene internetfähige Geräte, sind auch außerhalb der Homezone online und nutzen dort fremde Netzzugänge.

Um den neuen Herausforderungen durch Veränderungen im Netz, bei den Geräten und bei der Nutzung durch Kinder und Jugendliche zeitgemäß begegnen zu können, sollen alle Möglichkeiten des technischen Jugendschutzes geprüft werden.

Jugendschutzprogramme sind für viele onlinefähige Geräteklassen nicht verfügbar. Im Social Web bleiben sie weitgehend wirkungslos, die Inhalte sind in die Kommunikation der User eingebunden und fluktuieren zu sehr. Die Dienste sind stark verknüpft, grundlegende Funktionalitäten wie das Liken und Sharen sind zum Teil tief in den Betriebssystemen verschiedener Geräte verankert.[2] Die großen Angebote wie Facebook, YouTube oder Twitter setzen flächendeckend verschlüsselte Verbindungen (HTTPS) ein, die mit klassischen Filterarchitekturen nicht differenziert zu filtern sind.

Der technische Schutz wird nur wirksam, wenn verfügbare Mechanismen auch aktiviert werden. Derzeit nutzen nur wenige Eltern Jugendschutzprogramme. Die Gründe reichen von der Unkenntnis konkreter Produkte über fehlende Wirksamkeit bis hin zu komplizierter Konfiguration.[3] Die Anforderung, dass Schutzmechanismen für Eltern einfach handhabbar sein müssen, wird noch wichtiger, da die aktuelle JMStV-Novelle erstmals die Möglichkeit vorsieht, auch proprietäre Schutzmechanismen geschlossener Systeme als Jugendschutzprogramme anzuerkennen. Dezentrale Jugendschutzfunktionen für einzelne Anwendungen auf unterschiedlichen Geräten können selbst technisch versierte Eltern überfordern. Im ungünstigsten Fall müssten Eltern auf jedem einzelnen Gerät – und dort in jeder einzelnen Anwendung – sichere Konfigurationen einrichten. Zu entwickeln sind deshalb Überlegungen, wie Systeme wirkungsvoll kombiniert werden können und welche Schnittstellen dafür benötigt werden.

Flächendeckender Jugendschutz wie im Bereich der Trägermedien ist im globalen, vernetzten und konvergenten Medium Internet nicht mehr möglich. Um möglichst große Schutzwirkungen zu erzielen, müssen Konzepte, Strategien und Ressourcen auf Angebote fokussiert werden, die hohe Risiken für Kinder und Jugendliche bergen und von ihnen intensiv genutzt werden. Notwendig sind deshalb eine Analyse der jugendlichen Nutzung, ein intelligentes Risikomanagement und eine Priorisierung der Arbeitsfelder (z. B. nach dem Pareto-Prinzip).

Eine solche Priorisierung sollte sich auf aktuelle Erkenntnisse aus dem Alltag von Kindern und Jugendlichen stützen. Die im Folgenden dargestellte Telemediennutzung durch Kinder und Jugendliche basiert auf vorliegenden Umfragedaten und Erfahrungen aus der täglichen Arbeit von jugendschutz.net. Um Informationslücken zu schließen und einer Priorisierung zuverlässige und vergleichbare Daten zugrundezulegen, ist eine regelmäßige, standardisierte Erhebung des Nutzungsverhaltens zu empfehlen.

---

[1] ARD/ZDF-Onlinestudie 2014, S. 383. Bereits 2014 verfügte jeder Haushalt mit Internetanschluss über durchschnittlich fünf internetfähige Endgeräte.

[2] Beispielsweise verfügen Android und iOS über Funktionen, Inhalte per Knopfdruck in Sozialen Netzwerken zu teilen. Die Zugangsdaten zu den entsprechenden Diensten lassen sich bereits im System hinterlegen.

[3] KIM-Studie 2014, S. 68.

2 Telemediennutzung durch Kinder und Jugendliche

Die Anforderungen an den technischen Jugendmedienschutz sind maßgeblich durch die Nutzungsgewohnheiten von Kindern und Jugendlichen bestimmt. Zu berücksichtigen sind unterschiedliche Onlinedienste, Anwendungen und Endgeräte, die sie im Alltag nutzen. Kinder gehen immer früher online,[4] bereits Vorschulkinder surfen selbstständig im Internet.[5]

Neben der Art der Nutzung verändert sich auch deren Häufigkeit. Der überwiegende Teil der Jugendlichen ist beinahe permanent online.[6] 40 % der Kinder, die das Internet nutzen, waren 2014 täglich online. 2010 waren es noch 26 %.[7]

2.1 Relevante Risiken

Mit den Veränderungen des Netzes und der veränderten Nutzung durch Kinder und Jugendliche ändern sich auch die Gefährdungspotenziale. Die Risiken beschränken sich nicht mehr nur auf die Konfrontation mit beeinträchtigenden Inhalten wie Pornografie, Gewalt oder Selbstgefährdung. Insbesondere mit der Nutzung von Messengern und Sozialen Netzwerken bekommen Kontaktrisiken wie sexuelle Belästigungen, Cybermobbing oder die ungewollte Preisgabe persönlicher Daten einen großen Stellenwert. In Apps, besonders häufig aber auch auf Spieleseiten, wird zudem die Unerfahrenheit von Kindern durch unzulässige Werbung und Kaufapelle ausgenutzt.

Besonders jüngere Kinder achten nicht auf den Schutz ihrer Privatsphäre im Netz.[8] Schon 10 % der Kinder im Alter von etwa 10 Jahren teilen selbstgemachte Fotos in Sozialen Netzwerken. Bei Jugendlichen ist es über die Hälfte.[9] Zusätzlich kann die Verknüpfung verschiedener Dienste zu unbedachter oder unbeabsichtigter Datenpreisgabe führen. Durch die zunehmende Nutzung mobiler Endgeräte werden immer häufiger auch Standortdaten und Bewegungsprofile erhoben.

Bei den Anforderungen an technische Schutzsysteme sind deshalb folgende Risikobereiche zu berücksichtigen:

- Konfrontation mit ungeeigneten Inhalten
- Kommunikations- und Interaktionsrisiken
- ungewollte Preisgabe persönlicher Daten

2.2 Verwendete Dienste

Der Schwerpunkt der Internetnutzung von Jugendlichen liegt auf der Kommunikation und Interaktion. Sie nutzen überwiegend Kommunikations-, Foto- und Videodienste des Social Web.[10] YouTube, Facebook und WhatsApp sind die meistgenutzten Dienste, weitere Nennungen entfallen auf Instagram, SnapChat, Twitter, Tumblr oder Vine. Klassische Webseiten werden durch Jugendliche nur noch verhältnismäßig selten besucht, lediglich bei der Suche nach Informationen geben Jugendliche an, Google, Nachrichtenportale oder Webseiten von Zeitungen oder Fernsehsendern zu nutzen.

Kinder rufen im Vergleich zu Jugendlichen häufiger klassische Websites (Kinderseiten) auf oder suchen im Internet mithilfe einer Suchmaschine wie Blinde Kuh, FragFinn oder Google nach Informationen. Häufig werden auch Spieleseiten wie SpielAffe besucht.[11] Allerdings ist auch bei Kindern die Nutzung von Diensten des Social Web verhältnismäßig weit verbreitet. Communitys wie Facebook und Messenger wie WhatsApp gewinnen ab einem Alter von etwa 8 bis 10 Jahren deutlich an Bedeutung, obwohl Facebook in seinen allgemeinen Geschäftsbedingungen ein Mindestalter von 13 bzw. 16 Jahren vorschreibt.

---

[4] Bitkom 2014, S. 12; KIM-Studie 2014, S. 32, Im Alter von etwa 10–12 Jahren sind die meisten Kinder online.

[5] DIVSI: DIVSI u9-Studie, S. 71.

[6] JIM-Studie 2015, S. 29.

[7] KIM-Studie 2014, S. 33.

[8] Bitkom 2014, S. 21.

[9] Bitkom 2014, S. 18.

[10] JIM-Studie 2015, S. 31.

[11] KIM-Studie 2014, S. 34.

Bei den Anforderungen an den technischen Jugendschutz sind deshalb folgende Dienste besonders zu berücksichtigen:

- Kommunikationsdienste (z. B. WhatsApp, Snapchat)
- Medien- und Blogging-Plattformen (z. B. YouTube, Instagram, Tumblr, Vine)
- Soziale Netzwerke (z. B. Facebook)

2.3 Bevorzugte Zugänge

Kinder und Jugendliche gehen immer häufiger mobil online und nutzen dabei Apps. Der Browser als klassisches Surf-Werkzeug auf dem Desktop-PC verliert zunehmend an Bedeutung. Zum Teil sind Angebote ausschließlich für die Nutzung über eine App konzipiert (z. B. WhatsApp, Snapchat, Instagram) und lassen sich nur eingeschränkt oder gar nicht über einen Browser nutzen. Mit deutlichem Abstand am häufigsten nutzen Jugendliche Messenger (91 %). Darauf folgen die Apps der Sozialen Netzwerke (37 %), Bilderdienste und Videoportale (34 %) sowie Spiele- und Musik-Apps.[12]

In aktuellen Studien finden sich keine Angaben zum Verhältnis von App- zu Browserzugriffen auf Dienste wie Facebook auf Mobilgeräten. Es ist davon auszugehen, dass Kinder und Jugendliche nur in Ausnahmefällen den Browser benutzen. Mehr als die Hälfte aller YouTube-Zugriffe erfolgt inzwischen über ein mobiles Endgerät.[13] Der klassische Webbrowser wird häufig von den Apps der genutzten Online-Dienste (z. B. Facebook oder YouTube) auf Smartphone oder Tablet ersetzt. Facebook beispielsweise drängt seine Nutzer immer stärker, die hauseigene Messenger-App statt die mobile Webseite des Dienstes zu verwenden.[14] In 90 % der Zeit, die User 2015 mobil online waren, nutzten sie Apps.[15]

Wie Kinder online gehen und welche konkreten Apps sie dabei nutzen, wird in aktuellen Studien nicht thematisiert. Messenger wie WhatsApp sind allerdings auch bei Kindern beliebt, wogegen die Apps Sozialer Netzwerke weniger häufig genutzt werden.[16]

Kinder und vor allem Jugendliche greifen inzwischen vornehmlich mithilfe eines Smartphones auf Onlineinhalte zu. Die mobilen Betriebssysteme Android und iOS unterscheiden sich grundsätzlich von Desktopsystemen wie Windows oder OSX (Apple). Während Anwendungen auf klassischen Desktopsystemen verhältnismäßig umfassende Zugriffsberechtigungen auf das System haben, sind Apps unter mobilen Betriebssystemen wie iOS oder Android nach außen weitgehend abgeriegelt.[17] Filteranwendungen haben daher keinen uneingeschränkten Zugriff auf den zu filternden Netzwerkverkehr. Die für mobile Systeme verfügbaren Schutzprogramme fungieren daher meist als eigenständiger Browser, um dieses Problem zu umgehen.

Klassische Jugendschutzfilter in Form von Drittanbietersoftware können prinzipbedingt also nicht Inhalt von Apps auf mobilen Geräten filtern. Lediglich die komplette Blockade von einzelnen Apps ist bei einigen Anwendungen möglich.

Bei den Anforderungen an den technischen Jugendschutz sind deshalb folgende Zugänge besonders zu berücksichtigen:

- Zugang per App (z. B. WhatsApp, Facebook Messenger, Instagram, YouTube und Snapchat)
- Zugang per Browser (z. B. Google)

[12] JIM-Studie 2015, S. 50.

[13] https://www.youtube.com/yt/press/de/statistics.html

[14] http://www.heise.de/newsticker/meldung/Facebook-verschaerft-den-Messenger-Zwang-3227140.html

[15] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/attachment/percent-time-spent-on-mobile-apps-2016/

[16] KIM-Studie 2014, S. 49 f.

[17] http://developer.android.com/guide/topics/security/permissions.html

2.4 Relevante onlinefähige Geräte/Betriebssysteme

Mobile Endgeräte wie Smartphone und Tablet verdrängen immer deutlicher den klassischen Desktop-PC und auch den Laptop.

Smartphones haben bereits 2014 Desktop-PC und Laptop als Geräteklasse abgelöst, die von Jugendlichen am häufigsten für den Onlinezugang genutzt wird. Annähernd 90 % der 16- bis 18-Jährigen nutzen ihr Smartphone, um auf das Internet zuzugreifen.[18] Diese Entwicklung dürfte auch in Zukunft weiter anhalten. Zusätzlich sind im Haushalt häufig weitere internetfähige Geräte wie Spielekonsolen oder Smart-TVs vorhanden.

Bei den Anforderungen an den technischen Jugendschutz sind deshalb folgende onlinefähige Geräte besonders zu berücksichtigen:

- Smartphones
- Desktop-PC
- Smart-TV
- Spielkonsolen

Häufig werden auf verschiedenen Geräten dieselben oder ähnliche Betriebssysteme eingesetzt (z. B. Android auf Smartphones und Smart-TV, Windows 10 auf Desktop-PC und der Xbox-One). Besonders zu berücksichtigen sind daher:

- Google Android
- Microsoft Windows
- Apple iOS

2.5 Erwartungen von Eltern an Jugendschutzsysteme[19]

Etwa ein Viertel der Eltern setzt eine Jugendschutzsoftware ein (Stand 2012). Hierunter dürften allerdings sämtliche technische Maßnahmen durch Eltern fallen (z. B. auch reine Zeitsteuerungen). Wirksamkeit entfalten nutzerautonome Schutzsysteme nur, wenn sie aktiviert werden. Erfüllen technische Lösungen nicht die Erwartungen von Eltern, werden sie nicht genutzt. Eltern sehen technische Jugendschutzlösungen grundsätzlich als nützliches Werkzeug der Medienerziehung. Die Akzeptanz der Programme hängt allerdings neben individuellen Aspekten vor allem stark von zwei Faktoren ab: Eltern akzeptieren die Systeme nur, wenn sie ihre Medienerziehung wirksam unterstützen und sich einfach in der Erziehungspraxis nutzen lassen.

Bei den Anforderungen an technische Schutzsysteme sind deshalb folgende Erwartungen von Eltern zu berücksichtigen:

- hohe Wirksamkeit beim Schutz vor Risiken
- einfache Handhabung im Erziehungsalltag

[18] Bitkom 2014, S. 14.

[19] Vgl. Dreyer/Hajok/Hasebrink/Lampert (2012), S. 18 ff.

3 Für den technischen Jugendschutz relevante Entwicklungen des Netzes

Aus technischen Veränderungen im Bereich des Internets ergeben sich Konsequenzen für den technischen Jugendmedienschutz. Herausforderungen in diesem Zusammenhang sind vor allem die Entwicklung zum Social Web, die vermehrte Konvergenz der Medien und die zunehmende Verschlüsselung von Inhalten.

3.1 Entwicklung zum Social Web

Klassische Webseiten sind meist statisch und vor allem themenspezifisch. Von ihnen ausgehende Gefährdungspotenziale beschränken sich in der Regel auf die Konfrontation mit ungeeigneten Inhalten einer bestimmten Kategorie (z. B. pornografische Website). Die Filterung eines solchen Angebots ist vergleichsweise einfach, in der Regel kann eine komplette Website auf der Ebene der Domain blockiert werden. Im Bereich des Social Web beinhalten Angebote dagegen häufig eine Vielzahl von Themen. Hinzu kommt eine unüberschaubare Masse und hohe Fluktuation an nutzergenerierten Inhalten. Ungeeignete Inhalte verschiedenster Gefährdungsbereiche finden sich hier neben unbedenklichen Inhalten.

Hinzu kommt, dass Kinder und Jugendliche im Social Web Kommunikations- und Interaktionsrisiken wie Belästigungen, Cybermobbing oder -grooming ausgesetzt sind. Häufig werden Nutzerdaten großer Dienste des Social Web für Werbezwecke ausgewertet oder weitergegeben. Gerade jüngere Kinder sind sich nicht bewusst, dass sie mit ihren Nutzerdaten „bezahlen“ und sie preisgeben.

Bei den Anforderungen an den technischen Jugendschutz sind deshalb folgende Herausforderungen des Social Web besonders zu berücksichtigen:

- unüberschaubare Masse, Änderungsgeschwindigkeit und Vernetzung von Inhalten im Social Web
- Kommunikation und Interaktion als Risiko
- Preisgabe persönlicher Daten

3.2 Zunehmende Konvergenz der Medien

Während die Internetnutzung früher auf einen einzelnen PC beschränkt und klar von der Nutzung anderer Medien (z. B. Rundfunk, Filme, Spiele) abgrenzbar war, werden verschiedene Medien, Gerätetypen und Dienste immer häufiger verknüpft. Smart TVs bieten beispielsweise neben herkömmlicher Fernsehnutzung auch die Nutzung von Diensten des Social Web oder des klassischen Webs über einen Browser. Zum Teil lassen sich identische Inhalte auf einem Gerät über Rundfunk oder Online-Dienste konsumieren. Auch die Grenzen zwischen verschiedenen Diensten verschwimmen immer häufiger. Inhalte können durch Verknüpfung von einem Dienst in den anderen eingebunden werden (z. B. YouTube-Videos auf Facebook). Aber auch die Funktionen der Dienste gleichen sich zum Teil an (z. B. bietet Facebook wie YouTube die Möglichkeit, Videos hochzuladen oder wie bei YouNow Ereignisse in Echtzeit zu streamen).

Bei den Anforderungen an den technischen Jugendschutz sind deshalb folgende Herausforderungen der Konvergenz besonders zu berücksichtigen:

- Unterschiedliche Mediengattungen können auf verschiedenen Gerätetypen genutzt werden.
- Globale Dienste bieten vielfältige Nutzungsmöglichkeiten.

3.3 Verschlüsselung der Datenübertragung

Verschlüsselte Verbindungen wurden bisher hauptsächlich in sicherheitsrelevanten Bereichen wie dem Onlinebanking oder -shopping eingesetzt. Im Zuge aktueller Diskussionen um Datenspionage gewinnen sichere Verbindungen und Ende-zu-Ende-Verschlüsselungen immer stärker an Bedeutung. Wenn im Internet Nutzerdaten übermittelt werden, wird inzwischen Verschlüsselung eingesetzt. Initiativen wie „Let's Encrypt“ streben eine flächendeckende Nutzung an,[20] „Firefox“ soll künftig keine ungesicherten Verbindungen mehr unterstützen.[21] Verschlüsselte Verbindungen dürften sich daher zukünftig auch bei statischen Webseiten etablieren.

[20] https://letsencrypt.org

[21] https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/

Bei verschlüsselten Verbindungen ist der eigentliche Seitenaufruf für Dritte nicht mehr im Klartext lesbar, nur die Domain, zu der eine Verbindung aufgebaut werden soll, können sie noch identifizieren. Daraus ergibt sich, dass klassische Jugendschutzprogramme nur auf Domain-Ebene filtern und verschlüsselte Websites oder Social-Web-Plattformen nur noch komplett blockieren oder freischalten können. Tiefe Pfade (beispielsweise URLs zu einem bestimmten YouTube-Video oder Facebook-Profil) können sie prinzipbedingt nicht differenziert filtern.

Mit der Zunahme von Ende-zu-Ende-Verschlüsselung wird die Filterung auf dem Übertragungsweg (z. B. WLAN-Router, Netzknoten, Access-Provider) zunehmend obsolet. Differenzierte Filterung ist nur noch vor der Verschlüsselung von Seitenaufrufen (z. B. per Blacklist) oder nach der Entschlüsselung übertragener Inhalte (z. B. Echtzeitanalyse) im Browser oder in Apps möglich.

Bei den Anforderungen an den technischen Jugendschutz sind deshalb folgende Herausforderungen der Verschlüsselung besonders zu berücksichtigen:

- Verschlüsselte Webangebote lassen sich mit klassischen Jugendschutzprogrammen oder auf dem Übertragungsweg nicht differenziert filtern.
- Eine differenzierte Filterung ist nur vor der Verschlüsselung oder nach der Entschlüsselung möglich.

4 Verfügbare Mechanismen des technischen Jugendmedienschutzes

Die Mechanismen des technischen Jugendschutzes lassen sich im Wesentlichen unterteilen in Filtersysteme, Klassifizierungssysteme sowie Jugendschutzoptionen in Endgeräten, Anwendungen und Diensten. Systeme der Zugangskontrolle wie geschlossene Benutzergruppen bleiben hier unberücksichtigt.

4.1 Filtersysteme

Filtersysteme sind derzeit in unterschiedlichen Formen verfügbar. Dabei lässt sich grundsätzlich zwischen PC- und Mobil-Anwendungen sowie Netzwerklösungen wie Routern oder Proxyservern (z. B. beim Access-Provider) unterscheiden. Anwendungen für den klassischen PC sind dabei am weitesten verbreitet. Einige Programme sind in verschiedenen Versionen für mehrere Plattformen erhältlich. Der Funktionsumfang unterscheidet sich dabei oft je nach Gerät.

Filtersysteme arbeiten in der Regel mit einer Kombination von Blacklists, um ungeeignete Inhalte auszuschließen, und Whitelists, um geeignete Angebote zugänglich zu machen. Nur wenige Produkte analysieren Inhalte in Echtzeit. Um (un)geeignete Inhalte zu erkennen, greifen alle Filter auf verschiedene Mechanismen zurück.

4.1.1 Redaktionelle Klassifizierung

Die redaktionelle Einstufung von Angeboten durch geschultes Personal führt zu vergleichsweise zuverlässigen Bewertungen von Inhalten. Aufgrund des zeitlichen Aufwands wird dieser Mechanismus nur für Whitelists (z. B. FragFinn-Liste mit kindgeeigneten Inhalten), besondere Blacklists (z. B. BPjM-Liste mit indizierten Medien) oder Qualitätskontrollen von automatisierten Klassifizierungsverfahren eingesetzt.

4.1.2 Crowd-basierte Klassifizierung

Crowd-basierte Einstufungen werden durch Besucher von Webseiten z. B. mithilfe von Browser-Plugins vorgenommen und lassen sich für die Befüllung von Black- und Whitelists nutzen. Beispiele sind Web of Trust für Webseiten und YouRateIt für Videos auf Plattformen des Social Web. Die Qualität der Einstufungen soll hier durch die Menge an User-Bewertungen sichergestellt werden. Dieses Verfahren wird nur selten eingesetzt.

4.1.3 Automatisierte Klassifizierung

Bei automatisierten Verfahren werden Webinhalte durch Programme eingestuft, wodurch neben der Befüllung von Black- und Whitelists auch eine Filterung in Echtzeit ermöglicht werden kann. Die in Filtersystemen derzeit eingesetzten Erkennungsalgorithmen befinden sich allerdings meist auf einem veralteten Stand und arbeiten häufig nur mit fehleranfälligen Stichwortlisten.

Fortschrittlichere Methoden der Inhaltsanalyse basieren auf „intelligenten" Algorithmen der Bild-, Video- und Textanalyse und können auch den Kontext berücksichtigen. Die Forschung und auch Praxisanwendung zeigen hier große Fortschritte. Persönliche Assistenten wie Siri (Apple), Now (Google) oder Cortana (Microsoft) sind beispielsweise in der Lage, Sprache zu interpretieren und Informationen aus unterschiedlichen Gebieten zu verknüpfen. Mechanismen der „Künstlichen Intelligenz" wären gut für die Erkennung jugendschutzrelevanter Inhalte geeignet[22], werden aber nach aktuellem Kenntnisstand kaum bei Jugendschutzfiltern eingesetzt. Quelloffene Grundlagen zur Umsetzung solcher Techniken sind verfügbar.[23] Die Entwicklung entsprechender Funktionen könnte also vergleichsweise kostengünstig auf bereits vorhandene Systeme aufbauen.

Die verfügbaren Filter, die Inhalte beim Abrufen in Echtzeit analysieren, greifen in der Regel auch auf einfache Techniken der automatisierten Klassifizierung zurück und arbeiten entsprechend ungenau. Einzig der Echtzeitfilter, der in die Betriebssysteme von Apple integriert ist, zeigt hier gute Ansätze. Im Social Web weist er eine Filterleistung auf, die mit anderen US-amerikanischen Produkten im klassischen Web vergleichbar ist.[24]

Bezüglich der Anforderungen an den technischen Jugendschutz können Filter die folgenden Beiträge leisten:

[22] Fraunhofer-Studie 2014, S. 258.

[23] Beispielsweise TensorFlow von Google: https://www.tensorflow.org

[24] jugendschutz.net (2015)

- Filtersysteme können bei Konfrontationsrisiken Wirksamkeit entfalten, sie bieten aber keinen Schutz bei Kommunikationsrisiken oder wenn junge User ungewollt persönliche Daten preisgeben.
- Filtersysteme bieten Schutz bei der Internetnutzung über Browser, sie können aber nicht den Zugang über Apps filtern.
- Filtersysteme sind für Desktop-PC, teilweise auch für Smartphones und Spielekonsolen verfügbar, bei Windows und Apple iOS sind sie Bestandteil des Betriebssystems.
- Listenbasierte Filtersysteme versagen im Social Web bzw. bei Inhalten, die sich so schnell ändern, dass eine zeitgerechte Aktualisierung der Listen nicht möglich ist. [25]
- Bei verschlüsselten Angeboten können listenbasierte Filtersysteme nur komplette Domains und nicht auf Pfadebene differenziert filtern.

4.2 Altersklassifizierung

Altersklassifizierungen (z. B. age-de.xml, IARC) sind maschinenlesbare Markierungen der Alterseignung von Angeboten durch deren Anbieter. Sie ermöglichen Filtersystemen eine altersdifferenzierte Entscheidung, ob sie das Angebot blockieren oder zulassen. Um Anbietern die Klassifizierung zu erleichtern und die Qualität der Einstufungen zu sichern, werden in der Regel Fragebögen angeboten, die wichtige Kriterien des Jugendschutzes abfragen. Schutzwirkung entfalten Altersklassifizierungen, wenn viele Angebote von ihren Anbietern zutreffend gelabelt werden und Eltern einen Jugendschutzfilter einsetzen, der diese Informationen ausliest.

4.2.1 Internet Content Rating Association – Klassifizierung von Webseiten mit Deskriptoren

Mit dem System der Internet Content Rating Association (ICRA) wurde Ende der 1990er Jahre ein erstes System zur Klassifikation von Telemedieninhalten geschaffen. Um international anschlussfähig zu sein, sollte das System den Inhalt einer Webseite möglichst neutral (enthält Gewalt, Darstellungen von Nacktheit, vulgäre Sprache) beschreiben. Verbreitete Browser wie der Internet Explorer von Microsoft konnten das Labelsystem auslesen. Eltern hatten die Möglichkeit, Webseiten nach einzelnen Deskriptoren zu blockieren oder sich Schablonen für bestimmte Einsatzzwecke herunterzuladen. Das System scheiterte an der Komplexität der Deskriptoren und dem geringen Umfang klassifizierter Seiten.[26]

4.2.2 age-de.xml – Altersklassifizierung von Webseiten

Aktuell können Anbieter in Deutschland ihre Webseiten mit dem age-de.xml-Labelstandard klassifizieren. Dabei handelt es sich um eine Datei, die auf dem Webserver abgelegt wird und die Angaben zur Alterseignung enthält. Anbieter können sich bei der Generierung durch einen Fragebogen der FSM unterstützen lassen. Das System lässt eine Differenzierung innerhalb des Angebots und verschiedene Labeltypen (xml-Datei, http-header, html-meta, Zeitsteuerung) zu.[27] Anerkannte Jugendschutzprogramme können dieses Label auslesen und aufgerufene Inhalte je nach Alterseinstellung blockieren.[28] Nur wenige Webseiten sind mit age-de klassifiziert, die differenzierte Klassifizierung funktioniert nicht im Social Web oder bei verschlüsselten Angeboten.

4.2.3 IARC – Altersklassifizierung von Spielen/Programmen

Beteiligt an der Entwicklung sind in Deutschland die USK, PEGI auf europäischer Ebene, die australische Behörde für Altersklassifikation ACB, die kanadisch/amerikanische Selbstkontrolleinrichtung ESRB und die brasilianische Behörde für Altersklassifikation ClassInd. Die Einstufung in IARC basiert auf einem Fragebogen, den der Entwickler einer App ausfüllt. Anhand der Antworten generiert das System Labels für regionale Rating-Systeme wie USK oder PEGI. App-Stores binden IARC ein und behandeln Apps je nach Herkunft der Anwender entsprechend der regionalspezifischen Kennzeichnung.[29] Bisher nutzen Google, Nintendo, Microsoft und Mozilla das internationale IARC-System in ihren Onlinestores für Apps und Spiele.

---

[25] http://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats/ – 2015 wurden jede Minute 243.055 neue Fotos auf Facebook hochgeladen. Die Zahl der auf Facebook geteilten Inhalte pro Tag betrug 4,75 Milliarden.

[26] http://philarcher.org/icra/ICRAFail.pdf, S. 6.

[27] http://www.age-label.de

[28] http://www.miracle-label.eu – Das Projekt „MIRACLE" stellt auf europäischer Ebene den Versuch dar, ein übergreifendes System der Alterskennzeichnung im Bereich der Telemedien zu schaffen. Das Vorhaben ist eng mit dem age.xml-Standard verknüpft.

[29] https://www.globalratings.com

Bezüglich der Anforderungen an den technischen Jugendschutz können Klassifizierungssysteme die folgenden Beiträge leisten:

- Altersklassifizierungen funktionieren derzeit nur bei Inhalten bzw. Konfrontationsrisiken, nicht berücksichtigt werden Kommunikationsrisiken oder wenn junge User persönliche Daten preisgeben.
- age-de kann nur bei Webseiten Schutz bieten, die per Browser aufgerufen werden; IARC nur beim Download von Spielen/Apps aus Stores, die das Klassifizierungssystem einsetzen.
- age-de verfügt über eine allgemein zugängliche Schnittstelle für Filtersysteme, IARC kann nur über proprietäre Mechanismen (Alterskonfiguration des jeweiligen Stores) genutzt werden.
- age-de kann bei verschlüsselten Angeboten nur komplette Domains klassifizieren, d.h. Dienste des Social Web können nur komplett blockiert oder freigeschaltet werden.

4.3 Sichere (Vor-)Konfiguration

Dienste oder Betriebssysteme bieten Jugendschutzfunktionen, die Kinder und Jugendliche dienst- bzw. geräteweit vor Risiken unterschiedlicher Art schützen können. Beispielsweise kann ein Videodienst ungeeignete Inhalte für Kinder blockieren, indem der Betreiber ein System integriert, das auf Wirkprinzipien von Jugendschutzfiltern zurückgreift. Die Methode der Einstufung und Filterung kann sich dabei an den Besonderheiten des jeweiligen Dienstes ausrichten, um eine möglichst wirksame und effiziente Filterung zu erreichen.

Besonders bei kommunikationsorientierten Diensten (z. B. Messenger, Soziale Netzwerke) lassen sich darüber hinaus Funktionen zur Minderung von Kontakt- und Interaktionsrisiken integrieren. Diese können beispielsweise eine Beschränkung der Reichweite von nutzergenerierten Inhalten auf einen eingeschränkten Kreis von Adressaten oder eine beschränkte Auffindbarkeit und Ansprechbarkeit des Nutzerprofils durch Dritte umfassen.

Bei der Nutzung von Diensten werden üblicherweise persönliche Daten gesammelt und weiterverwertet. Eingriffsmöglichkeiten können vom genutzten Dienst bereitgestellt werden. Neben der Deaktivierung der Datenerfassung (z. B. Standortdaten, Surfverhalten) kann auch die Verwertung (Weitergabe oder Nutzung für personalisierte Werbung) abgeschaltet werden.

Alle gängigen Betriebssysteme bieten Jugendschutzfunktionen. Diese ermöglichen im Vergleich zu Produkten von Drittanbietern weitergehende Eingriffe. Da mobile Betriebssysteme Apps abkapseln, können Programme von Drittanbietern nur wenig Einfluss auf sie nehmen. Die Konfiguration von Jugendschutzoptionen über die Systemeinstellungen ist für Nutzer auch naheliegender, da an dieser Stelle üblicherweise alle relevanten Einstellungen vorgenommen und auch Benutzerkonten verwaltet werden. Darüber bietet das Konzept der Verankerung des Jugendschutzes auf Ebene des Betriebssystems vielfältige Anknüpfungspunkte und Schnittstellen.

Bezüglich der Anforderungen an den technischen Jugendschutz kann die Konfiguration von Diensten und Betriebssystemen die folgenden Beiträge leisten:

- Mithilfe einer sicheren (Vor-)Konfiguration lassen sich auch Kommunikations- und Interaktionsrisiken reduzieren.
- Durch Jugendschutzfunktionen beim Anbieter lassen sich Probleme durch verschlüsselte Verbindungen umgehen. Auch eine hohe Fluktuation von Inhalten im Social Web lässt sich besser behandeln.
- Im Dienst verankerte Funktionen sind plattformunabhängig. Ein separates System für unterschiedliche Geräte ist nicht nötig.
- Über sichere Konfigurationen in Betriebssystemen lassen sich Risiken global reduzieren (z.B. Übermittlung von Standortdaten abschalten) oder Kauf/Nutzung riskanter Programme beschränken

5 Schutzfunktionen in von Kindern und Jugendlichen genutzten Diensten, Anwendungen, Geräten

5.1 Einstellungen in Diensten und zugehörigen Apps

Kinder und Jugendliche nutzen eine Vielzahl von Diensten des Internets und dies in der Regel über die dazu gehörenden Apps. Neben Smartphone und Tablet sind viele Apps auch auf Spielekonsolen, Blu-ray-Playern und Set-Top-Boxen lauffähig. Einige Dienste, bzw. deren App-Versionen, verfügen über Jugendschutzoptionen oder Konfigurationen, die sich für Jugendschutzzwecke verwenden lassen. Die Bandbreite reicht hier von Mechanismen, die ungeeignete Inhalte blockieren (z. B. Filtersysteme, Altersklassifizierungen), bis hin zu Einstellungen, die Kommunikationsrisiken oder Risiken der ungewollten Datenpreisgabe reduzieren (z. B. Blockade ungewollter Kontakte, Beschränkungen der Auffindbarkeit in Suchmaschinen, altersgetrennte Bereiche). In einigen Diensten existieren auch proprietäre Klassifizierungsmechanismen, die Inhalte des jeweiligen Dienstes als für Kinder und Jugendliche ungeeignet einstufen. Allerdings unterscheiden sich hier sowohl die Maßstäbe für die Einstufung als auch die Umsetzung. Die Klassifizierung ist meistens eine Option beim Upload von Inhalten oder wird nach Beschwerden durch den Betreiber vorgenommen.

5.1.1 App-Stores: iTunes, Google Play und Microsoft

Der App-Store von Apple ermöglicht das Herunterladen von Desktopanwendungen oder Apps. Auch Musik, E-Books und Videoinhalte sind im iTunes-Store erhältlich. Die Altersbewertung nehmen App-Entwickler selbst vor, bei Videoinhalten werden FSK-Kennzeichen übernommen. Die Schutzoptionen werden in den Systemeinstellungen des jeweiligen Betriebssystems aktiviert. Für Eltern ist dies ein übersichtliches System, mit dem sie Kauf und Nutzung von Apps und Medien altersdifferenziert beschränken können. Da die Einstellungen für alle Geräte von Apple einheitlich konzipiert sind, müssen sich Eltern lediglich mit einem System vertraut machen.

Apps, Musik, Filme, TV-Serien oder E-Books für Android können über den Play-Store von Google heruntergeladen werden. Google übernimmt für Apps die IARC-Altersklassifizierungen und gibt sie im deutschen Store als USK-Onlinelabel aus, Filme und Fernsehinhalte sind mit FSK-Kennzeichen versehen. Zusätzlich können Käufe von „expliziter" Musik eingeschränkt werden. Um Inhalte nach Alterseignung zu filtern, müssen die entsprechenden Optionen im Play-Store selbst ausgewählt werden. Die Filterung betrifft allerdings nur den Einkauf. Bereits heruntergeladene Apps und Medien können weiterhin ausgeführt werden.

Auch Microsoft übernimmt die IARC-Klassifizierungen. Allerdings ist nur ein Teil der Apps des Windows-Stores mit IARC gelabelt,[30] Filme und Fernsehinhalte tragen ein FSK-Kennzeichen. Die Alterseinstellungen für den Microsoft Store erfolgen über Jugendschutzoptionen im Betriebssystem, sie werden nur bei der Nutzung wirksam. Das mobile Betriebssystem Windows Phone verfügt über einen separaten Store. Die Altersbeschränkungen beim Herunterladen von Apps beziehen sich auf die Altersangabe bei der Registrierung des Nutzerkontos.

Alle Funktionen der App-Stores beschränken sich auf das proprietäre System des jeweiligen Herstellers. Apple integriert die Optionen des Stores in das Betriebssystem, bei Microsoft gibt es Einstellungen im Betriebssystem (z. B. Kinderecke) und im Store. Bei Android müssen Einstellungen im Store selbst vorgenommen werden. Schnittstellen zur Nutzung der Funktionen durch Jugendschutzprogramme sind nicht vorhanden.

5.1.2 Medien- und Blogging-Plattformen: YouTube, Vine, Twitter, Instagram und Tumblr

Video- und Blogging-Dienste ermöglichen das Hochladen und Betrachten von Medieninhalten, woraus in erster Linie Konfrontationsrisiken resultieren. Je nach Ausgestaltung der Plattformen spielen darüber hinaus Kommunikationsrisiken und ungewollte Datenpreisgabe eine Rolle.

YouTube ist aktuell das verbreitetste Videoportal und als App auf vielen Geräten bereits vorinstalliert. YouTube verfügt über einen sicheren Modus, der Videos ausblendet, „die von Nutzern gemeldet oder anderweitig als potenziell unangemessen aufgefallen sind".[31] Der sichere Modus kann über eine Programmierschnittstelle von Filtersystemen aktiviert werden.[32] Darüber kann das Autoplay ausgeschaltet werden, das häufig zu ungewoll-

[30] Stichtag ist der 30.09.16, danach werden die nicht-gekennzeichneten Apps aus dem Windows-Store entfernt.

[31] http://www.youtube.com

[32] http://bluecoat.force.com/knowledgebase/articles/Solution/EnforceYoutubeSafetyMode

ten Konfrontationen führt. Hierdurch wird die Wiedergabe nach dem Anschauen eines Videos gestoppt und nicht durch ein vorgeschlagenes Video fortgesetzt.[33]

Instagram ist ein Foto- und Videodienst, der primär für die Nutzung über eine App konzipiert ist. Fotos können kommentiert werden. Der Dienst bietet die Möglichkeit, eigene Inhalte nur für Follower sichtbar zu machen. Einzelne Nutzer können blockiert werden.

Twitter ist ein Nachrichtendienst des Social Web. Twitter bietet lediglich die Möglichkeit, alle eigenen Medien pauschal als „sensible Inhalte" zu kennzeichnen. Vor „sensiblen Inhalten" kann gewarnt werden. Hierzu muss eine entsprechende Option aktiviert werden. Zusätzlich wird vor eingebundenen Vines (s. u.) gewarnt, die beim Upload als „sensitive content" markiert wurden. Eine Blockade von Inhalten auf Basis der Altersklassifizierung ist nicht möglich. Darüber hinaus kann man einzelne Nutzer blockieren und einstellen, von welchem Personenkreis Nachrichten erhalten werden.

Tumblr ermöglicht es Nutzern, eigene Blogs mit geringem Aufwand zu erstellen. Tumblr-Blogs sind als Subdomain von tumblr.com organisiert, was eine Filterung durch externe Programme prinzipiell erleichtert. Hier unterscheidet sich die Plattform von anderen Diensten des Social Web, deren Nutzerseiten meist in Unterordnern abgelegt sind. User können ihre eigenen Inhalte als „NSFW" (not safe for work) klassifizieren. NSFW-Inhalte werden im sicheren Modus ausgefiltert, unangemeldeten Nutzern und auf Tag-Seiten[34] nicht angezeigt sowie bei Google nicht als Fundstelle ausgegeben.

Vine ist ein Videoportal des Kurznachrichtennetzwerks Twitter, das es ermöglicht, kurze Videoclips von maximal 6 bzw. 140 Sekunden Länge („Vines") zu erstellen. „Vines" können als „sensitive media" markiert werden. Bei ihrem Aufruf erscheint lediglich eine Warnung, die weggeklickt werden kann. In Kanälen werden diese nicht dargestellt.

Die Jugendschutzfunktionen der Dienste gelten jeweils nur in den jeweiligen Diensten, Schnittstellen für Jugendschutzprogramme (Ausnahme ist YouTube) sind nicht vorhanden.

5.1.3 Soziale Netzwerke und Kommunikationsdienste: Facebook, WhatsApp und Snapchat

In Dienste, die vor allem auf Kommunikation ausgelegt sind, sind Kinder und Jugendliche allen relevanten Risiken ausgesetzt, da neben der Kontaktaufnahme von Nutzern auch Bild-, Ton- und Videomaterial ein wichtiger Bestandteil der Plattformen ist.

Facebook ist das größte soziale Netzwerk und bietet Usern die Möglichkeit, einzelne Seiten als ungeeignet für Jugendliche zu markieren.[35] Diese werden lediglich erwachsenen Usern angezeigt. Allerdings greift diese Schutzmaßnahme nur bei eingeloggten Nutzern. Zusätzlich werden bei Inhalten, die der Support nach Meldung für Minderjährige als ungeeignet einstuft, mit einem Warnhinweis versehen. Auch diese werden Minderjährigen nicht angezeigt. Der Dienst bietet auch verschiedene Einstellungen zur Privatsphäre, mit denen Kontaktrisiken reduziert werden können. Beispielsweise können Zugriffe auf Profilinhalte nur für Freunde freigegeben werden. Bei einer Anmeldung als Minderjähriger ist die Auffindbarkeit bei Google ausgeschaltet. Darüber hinaus sind in diesem Fall viele Kontakt- und Veröffentlichungsoptionen auf Freunde beschränkt und lassen sich zum Teil auch nicht manuell verändern. Eine Altersprüfung findet bei Facebook nicht statt. Kinder können sich problemlos als Erwachsene registrieren.

In Googles sozialem Netzwerk „Google+" können Nutzer auswählen, für welches Alter ihre Inhalte geeignet sind.[36] Die Einstellung lässt sich allerdings nur für das komplette Profil und nicht für einzelne Inhalte vornehmen. Entsprechend gelabelte Profile sind nur für Nutzer mit einem passenden Alter sichtbar. Auch lässt sich die Auffindbarkeit des Profils in Suchmaschinen beschränken. Der Personenkreis, dem eingestellte Inhalte angezeigt werden, lässt sich auswählen. Für Jugendliche gibt es keine Voreinstellung.

---

[33] Google bietet mit YouTube Kids eine auf junge Kinder zugeschnittene App an, welche aktuell jedoch nur in den USA erhältlich ist. Die App ist einfach aufgebaut und bietet durch Google als kindgeeignet ausgewählte Inhalte.

[34] Tag-Seiten zeigen Inhalte zu einem bestimmten Schlagwort.

[35] https://www.facebook.com/help/376841469095893

[36] https://support.google.com/plus/answer/6020454?hl=de

Der Messenger WhatsApp ermöglicht das Versenden von Kurznachrichten an Kontakte und ersetzt häufig die herkömmliche SMS. Die App bietet keine expliziten Jugendschutzfunktionen, nur einzelne Kontakte können geblockt werden. Auch ähnliche Messenger wie z. B. Telegram bieten keine zusätzlichen Jugendschutzfunktionen.

Über den Messenger Snapchat lassen sich Bilder, Videos und Textnachrichten an Kontakte versenden, welche nur eine bestimmte Zeit (wenige Sekunden) angezeigt werden. Die Botschaften lassen sich einmal wiederholen. Snapchat bietet wenige Einstellungen zur Privatsphäre, diese sind nach der Anmeldung als Minderjähriger aber so vorkonfiguriert, dass Konfrontations- und Kontaktrisiken reduziert werden. Beispielsweise ist der Austausch von „Snaps" (Botschaften) nur zwischen befreundeten Nutzern möglich.

Tinder ist eine Dating-App, die auf Basis von Facebook-Profilen funktioniert. Nutzer werden die Profilbilder anderer Teilnehmer in einem wählbaren Umkreis angezeigt. Falls zwei Teilnehmer beidseitig Interesse zeigen, können sie eine Unterhaltung öffnen. Nutzer sind nach Alter separiert. Das bedeutet, dass z. B. Minderjährige über die App nicht mit Volljährigen in Kontakt treten können. Darüber hinaus bietet auch Tinder bis auf die Deaktivierung der Standortdienste keine für den Jugendschutz relevanten Optionen. Seit Juni 2016 lässt Tinder keine Anmeldung von Minderjährigen mehr zu.

Die Jugendschutzfunktionen der Dienste gelten nur im jeweiligen Dienst. Schnittstellen für Jugendschutzprogramme sind nicht vorhanden.

5.1.4 Suchmaschinen

Die verbreiteten Suchmaschinen Google und Bing bieten Optionen für eine sichere Suche. Die Funktion lässt sich jeweils ein- oder ausschalten und blockiert Inhalte, die Filtermechanismen des Suchmaschinenanbieters als nicht jugendfrei einstufen. Dabei werden neben der normalen Websuche auch die jeweiligen Bildersuchen gefiltert. Bing und Yahoo ermöglichen zusätzlich eine Abstufung des Filters in „streng" und „mittel" bzw. „moderat". Die SafeSearch-Funktionen lassen sich über Programmierschnittstellen von Jugendschutzfiltern aktivieren.[37]

5.1.5 Video-on-Demand: Netflix, Maxdome und Amazon Prime Video

Aktuell weit verbreitet sind Dienste, die das Streaming von Filmen und Fernsehserien erlauben. Die in Deutschland am weitesten verbreiteten Angebote sind Netflix, Maxdome, Amazon Prime Video, Watchever und Sky Online.[38] Die Dienste sind meist als App für verschiedene Plattformen (mobile Endgeräte, Smart-TVs, Spielkonsolen) oder über den Browser verfügbar. Eltern können eine FSK-Altersstufe festlegen, ab der eine PIN eingegeben werden muss, um entsprechende Inhalte abzurufen. Bei Inhalten ab 18 ist die PIN-Eingabe obligatorisch, dabei kommen unterschiedliche Verifizierungsmechanismen zum Einsatz.

Netflix bietet als einziger Dienst separate Kinderkonten an. Welche Altersstufe hier zugrunde liegt, ist unklar. Es ist nicht möglich, ein Kinderkonto auf eine konkrete FSK-Altersstufe voreinzustellen. Auch kann das Elternprofil nicht mit einem Passwort gesichert werden.

Die Jugendschutzfunktionen der Dienste gelten jeweils nur dienstweit, orientieren sich aber an FSK-Kennzeichnungen. Schnittstellen für Jugendschutzprogramme sind nicht vorhanden.

5.2 Optionen in Endgeräten/Betriebssystemen

Von Betriebssystemen gehen, bis auf möglicherweise eine ungewollte Datenpreisgabe, keine Nutzungsrisiken aus. Sie bieten zentrale Einstellungen für Anwendungen und Dienste auf dem Gerät. Zum Teil lassen sich Betriebssystem und integrierte Dienste nicht klar trennen. Vor allem bei Spielekonsolen ist dies der Fall, da hier besonders viele Funktionen mit dem System verbunden sind.

Die von Kindern und Jugendlichen genutzten Endgeräte und Betriebssysteme unterscheiden sich hinsichtlich der integrierten Jugendschutzfunktionen. Weit verbreitet ist die Möglichkeit, Anwendungen für Nutzer zu sper-

[37] Beispielsweise bei Google: https://developers.google.com/image-search/v1/jsondevguide

[38] Hansen & Jurran (2016), S. 103.

ren, teilweise sind auch Webfilter integriert. Die meisten Systeme verfügen über eine Verkaufsplattform zur Installation von Anwendungen. Auch diese bieten zum Teil Alterseinschränkungen, die direkt über die Systemeinstellungen vorgenommen werden können.

5.2.1 Windows

Microsoft bietet mit „Family Safety" unter Windows eine zentrale Verwaltung für Jugendschutzoptionen an. Die Einstellungen von Kinderprofilen können online vorgenommen werden und sind so für Eltern von jedem Gerät mit Internetzugriff aus konfigurierbar.

Das System verfügt über einen integrierten Webfilter, Zeitsteuerung, Protokollfunktion, Altersbeschränkung für Apps, Spiele und Medien sowie die Möglichkeit, den Zugriff auf ausgewählte Anwendungen zu blockieren. Darüber hinaus kann der Einkauf im Windows-Store anhand von Alterseinstellungen reguliert werden. Der Webfilter verfügt über keine Altersdifferenzierung, bietet aber eine nutzerdefinierte White- und Blacklist und die Funktion, SafeSearch bei Suchmaschinen zu aktivieren. Die Einstellungen gelten für das jeweilige Kinderprofil und wirken sich auf Geräte mit Windows 10 aus, auf denen das Profil angemeldet ist. Softwareentwickler haben die Möglichkeit, über eine Schnittstelle auf die Einstellungen zuzugreifen.[39]

Allerdings befindet sich der Umstieg auf ein einheitliches Betriebssystem bei Microsoft momentan noch in Entwicklung. Die Spielekonsole Xbox One ist zwar inzwischen mit Windows 10 ausgestattet. Sie verfügt über Jugendschutzoptionen unter dem Namen „Family Safety", ist aber nicht in die zentrale Verwaltung eingebunden. Auch Windows Phone ist nicht komplett in das Gesamtkonzept integriert und bietet lediglich eine „Kinderecke". Diese lässt sich mit ausgewählten Apps bestücken und soll Kindern eine sichere Nutzungsumgebung bieten. Die mobile Version Windows Phone wird nach und nach durch eine Variante von Windows 10 ersetzt.

5.2.2 iOS/OS X

Die Betriebssysteme von Apple bieten vergleichsweise umfangreiche Jugendschutzfunktionen. Da vor allem das mobile System iOS einen großen Marktanteil besitzt, beschränkt sich die Darstellung hierauf. Im Mac Betriebssystem OS X sind vergleichbare Funktionen integriert.

Das System enthält einen integrierten Webfilter, welcher neben nutzerseitigen Black- und Whitelists lediglich die Möglichkeit bietet, die Filterung ein- oder auszuschalten. Eine Filterung nach Altersstufen findet somit nicht statt. Der Filter ist das einzige bisher bei jugendschutz.net getestete System, das verschlüsselte Seiten auch auf Pfadebene filtert. Damit kann mit den Apple-Betriebssystemen auch im Social Web differenziert gefiltert werden. Der Filter funktioniert allerdings lediglich im Standard-Browser. Nur in Ausnahmefällen greifen Apps zur Darstellung von Webinhalten auf dasselbe Browser-Backend zurück, nur in diesen Fällen wirkt der Filter auch in den betreffenden Apps.

Über die Systemeinstellungen ist eine Filterung im App-Store nach den ausgegebenen Altersstufen (4+, 9+, 12+, 17+) möglich. Bei aktiviertem Filter können nur Apps der erlaubten Altersstufen im App-Store geladen und Medieninhalte mit einer entsprechenden Alterskennzeichnung abgerufen werden. Bereits geladene Apps werden nur angezeigt, wenn sie den erlaubten Altersstufen entsprechen. Auch kann der App-Store komplett ausgeblendet werden. Das Installieren und Löschen von Apps sowie In-App-Käufe können deaktiviert werden. Zusätzlich lassen sich Filme aus dem iTunes-Store nach FSK-Kennzeichnung freigeben, einzelne Apps blockieren sowie In-App-Käufe beschränken. OS X enthält im Gegensatz zu iOS eine Zeitsteuerung. Auch können hier die Einstellungen für mehrere unterschiedliche Profile vorgenommen werden.

5.2.3 Android

Android bietet ab Version 4.3 sogenannte „eingeschränkte Profile". Diese ermöglichen es, den Zugriff auf Apps zu beschränken. Das Konzept der eingeschränkten Profile bietet eine Schnittstelle zwischen Betriebssystem und Apps. Entwickler haben so grundsätzlich die Möglichkeit, Jugendschutzfunktionen in ihre Programme zu integrieren und die Konfiguration direkt über die Konteneinstellungen anzubieten.[40] Diese Option wird nach aktuellem Kenntnisstand nur von wenigen Apps genutzt, bietet aber vielversprechende Möglichkeiten. Beispiels-

[39] https://msdn.microsoft.com/en-us/library/windows/desktop/ms711654%28v=vs.85%29.aspx
[40] http://developer.android.com/about/versions/android-4.3.html#RestrictedProfiles

weise könnten die Apps der Sozialen Netzwerke auf diesem Weg eine sichere Voreinstellung erzwingen. Darüber hinaus bietet Android in der aktuellen Version keine weiteren für den Jugendschutz relevanten Optionen.

5.2.4 Spielekonsolen

Aktuelle Spielekonsolen bieten inzwischen einen breiten Funktionsumfang und stellen eine Art Medien- und Kommunikationszentrale im Wohnzimmer dar. Am weitesten verbreitet sind Nintendo Wii U, Sony Playstation 4 und Microsoft Xbox One. Die Geräte verfügen über einen Browser und ermöglichen so den vollen Zugriff auf das Internet. Darüber hinaus können Apps verschiedener Dienste (z. B. YouTube, Facebook oder Netflix) installiert und über vielfältige Wege verknüpft werden.[41] Bezüglich der Nutzungsmöglichkeiten sind die aktuellen Konsolen mit PC, Tablet und Smartphone vergleichbar. Alle genannten Konsolen verfügen über integrierte Jugendschutzfunktionen, wobei der Umfang und die Umsetzung zum Teil stark variieren. Keines der Systeme bietet einen umfassenden Schutz. Auch ist die Konfiguration von Kinderprofilen zum Teil für technisch unerfahrene Eltern nur schwer umzusetzen.

Lediglich die Xbox One verfügt über einen integrierten Webfilter. Dieser ist an die Windows-Version des Filters von Microsoft angelehnt und zeigte im Test dieselbe Wirksamkeit. Die zentrale Verwaltung über Microsoft Family Safety ist allerdings nicht umgesetzt. Alle Konsolen bieten Datenschutzoptionen, die z. B. die Sichtbarkeit des eigenen Profils beschränken oder regeln, ob Inhalte geteilt werden können. Die Datenschutzoptionen der Xbox One lassen sich per Vorgabe (Kinder, Teenager und Erwachsene) verwalten. Dies vereinfacht die Konfiguration deutlich, da die Konsole über eine Vielzahl an Datenschutzeinstellungen verfügt.

Die Nintendo Wii bietet keinen Webfilter und lässt lediglich eine komplette Sperre des Browsers zu. Die Konsole verfügt jedoch über umfangreiche Optionen zur sicheren Konfiguration innerhalb der Nintendo-eigenen Angebote. Eltern können Profile für Kinder anlegen. Neben Alterseinschränkungen für Spiele und Medieninhalte (nach USK/FSK) für den Onlinestore können beispielsweise der Austausch von nutzergenerierten Medien eingeschränkt oder Kommunikationsmöglichkeiten innerhalb des Nintendo-Netzwerks reguliert werden. Abhängig vom Alter eines Profils ist eine Blockade des vorinstallierten Chat-Programms voreingestellt. Die Konsole protokolliert die Nutzung je nach Profil, sodass Eltern kontrollieren können, wie lange die Konsole für welche Aktivitäten genutzt wurde.

Auf der Playstation 4 lassen sich Kinderkonten einrichten und mit Einschränkungen (Kommunikationsfunktionen und das Teilen von Medien blockieren sowie die Einrichtung eines monatlichen Ausgabelimits) versehen. Wichtige Optionen wie die Freigabe von Spielen oder Medieninhalten nach Alterseinstufung sind aber nur systemweit einstellbar und müssen, je nachdem wer gerade die Konsole nutzt, umständlich geändert werden. Für die Konsole ist ein kostenpflichtiger Webfilter eines Drittanbieters verfügbar.

5.2.5 Smart-TV

Smart-TVs verfügen über eine Internetverbindung und ermöglichen meist die Installation von Drittanbieteranwendungen. Der Funktionsumfang der Geräte ist inzwischen mit dem eines Tablets zu vergleichen. In Deutschland ist bereits jeder vierte Fernseher ein Smart-TV.[42] Über die Apps von Streaming-Diensten kann auf deren Angebote zugegriffen werden. In der Regel ist auch das Surfen über einen integrierten Browser möglich. Die genutzten Betriebssysteme unterscheiden sich je nach Anbieter sehr stark. Verbreitete Systeme sind „Tizen OS" (Samsung), „webOS" (LG) und „Android TV" (Sony/Panasonic). Bei den meisten auf Smart-TVs lauffähigen Apps handelt es sich um verhältnismäßig einfache Anwendungen, die den Zugriff auf einen bestimmten Dienst ermöglichen. Apps gängiger Social-Web-Dienste (z. B. YouTube, Facebook) sind bereits ab Werk vorinstalliert. Daneben lassen sich zusätzliche Apps (in ähnlicher Bandbreite wie Apps für mobile Endgeräte) über herstellereigene App-Stores nachinstallieren.

Schutzfunktionen von Smart-TVs marktführender Hersteller (LG, Samsung, Sony und Panasonic) beschränken sich meist auf den Rundfunk. In der Regel existiert ein Menüpunkt „Kindersicherung", welcher mit einer 4-stelligen PIN gegen Zugriff durch Kinder und Jugendliche gesichert ist. Hier kann eine Sender- oder Programmsperre aktiviert werden. Ebenso können Apps per PIN gesperrt werden.

[41] Beispielsweise können auf der Playstation 4 Spielevideos, Screenshots oder Erfolge direkt über eine Schnittstelle auf YouTube, Facebook oder Twitter geteilt werden.

[42] Knab (2014), S. 12

Bei auf Android-TV basierenden Modellen kommt ein ähnliches Betriebssystem zum Einsatz wie auf Android Tablets. Mit diesem System ausgestattete Geräte sind in ihrer Funktionalität vergleichbar mit mobilen Endgeräten. Die Geräte haben Zugriff auf den Play Store und sind in der Lage, dort angebotene Spiele zu installieren.[43]

Neben Fernsehgeräten existiert eine Vielzahl an Produkten, die das Streaming von Inhalten auf ein Fernsehgerät zulassen. Dies sind meist Set-Top-Boxen, welche als Bild- und Tonquelle an den Fernseher angeschlossen werden. Die Geräte bieten einen mit Smart-TVs vergleichbaren Funktionsumfang. Die verbreitetsten Geräte sind Amazon Fire TV, Apple TV, Google Nexus Player, Google Chromecast. Fire TV lässt sich per PIN sichern. Google Nexus Player (Android) bietet die Jugendschutzfunktionen von Android. Im Gegensatz zu iOS haben Entwickler unter TVOS (Apple TV) Zugriff auf die Alterseinstellungen. Dies böte die Möglichkeit für Video-on-Demand Dienste (z. B. Netflix oder Maxdome), ihren Inhalt entsprechend der Systemeinstellungen für Filme zu filtern.[44] Auch Blu-ray-Spieler und Festplattenrekorder sind inzwischen meist vernetzt und bieten zum Teil die Möglichkeit der Installation von Apps oder einen integrierten Webbrowser an.[45]

[43] https://play.google.com/store/apps/collection/promotion_3000e24_androidtv_games_all?hl=de

[44] https://developer.apple.com/library/tvos/documentation/TVMLJS/Reference/TVJSRestrictions_Ref/index.html

[45] http://www.samsung.com/de/consumer/tv-av/audio-video/blu-ray-dvd-player/BD-H5500/EN

6 Zukunftsfähiges integriertes Schutzkonzept

Technische Schutzsysteme sollen Risiken für Kinder und Jugendliche reduzieren und Eltern bei der Medienerziehung unterstützen. Um den Anforderungen eines zeitgemäßen Jugendschutzes gerecht zu werden, müssen sie die Nutzungsgewohnheiten von Kindern und Jugendlichen berücksichtigen, akzeptable Wirksamkeit gewährleisten und für Eltern einfach zu handhaben sein. Ansonsten entfalten sie keine ausreichende Schutzwirkung oder werden nicht aktiviert.

Die Herausforderung besteht darin, existierende Schutzmöglichkeiten in den Bereichen Inhaltsfilterung (Schutz vor Konfrontationsrisiken) und sichere Konfiguration (Schutz vor Kommunikations- und Interaktionsrisiken) so zu verbinden und weiterzuentwickeln, dass junge User in wichtigen Risikobereichen, in relevanten Diensten und auf den am häufigsten genutzten Geräten möglichst gut geschützt sind. Gleichzeitig müssen Eltern die Schutzoptionen noch einfach einstellen können.

6.1 Jugendschutzfilter: Blockieren einschlägiger Inhalte auf klassischen Websites

Die verfügbaren Schutzlösungen filtern klassische Websites mit einschlägigen Inhalten (z. B. pornografische, gewaltverherrlichende und extremistische Webseiten) oder blockieren komplette Dienste (z. B. Tumblr) oder Protokolle (z. B. HTTPS). Jugendschutzprogramme können die Konfrontation mit beeinträchtigenden oder gefährdenden Inhalten in akzeptablem Umfang reduzieren, nicht aber Risiken im Bereich der Kommunikation oder der Preisgabe persönlicher Daten.

Die Filterquoten können verbessert werden, wenn Schutzsoftware neuere Technologien der Analyse von Inhalten einsetzen würden. Filteranbieter können dabei unterstützt werden, indem geeignete Daten für das Training „intelligenter" Erkennungssysteme zur Verfügung gestellt werden. Auch Inhalteanbieter können ihren Beitrag zur Steigerung der Wirksamkeit leisten, indem sie die Alterseignung ihre Inhalte in maschinenlesbarer Form klassifizieren.

Da eine Filterung von Inhalten des Social Web aufgrund der hohen Fluktuation nicht mehr auf Basis von URL-Listen funktionieren kann, müssen Erkennungsmechanismen eingesetzt werden, die Inhalte (auch Bilder, Videos) in Echtzeit klassifizieren. Ohne den Einsatz fortschrittlicher Erkennungsverfahren (z. B. maschinelles Lernen) ist die Filterung der täglichen Menge an neu generierten Inhalten nicht mehr umsetzbar, klassische Blacklisting-Systeme können nur die Basis bilden.

Die Filterung funktioniert in der Regel nicht, wenn Kinder und Jugendliche per App online gehen. Mobile Betriebssysteme kapseln die einzelnen Apps sehr stark voneinander ab (sie laufen in einer jeweils eigenen Sandbox), was den Zugriff separater Filterprogramme auf deren Datenverkehr und Inhalte unmöglich macht oder wesentlich erschwert. Jugendschutzfilter können hier die Apps nur komplett blockieren oder proprietäre Schutzoptionen von Apps oder Diensten aktivieren.

Mit zunehmender Verschlüsselung von Websites können klassische Filterprogramme nur noch die Hauptdomains blockieren, aber einzelne Inhalte nicht mehr differenziert filtern (sie können nur noch aktiv werden, bevor Browser und Server die Art der Verschlüsselung vereinbart haben). Ausnahmen sind Systeme, die abgerufene Inhalte in Echtzeit analysieren, oder Browser, die eine eigene Filterfunktion bieten und aufgerufene Adressen mit Blacklists abgleichen können, bevor sie verschlüsselt werden.

Filtersysteme sind nicht für alle Geräteklassen verfügbar, die meisten werden für PCs angeboten, einige auch für Smartphones und Spielekonsolen. Für Smart-TV oder neue Gerätekategorien wie vernetzte Spielzeuge (Internet of Things) gibt es derzeit keine Jugendschutzfilter. Auch hier könnten Browser mit Filteroptionen, die auf verschiedenen Geräteklassen funktionieren (z. B. Google Chrome ist für PCs, Smartphones, Tablets und Smart-TV verfügbar), eine Perspektive bieten.

Filtersysteme sind meist auf einzelnen Geräten von Usern installiert, Filter für Router (z. B. Cybits) oder beim Access-Provider (wie in Großbritannien) sind in Deutschland selten. Sie erleichtern zwar die Handhabung und können alle onlinefähigen Geräte in einem Haushalt filtern, funktionieren aber nur bei unverschlüsselten Angeboten und sind durch die Wahl eines anderen Netzzugangs (Mobilfunk, WLAN-Hotspots) sehr einfach zu umgehen.

6.2 Schutzfunktionen von Diensten: Reduktion von Risiken im Social Web

Die verfügbaren Schutzfunktionen von Diensten aktivieren Mechanismen, mit denen Betreiber beeinträchtigende Inhalte für bestimmte Altersgruppen ausblenden, den Zugriff von Fremden auf Daten von Usern blockie-

ren oder die Reichweite der Äußerungen jugendlicher User begrenzen. So können Konfrontationen mit beeinträchtigenden Inhalten und Risiken der Belästigung durch Dritte oder der ungewollten Datenpreisgabe reduziert werden.

Die proprietären Funktionen können besseren Schutz bieten, wenn die Betreiber der Plattformen ihre Vorsorge verbessern (z. B. Einsatz neuerer Analysemechanismen beim Upload von Inhalten, Optionen der Klassifizierung), ihre Supportstrukturen optimieren und sichere Nutzungsoptionen für Kinder und Jugendliche anbieten. Betreiber können dabei unterstützt werden, indem geeignete Daten für das Training von Erkennungsprozessen zur Verfügung gestellt werden.

Die sichere Konfiguration von Diensten für Kinder und Jugendliche bietet keinen Schutz, wenn sie von Freunden gemobbt oder belästigt (z. B. Sexting) werden oder gefährdende Videos (z. B. Gewaltvideos als Mutprobe) von ihnen zugeschickt bekommen. Sie entfaltet Schutzwirkung in der öffentlichen Kommunikation, indem der Kreis von Adressaten eingeschränkt wird. Bei der Kommunikation im privaten Umfeld oder in geschlossenen Zirkeln ist Schutz kaum möglich oder zulässig (Fernmeldegeheimnis).

Die Schutzeinstellungen von Diensten entfalten ihre Schutzwirkung auch beim Zugriff über Apps und mobilen oder verschlüsselten Verbindungen, da es sich um proprietäre Mechanismen handelt, die nicht auf einzelnen Geräten aktiviert werden. Die Sicherungen basieren auf Einstellungen im Backend der Dienste und funktionieren unabhängig davon, welche Geräte Kinder und Jugendliche nutzen oder ob sie per Browser oder App auf die Angebote des Dienstes zugreifen.

Die Schutzfunktionen von Diensten sind proprietäre Systeme, die nur im jeweiligen Dienst wirksam sind. Die Aktivierung geschieht dabei in der Regel über diensteigenen Einstellungen. Nur in wenigen Fällen stellen die Betreiber Schnittstellen zur Verfügung, mit denen sichere Einstellungen extern durch Jugendschutzfilter (z. B. Family Safety in der Google-Suche) oder Betriebssysteme (z. B. altersdifferenzierte Download-Beschränkungen von iTunes über iOS) vorgenommen werden können.

6.3 Einfache Handhabung: Integration in ein Gesamtmodell

Jugendschutzprogramme können Inhalte auf klassischen Websites filtern, aber keine sichere Nutzung von Diensten des Social Web gewährleisten. Die sichere Konfiguration von Diensten im Social Web bietet Schutz in allen Risikobereichen, aber nur begrenzt auf den jeweiligen Dienst. Für Eltern ist es schwer möglich, den Überblick zu behalten und alle möglichen Schutzoptionen auf allen onlinefähigen Geräten zu aktivieren, die ihre Kinder nutzen.

Um Eltern ein handhabbares Jugendschutzsystem zu bieten, müssen verfügbare Mechanismen so weit wie möglich in ein Gesamtsystem integriert werden. Für die Aktivierung an einer zentralen Stelle bieten sich die Systemeinstellungen von Betriebssystemen an. Microsoft Windows, Google Android und Appel iOS verfügen bereits über Konfigurationsmöglichkeiten, die beispielsweise die Übermittlung persönlicher Daten oder des jeweiligen Standorts blockieren können. Auf diese Funktionen könnte aufgesetzt werden.

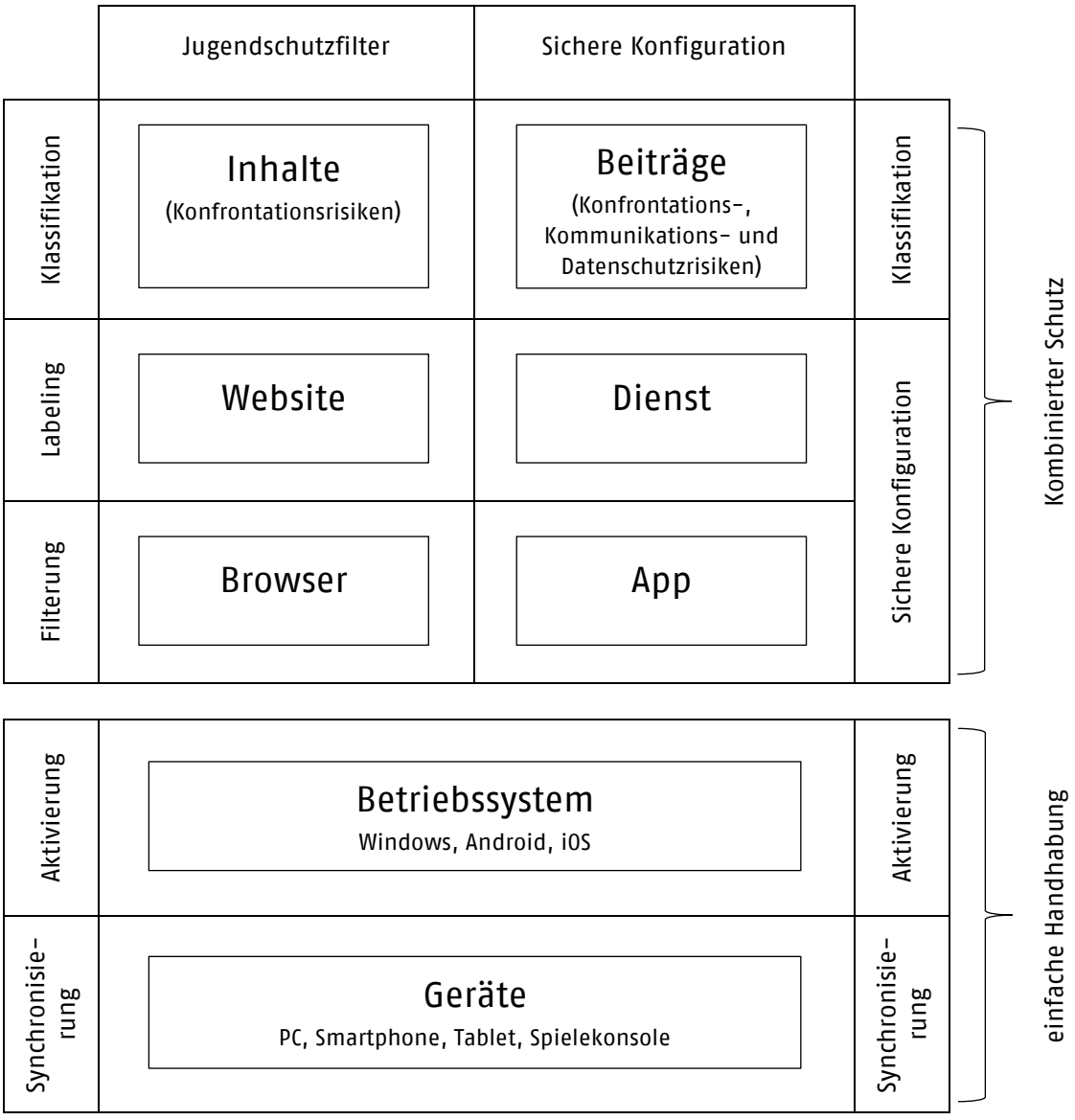
Die Betriebssysteme lassen sich mit Online-Accounts der Hersteller (Microsoft-Konto, Google-Konto, Apple ID) verknüpfen. Bei Geräten mit dem gleichen Betriebssystem könnten die Jugendschutzeinstellungen auch über verschiedene Geräte so einfach synchronisiert werden. Perspektivisch wäre darüber hinaus die Nutzung eines plattformunabhängigen Cloud-Dienstes zur Synchronisierung der Einstellungen auch zwischen unterschiedlichen Betriebssystemen denkbar.

Für das Gesamtmodel wird eine Aktivierungsoption der sicheren Konfiguration in den Systemeinstellungen des jeweiligen Betriebssystems benötigt. Um den Konfrontationsschutz bei klassischen Websites zu gewährleisten, müssten mit der Aktivierung alle Browser auf dem jeweiligen Gerät blockiert werden (z. B. über eine Altersklassifizierung der jeweiligen Browser-App). Nur die Nutzung von Browsern wäre zuzulassen, in die Jugendschutzfilter nach dem Stand der Technik integriert sind.

Mit der Aktivierung der sicheren Konfiguration wären auch alle jugendschutzrelevanten Apps zu blockieren, deren Altersklassifizierung (z. B. IARC) nicht der Alterseinstellung im Betriebssystem/User-Profil entspricht (dies ist heute bei iOS schon der Fall). Dienste bzw. deren Apps mit altersdifferenzierten Konfigurationsoptionen müssten sichere Einstellungen aktivieren und relevante Schutzoptionen über die Betriebssystemeinstellungen bereitstellen.

Voraussetzungen für das Gesamtmodell wären

- ein plattformübergreifender **Browser** mit integriertem Jugendschutzfilter
- **sichere Konfigurationsoptionen** bei den wichtigsten Social-Web-Diensten
- **Alterseinstellungen** in den drei von Kindern und Jugendlichen häufig genutzten Betriebssystemen
- eine **Schnittstelle** zwischen Betriebssystem und Apps/Browser zum Aktivieren sicherer Konfigurationen



Gesamtmodell zukunftsfähigen technischen Jugendschutzes

7 Kriterien für Jugendschutzprogramme und Teillösungen

Der JMStV sieht vor, dass Inhalteanbieter ihre Schutzpflichten bei beeinträchtigenden Telemedien auch durch Programmierung für ein anerkanntes Jugendschutzprogramm erfüllen können. Deshalb hat die KJM 2011 Kriterien für die Anerkennung von Jugendschutzprogrammen im Bereich des World Wide Web formuliert.[46] Sie behalten im Wesentlichen ihre Gültigkeit, auch wenn mit der Novellierung des JMStV die Anerkennungsbefugnis auf die anerkannten Einrichtungen der Freiwilligen Selbstkontrollen übergeht und der KJM lediglich die Aufgabe zufällt, Kriterien für Eignungsanforderungen festzulegen und mit den Selbstkontrollen abzustimmen.

§ 11 Abs. 3 des JMStV spricht in diesem Zusammenhang von „Richtlinien", die die KJM im Benehmen mit den anerkannten Einrichtungen der Freiwilligen Selbstkontrollen festlegen kann. Darunter sind keine Jugendschutzrichtlinien zur Durchführung des Staatsvertrags zu verstehen, die von den Gremien der Landesmedienanstalten erlassen werden und die die Herstellung des Benehmens mit ARD und ZDF vorsehen. Gemeint sind Leitlinien und Bewertungsmaßstäbe der KJM, die mit den Selbstkontrollen abgestimmt werden. Diese können sich an der Formulierung der bestehenden Kriterien orientieren.

Der neue Staatsvertrag präzisiert die Anforderungen an Jugendschutzprogramme. Die Präzisierungen sind in den Kriterien der KJM jedoch bereits weitgehend berücksichtigt, da die KJM 2011 die Regelungen des gescheiterten 14. RÄndStVG zu Grunde gelegt hat. Die Anforderungen an Jugendschutzprogramme bleiben auf den Schutz vor entwicklungsbeeinträchtigenden Inhalten beschränkt, der Schutz vor Kommunikationsrisiken oder ungewollter Preisgabe persönlicher Daten werden im JMStV nicht geregelt.

Nur bei der Option, künftig auch so genannte Teillösungen anzuerkennen, die den Zugang zu Telemedien innerhalb geschlossener Systeme ermöglichen oder für einzelne Altersstufen ausgelegt sind, geht der neue Staatsvertrag darüber hinaus. Sie sind nach den Vorgaben des novellierten JMStV als eine Untergruppe von Jugendschutzprogrammen zu verstehen. Die Anforderungen für Jugendschutzprogramme gelten deshalb auch für Teillösungen. Da sie jedoch Besonderheiten aufweisen und Fragen der Abgrenzung aufwerfen, ist eine gesonderte Betrachtung sinnvoll.

7.1 Anpassungen der Kriterien für die Eignungsprüfung von Jugendschutzprogrammen

Die Kriterien der KJM zur Anerkennung von Jugendschutzprogrammen können grundsätzlich beibehalten werden. Lediglich einige Anpassungen sind nötig, um Neuregelungen des JMStV zu berücksichtigen und den veränderten Rahmenbedingungen gerecht zu werden.

7.1.1 Nutzerautonomer Jugendschutzfilter

Jugendschutzfilter sollen Eltern bei der Medienerziehung unterstützen. Diese sollen die volle Kontrolle über Jugendschutzprogramme haben, damit sie die Software in ihrem Sinne einsetzen können. Das Kriterium der Nutzerautonomie bleibt für die Bewertung von Jugendschutzprogrammen weiterhin relevant und kann ohne Änderungen übernommen werden.

7.1.2 Funktionsfähiges und handhabbares Filterprogramm

Jugendschutzfilter müssen benutzerfreundlich sein, damit Eltern sie auch einsetzen. Sie dürfen keine unrealistischen Anforderungen an ihren technischen Sachverstand stellen und keine hohen Kosten verursachen. Die bestehenden Formulierungen in den Kriterien der KJM können auch hier grundsätzlich beibehalten werden.

Die Forderung in den ersten Staatsvertragsentwürfen, dass Jugendschutzprogramme „jeweils für die am meisten genutzten Betriebssysteme zur Verfügung stehen" müssen, wurde in der finalen Version gestrichen. Damit reicht weiterhin der Nachweis, dass ein Jugendschutzprogramm auf einer Plattform funktionsfähig ist.

Plattform- und geräteübergreifende Schutzfunktionen werden in der Begründung des Staatsvertrages erstmals als Ziel formuliert, um die einfache Handhabung für Eltern bei einer Vielfalt von Jugendschutzprogrammen und Teillösungen zu gewährleisten. Die KJM kann in ihren Richtlinien Vorgaben für die dafür nötigen Schnittstellen aufstellen. Vor diesem Hintergrund ist künftig von Jugendschutzprogrammen zu fordern, dass sie verfügbare und für sie erreichbare Schutzeinstellungen in Diensten, die von Kindern und Jugendlichen häufig genutzt werden, aktivieren (z.B. Safe Search bei Google und Bing, Family Safety in YouTube). Diese Anforderung wäre als zusätzliches Kriterium zu formulieren.

[46] http://www.kjm-online.de/fileadmin/Download_KJM/Rundfunk/Informationen-fr-JSP-Anbieter_Stand_2011-05-11.pdf

7.1.3 Hohe Zuverlässigkeit bei der Blockade unzulässiger Inhalte

Ein wesentliches Kriterium für die Bewertung von Jugendschutzfiltern ist deren Zuverlässigkeit bei der Blockade beeinträchtigender und gefährdender Inhalte. Die hohe Zuverlässigkeit konnte bisher nur aus der globalen Zielsetzung abgeleitet werden, Kindern und Jugendlichen einen altersdifferenzierten Zugang zu Telemedien zu ermöglichen. Der neue JMStV greift Regelungen des gescheiterten 14. RÄndStVG auf und fordert erstmals ausdrücklich, dass Jugendschutzprogramme beeinträchtigende Inhalte nach dem Stand der Technik ausfiltern müssen. Die Erkennungsleistung müsse sich dabei an den stetig fortschreitenden technischen Entwicklungen messen lassen.

Die Kriterien der KJM sehen bisher vor, dass Jugendschutzprogramme unabhängig vom Stand der Technik eine Zuverlässigkeit von mindestens 80 % bei der Blockade beeinträchtigender und gefährdender Inhalte aufweisen müssen. Geprüft wurde die Zuverlässigkeit von jugendschutz.net mit einem gewichteten Testbett aus Webseiten, dessen Eckpunkte von der KJM beschlossen und mit der FSM abgestimmt waren. In der Struktur der Testszenarien spiegeln sich die aktuellen Nutzungsweisen junger User nicht mehr ausreichend wider. Künftig sind beispielsweise Beiträge im Social Web stärker zu berücksichtigen. Das neue Testverfahren muss jedoch von den Selbstkontrollen entwickelt werden, die Jugendschutzprogramme anerkennen und prüfen müssen.

Erstmals definiert der neue JMStV den Stand der Technik und fordert in der Begründung eine Erkennungsleistung, die dem „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen" entspricht. Er überträgt der KJM die Aufgabe, im Benehmen mit den Freiwilligen Selbstkontrollen Richtlinien festzulegen, die den einzuhaltenden Stand der Technik inhaltlich ausformen und einen hohen Standard gewährleisten. Auch hier handelt es sich nicht um Richtlinien der Landesmedienanstalten nach § 15 JMStV, sondern um ein "flexibles Instrument" der KJM, das ermöglichen soll, mit den technischen Entwicklungen Schritt zu halten.

Mangels Definition des Stands der Technik in den bisherigen Staatsverträgen forderten die Kriterien der KJM bisher eine Zuverlässigkeit, die sich im oberen Drittel des Leitungsspektrums von Jugendschutzfiltern bewegt. Die anerkannten Jugendschutzprogramme erfüllten dieses Kriterium regelmäßig, da sie eine höhere Filterleistung als andere, meist ausländische Jugendschutzfilter aufwiesen. Die anerkannten Jugendschutzprogramme binden beispielsweise die FragFINN-Liste ein und erreichen alleine damit eine höhere Filterleistung als ausländische Programme. Da der neue Staatsvertrag auf fortschrittliche Verfahren der Erkennung beeinträchtigender Inhalte rekurriert, können die Filterquoten anderer Jugendschutzfilter nicht mehr der Maßstab sein.

Um Jugendschutzfilter nach den Vorgaben des neuen Staatsvertrages beurteilen zu können, muss ein Verfahren zur Ermittlung des Stands der Technik festgelegt werden. Mit der Feststellung des fortgeschrittenen Stands der Technik wären Institute zu beauftragen, die die Möglichkeiten und Grenzen von Mechanismen zur Detektion jugendschutzrelevanter Online-Inhalte beurteilen können.[47] Der Stand der Technik muss in regelmäßigen Abständen ermittelt werden, um der Anforderung in der Begründung zu genügen, dass sich Jugendschutzprogramme an den stetig fortschreitenden technischen Entwicklungen messen lassen müssen.

7.1.4 Altersdifferenzierter Zugang und zutreffende Auswertung der Altersklassifizierung

Jugendschutzprogramme sollen einen altersdifferenzierten Zugang zu Telemedieninhalten bieten und Altersklassifizierungen korrekt auslesen, um den unterschiedlichen Bedürfnissen von Kindern und Jugendlichen gerecht zu werden. Die Kriterien der KJM können hier im Wesentlichen beibehalten werden.

Die Anforderung an Jugendschutzprogramme, dass sie auch internationale Alterskennzeichnungen auslesen sollen, wurde nach einer Anhörung von Unternehmen, Verbänden und Selbstkontrollen aus den JMStV-Entwürfen gestrichen. Jugendschutzprogramme müssen damit nur die maschinenlesbaren Klassifizierungen nach dem age-de-Standard auswerten können. Laut Staatsvertragsbegründung bleibt die Berücksichtigung internationaler Altersklassifizierungen wie IARC Modellversuchen vorbehalten, in denen sie auch im deutschen Rechtssystem erprobt und implementiert werden können.

Der neue JMStV eröffnet die Möglichkeit, auch Jugendschutzprogramme anzuerkennen, die nur für einen bestimmten Altersbereich ausgelegt sind (z.B. sichere Surfräume für Kinder). Das Kriterium der Altersdifferenzierung muss also entsprechend ergänzt werden. Um eine Begrenzung auf sehr kleine Alterskohorten zu vermeiden (z. B. 12-14 Jahre), könnte eine Auslegung für Kinder (unter 12) oder Jugendliche (ab 12 Jahren) als Mindest-

[47] Z. B. das Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme, das 2013 auch die Studie zu den Möglichkeiten und Grenzen von Verfahren zur Detektion jugendschutzrelevanter Web-Inhalte erarbeitet haben (http://www.iais.fraunhofer.de/uploads/media/Fraunhofer_Jugendmedienschutz_2013-02-25_01.pdf)

anforderung vorgegeben werden.[48] Da die bisherigen Altersgruppen „12 bis unter 16 Jahre“ und „16 bis unter 18 Jahre“ in der Praxis von Jugendschutzprogrammen nur von geringer Relevanz sind, könnte im Bereich der Jugendlichen auf die Forderung einer weiteren Differenzierung verzichtet werden.

7.1.5 Anpassung an den Stand der technischen Entwicklung

Die Kriterien der KJM sehen vor, dass die Anbieter ihre anerkannten Jugendschutzprogramme kontinuierlich weiterentwickeln und über erzielte Fortschritte berichten müssen. Da der neue Staatsvertrag diese Forderung bestätigt, sind hier keine Änderungen der Kriterien nötig. Zu klären ist, wie und in welchen Abständen überprüft werden soll, wie das Jugendschutzprogramm an die technische Entwicklung angepasst wurde.

7.1.6 Verbreitung von Jugendschutzprogrammen

Die Schutzoption Jugendschutzprogramme kann nur gewährleisten, dass Kinder und Jugendliche üblicherweise auf beeinträchtigende Inhalte nicht zugreifen können, wenn die Programme weit verbreitet sind und von vielen Eltern eingesetzt werden. Erste Überlegungen für den neuen Staatsvertrag sahen hier Mindestquoten für die Steigerung der Verbreitung vor. Auch Vorinstallation und die Frage, ab welchem Verbreitungsgrad Jugendschutzprogramme als wirksamer Schutz vor beeinträchtigenden Inhalten ausreichen, wurden diskutiert. In der beschlossenen Fassung bleibt das Thema Verbreitung aber ausgespart, so dass die bestehenden Kriterien auch in diesem Punkt übernommen werden können.

Anbieter von Jugendschutzprogrammen können nicht allein für die Steigerung der Verbreitung verantwortlich gemacht werden. Die Verbreitung ihrer Programme hängt von verschiedenen Faktoren ab (z. B. Konzept elterlicher Medienerziehung), die sie nicht beeinflussen können. Die Anforderung, dass die Anbieter der Programme über Verbreitungskonzepte und die Erfolge ihrer Bemühungen berichten sollen, sollte aber beibehalten werden. Es sollte auch in ihrem Interesse liegen, ihre Produkte zu bewerben.

7.2 Teillösungen für geschlossene Systeme

Der neue Staatsvertrag sieht erstmals die Anerkennung von Programmen vor, die den Zugang zu Telemedien innerhalb geschlossener Systeme ermöglichen, die über eine eigene Jugendschutzlösung verfügen. Mit dieser Regelung soll funktionierenden Teillösungen eine Eignungsprüfung nicht verweigert werden.

Der JMStV formuliert die Anerkennung von Programmen für geschlossene Systeme als Sonderfall umfassender Jugendschutzprogramme. Auch die Teillösungen müssen daher die gesetzlichen Anforderungen an Jugendschutzprogramme erfüllen. Neben Benutzerfreundlichkeit, Nutzerautonomie und einer ausreichenden Erkennungsleistung müssen sie auch Alterskennzeichnungen auslesen und Anbietern von Telemedien die Möglichkeit bieten, ihre Angebote für den Schutzmechanismus des geschlossenen Systems zu programmieren.

Die Begründung nennt zwar Spielekonsolen und Pay-TV-Plattformen als Beispiele für geschlossene Systeme, letztlich bleibt aber offen, was darunter zu verstehen ist. Spielekonsolen bieten heute den Zugang zu unterschiedlichen Arten von Telemedien: angefangen von Onlinespielen über Video-Streaming bis hin zu Websites. Handelt es sich um ein geschlossenes System, wenn die Teillösung nur bei Onlinespielen funktioniert, beim Websurfen aber freien Zugang gewährt? Die KJM muss in ihren Kriterien definieren, wann ein geschlossenes System gegeben ist.

7.2.1 Anforderungen an Alterskennzeichnungen

Anbieter genügen ihren Schutzpflichten im JMStV, wenn sie ihre entwicklungsbeeinträchtigenden Inhalte mit einer Alterskennzeichnung versehen, die von geeigneten Jugendschutzprogrammen und Teillösungen ausgelesen werden können. Voraussetzung jeder Anerkennung ist die Programmierbarkeit von Inhalten nach dem Prinzip Schlüssel (Label) und Schloss (Jugendschutzprogramm). Die Begründung des Staatsvertrages fordert deshalb auch, dass Jugendschutzprogramme technische Alterskennzeichnungen richtig auslesen müssen.

Der JMStV macht hier keine Vorgaben bezüglich der technischen Kennzeichnungen. Die KJM fordert in den Kriterien, dass alle anerkannten Jugendschutzprogramme den Klassifizierungsstandard age-de auswerten müssen. Diese Festlegung ist für Jugendschutzprogramme, die beeinträchtigende Inhalte im offenen WWW ausfiltern sollen, auch weiterhin sinnvoll. Nur über die Festlegung eines Programmierstandards kann sichergestellt werden, dass das Zusammenspiel von Schlüssel und Schloss funktioniert und alle anerkannten Jugendschutzprogramme die Programmierung eines Anbieters erkennen und richtig interpretieren können.

[48] Weiterhin nicht anerkennungsfähig wären Jugendschutzfilter, die keinerlei Altersdifferenzierung aufweisen.

Bei geschlossenen Systemen bietet der Anbieter seine Inhalte nur innerhalb der Grenzen einer genau definierten Plattform an. Hier wäre auch zu wünschen, dass etablierte und qualifizierte Kennzeichnungen eingesetzt werden (z.B. USK- oder FSK-Kennzeichen), es besteht aber keine Notwendigkeit für eine Standardisierung. Der Anbieter genügt seinen Schutzpflichten auch dann, wenn er sein Angebot mit einem proprietären Kennzeichen des geschlossenen Systems klassifiziert, solange er damit verhindert, dass junge User auf seine ungeeigneten Inhalte zugreifen können. Auch proprietäre Klassifizierungen (z. B. ein Label "not suitable for children" beim Upload auf eine Videoplattform) sind damit ausreichend, sofern sich das Label einer bestimmten Altersgruppe zuordnen lässt und das geschlossene System Eltern eine Schutzoption bietet.

7.2.2 Definition von Geschlossenheit und Beispiele für anerkennungsfähige Teillösungen

In die Prüfung, ob es sich bei einem Programm um eine anerkennungsfähige Teillösung für ein geschlossenes System handelt, sind drei Anforderungen einzubeziehen:

- **Zugang zu Telemedien innerhalb eines geschlossenen Systems**
  Zugang zu Telemedien wird ermöglicht, wenn im geschlossenen System Inhalte von Dritten verfügbar gemacht werden. Ein System ist geschlossen, wenn alle Vorgänge an herstellereigenen Standards gebunden sind und in der Regel den Rahmen des Systems nicht verlassen können.
- **(proprietäre) Schutzfunktion mit der Konfigurationsmöglichkeit für mindestens eine Altersstufe**
  Altersdifferenzierte Schutzmechanismen liegen vor, wenn Eltern Einstellmöglichkeiten angeboten werden, welche sich auf Vorgänge innerhalb des geschlossenen Systems auswirken und sich zumindest für eine Altersstufe konfigurieren lassen.
- **Option für Anbieter, die Alterseignung ihrer Telemedien zu programmieren**
  Die Fähigkeit des Auslesens einer Alterskennzeichnung liegt vor, wenn das System eigene Klassifizierungsmöglichkeiten für Inhalte von Dritten anbietet oder vorhandene Klassifizierungen auswerten kann (z.B. FSK-Kennzeichen, IARC-Label).

Auf Basis dieser Anforderungen können die in Kapitel 5 diskutierten Schutzfunktionen von Anwendungen, Diensten und Geräten eingeordnet werden, die von Kindern und Jugendlichen häufig genutzt werden. In der Regel sind onlinefähige Geräte bzw. deren Betriebssysteme nicht als geschlossene Systeme im Sinne des § 11 Abs. 2 JMStV einstufen, da sie auch einen offenen Zugang zum World Wide Web ermöglichen. Lediglich Teilbereiche der Geräte bzw. deren Betriebssysteme erfüllen das Kriterium der Geschlossenheit des Zugangs zu Telemedien. Anerkennungsfähige Teillösungen sind vor allem im Bereich der Dienste zu finden.

Die folgenden Beispiele sollen verdeutlichen, wann eine geschlossene Teillösung vorliegt:

Der Google Play Store ist ein geschlossenes System, das den Zugang zu Telemedien von Dritten ermöglicht, indem es Apps und Medieninhalte zum Download auf Android-basierte Geräte (Smartphones, Tablets, Smart-TV) anbietet, die im Store gespeichert sind. Der Store verfügt über eine altersdifferenzierte Schutzfunktionen, deren Einstellungen sich nur innerhalb des Stores auswirken und die den Download altersdifferenziert beschränken können. Das Schutzprogramm wertet dazu IARC-Klassifizierung aus, d. h. Anbieter haben die Möglichkeit, ihre Apps altersdifferenziert für den Google Play Store zu programmieren. Google Play und vergleichbare Stores wären demnach als Teillösungen anerkennungsfähig.

Nicht anerkennungsfähig ist IARC als eigenständiges System. Hierbei handelt es sich um ein Klassifizierungssystem. Die Altersklassifizierungen mit IARC können Bestandteil der Filterfunktion eines geschlossenen Systems sein. IARC selbst verfügt aber über keine Schutzfunktionen und ist kein geschlossenes System, das Zugang zu Telemedien ermöglicht. Ähnliches gilt für die FragFINN-Whitelist oder das BPjM-Modul. Sie können als klassifizierende Listen in Jugendschutzprogrammen und Teillösungen eingesetzt werden.

Der Video-on-Demand-Dienst von Netflix ist ein geschlossenes System, das den Zugang zu Telemedien von Dritten ermöglicht, indem es audiovisuelle Inhalte per Streaming über unterschiedliche Zugänge (per Browser oder App) für unterschiedliche Geräte und Betriebssysteme anbietet. Der Dienst verfügt über eine proprietäre Schutzoption, die in allen Nutzungsvarianten einen altersdifferenzierten Zugang zu Filmen ermöglicht. Das Schutzprogramm wertet dazu FSK-Kennzeichen aus, d. h. Anbieter haben die Möglichkeit, ihre Filme für das Netflix-Streaming altersdifferenziert zu programmieren. Auch vergleichbare Video-on-Demand-Dienste wären demnach anerkennungsfähig.

Smart-TV-Geräte oder deren Betriebssysteme sind nicht anerkennungsfähig. Sie sind keine geschlossenen Systeme, sie bieten keine Programmiermöglichkeit für Anbieter und verfügen über keine Schutzoptionen, die

einen altersdifferenzierten Zugang zu Telemedien ermöglichen. Ähnliches gilt beispielsweise für das Betriebssystem Android. Es verfügt zwar über Schutzoptionen („eingeschränkter Benutzer"), ihm fehlen aber die Geschlossenheit des Systems, die Altersdifferenzierung beim Schutz und die Programmierbarkeit für Anbieter.

Die Spielekonsole Nintendo Wii bietet neben der eigentlichen Spielefunktion auch einen eigenen Kommunikationsdienst, einen App Store und einen Browser. Während die Schutzoptionen des App-Stores als Teillösung anerkennungsfähig wären (Nintendo greift auf USK-Kennzeichen zurück und bietet damit Programmiermöglichkeiten), ist dies beim Schutzsystem der Wii als Ganzes nicht der Fall. Es handelt sich zwar in weiten Teilen um ein geschlossenes System, aber der Zugang zu Telemedien wird durch den integrierten Browser geöffnet.[49]

Das Videoportal YouTube ist ein geschlossenes System, das den Zugang zu Telemedien von Dritten ermöglicht. Der Dienst ist auf unterschiedlichen Wegen (Browser, App) und Geräten zu erreichen, verfügt in jedem Fall aber über eine proprietäre Schutzfunktion, die den Zugriff von Kindern und Jugendlichen altersdifferenziert beschränkt. User haben beim Einstellen von Videos die Möglichkeit, ihren Inhalt als „ungeeignet für Jugendliche" zu programmieren. YouTube und vergleichbare Dienste mit altersdifferenzierten Schutzoptionen wären demnach als Teillösung anerkennungsfähig, die nur für eine bestimmte Altersgruppe ausgelegt ist.

Die FragFINN-App ermöglicht den Zugang zu Telemedien von Dritten. Sie bietet eine Schutzfunktion, die auf eine Altersgruppe (Kinder) ausgelegt ist und nur kindgeeignete Websites passieren lässt, die in der FragFINN-Whitelist verzeichnet sind. Die App ist aber kein geschlossenes System, das alle Inhalte auf den Webservern der jeweiligen Anbieter gespeichert sind. Die FragFINN-App ist ein Browser mit Filteroptionen, der Angebote im offenen WWW präsentiert. Dies gilt auch für vergleichbare Filter-Apps, die für Smartphones angeboten werden.

Der KinderServer erschließt einen sicheren Surfraum für Kinder und ist auch als Browser-Plug-In verfügbar. Als Teillösung ist das Plug-In genauso wenig anerkennungsfähig wie die FragFINN-App, da Inhalte aus dem offenen WWW zugänglich gemacht werden. Da der KinderServer aber auch age-de-Label ausliest und Anbietern damit Programmiermöglichkeiten bietet, wäre das Plug-In als Jugendschutzprogramm anerkennungsfähig, das nur auf die Altersgruppe Kinder ausgelegt ist.

7.2.3 Schnittstellen für plattform- und geräteübergreifende Lösungen

Die Anerkennung von Teillösungen kann zu einer für Eltern schwer zu bewältigenden Vielfalt anerkannter Schutzprogramme führen. Ein gutes Beispiel sind Smart-TV-Geräte, die unterschiedliche Streaming-Apps anbieten. Eltern müssten hier jeden proprietären Schutzmechanismus einzeln aktivieren und konfigurieren. Der Staatsvertragsgeber hat dieses Risiko gesehen und plattform- und geräteübergreifende Lösungen als Ziel formuliert. Dafür werden Schnittstellen benötigt, mit denen Eltern proprietäre Teillösungen übergreifend konfigurieren können. Laut Staatsvertrag ist die KJM künftig zuständig, Vorgaben für geeignete Schnittstellen zu entwickeln und das Benehmen mit den anerkannten Freiwilligen Selbstkontrollen darüber herzustellen.

Geräteübergreifender Schutz wäre mit klassischen Jugendschutzprogrammen möglich, wenn sie über Schnittstellen zur Steuerung von Teillösungen verfügten, auf allen genutzten Geräten installiert wären und Einstellungen zwischen allen Diensten synchronisieren könnten. Einige Jugendschutzfilter ermöglichen die Synchronisierung zwischen einigen Geräteklassen bereits. Voraussetzung für plattform- bzw. diensteübergreifenden Schutz wäre aber, dass alle proprietären Systeme eine Aktivierungs- und Konfigurationsoption für Jugendschutzprogramme bereitstellen würden. Dies scheint angesichts der globalen Aufstellung wichtiger Dienste unrealistisch, auch weil Jugendschutzprogramme eine Schutzoption sind, die auf Deutschland beschränkt ist.

Alternativ ließe sich plattform- und diensteübergreifender Schutz über die Betriebssysteme herstellen. Sie bieten bereits Ansätze zentraler Konfiguration und verfügen über Synchronisierungsmechanismen für Einstellungen, auf denen aufgesetzt werden kann. Proprietäre Schutzmechanismen könnten über eine Schnittstelle zentral verwaltet werden (z.B. alle Streaming-Apps eines Smart-TV), wenn sie Apps die Möglichkeit böten, proprietäre Schutzoptionen über das Betriebssystem zu aktivieren bzw. Alterseinstellungen dort abzufragen.

Auf der Ebene des Betriebssystems gibt es auch mehr Konfigurationsmöglichkeiten als über externe Jugendschutzprogramme. Im Betriebssystem können auch globale Schutzeinstellungen vorgenommen (z. B. Beschränkung, Standortdaten zu übermitteln) sowie Apps oder Dienste blockiert werden, die keine Schutzmechanismen anbieten. Die Verwaltung von Jugendschutzoptionen über das Betriebssystem ist darüber hinaus intuitiver, da Eltern an dieser Stelle alle Geräteeinstellungen vornehmen.

[49] Das Schutzsystem kann beispielsweise auch Kommunikationsrisiken reduzieren, indem es die Kommunikation im Nintendo-Netzwerk beschränkt. Die Regelungen des JMStV beziehen sich aber nur auf den Schutz vor entwicklungsbeeinträchtigenden Inhalten.

Seitens der KJM wären in den Richtlinien Vorgaben zu machen, welche Schnittstellen Teillösungen für die plattform- und diensteübergreifende Konfiguration von Schutzmechanismen zur Verfügung stellen müssen.

8 Weiterentwicklung des technischen Jugendschutzes

Angesichts global agierender Akteure im Internet kann sich der Jugendschutz nur Gehör verschaffen, wenn die Kräfte gebündelt, alle Instrumente genutzt und die europäische Ebene einbezogen wird. Um die Wirksamkeit des technischen Jugendschutzes weiterzuentwickeln bzw. Entwicklungen im Sinne eines kohärenten Gesamtsystems anzuregen, werden zwei Instrumente benötigt, die ineinandergreifen sollten:

- **Entwicklungsfonds**, um die Wirksamkeit von Schutzmechanismen zu fördern. und
- **Positivkennzeichnung**, um Anreize für die Entwicklung sicherer Produkte zu schaffen.

Entwicklungsförderung und Anreize für Diensteanbieter sollten auf einer gemeinsamen Initiative von Bund und Ländern basieren. Anknüpfungspunkte dafür bieten der neue JMStV (Richtlinienkompetenz der KJM bei Jugendschutzprogrammen und Schnittstellen), die Novellierung des JuSchG (erweiterte Schutzziele und "dialogische Anbieterregulierung") und der Abschlussbericht der Bund-Länder-Kommission zur Medienkonvergenz. Dort sind Entwicklungsfonds und Positivkennzeichnung als gemeinsame Aufgaben ausdrücklich erwähnt. Demnach ist es Aufgabe eines Beirats von Bund, Ländern und Landesmedienanstalten bei der modernisierten BPjM,

- Projekte des technischen Jugendmedienschutzes zu fördern, die eine sichere Mediennutzung durch Kinder ermöglichen und offene Standards und Schnittstellen zur Verbreitung sicherer Nutzungsmodi verankern und
- auf die Vereinbarung und Verbreitung von Kennzeichen hinzuwirken, die auf besonders für Kinder geeignete Inhalte oder Plattformen hinweisen oder eine inhaltliche Beurteilung der von einem Medium oder einer Plattform ausgehenden Risiken ermöglichen.

8.1 Allgemeine Ziele und Schwerpunktsetzung

Die ursprünglichen Überlegungen für den Entwicklungsfonds, allein auf die Weiterentwicklung von Jugendschutzprogrammen zu setzen, sind durch die technische Entwicklung und Veränderungen im Nutzungsverhalten von Kindern und Jugendlichen überholt. Mit zunehmender Verschlüsselung von Web-Angeboten und überwiegender Nutzung mobiler Apps wird der Bereich der Telemedien, in denen Jugendschutzprogramme Wirksamkeit entfalten können, immer kleiner. Es ist zwar möglich, ihre Leistung zu steigern, beispielweise durch die Optimierung von Filtermechanismen (z. B. Nutzung aktueller Erkennungsmechanismen). Da die Reichweite klassischer Jugendschutzprogramme auf dem PC aber stetig abnimmt, ist damit kein großer Schutzgewinn mehr verbunden.

8.1.1 Zeitgemäße Filtermechanismen und einfache Handhabbarkeit

Als anerkanntes Jugendschutzprogramm wird voraussichtlich nur JusProg fortbestehen. Die Telekom wird ihre Kinderschutz Software demnächst einstellen oder mit JusProg verschmelzen, ihre viel versprechenden Pläne eines plattform- und geräteübergreifenden Schutzsystems in der Cloud werden nicht weiter verfolgt. Cybits hat seine Anerkennung zurückgegeben, Child-Protect von Vodafone ist mit aktuellen Android-Versionen nicht mehr kompatibel und das neue Jugendschutzprodukt für Smartphones soll nur noch eigenen Kunden kostenpflichtig angeboten werden. Ein Entwicklungsfonds, der nur auf die Weiterentwicklung bestehender Jugendschutzprogramme fokussiert, wäre damit ein Förderprogramm für JusProg und würde im Wesentlichen die Unternehmen entlasten, die JusProg tragen.

Soll der Fonds Impulse für die Weiterentwicklung des technischen Jugendschutzes setzen, muss er sich von vorhandenen Schutzprogrammen lösen und auf zukunftsfähige Mechanismen fokussieren. Der Fonds sollte innovative Ansätze unterstützen, um beispielsweise eine größere Plattformabdeckung bei Jugendschutzprogrammen (z. B. Smartphones) und die Entwicklung zeitgemäßer Konzepte (z. B. Filterung im Browser) oder Filtermechanismen (z. B. Echtzeiterkennung) zu erreichen.

8.1.2 Sichere Konfiguration und Safety by Design

Die im Bericht der Bund-Länder-Kommission thematisierte Positivkennzeichnung kindgeeigneter Inhalte gibt es bereits in Form von Förderprogrammen, Gütesiegeln und Empfehlungsdiensten (z. B. Netz für Kinder, Blinde Kuh, Erfurter Netcode, Klick-Tipps). Mit FragFINN besteht eine große Sammlung unbedenklicher Websites. Die bestehenden Kennzeichen und Whitelists bleiben aber dem klassischen Web verhaftet, dessen Nutzung auch bei Kindern abnimmt. Ein weiteres Siegel für besonders kindgerechte Inhalte würde nur in Konkurrenz zu bestehenden Initiativen treten und den Schutz von Kindern im Internet nicht wesentlich verbessern.

Ziel einer Positivkennzeichnung sollte es vielmehr sein, Orientierung dort zu vermitteln, wo sie fehlt. Eltern mangelt es derzeit vor allem an Hilfestellung, welche Social-Web-Dienste und Kommunikations-Apps ihre Kinder gefahrlos nutzen bzw. wie sie die Risiken dort reduzieren können. Da beispielsweise IARC und andere Klassifizierungssysteme die Kommunikations- und Datenschutzrisiken von Spielen und Apps (bisher) nicht berücksichtigen, wäre eine Kennzeichnung für besonders für Kinder geeignete Diensten und Apps eine wichtige Unterstützung für Eltern.

Mit zunehmender Nutzung des Internets über Apps und der Kapselung von Inhalten in proprietären Systemen, die für Jugendschutzprogramme nicht mehr erreichbar sind, wächst die Bedeutung großer Dienste für den technischen Jugendschutz. Letztlich hängt das Schutzniveau für Kinder und Jugendliche im Internet davon ab, welche Anstrengungen wichtige Betreiber unternehmen. Es macht jedoch keinen Sinn, global Player wie Google, Facebook oder Microsoft bei der Entwicklung von Schutztechniken zu unterstützen. Sie verfügen über wesentlich umfangreichere Mittel und bessere Ressourcen (z. B. im Bereich der automatisierten Inhalteerkennung oder des Machine Learnings).

Ziel einer Positivkennzeichnung muss es sein, Unternehmen zu motivieren, Techniken, die bei ihnen bereits verfügbar sind, auch für den Jugendschutz einzusetzen (z. B. Whitelisting für Chrome, YouTube for Kids, Content-ID), Safety by Design bei der Produktentwicklung zu praktizieren und sichere Nutzungsoptionen (z. B. altersdifferenzierte Konfiguration) anzubieten und ihre Dienste im Sinne von Safety by Default für Kinder und Jugendliche sicher vorzukonfigurieren.

8.2 Priorisierung und Fokussierung auf aktuelle Bedarfe

Voraussetzung für zielgerichtete Aktivitäten zur Verbesserung des technischen Jugendschutzes ist die Kenntnis, welche Dienste Kinder und Jugendliche wie nutzen und welche technische Schutzmöglichkeiten zur Verfügung stehen. Eine regelmäßige Erhebung ist Voraussetzung für Schwerpunktsetzungen im Entwicklungsfonds und bei der Schaffung von Anreizen über Positivkennzeichen. Für die Ermittlung der Nutzungsschwerpunkte (JuSchG-Eckpunkte) und des fortgeschrittenen Stands der Technik (novellierter JMStV) ist die KJM zuständig.

8.2.1 Regelmäßige Erhebung der Telemediennutzung und des fortgeschrittenen Stands der Technik

Internet-Dienste und onlinefähige Geräten ändern sich so schnell wie ihre Nutzung durch Kinder und Jugendliche. Um sicherzustellen, dass technische Jugendschutzlösungen dort ansetzen, wo Kinder und Jugendliche sich im Internet bewegen, sollte ihre Telemediennutzung jährlich erhoben werden. Ziel wäre die Feststellung aktueller Trends (Art des Zugangs, genutzte Dienste) sowie konkreter, daraus resultierender Schutzbedarfe.

Die Techniken, die für Jugendschutzlösungen eingesetzt werden können, entwickeln sich gerade im Bereich des Machine Learnings sehr schnell weiter. Um auf aktuelle Bedarfe fokussieren und neue Verfahren einbeziehen zu können, muss der fortgeschrittene Stand der Stand der Filtertechnik und der sicheren Konfiguration von Diensten regelmäßig erhoben und mit den festgestellten Schutzbedarfen abgeglichen werden.

8.2.2 Priorisierung und Formulierung realistischer Ansprüche

Der Entwicklungsfonds sollte ursprünglich gemeinsam von Bund, Ländern und Unternehmen getragen werden und mit 1,5 Mio. Euro jährlich ausgestattet sein. Die aktuellen Überlegungen gehen davon aus, dass sich nur noch BMFSFJ und interessierte Landesmedienanstalten beteiligen. Voraussichtlich wird weniger als die Hälfte an Fördergelder zur Verfügung stehen. Umso wichtiger wird es sein, die verfügbaren Ressourcen an den Stellen einzusetzen, an denen der dringendste Handlungsbedarf besteht, und Aufgaben in Angriff zu nehmen, die mit Mitteln des Fonds realisierbar sind und möglichst große Schutzwirkung erzielen.

Für die Priorisierung wäre folgendes Raster zu empfehlen:

- Maßnahmen, die **den Schutz jüngerer Kinder** verbessern, da sie besonders schutzbedürftig sind und technische Schutzlösungen in dieser Altersgruppe einen besonderen Stellenwert einnehmen,[50]
- Maßnahmen, die **veränderte Nutzungsgewohnheiten** (Social Web, mobile Endgeräte) von Kindern und Jugendlichen sowie daraus entstehende Gefährdungsbereiche berücksichtigen und
- Maßnahmen, die die **Handhabbarkeit** des technischen Jugendschutzes für Eltern verbessern und als Proof-of-Concept für plattform- und geräteübergreifende Ansätze ausgelegt sind.

[50] Siehe dazu die Ergebnisse des Diskussionsprozesse im I-KiZ zum Intelligenten Risikomanagement (http://www.i-kiz.de/jahresbericht2015)

Zielesetzungen für den Entwicklungsfonds sollten so formuliert werden, dass sie auch in einem überschaubaren Zeitraum realisierbar sind. Daher gilt es, sich auf ausgewählte vielversprechende Konzepte zu konzentrieren, Entwicklungen zu beschleunigen (z. B. durch Aufgreifen von Konzepten von Plattformbetreibern oder anderer Länder) sowie verfügbare Mechanismen für den Jugendschutz nutzbar zu machen.

8.3 Entwicklungsfonds für technischen Jugendschutz

Unter Berücksichtigung der oben dargestellten Priorisierung sollten technische Entwicklungen angeregt und unterstützt werden, die die Sicherheit von Kindern erhöhen, zeitgemäße Filtertechniken fördern und die Benutzerfreundlichkeit des technischen Jugendschutzes für Eltern verbessern. Diese allgemeinen Entwicklungsziele sollten über einen vorgelagerten Ideenwettbewerb konkretisiert, ausgewählte Ideen über den Fonds umgesetzt werden.

8.3.1 Onlinesicherheit für Kinder in öffentlichen Netzen

Das Einstiegsalter bei der Internetnutzung sinkt und die Verfügbarkeit von Smartphones in Kinderhand nimmt weiter zu. Mithilfe technischer Schutzlösungen können Eltern ihre Kinder im Privathaushalt grundlegend vor beeinträchtigenden Inhalten und Übergriffen schützen. Öffentliche Einrichtungen wie (Grund-)Schulen und Bibliotheken sowie Betreiber von WLAN-Hotspots stehen vor dem Problem, wie sie Kindern einen sicheren Netzzugang ermöglichen können.

Für die Filterung auf Routern stellt insbesondere die zunehmende Verbreitung verschlüsselter Verbindungen eine technische Herausforderung dar. Zu entwickeln sind praxistaugliche Ideen für schulische, pädagogische und öffentliche Netzwerke, um Eltern die Möglichkeit zu geben, ihre Kinder auch im öffentlichen Raum vor Konfrontationen und Übergriffen im Internet zu schützen. Vorhandene Konzepte (z. B. KinderServer), Ressourcen (z. B. BPjM-Modul, JusProg-Blacklist, fragFINN-Whitelist) und technische Standards (Altersklassifizierungen) sollten in die Überlegungen einbezogen werden.

8.3.2 Browserbasierte Filterung beeinträchtigender Onlineinhalte

Browser bieten die Voraussetzungen für zeitgemäße Filterkonzepte. Sie sind die zentrale Schnittstelle zu klassischen Websites, geräte- und betriebssystemübergreifend verfügbar und für die Filterung nutzbar. Neben den Apps wichtiger Dienste des Social Web gehört eine Browser-App zum üblichen Instrumentarium von Kindern und Jugendlichen auf dem Smartphone. Schutzmechanismen im Browser greifen auch bei sicheren Verbindungen, da sie vor der Verschlüsselung von Seitenaufrufen oder nach der Entschlüsselung der abgerufenen Inhalte filtern können.

Zu entwickeln sind praxistaugliche Ideen, wie Browser für die Filterung (verschlüsselter) beeinträchtigender Inhalte besser genutzt werden können. Um Eltern eine einfache Aktivierung des Schutzes zu ermöglichen, sollten sich Filtermodule nahtlos in den Browser integrieren und mit wenig Aufwand zu betreiben sein (z. B. automatische Updates). Vorhandene Ressourcen (Black- und Whitelists, Altersklassifizierungen) und Schnittstellen (z. B. zu Jugendschutzoptionen in Betriebssystemen und Diensten) sollten genutzt werden.

8.3.3 Zentrale Aktivierung diensteübergreifender Schutzfunktionen

Kinder und Jugendliche sind vor allem mit Apps und in Kommunikationsdiensten online, deren Inhalte Jugendschutzprogramme nicht filtern können. Wirksamer Schutz vor Beeinträchtigungen und Belästigungen setzt Sicherungsmöglichkeiten in zentralen Diensten voraus, die von den Betreibern zur Verfügung gestellt werden. Sollen diese proprietären Schutzoptionen einzelner Dienste von Eltern einfach zu handhaben sein, müssen sie an zentraler Stelle aktiviert werden können. Da Nutzerinnen und Nutzer es gewohnt sind, Einstellungen in der Systemkonfiguration von Geräten vorzunehmen, eignet sich hierfür das jeweilige Betriebssystem.

Zu entwickeln sind praxistaugliche Konzepte, wie anwendungsübergreifende Aktivierung von Schutzoptionen über das Betriebssystem gestaltet werden kann und welche standardisierten Anforderungen an die Kommunikation zwischen Betriebssystem und Apps zu stellen sind. Um Eltern eine systemweite Konfiguration von Jugendschutzfunktionen zu bieten, müssen vorhandene Konzepte (z. B. Einschränkungen unter iOS, eingeschränkte Profile unter Android) Klassifizierungssysteme (z. B. IARC) und Schnittstellen zu Ressourcen (z. B. BPjM-Modul) berücksichtigt und Vorschläge zu deren Weiterentwicklung formuliert werden.

8.4 Positivkennzeichnung für sichere Angebote

Über eine Positivkennzeichnung könnten Eltern Orientierung bekommen, welche Dienste und Betriebssysteme für Kinder besonders geeignet sind, und Unternehmen motiviert werden, sichere Nutzungsmöglichkeiten für Kinder und Jugendliche anzubieten (Safety by Default) bzw. zu entwickeln (Safety by Design).

8.4.1 Positivkennzeichnung für Betriebssysteme

Betriebssysteme sind im Rahmen eines integrierten Schutzkonzepts der ideale Ort, um Jugendschutzoptionen zu konfigurieren und an installierte Apps weiterzugeben. Da systemweite Einstellungen in der Regel über das Betriebssystem vorgenommen werden, sind Schutzoptionen an dieser Stelle für Eltern am einfachsten zu handhaben. Best Practices sollten hervorgehoben und unterstützt werden.

Voraussetzungen für die Vergabe einer Positivkennzeichnung wären erfüllt, wenn

- eine Schnittstelle zur geräteweiten Konfiguration von Jugendschutzoptionen nach zuvor festgelegten Standards bereitgestellt wird,
- betriebssystemeigene Dienste und relevante Funktionen (z. B. App Stores, Medienspieler oder integrierte Kommunikationsanwendungen) eine sichere Konfigurationsmöglichkeiten bieten, die sich über die zentrale Verwaltung aktivieren lassen, und
- ggf. vorhandene Standards zur plattformneutralen Synchronisierung von Jugendschutzoptionen unterstützt werden.

Die bekanntesten Betriebssysteme verfügen bereits über Jugendschutzfunktionen und decken einen Teil der genannten Anforderungen ab. Um die Voraussetzungen für eine Positivkennzeichnung zu erfüllen, wären keine grundlegenden Neuentwicklungen seitens der Hersteller nötig. Dies wäre unrealistisch. Mit der Positivkennzeichnung könnten aber ggf. nötige Erweiterungen (z. B. Filterfunktion von integrierten Browsern) und Anpassungen (z. B. eine einheitliche, systemweite Alterseinstellung) angeregt und unterstützt werden.

8.4.2 Positivkennzeichnung für Dienste/Apps

Im Sinne eines übergreifenden Jugendschutzkonzepts werden Dienste benötigt, die Funktionen zur sicheren Konfiguration ihres Angebots zur Verfügung stellen, welche sich über Einstellmöglichkeiten im Betriebssystem aktivieren und verwalten lassen.

Die Voraussetzungen für die Vergabe einer Positivkennzeichnung für einen Dienst und die zugehörige App wären erfüllt, wenn

- eine altersdifferenzierte, in relevanten Gefährdungsbereichen wirksame, sichere Konfiguration bereitgestellt wird,
- die sichere Konfiguration über das Betriebssystem aktiviert werden kann.

Die meistgenutzten Dienste verfügen bereits über (rudimentäre) Funktionen, die sich für den Jugendschutz einsetzen lassen. Um die Voraussetzungen für eine Positivkennzeichnung zu erfüllen, wären keine kompletten Neuentwicklungen nötig. Mit dem Kennzeichen könnte aber signalisiert werden, welche Funktionen für besonders wichtig gehalten werden, und entsprechende Erweiterungen und Anpassungen angestoßen werden.

9 Literaturverzeichnis

http://www.age-label.de (17. Februar 2016).

Archer, Phil (2009): ICRAfail. A Lesson for the Future. http://philarcher.org/icra/ICRAfail.pdf.

Bitkom (2014): *Jung und vernetzt. Kinder und Jugendliche in der digitalen Gesellschaft.* Berlin: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V..

https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/ (12. Januar 2016).

http://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats (16. Februar 2016).

http://bluecoat.force.com/knowledgebase/articles/Solution/EnforceYoutubeSafetyMode (11. Januar 2016)

http://developer.android.com/about/versions/android-4.3.html#RestrictedProfiles (18. Februar 2016).

https://developer.android.com/guide/topics/security/permissions.html (18. Februar 2016).

https://developer.apple.com/library/tvos/documentation/TVMLJS/Reference/TVJSRestrictions_Ref/index.html (18. Februar 2016).

https://developers.google.com/image-search/v1/jsondevguide (13. Januar 2016).

DIVSI (2015): *DIVSI u9-Studie. Kinder in der digitalen Welt.* Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet.

Dreyer, Stephan / Hajok, Daniel / Lampert, Claudia (2012): *Jugendschutzsoftware im Elternhaus – Kenntnisse, Erwartungen und Nutzung. Stand der Forschung.* Hamburg: Verlag Hans-Bredow-Institut.

van Eimeren, Birgit & Frees, Beate (2014): *Ergebnisse der ARD/ZDF-Onlinestudie 2014.* In: Media Perspektiven, 7-8/2014, S. 378-396.

https://www.facebook.com/help/376841469095893 (2. Februar 2016).

Fraunhofer-Institut für intelligente Analyse- und Informationssysteme IAIS (2013): *Studie zum technischen Jugendmedienschutz: Möglichkeiten und Grenzen von Verfahren zur Detektion Jugendschutzrelevanter Web-Inhalte.* Sankt Augustin. http://www.iais.fraunhofer.de/fileadmin/user_upload/Abteilungen/NM/pdfs/Fraunhofer_Jugendmedienschutz_2013-02-25.pdf.

https://www.globalratings.com (17. Februar 2016).

http://www.heise.de/ix/artikel/Oder-so-aehnlich-1765809.html (19. Mai 2016).

http://www.heise.de/newsticker/meldung/Facebook-verschaerft-den-Messenger-Zwang-3227140.html (6. Juni 2016).

I-KiZ (2016): *Jahresbericht.* http://www.i-kiz.de/wp-content/uploads/2015_I-KiZ_Jahresbericht.pdf (20. April 2016).

jugendschutz.net (2014): *Bericht zum neunten Test von Jugendschutzfiltern.* Mainz.

Jurran, Nico & Hansen, Sven (2016): *Video total. Flatrate statt Fernsehen.* In: c't 2016/4, S. 103-117.

KJM (2011): *Kriterien der KJM für die Anerkennung von Jugendschutzprogrammen im Bereich des World Wide Web.* http://www.kjm-online.de/fileadmin/Download_KJM/Rundfunk/Informationen-fr-JSP-Anbieter_Stand_2011-05-11.pdf (27. Januar 2016).

Knab, Sonja (2014): *Smart-TV Effects 2014-II.* http://www.burda-forward.de/uploads/tx_mjstudien/ForwardAdGroup_SmartTVEffects_2014-1.pdf?PHPSESSID=59b87dc1a35b96a3fd7b580f706c7cbd (14. Januar 2016).

https://letsencrypt.org (16. Februar 2016).

Medienpädagogischer Forschungsverbund Südwest. 2015. *JIM-Studie 2015.* *http://www.mpfs.de/fileadmin/JIM-pdf15/JIM_2015.pdf* (14. Januar 2016).

Medienpädagogischer Forschungsverbund Südwest. 2014. *KIM-Studie 2014.* *http://www.mpfs.de/fileadmin/KIM-pdf14/KIM14.pdf* (14. Januar 2016).

http://www.miracle-label.eu (17. Februar 2016).

https://msdn.microsoft.com/en-us/library/windows/desktop/ms711654%28v=vs.85%29.aspx (18. Februar 2016).

https://play.google.com/store/apps/collection/promotion_3000e24_androidtv_games_all?hl=de (19. Februar 2016).

http://www.samsung.com/de/consumer/tv-av/audio-video/blu-ray-dvd-player/BD-H5500/EN (15. Februar 2016).

http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/attachment/percent-time-spent-on-mobile-apps-2016/ (9. Februar 2016).

https://support.google.com/plus/answer/6020454?hl=de (9. Februar 2016).

https://www.tensorflow.org/ (10. Februar 2016).

https://www.youtube.com (15. Februar 2016).

https://www.youtube.com/yt/press/de/statistics.html (16. Februar 2016).