2019 BERICHT

Technischer Jugend-medienschutz

Zeitgemäße Entwicklung und
zukunftsfähiges Schutzkonzept

JUGENDSCHUTZ.NET

IMPRESSUM

Kontakt
jugendschutz.net
Wallstraße 11, 55122 Mainz
Tel.: 06131 3285-20
Fax: 06131 3285-22
buero@jugendschutz.net
www.jugendschutz.net

Autoren
Mark Bootz, Andreas Marx

Verantwortlich
Stefan Glaser

Grafische Gestaltung
elements of art

Druck
Heinrich Fischer - Rheinische Druckerei GmbH

Stand
Juni 2019

jugendschutz.net arbeitet mit gesetzlichem Auftrag und ist das gemeinsame Kompetenzzentrum von Bund und Ländern für den Schutz von Kindern und Jugendlichen im Internet.

Bundesministerium für Familie, Senioren, Frauen und Jugend

kjm Kommission für Jugendmedienschutz
die medienanstalten

Gefördert vom
Bundesministerium für Familie, Senioren, Frauen und Jugend

im Rahmen des Bundesprogramms
Demokratie leben!

GUTES AUFWACHSEN MIT MEDIEN

MKFS Medienkompetenz Forum Südwest
STIFTUNG

Sehr geehrte Leserinnen und Leser,

eine zunehmend digitalisierte Umwelt hat großen Einfluss auf die Mediennutzung von Kindern und Jugendlichen. Smartphones und Tablets sind auch unter Kindern weit verbreitet und die mobile Nutzung von Internetangeboten ohne elterliche Aufsicht ist zu einer Selbstverständlichkeit geworden. Dabei sind vor allem Social-Media-Dienste globaler Anbieter besonders beliebt.

Der Lagebericht von jugendschutz.net zeigt jedoch, dass die derzeitigen technischen Jugendschutzlösungen nicht zufriedenstellend funktionieren. Gerade im Bereich des Social Web und für mobile Anwendungen fehlen moderne, altersdifferenzierte Filtersysteme, die vor allem jüngere Kinder vor beeinträchtigenden oder gefährdenden Inhalten, vor Interaktionsrisiken oder Kostenfallen schützen. Veraltete Erkennungsverfahren in den aktuellen Jugendschutzprogrammen führen bei Social-Media-Angeboten vielmehr zu einem massiven Overblocking. Dieser Ausschluss der Kinder steht ihrem Recht entgegen, altersgerecht am Leben im digitalen Raum teilnehmen zu können, und ist somit keine akzeptable Lösung.

Es liegt in der Verantwortung der Anbieter, eine sichere Umgebung für Kinder und Jugendliche zu schaffen und Schutzoptionen bereits in die Konzeption ihrer Angebote zu integrieren. Zeitgemäße Ansätze wie das Hash-Verfahren werden längst erfolgreich eingesetzt, um die Verbreitung von Missbrauchsdarstellungen oder Urheberrechtsverletzungen zu verhindern. Diese und weitere Ansätze, auch aus dem Bereich der künstlichen Intelligenz, sollten Anbieter ebenso für den Jugendschutz nutzen und zukunftsfähige technische Lösungen entwickeln.

jugendschutz.net entwirft in diesem Bericht ein Modell eines modernen Schutzkonzeptes und leistet damit einen weiteren wichtigen Diskursbeitrag zum Thema technischer Jugendmedienschutz. Dafür gilt ihnen mein Dank.

Dr. Wolfgang Kreißig
Vorsitzender der Kommission für Jugendmedienschutz (KJM)

KINDER UND JUGENDLICHE ONLINE

Zur Entwicklung eines zeitgemäßen technischen Jugendmedienschutzes ist der Blick auf das Nutzungsverhalten junger Userinnen und User und der Blick auf die derzeitigen Risiken wichtig. Jugendliche und zunehmend auch Kinder nutzen mobil die großen Social-Media-Dienste, die von globalen Anbietern betrieben werden. Diese Angebote wurden nicht für Minderjährige entwickelt. Sie werden hauptsächlich von Erwachsenen genutzt. Deswegen sind dort viele beeinträchtigende und gefährdende Inhalte zu finden.

Zu den Konfrontationen mit Gewalt, Pornografie und Extremismus sind Mobbing, sexuelle Belästigung und Grooming getreten. Auch Kostenfallen in Spiele-Apps und ungewollte Weitergabe von persönlichen Daten sind Risiken.

Bei herkömmlichen Webseiten können Kinder und Jugendliche durch die Blockade kompletter Domains vor ungeeigneten Inhalten geschützt werden. Social-Media-Dienste bieten dagegen vielfältige Inhaltsformen: Texte, Bilder und Videos, die zudem von Userinnen und Usern eingestellt werden. Die Masse, Vielfalt und Flüchtigkeit stellen den technischen Jugendschutz vor enorme Herausforderungen.

Nutzung: Kinder zunehmend mobil in Social Media unterwegs

Mit 97 % besaßen laut JIM-Studie 2018 praktisch alle 12- bis 19-Jährigen ein Smartphone. Es ist für sie weiterhin das am häufigsten eingesetzte Gerät zur Internetnutzung. Der klassische Desktop-Computer spielt mit 8 % Nutzung kaum noch eine Rolle.

Während Kinder noch speziell für sie konzipierte Seiten mit geeigneten Inhalten nutzen (KIM-Studie 2016), sind Jugendliche vor allem YouTube, WhatsApp, Instagram, Netflix, Snapchat und Facebook wichtig. Sowohl Kinder als auch Jugendliche suchen mit Google nach Informationen.

75 % der 10- bis 13-Jährigen (20 % der 6- bis 9-Jährigen) nutzen Messenger wie WhatsApp. Immerhin rund ein Drittel der 10-Jährigen kommuniziert auf Facebook. Jeweils rund 20 % nutzen Instagram und Snapchat. Diese Dienste dürfen laut AGB erst ab 13 Jahren genutzt werden, WhatsApp sogar erst ab 16 Jahren.

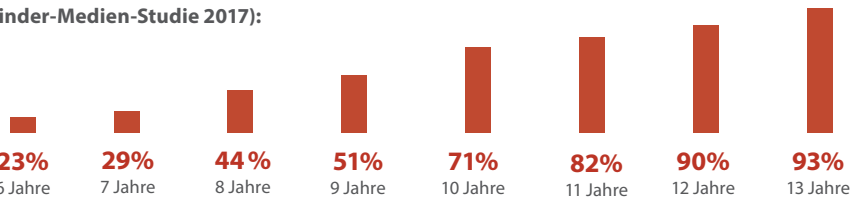
Risiken: Belästigung, Mobbing und Grooming durch Interaktion

Die signifikantesten Risiken sind Cybermobbing und die Begegnung mit Hassbotschaften. Jeder fünfte Jugendliche (19 %) gab 2018 an, dass falsche oder beleidigende Inhalte über seine Person online verbreitet wurden (2017: 20 %). Zwei Drittel der 12- bis 19-Jährigen waren laut JIM-Studie 2018 schon einmal mit Hasskommentaren in Social Media konfrontiert.

Die Drastik der Konfrontation mit beeinträchtigenden Inhalten hat sich durch die Dynamik der interaktiven Dienste und fehlende redaktionelle Betreuung verschärft. Die überraschende Übermittlung drastischer Inhalte kann Heranwachsende ängstigen und verstören.

Voreingestellte Autoplay-Funktionen verstärken negative Wirkungen, indem Gewaltvideos direkt abgespielt und weitere drastische Inhalte vorgeschlagen werden. Auch können Kinder und Jugendliche durch sozialen Druck bei so genannten Challenges zu gefährlichem Verhalten verleitet werden.

So viele Kinder haben ein eigenes Smartphone (Kinder-Medien-Studie 2017):



Fortschrittliche Techniken und verschlüsselter Datenverkehr nehmen zu

Dienste, Inhalte und Geräte im Netz sind heute nicht mehr isoliert voneinander zu betrachten. Nutzerinnen und Nutzer können praktisch auf jeder Plattform Bilder und Videos anschauen. Sie können sich mit anderen vernetzen, informieren und per Messenger von unterwegs oder zuhause kommunizieren.

Aktuelle Geräte vereinfachen den Zugang und die Interaktion im Netz, z. B. durch den Einsatz fortschrittlicher Techniken wie Spracherkennung. Selbst in Kinderzimmern boomt das „Internet der Dinge". Bis 2022 soll sich der weltweite Umsatz von vernetzten und internetfähigen Spielzeugen (Smart Toys) auf mehr als zehn Milliarden Euro verdreifachen. Die Zahl der weltweiten Nutzerinnen und Nutzer digitaler Assistenten soll 2019 auf fast 1,5 Milliarden steigen. Deutschland wird als fünftgrößter Markt prognostiziert.[1]

Früher wurden verschlüsselte Verbindungen nur für besonders sicherheitsrelevante Anwendungen wie Onlinebanking oder E-Mail-Portale genutzt. Heute findet der überwiegende Teil des Internetverkehrs verschlüsselt statt. 88 % der mit Google Chrome aufgerufenen Seiten sind HTTPS-Aufrufe, 2015 waren es nur 33 %.[2] Chrome ist mit einem Marktanteil von aktuell 69 % der mit Abstand am häufigsten genutzte Browser.[3]

Durch die Verschlüsselung des Datenverkehrs zwischen Webseite und Browser oder Apps können die Daten von Dritten nicht mitgelesen werden. Verschlüsselte Verbindungen stellen aber eine Herausforderung für Filtersysteme dar: Auf dem Übertragungsweg ist nur die aufgerufene Domain (z. B. www.jugendschutz.net) im Klartext auslesbar. Die Adresse von Unterseiten (z. B. www.jugendschutz.net/impressum/) ist nicht offen sichtbar.

1 bvdw.org/themen/studien/, gfu.de/insights-trends/praesentationen/

2 transparencyreport.google.com/https/overview

3 de.statista.com/statistik/daten/studie/157944/umfrage/marktanteile-der-browser-bei-der-internetnutzung-weltweit-seit-2009/

DER ZEITIGE FILTER TECHNIK

Jugendschutzprogramme wurden ursprünglich zur Filterung klassischer statischer Webseiten entwickelt. Diese Ansätze eignen sich nicht mehr zur differenzierten Filterung von Social-Media-Angeboten. Weder listenbasierte Filterung noch das derzeitige Prinzip der Altersklassifikation haben zu befriedigenden Jugendschutzlösungen geführt.

Bei der Filterung von Inhalten im Netz kommen verschiedene Techniken zum Einsatz. Dabei soll eine Kombination mehrerer Ansätze möglichst hohe Trefferquoten erzielen. Moderne Verfahren der automatischen Inhaltserkennung unterscheiden sich grundlegend von einfachen Keyword-Filtern und anderen Ansätzen mit starren Vordefinitionen. Durch Techniken des maschinellen Lernens werden schnell große Mengen von Daten klassifiziert.

Auf der Basis von „lernenden Algorithmen" können hohe Trefferquoten erreicht werden. Sie genügen den Anforderungen der meisten Anwendungsbereiche. Existierende Techniken, wie sie z. B. beim Urheberschutz bereits genutzt werden, werden aber noch nicht gewinnbringend auch für den Jugendmedienschutz eingesetzt.

Altersklassifizierung: Kein übergreifender Standard, zu geringe Verbreitung

Technisch einfach werden Angebote mit einem so genannten Alterslabel gefiltert. Sie lassen sich für die Einstufung einzelner Inhalte in Social Media und für komplette Webseiten nutzen. Der Anbieter ordnet eine vorgegebene Altersstufe zu und hinterlegt eine maschinenlesbare Altersinformation. Beim Aufruf einer Seite gleicht ein Jugendschutzprogramm das eingestellte Alter mit der auf der Webseite hinterlegten Altersinformation ab und entscheidet, ob die Seite angezeigt werden soll.

Ein gängiger Klassifizierungsstandard ist age-de. Das hinterlegte age-de-Label enthält Altersinformationen zur Gesamtseite und ggf. weiteren Unterseiten. Schwachpunkt des Systems: Das Alters-Labeling der Anbieter kann falsch sein, da die komplexe Alterseinstufung in der Regel von Laien durchgeführt wird.

Das Prinzip der Altersklassifikation entfaltet nur dann Wirkung, wenn die Kennzeichnung und das auslesende Programm weit verbreitet sind. age-de wird aber in der Regel nur auf deutschen Angeboten genutzt und selbst dort ist die Verbreitung gering. 2014 waren noch nicht einmal 1 % der meistbesuchten Webseiten gelabelt. Von den 100.000 meistbesuchten Seiten des Alexa-Rankings waren lediglich 172 mit age-de gekennzeichnet.

In den Diensten, die Kinder und Jugendliche am häufigsten besuchen, wird der age-de-Standard derzeit nicht oder nur unzureichend angewendet und entfaltet somit kaum eine Schutzwirkung.

Das Jugendschutzprogramm JusProg, das den age-de-Standard ausliest, nutzen nur wenige Eltern. Laut KIM-Studie 2016 verwendeten nur 21% der befragten Eltern überhaupt ein Jugendschutzprogramm; da hier unterschiedliche Programme angegeben werden, ist der Nutzungsanteil von JusProg vermutlich noch niedriger.

Black-/Whitelists: Durch Masse an Inhalten kaum aktuell zu halten

Die listenbasierte Filterung erfolgt in der Regel über URLs. Die Listen werden entweder redaktionell oder automatisiert generiert. Aufgrund der Datenmengen sind redaktionelle Sichtungen allerdings nur für Whitelists (Liste kindgeeigneter Inhalte) sinnvoll umsetzbar. Auch besondere Blacklists werden redaktionell bearbeitet, so enthält das BPjM-Modul der Bundesprüfstelle für jugendgefährdende Medien indizierte URLs.

Für jüngere Kinder eignet sich vor allem eine Whitelist. Sie lässt nur Webadressen zu, deren Inhalte für eine bestimmte Altersgruppe geeignet sind. Bei älteren Kindern und Jugendlichen können Blacklists eingesetzt werden, die bekannte, dem Alter unangemessene Inhalte blockieren.

Insbesondere bei „User generated Content" in Social Media stoßen Filterlisten schnell an ihre Grenzen: redaktionell können die Listen durch den rasanten Upload von neuen Inhalten nicht aktualisiert werden. Auf Instagram werden täglich ca. 95 Millionen Fotos hochgeladen[4], YouTube wächst jede Minute um weitere 400 Stunden Videomaterial.[5] Facebook erzeugt jeden Tag 4 Petabytes neuer Daten.[6] Das entspricht 4000 handelsüblichen Festplatten.

4 wired.co.uk/article/instagram-doubles-to-half-billion-users

5 brandwatch.com/blog/youtube-stats/

6 brandwatch.com/blog/facebook-statistics/

Hash-Werte: Zuverlässiges Erkennen von Dateien per digitalem Fingerabdruck

Hash-Verfahren erkennen Dateien (z. B. Bilder oder Videos) eindeutig wieder. Dazu wird aus der Datei ein Wert errechnet, der diese eindeutig identifiziert, dabei aber nichts über deren Inhalt aussagt. Auch ein „Zurückrechnen" des Hashs in den ursprünglichen Inhalt ist nicht möglich. Ein Hash-Wert ist somit vergleichbar mit einem Fingerabdruck.

Wie bei einer URL-Listenfilterung können Listen mit Hash-Werten von bekannten, gefährdenden Inhalte angelegt werden, um diese bei Aufruf zu erkennen und zu blockieren. Hash-Werte eignen sich durch ihre geringe Größe dazu, Daten schnell in einer großen Liste von Einträgen wiederzufinden.

Hash-Verfahren kommen in vielen Bereichen zum Einsatz. Ein weit verbreitetes Verfahren ist „PhotoDNA" von Microsoft. Google, Microsoft, Twitter und Facebook setzen es gegen die Verbreitung von Missbrauchsdarstellungen ein.

Keywords: Zur Erkennung von feststehenden Begriffen geeignet

Seit Beginn der Computertechnik werden Verfahren eingesetzt, um Muster automatisch zu erkennen. Sie verarbeiten eingehende Daten und ordnen sie Kategorien zu. Mit der fortschreitenden Verbreitung des Internets in den 1990er Jahren entstanden keywordbasierte Systeme zur automatischen Einordnung und Katalogisierung von Webseitentexten. Sie kamen auch in frühen Jugendschutzfiltern zum Einsatz. Allerdings mit vergleichsweise ungenauen Ergebnissen und merklichen Verzögerungen beim Seitenaufbau.

Auch aktuelle Jugendschutzfilter setzen einfache Texterkennungsmechanismen auf Basis von Schlüsselwörtern ein, um Blacklists automatisch zu befüllen oder Echtzeitfilterung umzusetzen.

Nicht zwangsläufig machen bestimmte Begriffe eine Webseite für Kinder und Jugendliche ungeeignet. Beispielsweise können Begriffe, die auf einen rechtsextremen oder sexuellen Kontext hindeuten, auch im Rahmen eines Lexikonartikels oder einer Aufklärungsseite enthalten sein.

Deswegen kann es bei einfachen Keyword-Verfahren zu hohem Over- und Underblocking kommen. Für eine automatische Erkennung von Mediendateien (z. B. Bilder oder Videos) eignen sich keywordbasierte Verfahren nicht.

Maschinelles Lernen: Schnell und zuverlässig große Datenmengen klassifizieren

Moderne Verfahren der automatischen Inhaltserkennung unterscheiden sich grundlegend von einfachen Keyword-Filtern und anderen Ansätzen mit starren Vordefinitionen. Sie nutzen Techniken des maschinellen Lernens (KI - künstliche Intelligenz), um schnell große Mengen von Daten zu klassifizieren.

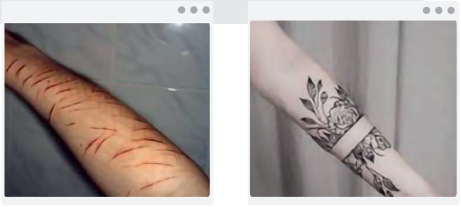
Geeignet sind KI-Verfahren derzeit für Bilder und Textinhalte. Sie werden bereits in vielfältigen Bereichen eingesetzt (z. B. Google Bildersuche). Ebenso existieren Verfahren zur automatischen Erkennung von Videoinhalten.[7]

„Lernende Algorithmen" erkennen anhand einer Menge an Beispielmaterial Gemeinsamkeiten und übertragen diese auf unbekanntes Material. Dadurch kann die Technik z. B. Objekte, Tiere und Personen auf Bildern erkennen. Ausschlaggebend für eine hohe Trefferquote sind das verwendete Trainingsmaterial und die Wahl des passenden Lernalgorithmus.

Im Gegensatz zu herkömmlichen Methoden der automatisierten Inhaltserkennung (z. B. Keywords bei Text oder starre, regelbasierte Erkennung bei Bildern) werden mit modernen Techniken hohe Trefferquoten erzielt. Sie genügen den Anforderungen der meisten Anwendungsbereiche.

7 z. B. cloud.google.com/video-intelligence/

DERZEITIGE FILTERTECHNIK



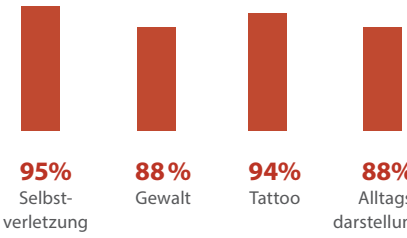
Selbstverletzungen und Tattoos lassen sich trotz Ähnlichkeit zuverlässig automatisch erkennen.
(Quelle: YouTube/Pinterest; Original unverpixelt)

jugendschutz.net prüfte 2017 und 2018 die automatische Erkennung von jugendschutzrelevanten Inhalten mithilfe moderner Techniken des maschinellen Lernens.[8] Getestet wurde ein bereits trainiertes, voll einsatzbereites System (Google Cloud Vision) und Programme, die das Training eines Erkennungsmechanismus ermöglichen (Facebook fastText und Google TensorFlow).

Dabei wurden Erkennungsquoten erreicht, die die Wirksamkeit gängiger Jugendschutzprogramme (ca. 80 % Trefferquote) mit vergleichsweise geringem Aufwand erreichen und zum Teil sogar übertreffen.

Zwar funktioniert kein automatisches Verfahren zu 100 % zuverlässig, dennoch ist die Erkennung durch künstliche Intelligenz den klassischen Filteransätzen in vielen Bereichen signifikant überlegen.

Früher benötigte das Training von KI-Modellen extrem hohe Rechenleistungen. Zum Teil waren Großrechner Tage oder sogar Wochen damit ausgelastet. Aufgrund der Weiterentwicklung der Hardware sowie der eingesetzten Algorithmen ist der Ressourcenbedarf heute deutlich geringer. Selbst auf handelsüblichen PCs lassen sich inzwischen Anwendungen ohne Probleme trainieren.



Automatische Bildererkennung (TensorFlow/Inception-v3): hohe Trefferquoten in allen Bildkategorien.
(Quelle: jugendschutz.net)

Beim eigentlichen Einsatz der Erkennungstechnik sind die Anforderungen relativ gering. Verfahren, die besonders auf leistungsschwache Hardware ausgelegt sind, ermöglichen heute die Erkennung von Bildern oder Textinhalten selbst auf mobilen Endgeräten in Sekundenbruchteilen und damit in Echtzeit.

Google CloudVision identifiziert zuverlässig Darstellungen wie Selbstverletzungen. (Quelle des getesteten Fotos unbekannt)

Künstliche Intelligenz (KI) / Maschinelles Lernen

Künstliche Intelligenz (KI) ist ein Teilgebiet der Informatik. Es befasst sich mit der Automatisierung intelligenten Verhaltens. Häufig wird auch der Begriff Maschinelles Lernen verwendet.

Maschinelles Lernen bezeichnet Systeme, die anhand von Beispielen Muster lernen und nach der Lernphase verallgemeinerte Entscheidungen erzeugen (z. B. das Erkennen von Objekten auf Bildern).

Insbesondere in Social Media fallen täglich gigantische Datenmengen an. Diese Daten sind das Kapital der Unternehmen. Für personalisierte Werbemaßnahmen setzen Dienste schon seit geraumer Zeit Machine-Learning-Verfahren ein. Aber auch in vielen anderen Bereichen wird KI unser Arbeits- und Privatleben nachhaltig verändern.

Heute kommt künstliche Intelligenz in vielfältiger Form zum Einsatz. Beispielsweise bei Navigation, Online-Einkauf, Ordnung von Foto-Alben und persönlichen Assistenten. Die größten Unternehmen investierten 2016 etwa 30 Milliarden US-Dollar in die Entwicklung künstlicher Intelligenz. Es sind jedoch auch kostenlose Programmbibliotheken verfügbar.

8 Testberichte jugendschutz.net zu fastText, Google Vision und Tensor Flow

DER ZEITIGE JUGENDSCHUTZ LÖSUNGEN

In der komplexen Welt des sich rasant entwickelnden Internets braucht effektiver Kinder- und Jugendmedienschutz eine Kombination von Maßnahmen: Neben regulatorischen und erzieherischen Elementen ist der technische Schutz wichtig. Der Jugendmedienschutz-Staatsvertrag sieht hierfür das Instrument der Jugendschutzprogramme vor.

Wirkung entfalten und verlässlich schützen können technische Schutzlösungen nur dann, wenn sie bei den beliebten Diensten und gängigen Geräten ansetzen und sämtliche Risiken berücksichtigen, die sich aus der Interaktion ergeben. Aktuelle Jugendschutzprogramme haben hier erhebliche Defizite.

Weder gibt es ein überzeugendes Konzept zur Klassifizierung von Inhalten, noch konnten sich die verfügbaren Programme bei Eltern durchsetzen. „Teillösungen für geschlossene Systeme", wie sie derzeit angeboten werden, können auf Dauer kein übergreifendes, umfassendes System ersetzen.

Eigenständige Jugendschutzfilter: Veraltete Erkennung auf Basis von Listen

Eigenständige Filtersysteme existieren als installierbare Programme und vor allem für den PC. Seltener eingesetzt werden Geräte wie Router (z. B. über die FritzBox und das integrierte BPjM-Modul).

Verfügbare Filterprogramme arbeiten in der Regel listenbasiert. Dieses veraltete Erkennungsverfahren arbeitet vergleichsweise unpräzise und führt zu Over- bzw Underblocking. Angebote des Social Web nutzen fast ausschließlich HTTPS-Verbindungen. Gängige Jugendschutzprogramme können damit in der Regel nicht umgehen. Sie sind beispielsweise nicht dazu in der Lage, auf Ebene von Profilen oder Videos zu filtern und dabei lediglich unerwünschte Inhalte auszublenden. Auch dies führt zu einem enormen Overblocking.

Proprietärer Schutz: Wirkung auf einzelne Dienste beschränkt

Der Gesetzgeber hat so genannte „Teillösungen für geschlossene Systeme" als anerkennungsfähige Jugendschutzprogramme vorgesehen. Sie können auch dort Wirkung entfalten, wo klassische Jugendschutzprogramme keinen Zugriff haben.

Als Teillösung anerkannt sind derzeit die Jugendschutzfunktionen der Nintendo Switch und des Streaming-Dienstes Netflix. Diese gewährleisten einen Schutz innerhalb des jeweiligen Dienstes oder Geräts. Bei Netflix ist der Schutz an das Nutzerkonto gebunden. Dadurch ist ein geräteübergreifender Schutz gegeben.

Proprietäre Schutzoptionen wirken sich lediglich auf den jeweils genutzten Dienst oder das betreffende Gerät aus. Beispiele hierfür sind: die SafeSearch-Funktion von Google und Privatsphäreeinstellungen in sozialen Netzwerken wie Facebook, die eine Kontaktaufnahme durch Fremde verhindert.

Auch auf Konsolen oder in Streaming-Diensten können Eltern Einstellungen vornehmen, um Kinder vor Inhalten (z. B. Spiele oder Filme) oder Interaktionsrisiken (z. B. Mobbing und Belästigung) zu schützen. Zum Teil wird bei den Diensten bereits künstliche Intelligenz zur Erkennung jugendschutzrelevanter Inhalte eingesetzt (z. B. Google SafeSearch).

Alterseinstufungen: Noch unbefriedigend

In Streaming-Diensten (z. B. Netflix) und App-Stores (z. B. Google Play) sind Alterskennzeichnungen weit verbreitet. Die Abdeckung der Labels ist hier häufig flächendeckend, da auf bereits vorhandene Alterseinstufungen (z. B. FSK oder USK) zurückgegriffen wird. Google nutzt in seinem Play-Store IARC zur Klassifizierung von Apps. IARC ermöglicht App-Anbietern, mithilfe eines Fragenkatalogs automatisch zu einer passenden Alterseinstufung zu kommen, die in unterschiedliche nationale Wertungen übersetzt werden kann.

Der IARC-Fragebogen berücksichtigt jedoch nur klassische Gefahren wie die Konfrontation mit Gewalt und Pornografie. Risiken, die durch Kommunikationsfeatures wie Mobbing und Belästigung entstehen können, werden nicht in die Bewertung einbezogen. Das gilt auch für Kostenfallen durch In-App-Käufe und ungeeignete Werbung.

Betreiber wie Google setzen bereits Hash-Verfahren (z. B. PhotoDNA) ein, um beispielsweise Inhalte mit Bezug zu Terrorismus und sexuelle Missbrauchsdarstellungen zu erkennen und deren Upload zu verhindern. Auch zur Erkennung von Urheberrechtsverletzungen sind entsprechende Techniken im Einsatz.

Google SafeSearch

Google ermöglicht das Aktivieren einer sicheren Suche, um Ergebnisse der Bildersuche auszublenden. Google setzt zur Erkennung der Inhalte die Technik ein, die von jugendschutz.net getestet wurde (Google Cloud Vision). Die Erkennung beschränkt sich auf wenige Kategorien, vor allem auf Pornografie und Gewalt.

ZUKUNFTSFÄHIGES SCHUTZKONZEPT

Die Herausforderungen für Systeme des technischen Jugendschutzmedienschutzes sind groß. Sie müssen alle Interaktionsrisiken berücksichtigen. Sie müssen mit verschlüsselter Übertragung umgehen. Und sie müssen Inhalte in Echtzeit filtern können. Es existieren inzwischen moderne Techniken, deren Potenziale für den Schutz von Kindern und Jugendlichen nutzbar gemacht werden müssen.

Es müssen Systeme eingesetzt werden, die dem allgemeinen technischen Stand entsprechen und dadurch das Schutzpotenzial maximal ausschöpfen. Um Schutz und Teilhabe junger Userinnen und User zu gewährleisten, braucht es altersdifferenzierte Systeme. Sie müssen leicht verfügbar und unkompliziert nutzbar sein, damit sie tatsächlich Wirksamkeit entfalten können.

Eine grundlegende Verantwortung liegt bei den großen Anbietern von Web-Diensten. Bei der Entwicklung von Soft- und Hardware müssen sie Jugendschutzfragen systematisch berücksichtigen (Safety by Design).

Integrierter Schutz durch Safety by Design

Inhalte werden in großen Mengen auf Social-Media-Dienste hochgeladen und dynamisch an andere Nutzer ausgespielt. Dabei werden Apps auf unterschiedlichen Geräten genutzt und Inhalte in andere Dienste eingebunden.

Eigenständige Jugendschutzlösungen, die lediglich klassische Webseiten mithilfe von (teils veralteten) Verfahren zur Inhaltserkennung filtern, können in diesem Szenario keinen umfassenden Schutz mehr entfalten.

Zukünftige Systeme sollten in Social-Media-Dienste integriert sein (Safety by Design), um Kinder und Jugendliche dort zu schützen, wo sie sich im Netz bewegen. Auch die Regulierung der Kommunikation und Interaktion zwischen Nutzerinnen und Nutzern und der technische Schutz vor daraus entstehenden Risiken kann nur durch die Dienste selbst erfolgen.

Um ungeeignete Inhalte auszublenden, sollten Social-Media-Dienste verschiedene Ansätze kombinieren. Automatisierte Inhaltserkennung und Listen mit Hash-Werten bereits bekannter problematischer Inhalte können genutzt werden, um diese zu filtern. Auch redaktionelle und nutzerseitige Alterseinstufungen eignen sich hier.

Altersdifferenzierter Ansatz für Schutz und Teilhabe

Die heutigen Herausforderungen für den technischen Jugendmedienschutz sind nicht neu. Kinder und Jugendliche nutzen das Internet heute nicht mehr nur passiv, indem sie Inhalte und Informationen konsumieren. Sie treten mit anderen in Kontakt. Ihre Daten werden dabei von den Betreibern der Dienste in großem Umfang erhoben.

Ein zukunftsfähiges Schutzkonzept muss Kinder und Jugendliche schützen und ihnen gleichzeitig eine unbeschwerte digitale Teilhabe ermöglichen. Zwar schützt das Blockieren kompletter Dienste und Sperrung ganzer Domains, wie es bei aktuellen Jugendschutzprogrammen geschieht, vor der Konfrontation mit ungeeigneten Inhalten. Es versperrt Kindern und Jugendlichen dadurch allerdings auch den Zugang zu geeigneten Inhalten auf demselben Dienst. Sie haben aber ein Recht auf Teilhabe.

Technischer Jugendmedienschutz muss altersangemessen konzipiert werden, um unterschiedlichen Ansprüchen zu genügen.

Kinder brauchen ein besonders hohes Maß an Schutz, zum Beispiel durch einen sicheren Surfraum. Mit zunehmendem Alter wird mehr Freiraum wichtig, um altersangemessene Erfahrungen zu ermöglichen und Kompetenzen zum Selbstschutz zu entwickeln. Ein modernes technisches Jugendschutzkonzept sollte daher vor allem auf den Schutz jüngerer Kinder ausgerichtet sein.

Einfache und flächendeckende Klassifizierung von Inhalten

Der Klassifizierung kommt in einem modernen System des technischen Jugendmedienschutzes eine wichtige Bedeutung zu. Hierüber werden inhaltsbezogene Informationen darüber bereitgestellt, ob ein bestimmtes Angebot für eine bestimmte Altersstufe geeignet ist oder nicht. Sie macht jedoch nur dann Sinn, wenn sie möglichst flächendeckend auch in den beliebten Social-Media-Diensten greift.

Um dies zu gewährleisten, könnten Anbieter eine Klassifizierung ermöglichen, die vom Nutzer/Nutzerin beim Upload des Inhalts erfolgt. Auf Basis dieser Klassifizierung können Filter geeignete Inhalte freischalten und ungeeignete Inhalte blockieren. Eine solche userseitige Klassifizierung funktioniert dann, wenn sie zum Standard entwickelt und niedrigschwellig gestaltet wird.

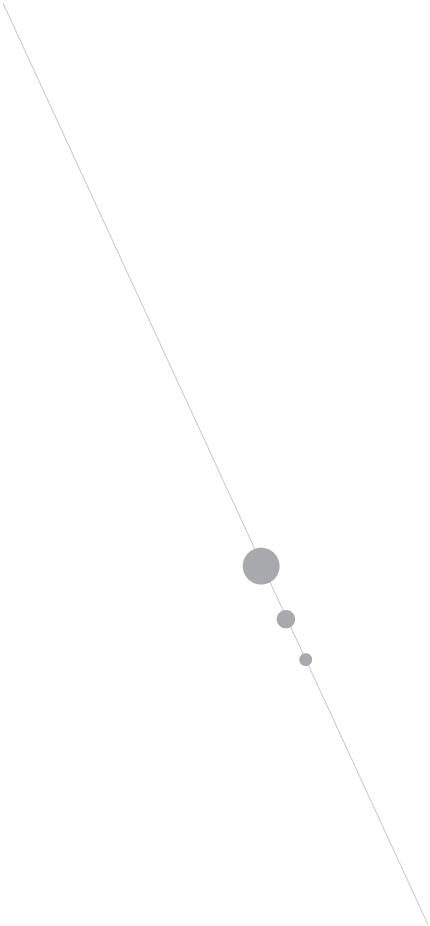
Geräteübergreifender und leicht zu konfigurierender Schutz

Ein anerkanntes Jugendschutzprogramm existiert momentan lediglich für den PC. Die Geräte, die Kinder und Jugendliche hauptsächlich nutzen, bieten kaum Schutzoptionen: Für Smartphones, Tablets und andere internetfähige Geräte existieren im besten Fall punktuelle Lösungen (z. B. Jugendschutzfunktionen von iOS und Google Family Link). Beim Großteil der installierten Apps entfalten sie aber keine Wirkung.

Ein geräteweiter Schutz lässt sich auf mobilen Geräten prinzipiell nicht ohne weiteres umsetzen. Mobile Betriebssysteme (Android und iOS) basieren auf dem Sandbox-Prinzip. Apps laufen in einer gekapselten Umgebung und der Zugriff (bspw. auf den Datenverkehr einer App) von außen ist in der Regel nicht möglich.

Ohne eine zentrale Verwaltung von Jugendschutzeinstellungen müssen Eltern bei jedem genutzten Dienst und jedem Gerät Einstellungen finden und einzeln aktivieren.

Damit Jugendschutzoptionen von Eltern akzeptiert und angewendet werden, müssen sie unkompliziert und ohne technisches Spezialwissen zu nutzen sein. Ansonsten laufen Ansätze ins Leere. Eine technische Schutzlösung muss deshalb so gestaltet sein, dass sie Eltern die zentrale Verwaltung der Accounts bzw. Einstellungen auf den Geräten ihrer Kinder ermöglicht.



MODELL MODERNES SCHUTZKONZEPT

Konzept

Insbesondere mobile Geräte ohne eigenständige, übergreifende Jugendschutzprogramme brauchen nutzungsübergreifende Schutzoptionen. Mithilfe von Schnittstellen und Standards für Geräte und Dienste wäre es z. B. möglich, den Zugang für Kinder und Jugendliche zentral abzusichern. Die Verwaltung der Einstellungen könnte dabei über die Betriebssysteme erfolgen.

Nutzung

Bereits bei der Einrichtung eines Smartphones oder Tablets sollten Eltern darauf hingewiesen werden, dass sie eine geräteweite Jugendschutzoption aktivieren können. Dafür müssen sie lediglich das Alter des Kindes angeben. Nutzen Kinder mehrere Geräte mit demselben Betriebssystem, werden die Altersinformationen synchronisiert. Eltern müssen keine Einstellungen in den einzelnen Apps vornehmen. Sie haben aber die Möglichkeit, Details anzupassen, falls die voreingestellten Optionen nicht ihren Vorstellungen entsprechen.

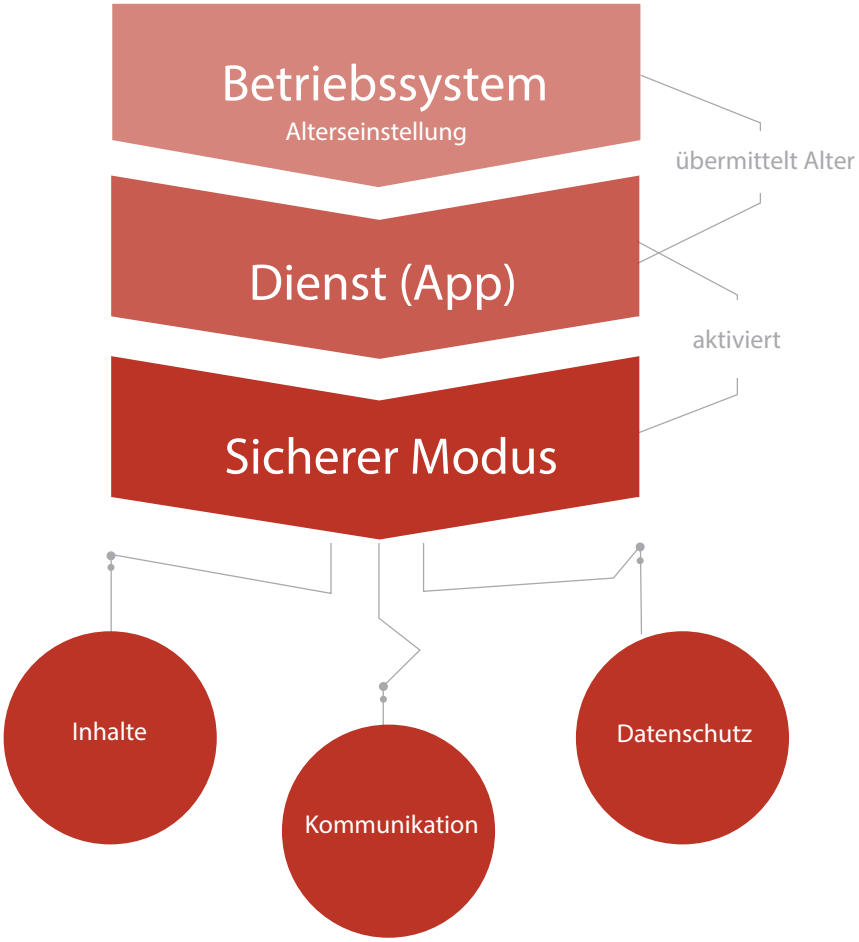
Zentral ausgewählte Jugendschutz- und Alterseinstellungen könnten über eine Schnittstelle an alle installierten Apps weitergegeben werden. Diese müssen auf die Information reagieren, indem sie einen sicheren Modus für Kinder aktivieren. In diesem sicheren Modus werden nur unbedenkliche Inhalte angezeigt. Sämtliche Kommunikations- und Datenschutzeinstellungen werden auf kindgeeignete Einstellungen gesetzt.

Voraussetzungen

Um eine zentrale Verwaltung zu erreichen, müssen die Hersteller von mobilen Betriebssystemen (Apple und Google) ermöglichen, dass Eltern eine bestimmte Altersstufe für die Nutzung eines Dienstes einstellen können. App-Anbieter müssen zur Einbindung kompatibler Jugendschutzoptionen verpflichtet werden.

Sobald über das Betriebssystem beispielsweise ein Alter „ab 6 Jahren" eingestellt wird, geht diese Information über eine Schnittstelle an alle genutzten Apps. Die Apps aktivieren daraufhin automatisch einen sicheren Modus „ab 6 Jahren". Ungeeignete Inhalte werden ausblendet und unangemessene Kontaktfunktionen (z. B. Kontaktaufnahme durch Fremde, öffentliche Sichtbarkeit des Profils) deaktiviert. Das Sammeln von Nutzerdaten wird unterbunden und In-App Käufe unmöglich gemacht. Die meisten Nutzerinnen und Nutzer sind nicht mit der Altersklassifizierung von Inhalten vertraut. In vielen Fällen, insbesondere bei Inhalten für ältere Kinder und Jugendliche, ist eine Einschätzung selbst für Experten schwierig. Deswegen sollte die Alterseinstufung möglichst schnell und einfach auf Basis eindeutiger Deskriptoren funktionieren.

Damit jüngere Kinder vor nicht klassifizierten beeinträchtigenden Inhalten geschützt sind, müsste grundsätzlich für alle Inhalte die Altersstufe „ab 12 Jahren" voreingestellt sein. Der Upload-Prozess wäre dadurch kaum komplizierter. Aber jüngere Kinder wären vor zufälliger Konfrontation geschützt.



(Quelle: jugendschutz.net)

Kindern und Jugendlichen ein gutes Aufwachsen mit Medien ermöglichen

Als gemeinsames Kompetenzzentrum von Bund und Ländern für den Jugendschutz im Internet recherchiert jugendschutz.net Gefahren und Risiken in jugendaffinen Diensten.

Die Stelle drängt Anbieter und Betreiber, ihre Angebote so zu gestalten, dass Kinder und Jugendliche sie unbeschwert nutzen können. Sie nimmt über ihre Hotline Hinweise auf Verstöße gegen den Jugendmedienschutz entgegen und sorgt dafür, dass diese schnell beseitigt werden.

Verstöße im Netz können gemeldet werden unter:

www.jugendschutz.net/hotline
hotline@jugendschutz.net

JUGEND SCHUTZ.NET