Beitrag

AKTUELL

Technische Herausforderungen an einen zukunftsfähigen Jugendmedienschutz

Ein Beitrag von Mark Bootz und Andreas Marx*

Angesichts fortschreitender Digitalisierung, zunehmender Konvergenz und veränderten Nutzungsgewohnheiten stellt sich die Frage, wie Jugendmedienschutz gestaltet sein muss, um den neuen Herausforderungen gerecht zu werden. Vor diesem Hintergrund hat die Kommission für Jugendmedienschutz (KJM) jugendschutz.net mit einem Gutachten zu zukunftsfähigen Konzepten des technischen Jugendmedienschutzes beauftragt[1]. Ausgehend von der aktuellen Nutzung durch Kinder und Jugendliche und den Entwicklungen im Internet hat jugendschutz.net darin die resultierenden Herausforderungen und Lösungsmöglichkeiten aufgearbeitet.

Mobile Nutzung und Dominanz des Social Web

Das Internet und seine Nutzung durch Kinder und Jugendliche verändern sich sehr schnell. Bis 2013 gingen Kinder und Jugendliche meist über den heimischen Desktop-PC online. Dieser war für Eltern leicht einsehbar. Zusätzlich ließen sich Risiken durch die Installation eines Jugendschutzprogramms reduzieren. Inzwischen gehen selbst Vorschulkinder online[2]. Junge User verfügen in der Regel über mehrere internetfähige Geräte und sind mit ihren Smartphones permanent connected[3]. Ein zukunftsfähiger technischer Jugendmedienschutz muss deshalb auch jüngere Usergruppen und die mobile Nutzung des Internet außerhalb der Homezone berücksichtigen.

Jüngere Kinder surfen zum Teil noch auf klassischen Webseiten, bei Jugendlichen spielen diese nur noch eine untergeordnete Rolle. Der Schwerpunkt der Nutzung liegt auf der Kommunikation und Interaktion. Bevorzugt werden vor allem große Kommunikations-, Foto- und Videodienste des Social Web[4]. Dort werden Kinder und Jugendliche nicht nur mit jugendgefährdenden Inhalten konfrontiert, sie sind auch Kommunikationsrisiken und dem Risiko ungewollter Datenpreisgabe ausgesetzt. Auch auf diese konvergierenden Risiken muss ein zukunftsfähiger technischer Jugendmedienschutz eine Antwort finden.

Verschlüsselung von Inhalten und Nutzung von Apps

Im Social Web existiert eine unüberschaubare und schnell wachsende Masse an Inhalten, die sich durch das User-Sharing extrem schnell verbreiten können. Die Black- und Whitelists klassischer Jugendschutzfilter sind für diese schnell fluktuierenden Inhalte zu statisch und zu langsam.

* Mark Bootz ist Leiter, Andreas Marx ist Mitarbeiter des Referats Technischer Jugendmedienschutz bei *Jugendschutz.net*

1 Gutachten: Perspektiven des technischen Jugendschutzes

2 DIVSI U9-Studie, S. 71

3 JIM-Studie 2016, S. 11

4 JIM-Studie 2016, S. 10ff

Während sichere Übertragungsprotokolle (HTTPS) ursprünglich nur bei sicherheitskritischen Vorgängen (z. B. Online-Banking oder -Shopping) eingesetzt wurden, werden seit den Snowden-Enthüllungen zur NSA (2013) immer mehr Verbindungen verschlüsselt. Aktuelle Jugendschutzprogramme können dann nur noch komplette Websites und Plattformen blockieren, aber nicht mehr einzelne gefährdende Seiten, Profile oder Videos ausfiltern.

95% der Jugendlichen besitzen inzwischen ein Smartphone. Es ist das am häufigsten genutzte Gerät, um online zu gehen[5]. Jugendliche rufen nur noch selten Inhalte über Browser ab und nutzen bevorzugt die Apps globaler Dienste[6]. In diesen Apps ist die Übertragung der Inhalte so gekapselt, dass für externe Programme keine Möglichkeit mehr besteht, riskante Inhalte oder Aktivitäten zu erkennen und zu blockieren.

Externe Jugendschutzprogramme und sichere Konfiguration von Diensten

Da externe Programme im Social Web kaum noch Schutzwirkung entfalten können, wächst die Verantwortung der Dienstanbieter für den Jugendmedienschutz. Nur sie können sichere Konfigurationen für Kinder und Schutzoptionen für Jugendliche anbieten, die Konfrontationsrisiken und die Gefahr reduzieren, belästigt, beleidigt oder ausgeforscht zu werden.

Viele Internetdienste verfügen über solche proprietäre Schutzfunktionen[7]. Neben Inhaltsfiltern (z. B. sicherer Modus von Suchmaschinen) sind oft Optionen verfügbar, die das Risiko von Belästigungen (z. B. Sperrung des Profils für Fremde) oder der Preisgabe persönlicher Daten reduzieren. Auch in Betriebssystemen können Inhaltsfilter oder Altersbeschränkungen aktiviert werden.

Die dienstspezifischen Optionen zum Schutz junger User bleiben derzeit nicht nur hinter den technischen Möglichkeiten zurück, sie unterscheiden sich auch von Dienst zu Dienst und sind auf den jeweiligen Dienst beschränkt. Diese Situation überfordert Eltern komplett. Sie müssen derzeit auf jedem Gerät und für jeden Dienst die passenden Schutzeinstellungen finden und aktivieren.

Integriertes Schutzkonzept und einfache Handhabung

Ein zeitgemäßes Schutzkonzept muss alle verfügbaren Mechanismen integrieren und einfach handhabbar machen. Dazu müssen technische Schutzfunktionen verbessert und die Filterung von Websites und proprietären Funktionen von Diensten in einem übergreifenden Konzept zusammengeführt werden.

Jugendschutzprogramme können Schutz bei klassischen Websites bieten, wenn sie entsprechend weiterentwickelt werden (z.B. in Richtung Echtzeitanalyse). Im Social Web können sie Kinder und Jugendliche aber nicht vor Konfrontations-, Kommunikations- und Datenschutzrisiken schützen. Hier müssen die Dienste ihre Schutzfunktionen im Sinne des ‚Safety by Design' verbessern.

Für die Schutzwirkung letztlich entscheidend ist aber, ob das System für Eltern einfach zu handhaben ist. Nur wenn es intuitiv und an zentraler Stelle konfigurierbar ist, wird es genutzt. In einem Szenario verteilter Schutzlösungen (verschiedene Dienste bieten eigene Schutzfunktionen) ist also eine zentrale Konfiguration – möglichst im Betriebssystem – unverzichtbar.

Indizierung als Baustein eines zukunftsfähigen Jugendmedienschutzes

Während offensichtlich jugendgefährdende Inhalte wie Pornografie einfach zu erkennen und auch technisch auszufiltern sind, fällt dies beispielsweise bei der Propagierung von Selbstgefährdungen, Gewalt oder Hass gegen Andersdenkende sehr viel schwerer. Indizierungen sind nicht nur Entscheidungen im Einzelfall, sondern liefern auch wichtige Kriterien und Orientierungshilfen.

5 JIM-Studie 2016, S. 22f

6 JIM-Studie 2016, S. 30

7 Gutachten: Perspektiven des technischen Jugendschutzes, S. 13ff

Das Internet ändert sich schnell. Insbesondere im Social Web entwickeln sich stetig neue Formate und Phänomene (z.B. Child-Beating-Videos, rassistischer „Humor“, drastische Kriegsbilder). Es ist Aufgabe der BPjM zu signalisieren, wann die Grenzen zur Jugendgefährdung überschritten werden. Dazu muss sie in ihrer Indizierungspraxis auch aktuelle Dienste berücksichtigen.

Adressbasierte Indizierung verliert an Schutzwirkung

Die derzeitige Praxis bei Telemedien basiert auf einer Listung jugendgefährdender Web-Adressen. Schutzwirkung entfaltet die Indizierung über Jugendschutzfilter, die den Aufruf indizierter URL blockieren. Über eine Selbstverpflichtung löschen Google und Bing auch indizierte Adressen aus ihren deutschen Suchindexen. Die Auffindbarkeit indizierter Medien wird so erschwert.

Jugendschutzprogramme können aufgrund zunehmender Verschlüsselung keine Einzelinhalte eines Dienstes (z.B. ein Hassprofil bei Facebook) mehr filtern. Damit verliert die adressbasierte Indizierung im Social Web ihre Wirkung. Die pauschale Blockade eines gesamten Dienstes (z.B. Facebook) durch Jugendschutzprogramme würde zu inakzeptablem Overblocking führen.

Auch in Bezug auf die Auffindbarkeit verliert die adressbasierte Indizierung an Wirkung. Einerseits gehen Jugendliche vor allem per Apps online und nutzen dort die proprietären Suchfunktionen der Social-Media-Dienste. Andererseits werden Inhalte vielfach geteilt und sind dann über eine Vielzahl von Adressen erreichbar, selbst wenn die Quelle bzw. deren URL bereits indiziert ist.
Inhalte werden inzwischen tausendfach geteilt und sind dann über Tausende von Adressen verfügbar, selbst wenn die Quelle indiziert wurde.

Inhalte von Onlinemedien indizieren

Bei einer URL handelt es sich um einen Verweis auf eine Fundstelle, deren Inhalt sich ändern und über viele andere Adressen zu finden sein kann. Im Falle herkömmlicher, vergleichsweise statischer Webseiten entstehen hieraus kaum Probleme. Im Social Web mit hoch dynamischen und stark verknüpften Inhalten stößt die Indizierung auf Basis einer URL aber an ihre Grenzen.

Im Bereich der Trägermedien werden die jugendgefährdenden Inhalte selbst indiziert – und nicht alle Orte, an denen sie zu finden sind. Auch für Telemedien wird eine inhaltsbasierte Indizierung benötigt, um beispielsweise ein vielfach geteiltes Video als jugendgefährdend klassifizieren zu können, ohne alle Orte und alle Adressierungsvarianten benennen zu müssen, an denen bzw. über die es zu finden ist.

Neben redaktionellen Daten (z. B. Titel oder Länge eines Videos) können so genannte digitale Fingerprints als Indizierungsmerkmal dienen. Audiovisuelle Inhalte sind damit eindeutig zu identifizieren. Solche Fingerprint-Mechanismen werden zur Identifizierung von Urheberrechtsverletzungen oder von Darstellungen des sexuellen Missbrauchs von Kindern seit Jahren erfolgreich eingesetzt.

Erweiterte Schutzwirkung durch Kooperation mit Dienstanbietern

Jugendschutzprogramme und Suchmaschinen nutzen derzeit das BPjM-Modul, um indizierte Adressen zu blockieren oder aus dem Suchindex zu löschen. Weiter entwickelte Filtersysteme könnten mit Hilfe von Fingerprints zusätzlich auch einen Abgleich vornehmen, ob auf einer Webseite indizierte audiovisuelle Inhalte zu finden sind. Gleiches gilt für Suchdienste.

Um die Schutzwirkung der Indizierung im Social Web aber deutlich zu steigern, wären Vereinbarungen mit Social-Media-Plattformen nötig, sodass sie audiovisuelle Inhalte löschen oder blockieren, deren Fingerprints von der BPjM gelistet sind. Das BPjM-Modul, das bisher nur Adressen umfasst, müsste dazu um Fingerprints erweitert werden, deren Formate mit den Betreibern abzustimmen wäre.

Die Plattformen müssten dazu keine prinzipiell neuen Mechanismen entwickeln. Bei allen großen Diensten wird beispielsweise Photo-DNA eingesetzt, um den Upload bekannter Darstellungen des sexuellen Missbrauchs von Kindern zu blockieren. Photo-DNA ist ein Fingerprinting-Mechanismus, der von Microsoft entwickelt wurde und sich als Industriestandard etabliert hat.

Indizierungswirkung über den Einzelfall hinaus

Gut begründete Indizierungen können den Unternehmen und ihren Supportabteilungen Orientierungshilfe geben und eine Wertedebatte zu den Rechten von Kindern unterfüttern. Die adressbasierte Indizierung erschwerte aber die Kommunikation, weil damit immer auch die Fundstellen der jugendgefährdenden Inhalte veröffentlicht und „beworben“ werden.

Mit einer inhaltsbasierten Indizierungen kann eine gesellschaftliche Debatte leichter initiiert werden, welche Merkmale die Jugendgefährdung definieren, wie die Verbreitung jugendgefährdender Inhalte begrenzt werden kann und wie Kinder und Jugendliche davor geschützt werden können. Dies wäre ein wichtiger Beitrag für einen zukunftsfähigen, technischen Jugendmedienschutz.