Jugendschutz in Mobilfunknetzen

Konzept für einen wirksameren Jugendschutz im Spannungsfeld der Chancen und Risiken des mobilen Kontextes

Marian Benner, Volker Gruhn, Sebastian Milenk

Universität Duisburg-Essen
Gerlingstraße 16
45127 Essen
marian.benner@uni-due.de
volker.gruhn@uni-due.de
sebastian.milenk@stud.uni-duisburg-essen.de

Abstract: Die technische Entwicklung im Bereich der Mobiltelefone ist so weit fortgeschritten, dass diese Geräte in der Lage sind, Inhalte aus dem Internet ohne große Einschränkungen darzustellen. Zudem zeigt die aktuelle JIM-Studie [JIM10], dass bereits eine sehr große Zahl von Kindern und Jugendlichen ein solches Gerät besitzt. Der Zugang zum Internet über den heimischen PC verliert zunehmend an Bedeutung. Ein Mobiltelefon bietet aber im Gegensatz zum PC kaum Möglichkeiten für Eltern, das Nutzungsverhalten ihrer Kinder zu kontrollieren und altersgerecht einzuschränken. Mobilfunkbetreiber haben sich im Rahmen von Selbstverpflichtungserklärungen zu rudimentären Schutzmaßnahmen verpflichtet, die sich aber nur auf die eigenen Inhalte und die der Vertragspartner beziehen. Ungeachtet dessen, dass die Gesetzgebung bislang noch keine wirksamen Mittel gefunden hat, den Zugang zu jugendgefährdenden Inhalten im Internet zu reglementieren, hat eine solche Einschränkung nur nationale Geltung. Dieser Beitrag widmet sich daher den folgenden Fragestellungen: Welche Ansätze gibt es zur Durchsetzung des Jugendschutzes in Mobilfunknetzen und wie effektiv sind diese? Mit welchem informationstechnischen Konzept lässt sich der Jugendschutz verbessern und welche Rolle kann darin ein soziales Netzwerk spielen?

1 Einleitung

Die rasante Weiterentwicklung mobiler Endgeräte, wie zum Beispiel der Smartphones oder der Internet-Tablets, hat die Verfügbarkeit von Medien für den Verbraucher auch in den mobilen Benutzungskontext gerückt. Der Zugriff auf das Internet und der Austausch von Videos und Bildern zwischen Endgeräten sind ortsunabhängig möglich und für viele Verbraucher alltäglich geworden. Der Markt für Mobiltelefone besteht bereits heute fast ausnahmslos aus Geräten, die internetfähig sind und Technologien für den bequemen Dateiaustausch wie Bluetooth integrieren.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

Die Nutzung von mobilen Endgeräten ist bei Kindern und Jugendlichen mittlerweile weit verbreitet. Über 96% der in Deutschland lebenden Jugendlichen verfügen über ein eigenes Mobiltelefon [JIM10]. Das Jugendamt der Stadt Nürnberg empfiehlt einen von den Eltern kontrollierten Umgang mit dem Mobiltelefon bereits ab einem Alter von 10 Jahren [SN08]. Und während es an PC-Systemen mittlerweile eine gewisse Auswahl an Kontrollmöglichkeiten gibt, sind viele Kinder und Jugendliche mit Mobiltelefon einem ungeschützten Zugang zum Internet ausgesetzt. Im Jahr 2010 wurde das Mobiltelefon von 13% der befragten Kindern und Jugendlichen für den Zugriff auf das Internet einem PC vorgezogen. Dieser Anteil hat sich im Vergleich zu 2008 mehr als verdreifacht [JIM10].

Trotz dieser Entwicklungen mangelt es den aktuellen Ansätzen zur Einhaltung des Jugendschutzes an Effektivität. Nationale Bestrebungen für eine Kennzeichnungspflicht von Internetseiten, wie sie zum Beispiel in der Neuauflage des Jugendmedienschutzstaatsvertrages [JMS10] vorgesehen waren, sind in vielerlei Hinsicht zu kritisieren. Erstens benötigen solche Gesetzesinitiativen im Rahmen der demokratischen Prozesse eine lange Zeit vom Kabinettsbeschluss bis zur Wirksamkeit und laufen so Gefahr, der Geschwindigkeit der technischen Entwicklung hinterher zu laufen. Zweitens haben sie nur Auswirkungen auf in Deutschland bereitgestellte Inhalte. Drittens ist eine altersgerechte Einstufung von vielen Internetseiten nur mit sehr hohem Aufwand möglich. Denn der Wandel zu Internetseiten, an deren Gestaltung vermehrt die Leser beteiligt werden, führt zu einer hohen inhaltlichen Dynamik. Die Betreiber müssten die Inhalte laufend kontrollieren und gegebenenfalls neu einstufen.

Die deutschen Mobilfunkanbieter haben im Juni 2005 einen Verhaltenskodex [FSM05] zum Jugendschutz unterzeichnet, der im Oktober 2007 um eine Selbstverpflichtung [FSM07] ergänzt wurde. Die Mobilfunkanbieter zeichnen sich darin für die eigenen Inhalte und die Inhalte von Vertragspartnern verantwortlich. Die Verfügbarkeit jugendgefährdender Inhalte im Internet wird durch diese Maßnahmen aufgrund des begrenzten Geltungsbereiches leider nur in geringem Maße eingeschränkt.

Eltern können das Problem zurzeit nur umgehen, indem sie die Internet- und Bluetooth-Funktionalität technisch komplett abschalten oder sogar die Nutzung eines Mobiltelefons allgemein untersagen. Dieser Ansatz führt aber dazu, dass die Kinder und Jugendlichen auch von vorteilhaften Diensten oder der Teilhabe an sozialen Netzwerken ausgeschlossen werden. Zudem kann Medienkompetenz nicht ohne eigene Erfahrungen mit dem Medium erworben werden.

Entlang einer Klassifizierung der Gefahren für Kinder und Jugendliche wird in den nachfolgenden Kapiteln aufgezeigt, wie den Gefahren bislang seitens des Staates, der Mobilfunkanbieter und der Eltern begegnet wurde. Die Ansätze werden kritisch bewertet und um ein eigenes Konzept ergänzt, welches die Risiken im mobilen Kontext minimieren soll. Schließlich wird ein Ausblick auf weiterführende konzeptuelle sowie implementierungsbezogene Fragestellungen gewährt.

ISBN 978-3-88579-286-4

2 Gefahren im mobilen Kontext

Durch die bereits eingangs erwähnten technischen Möglichkeiten aktueller mobiler Endgeräte, kommt es zu einer Bündelung von Risiken für Kinder und Jugendliche. Nigel Williams, der Gründer der Plattform „Childnet International“, eine Initiative die sich für ein kindgerechtes Internet einsetzt, beschreibt drei wesentliche Gefahrenkategorien, welche im Umgang mit dem Internet auftauchen: Content, Contact und Commerce (oft als CCC oder 3C abgekürzt). Diese Kategorien lassen sich auch auf den mobilen Kontext übertragen und sind daher für eine weitergehende Analyse hilfreich [CI03].

Die Gefahren verschärfen sich im Vergleich zur Nutzung von Desktop-Systemen insofern, als dass zusätzliche Aspekte (z. B. mangelnde Kontroll- und Konfigurationsmöglichkeiten am mobilen Endgerät oder das Verknüpfen von Positionsdaten zu Bewegungsprofilen) berücksichtigt werden müssen. Der ständige Zugang zu mobilen Endgeräten sowie eine ortsunabhängige Nutzung stellen neue Herausforderungen dar. Aufgrund der Mobilität der Geräte ist eine Nutzung in Abwesenheit der Erziehungsberechtigten vereinfacht möglich. Hinzu kommen die simplifizierten Möglichkeiten des unkontrollierten Dateiaustauschs und das Zusammenspiel von Techniken wie Kamera und Positionsbestimmung und die daraus resultierenden Gefahren. In den folgenden Abschnitten werden die Kategorien und ihre Auswirkungen im mobilen Kontext erläutert.

2.1 Gefährdung durch Content (Inhalt)

Kinder und Jugendliche können sich Zugänge zu Angeboten schaffen, die nicht für ihre Altersgruppe bestimmt sind. Dies kann etwa der Aufruf einer Internetseite mit gewaltverherrlichen, rassistischen oder pornographischen Bildern, Videos oder Texten sein. Jugendgefährdende Inhalte können dabei nicht nur über Internetseiten aufgerufen, sondern direkt von einem mobilen Endgerät zum anderen übertragen werden. [JIM10].

Gefährdung durch Content beinhaltet zudem das Erstellen von Inhalten. Das mobile Endgerät als ständiger Begleiter ermöglicht es, durch die im Gerät eingebaute Kamera in nahezu jeder Situation Bild- oder Videomaterial anzufertigen. Das heimliche Aufzeichnen von Bildern oder Videos, die Personen in prekären oder gar intimen Situationen zeigen, wird als eine neue Form des digitalen Mobbings gesehen und als „Cyberbullying“ bezeichnet. Es wird in die Privatsphäre der Person eingedrungen und versucht, sie auf erniedrigende Weise bloßzustellen und in eine Opferrolle zu drängen [BF07]

Die amateurhaften Aufnahmen von Schlägereien, welche gestellt oder real sein können, sind unter dem Begriff „Happy Slapping“ bekannt. Die erstellten Inhalte lassen sich über Mobiltelefone direkt austauschen oder werden über Videoportale im Internet verteilt [GR08].

Vielfach sind mobile Endgeräte heute zudem mit einer WLAN-Schnittstelle ausgestattet, worüber sich einerseits Daten austauschen lassen, aber auch die Nutzung von Internetanwendungen in verfügbaren Funknetzwerken kostenfrei ermöglicht wird. Andererseits trägt auch die erleichterte Bedienung solcher Geräte dank Multitouch-Displays und angepasster Anwendungen (Apps) zu einem verstärkten Konsum von Inhalten im Internet bei.

2.2 Gefährdung durch Contact (Kontakt)

„Neben der Unterhaltung ist das Motiv, andere Jugendliche kennen zu lernen, der am häufigsten genannte Grund für die Chat-Kommunikation“ [Kammerl]. Neben Chaträumen genießen Instant Messenger große Beliebtheit und werden von gut 60% der Jugendlichen täglich genutzt. Diese Programme können dazu genutzt werden, Dateien, darunter Bilder, Videos oder Musiktitel, unter einem großen Adressatenkreis zu verbreiten. [JIM10].

Vor allem in öffentlichen Chaträumen kommt es zu sexuellen Belästigungen, Beschimpfungen oder Vorfällen von Mobbing [JSN]. Häufig werden gerade junge Mädchen von Männern gezielt nach einem Treffen mit sexuellem Hintergrund gefragt.

Auch Beleidigungen oder das Verbreiten von falschen Tatsachen haben Einzug in die digitale Welt gefunden. Das Cybermobbing kann hierbei auf unterschiedlichen Arten stattfinden: Einerseits in textueller oder visueller Form in einer öffentlichen Arena (wie etwa in Sozialen Netzwerken oder Videoportalen, etwa Facebook, SchülerVZ, YouTube oder myVideo). Andererseits findet Mobbing in direktem Kontakt zum Opfer statt. Mittels Instant Messenger, E-Mail oder SMS werden die Opfer in persönlichen Nachrichten attackiert.

2.3 Gefährdung durch Commerce (Kosten)

Kosten können durch Telefonate, das Versenden von Kurz- oder Multimedianachrichten und das Benutzen der Internetverbindung entstehen. Hierbei handelt es sich jedoch zumeist um planbare Kosten, da Kinder und Jugendliche bewusst eine Leistung gegen ein Entgelt eintauschen. Anders sieht es bei den zum Teil aggressiv beworbenen Werbungen für Klingeltöne, Bilder, Videosequenzen oder Spiele aus. Bei sogenannten Abo-Fallen schließen Kinder und Jugendliche unwissentlich ein Abonnement ab. Die gesetzliche Informationspflicht zu anfallenden Kosten sowie der Kündigungsformalitäten werden in einem Mindestmaß erfüllt.

Eine klare Abgrenzung der drei Risikobereiche Content, Contact und Commerce ist nicht immer möglich. Ein als Premiumdienst angebotenes Handygame mit freizügig dargestellten Frauen, welches nicht eindeutig als Abonnement gekennzeichnet ist, stellt zum Beispiel eine Gefahr sowohl im Content als auch im Commerce Bereich dar.

ISBN 978-3-88579-286-4

3 Aktuelle Lösungsansätze

Um den drei Gefährdungsarten (CCC) entgegenzuwirken, wurden Maßnahmen sowohl von staatlicher als auch von Seiten der Mobilfunkanbieter unternommen. In einer Selbstverpflichtungserklärung der Mobilfunkanbieter haben diese sich unter anderem dazu verpflichtet, eine kostenfreie Hotline für Kinder und Jugendliche anzubieten. Diese soll nicht nur Kindern und Jugendlichen, sondern auch Eltern und Pädagogen als Anlaufstelle bezüglich jugendschutzrelevanter Informationen dienen. Auf nationaler Ebene wurde mit dem Jugendmedienschutz-Staatsvertrag (JMStV) eine Vereinbarung der Länder getroffen, die eine einheitliche Gesetzesgrundlage im Umgang mit jugendgefährdeten Sachverhalten bietet.

3.1 Content

Der von den Mobilfunkanbietern unterzeichnete Verhaltenskodex hält diese dazu an, Inhalte von Anbietern generell zu löschen, die gesetzwidrig sind, beispielsweise Kinder-, Tier- und Gewaltpornographie. Eine Deaktivierung der Schnittstellen mobiler Endgeräte, wie etwa der Bluetooth- oder Infrarotschnittstelle, verhindert einen direkten Datenaustausch. So kann die Verteilung von Bild- oder Videodateien zwischen mobilen Endgeräten unterbunden werden. Mobilfunkanbieter bieten zudem die Möglichkeit, den Datenzugang vom mobilen Endgerät ins Internet vollständig zu sperren.

Nachdem das „Gesetz zur Bekämpfung von Kinderpornographie in Kommunikationsnetzen“ [BW09] für einige Monate ausgesetzt wurde, hat sich die Koalitionsspitze der Bundesregierung für eine Löschung von Internetseiten mit pornographischen Inhalten anstelle der bisherigen Sperrung ausgesprochen [KR11]. Auch die zuvor durch das Land Nordrhein-Westfalen gescheiterte Novellierung des JMStV soll nach Vorstellung des Landes Sachsen-Anhalt erneut vorangetrieben werden [KR11b].

3.2 Contact

Online-Communities und soziale Netzwerke, wie etwa SchülerVZ haben Supportteams, die von Benutzern gemeldeten Fällen nachgehen [Sch01]. So können gemeldete Personen temporär oder auch vollständig aus dem Netzwerk verwiesen werden. Zudem werden Kurse zur Aufklärungsarbeit an Schulen angeboten, bei denen es um Cybermobbing und Datenschutz geht [Sch02]. Eine Vielzahl von Onlineangeboten und Anlaufstellen für Kinder und Jugendliche sowie Eltern werden vom Bund und den Ländern in Zusammenarbeit mit Verbänden angeboten..

An vielen mobilen Geräten lässt sich ein eingeschränkter Rufnummernkreis definieren. So können Kinder und Jugendliche nur noch vorher festgelegte Rufnummern anwählen bzw. werden nur noch bestimmte Nummer durchgelassen. [BW09]

3.3 Commerce

Über den Mobilfunkanbieter lässt sich die Nutzung von Premiumdiensten sperren. Anrufe zu Diensten wie Wettervorhersagen oder Erotikhotlines sind dann nicht mehr möglich. Ebenfalls kann der Multimedia Messaging Service (MMS) gesperrt werden. So lässt sich der Versand und Empfang von MMS und damit auch das Abschließen von (beispielsweise Klingelton-)Abonnements unterbinden.

Kindern und Jugendlichen wird zudem empfohlen, eine Prepaid-Karte zu benutzen. Im Gegensatz zu Postpaid-Verträgen ist hier eine ständige Kostenkontrolle gewährleistet. Die Prepaid Karte kann dabei nur genutzt werden, solange sie ein Guthaben aufweist.

4 Kritik

Ein wesentlicher Bestandteil bei der Problemlösung der drei Risikobereiche besteht in der vollständigen Deaktivierung der Konnektivität. So bieten die Netzbetreiber die dauerhafte Deaktivierung des Internetzugangs als buchbaren Service zum Erfüllen eines Jugendschutzes an. Oder es lässt sich der Internetzugang direkt an mobilen Endgeräten durch Sperren von Schnittstellen abschalten. Der Funktionsumfang wird hierbei künstlich eingeschränkt. Dies ist jedoch nicht nötig bzw. könnte sogar für den Nutzen im Bereich des eLearning hinderlich sein [HO11].

Trotz der Selbstverpflichtungserklärung und dem vereinbarten Verhaltenskodex werden auf den Eingangsportalen der Mobilfunkanbieter Inhalte beworben, die für Kinder und Jugendliche ungeeignet sind. Zwar wird der unmittelbare Zugriff auf den jugendgefährdenden Inhalt durch eine PIN verhindert, jedoch wird durch das Bewerben ein unnötiger Anreiz für Kinder und Jugendliche geschaffen [BF07]. Ebenfalls im Verhaltenskodex der Mobilfunkanbieter verankert ist die Verantwortung bezüglich des Jugendschutzes in Chaträumen. Den Betreibern wird es überlassen, sich um geeignete Schutzmechanismen und Vorkehrungen zu kümmern. [FSM07]

Die Nutzung eines eingeschränkten Rufnummernkreises greift bei eingehenden Anrufen nur solange der Anrufer seine Nummer nicht unterdrückt. Zwar lässt sich das Mobiltelefon auch so konfigurieren, dass Anrufe nur von und zu gespeicherte Rufnummern zulässig sind, jedoch wird so stark in den Nutzungsumfang des mobilen Endgerätes eingegriffen.

Als Maßnahme gegen Kinderpornographie forderte die Regierung eine Netzsperre [KL08]. Bei dem Aufruf solcher Seiten wurde der Besucher auf eine so genannte „Stopp Seite“ umgeleitet und erhielt die Information, dass der Zugang zu der aufgerufenen Seite gesperrt sei. Interessensgemeinschaften formierten sich, da sie durch die staatliche Kontrolle die Netzneutralität in Gefahr sahen. Zudem wurde diese Lösung als möglichen Einstieg in eine sonst nur aus autokratischen Ländern bekannte Internetzensur gewertet. Ein weiterer Kritikpunkt lag in der Effektivität der Netzsperren. So konnte gezeigt werden, dass das Umgehen dieser Netzsperren aus technischer Sicht mittels Änderung des DNS-Servers möglich sei [FB09].

ISBN 978-3-88579-286-4

Alle hier vorgestellten Lösungsansätze sind zumeist abhängig von Herstellern oder Mobilfunkanbietern. Es gibt keinen vereinbarten Standard bezüglich einer Geräteeinstellung seitens der Hersteller, die einem adäquaten Jugendschutz gerecht werden kann. Wenn ein Hersteller die Möglichkeit der Deaktivierung einer Schnittstelle bietet, so ist dies teilweise ein komplexer Vorgang und unterscheidet sich in der Vorgehensweise von denen anderer Hersteller.

Es kann also festgehalten werden, dass Kinder und Jugendliche auf Grund fehlender oder mangelhafter Schutzmaßnahmen im mobilen Kontext den Gefahren des Content, Contact sowie Commerce ausgesetzt sind. Ob es der Aufruf einer Internetseite, ein Gespräch im Chatraum oder das Herunterladen eines Klingeltons ist: Die Gefährdungen sind auf verschiedene Weise sichtbar. Gerade durch die Verbreitung von internetfähigen mobilen Endgeräten, wird die Brisanz auf Grund der ständigen Verfügbarkeit deutlich. Hinzukommt die Vielfalt an Geräten und Techniken, welche das Umsetzen eines einheitlichen Jugendschutzkonzeptes erschwert.

Bisherige Maßnahmen, wie etwa der JMStV oder die Selbstverpflichtungserklärung der Mobilfunkanbieter, wollen eine einheitliche, strukturierte Vorgehensweise in der Planung und Durchführung eines Jugendschutzes und gehen vom Ansatz in die richtige Richtung. Der in den meisten Konzepten im Zentrum stehende Lösungsansatz, die vollständige Deaktivierung von Funktionen und Schnittstellen, lässt jedoch erhebliche Mängel erkennen. Er macht den Bedarf einer umfassenden Lösung erkennbar, die an die besonderen Eigenschaften des Internets angepasst sind. Kinder und Jugendliche sollten zudem in den Prozess des mobilen Jugendschutzes aktiv mit einbezogen werden. Es fehlt ein plattformunabhängiges, wirkungsvolles Jugendschutzkonzept für den mobilen Kontext ohne eine dauerhafte Einschränkung des gesamten Funktionsumfangs. Das folgende Kapitel widmet sich dieser Lücke.

5 Konzept für einen wirksameren Jugendschutz im mobilen Kontext

Jugendschutzmaßnahmen sollten individuell betrachtet und behandelt werden. Kinder und Jugendliche lassen sich nicht eindeutig in Raster einteilen, wodurch beispielsweise der Einsatz von pauschalen Filtermechanismen alleine nicht ausreicht. Manchen Kindern und Jugendlichen können zum Beispiel aufgrund ihrer überdurchschnittlichen Medienkompetenz mehr Freiheiten eingeräumt werden. Ein Filtermechanismus kann jedoch als Grundlage gesehen werden, auf dem ein detaillierter Jugendschutz aufbaut.

Das hier vorgestellte Konzept zum Jugendschutz im mobilen Kontext ist daher in erster Linie darauf ausgerichtet, die vollständige Deaktivierung von Diensten, Schnittstellen oder Funktionen durch feinstufige, individuelle Einstellungen zu ersetzen. Es soll einerseits auf die Bedürfnisse der Kinder und Jugendlichen und andererseits auf die Anforderungen der Eltern zugeschnittene Jugendschutzprofile geben. Diese Profile sollen eine orts- und zeitbasierte Abschaltung bzw. Aktivierung von Funktionen und Schnittstellen ermöglichen.

Zudem sollen individuelle Filterlisten dafür sorgen, den aktuellen Stand an Jugendschutz-Maßnahmen am PC auch auf das mobile Endgerät zu übertragen. Die orts- und zeitbasierten Einstellungen sowie die Filterlisten sollen während der Nutzung dem Profil des Kindes bzw. des Jugendlichen dynamisch angepasst werden können. Dies soll über ein kollektives Echtzeit-Entscheidungssystem realisiert werden. Im weiteren Verlauf wird auf die einzelnen Elemente des Jugendschutzkonzeptes näher eingegangen. Spezifische Abläufe sollen erklärt werden, um die Funktionalität sowie das Zusammenspiel der einzelnen Elemente im Gesamtkontext darzulegen.

5.1 Architektur

In dem Jugendschutz-Konzept spielt es eine zentrale Rolle, dass Entscheidungen über die Freischaltung von Funktionen, Schnittstellen und Inhalten in Echtzeit in einem Social Web of Trust (SWOT) getroffen werden. Das SWOT ist ein Netzwerk aus Personen (z. B. befreundete Eltern, Verwandte und Bekannte), die gegenseitig ihr Vertrauen zueinander bewerten. Die Abbildung 1 zeigt die Einbettung des SWOT in die Architektur des Jugendschutz-Konzeptes.

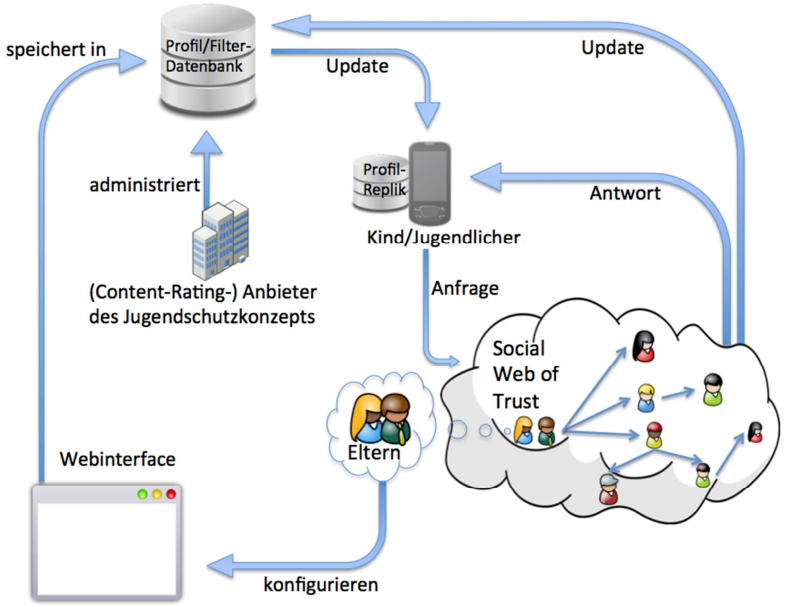

Abbildung 1: Architektur des Jugendschutz-Konzepts im mobilen Kontext

Über ein Webinterface wird von den Eltern ein auf das Kind bzw. den Jugendlichen zugeschnittenes Jugendschutzprofil erstellt und auf einer Profildatenbank abgelegt. Die Datenbank wird von einem Anbieter zur Verfügung gestellt und verwaltet. Der Anbieter stellt darüber hinaus auch verschiedene Listen für die Filterung von Inhalten bereit. Das mobile Endgerät des Jugendlichen besitzt eine Replik der aktuellen Profildaten und Filterlisten.

Eine auf dem mobilen Endgerät ausgeführte Anwendung sorgt für die Umsetzung der in dem Profil und den Listen enthaltenen Informationen zur Einschränkung von Funktionen, Schnittstellen und Inhalten. Möchte der Jugendliche eine deaktivierte Schnittstelle oder gesperrte Inhalte freischalten, kann er eine Anfrage an das SWOT senden. Im SWOT wird die Entscheidung über die Anfrage getroffen und auf das mobile Endgerät des Jugendlichen übertragen. Hat das SWOT sich für eine dauerhafte Änderung des Profils oder der Filterliste entschieden, wird auch die Profildatenbank aktualisiert. Auf diese Weise wird das Profil mehr und mehr den individuellen Anforderungen der Eltern und des Kindes bzw. des Jugendlichen angepasst.

5.2 Design des Social Web of Trust

Das SWOT lässt sich als ein Graph darstellen, in dem Personen als Knoten und deren Vertrauensbeziehung über gerichtete und gewichtete Kanten zwischen den Knoten abgebildet sind. Eltern nehmen an diesem Netzwerk teil und fügen Personen hinzu, denen sie den Jugendschutz betreffende Entscheidungen anvertrauen. Erzeugt man aus dem SWOT einen minimalen Spannbaum mit den Eltern als Wurzelknoten, kann ein Traversierungsalgorithmus eine Liste mit absteigenden Vertrauenswerten generieren. Diese Liste kann dann sukzessive abgearbeitet werden, um eine Person zu identifizieren, welche den höchsten Vertrauenswert besitzt und somit für eine Entscheidung am geeignetsten erscheint (siehe Abbildung 2). Kommen mehrere Personen aufgrund identischer Vertrauenswerte für eine Entscheidung in Frage, wird die Anfrage an alle potentiellen Personen geleitet.

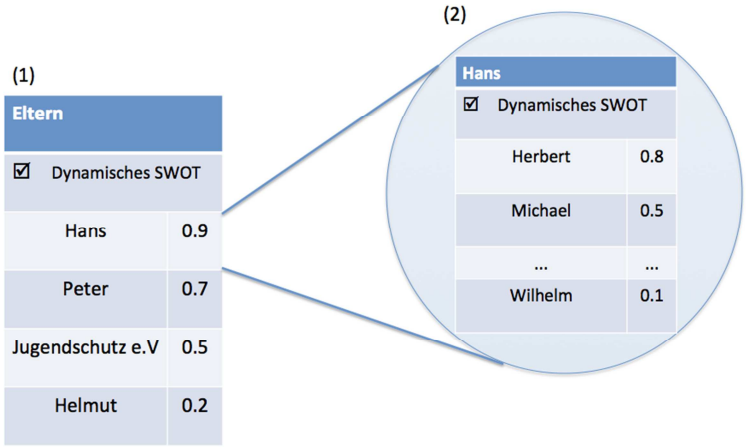

Abbildung 2: Beispiel dynamisches Social Web of Trust

Die Traversierung des Spannbaumes kann allerdings unerwünscht sein, zum Beispiel weil Eltern grundsätzlich ausschließen wollen, dass unbekannte Personen Entscheidungen über den Grad des Jugendschutzes treffen können. Daher gibt zwei Formen des SWOT, die je nach Sicherheitsbedürfnis der Eltern genutzt werden können: Das manuelle SWOT und das dynamische SWOT.

Es lässt sich allerdings zeigen, dass die Entscheidungsqualität beim dynamischen SWOT höher ist, obwohl unbekannte Personen beteiligt sind. Geht man beispielsweise davon aus, dass Hans aus der Liste auf Abbildung 2 nicht erreichbar ist, so kann durch Herbert eine Entscheidung getroffen werden, der die Eltern eher vertrauen als wenn sie von Peter getroffen worden wäre. Denn Herbert besitzt einen Vertrauenswert von 0,72 (0,8 multipliziert mit 0,9) und ist damit etwas vertrauenswürdiger als Peter, der einen Vertrauenswert von nur 0,7 besitzt. Bei der Nutzung des dynamischen SWOT ist wichtig, dass die Eltern sich bewusst sein müssen, dass sie mit ihrer Vertrauenseinschätzung auch die Vertrauenseinschätzungen des Bekannten beurteilen.

Unabhängig von der Wahl des manuellen oder dynamischen SWOT ist offensichtlich, dass die Effizienz des SWOT mit der Anzahl erreichbarer Personen in direktem Zusammenhang steht. Denn sobald eine Person nicht erreichbar ist, muss eine andere Person befragt werden, die zwar manchmal einen gleichen, in den meisten Fällen aber einen schlechteren Vertrauenswert aufweisen wird. Aufgrund dieses Sachverhaltes ist – insbesondere im Zusammenhang mit dem dynamischen SWOT – die Definition eines minimalen Vertrauens notwendig. Wird dieser Vertrauenswert im Verlauf des Algorithmus unterschritten, fällt die Entscheidung automatisch gegen eine Freischaltung des Inhaltes oder der Schnittstelle.

Um eine zu große Belastung einzelner SWOT-Teilnehmer zu verhindern, können die Anfragen an das SWOT in einem Protokoll (Log-Datei) ausgewertet werden. Wenn eine zuvor definierte Anzahl an offenen Anfragen überschritten wird, kontaktiert das System automatisch die nächste berechtigte Person. Ist keine weitere Person auffindbar oder wird dadurch das minimale Vertrauen unterschritten, bleibt der Inhalt oder die Schnittstelle gesperrt.

5.3 SWOT-Beispielszenario: Freischaltung von gesperrten Inhalten oder Schnittstellen

Für ein beispielhaftes Szenario wird vorausgesetzt, dass ein Kind oder Jugendlicher in einer bestimmten Nutzungssituation eine gesperrte Internetseite betreten oder deaktivierte Schnittstelle benutzen möchte und eine entsprechende Meldung auf dem Display erscheint. Er ist mit der Sperre bzw. der Deaktivierung nicht einverstanden und bittet daher das SWOT um Freischaltung (siehe Abbildung 3).

ISBN 978-3-88579-286-4

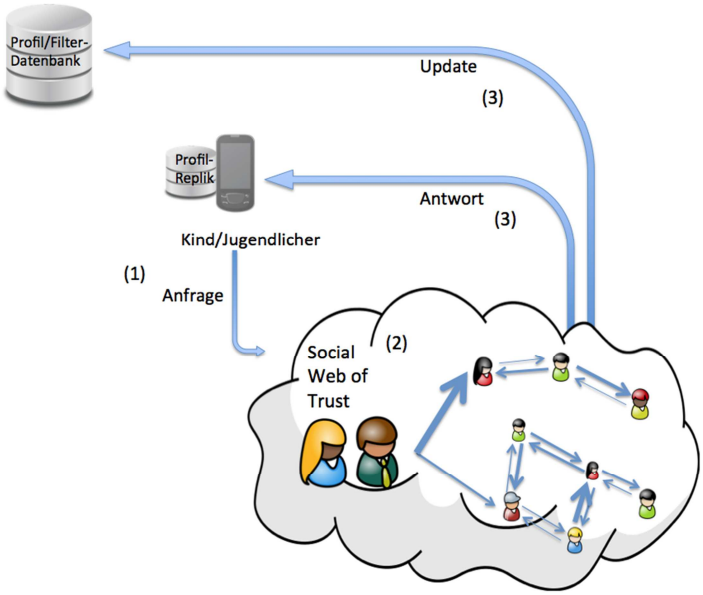

Abbildung 3: Anfrage an ein dynamisches SWOT zur Freischaltung von Inhalten/Funktion

Nachdem gemäß dem vorab aufgeführten Algorithmus eine entscheidungsbefugte Person identifiziert wurde, werden ihr alle verfügbaren relevanten Informationen übermittelt, wie z. B. eine Vorschau der gesperrten Internetseite oder der Name des Gerätes, zu dem eine Bluetooth-Verbindung hergestellt werden soll. Die Entscheidung wird gefällt und im Anschluss an das mobile Endgerät des Kindes bzw. des Jugendlichen übertragen. Die auf dem Gerät ausgeführte Software sorgt dann für die Freischaltung.

Falls die Entscheidung positiv ausgefallen und der Entscheidungsträger auch für dauerhafte Profiländerungen befugt ist, wird die Information an den Datenbankserver des Anbieters gesendet, um das Profil des Jugendlichen zu aktualisieren. Bei einer negativen Entscheidung sollte dem Jugendlichen idealerweise eine kurze Begründung der Ablehnung mitgeteilt werden.

Damit der gesamte Algorithmus der Entscheidungsfindung terminiert, wird nach Ablauf einer vorgegebenen Zeitspanne ein Timeout-Signal erzeugt und ein entsprechender Hinweis auf dem mobilen Endgerät angezeigt. Der Jugendliche weiß dann, dass die SWOT zum aktuellen Zeitpunkt nicht entscheidungsfähig ist und kann die Freischaltung zu einem späteren Zeitpunkt erneut anfordern.

Als Entscheidungshilfe bei der Freigabe von Bluetooth-Datenverbindungen können lediglich Geräte- und Dateinamen, sowie Dateigrößen hinzugezogen werden. Hierbei besteht allerdings die Gefahr, dass diese Angaben eine geringe Qualität aufweisen, z. B. durch nicht aussagekräftige oder manipulierte Geräte- und Dateinamen. Die Eltern müssen über diese Sachverhalte informiert werden, sodass sie die Risiken korrekt einschätzen können.

5.4 Konfiguration des Jugendschutz-Profils per Webinterface

Wie bereits zu Beginn des Kapitels angedeutet, müssen die Eltern über ein Webinterface ein für ihr Kind individuelles Jugendschutzprofil konfigurieren (siehe Abbildung 4).

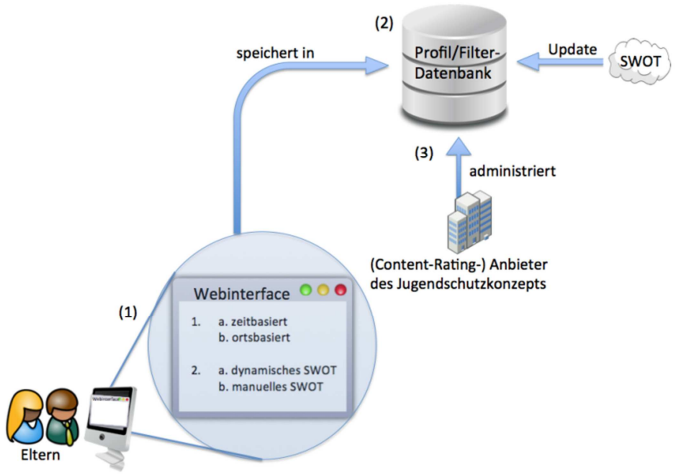

Abbildung 4: Profilkonfiguration über ein Webinterface

Eine mögliche Zeitvorgabe wäre beispielsweise werktags in der Zeit von 08.00 bis 15.00. So könnte das Erstellen von gefährdeten Inhalten während des Schulbetriebes unterbunden werden, ohne die Gerätefunktion der Kinder und Jugendlichen in ihrer Freizeit einzuschränken. Neben der manuellen Festlegung dieser Zeit könnte auch ein vordefinierter Zeitplan auf Grundlage der Schulferien des zugehörigen Bundeslandes eingebunden werden.

Mit Hilfe der Positionsbestimmung kann zudem eine Aktivierung bzw. Deaktivierung von Funktionen an den Ort gekoppelt werden. Das Webinterface kann zu diesem Zweck im Sinne eines sogenannten Mashups mit Google Maps verknüpft werden, sodass die Eingabe des Ortes auch ohne Kenntnis der exakten geographischen Koordinaten möglich ist. Dadurch lässt sich eine automatische Abschaltung der Kamerafunktion auf dem Schulgelände realisieren.

In Kombination mit öffentlichen oder von Dienstleistern bereitgestellten Listen von Geodaten können Regeln auch auf mehrere Orte gleichen Typs angewendet werden (zum Beispiel auf allen Spielplätzen oder Schulhöfen im Bundesland). Der Ort lässt sich mittlerweile anhand vieler auf dem mobilen Endgerät vorhandenen Schnittstellen ermitteln, sodass die Abschaltung einer bestimmten Schnittstelle (GPS oder WLAN) nicht zwangsweise dazu führt, dass keine Positionsbestimmung mehr möglich ist.

Die ortsbasierte Konfiguration lässt sich selbstverständlich mit der zeitbasierten Konfiguration kombinieren. Sollte beispielsweise eine ortsbasierte Konfiguration durchgeführt worden sein und das mobile Endgerät des Kindes oder Jugendlichen trotz der vielen Möglichkeiten nicht durch eine Positionsbestimmung geortet werden können, so greift die zeitbasierte Konfiguration.

Die Anpassung des Profils und der Filterlisten finden im Anschluss an die Konfiguration in einem evolutionären Prozess statt, der durch die Entscheidungen des SWOT über die Freischaltung von Funktionen bestimmt ist. Entscheidungen können temporäre oder dauerhafte Gültigkeit haben. Ein Eintrag in einer Profildatenbank könnte zum Beispiel wie in der Tabelle 1 abgebildet werden.

Tabelle 1: Beispiele für Einträge in der Profil-Datenbank

#	**Schnitt-stelle**	**Regeltyp (ein/aus)**	**Ort**		**Zeit**		
			Geogr. Koord.	Umkreis (km)	Wochentag (Bitmuster)	von	bis
1	Bluetooth	Aus	47° 25’ N 010° 59’ E	2	1111100	01.12.2011	29.12.2011
2	Mobiles Internet	Ein	47° 30’ N 010° 54’ E	0,5	0000011	01.01.2011	31.12.2011

Darüber hinaus wählen die Eltern auf dem Webinterface das Alter ihres Kindes aus, woraufhin die passenden Filterlisten des Anbieters angezeigt werden. Auf Alter und Kultur zugeschnittene Profil-Templates können zudem eine Empfehlung zur Konfiguration des Jugendschutzes bieten und anschließend individuell angepasst werden. Zur besseren Benutzbarkeit können die Eltern mittels zwischen einem Anfänger- und Expertenmodus wählen. Während der Expertenmodus viele Einstellungsmöglichkeiten bietet und die verwendeten Begriffe auf eine entsprechende Benutzergruppe zugeschnitten ist, enthält der Anfängermodus eine allgemeinere Bedienoberfläche mit grob gefassten Einstellungsoptionen sowie von der Technik stark abstrahierte Begriffe.

Nachdem die Grundeinstellungen vorgenommen wurden und die Standardprofile geladen wurden, können die Eltern entscheiden, welche Inhalte zusätzlich auf den Filterlisten gesperrt bzw. erlaubt sein sollen. Dadurch können sie auf die individuelle Medienkompetenz und das individuelle Nutzungsverhalten des Kindes Rücksicht nehmen. Die Konfiguration des Profils kann jederzeit durch die Eltern angepasst werden, zum Beispiel zur Unterstützung pädagogischer Maßnahmen.

5 Zusammenfassung und Ausblick

Die Verbreitung von internetfähigen mobilen Endgeräten nimmt zu. Einhergehend sind die rasante technische Entwicklung und ein wachsendes Angebot an Inhalten zu beobachten. Damit verbunden steigen die Gefahren für Kinder und Jugendlichen die nun vereinfacht an gefährdende Inhalte gelangen. Es wurde gezeigt, dass bisherige Maßnahmen zur Bekämpfung der drei Arten von Gefahren (Content, Contact, Commerce) Lücken aufweisen. Das vorgestellte Konzept zum Jugendschutz auf mobilen Endgeräten enthält einen Ansatz, wie die Lücken verringert oder gar geschlossen werden könnten.

Durch das kollektive Echtzeit-Entscheidungssystem SWOT wird ein Netzwerk erzeugt, das Entscheidungen unmittelbar dann treffen kann, wenn sie akut sind. So ist ebenfalls das dauerhafte Sperren von Schnittstellen oder dem mobilen Internet nicht mehr notwendig. Durch die temporäre Deaktivierung von Schnittstellen kann ein Jugendschutz gewährleistet werden, ohne dabei den Funktionsumfang des mobilen Endgerätes des Kindes oder Jugendlichen übermäßig zu beeinträchtigen.

Durch den angepassten Jugendschutz wird die individuelle Entwicklung des einzelnen Kindes und Jugendlichen unterstützt. Dies ist jedoch verbunden mit einer hohen Bereitschaft zur Mitarbeit seitens aller Beteiligten, da die Qualität des Jugendschutzes stark von der Aktivität der am SWOT teilnehmenden Personen abhängt. Denn falls eine entscheidungsbefugte Person nicht erreichbar ist, wird nur eine Person mit gleich hohem oder geringerem Vertrauenswert hinzugezogen.

Das vorgestellt Jugendschutzkonzept ist nicht allein für mobile Endgeräte bestimmt und kann sowohl in Kombination, als auch separat als Desktoplösung realisiert werden. So können auch an einem stationären Computer eingerichtete Profileinstellungen durch ein SWOT freigeschaltet werden. Eine reine Desktop-Lösung für die Teilnehmer des SWOT ist allerdings nicht sehr sinnvoll. Aus den bereits genannten Gründen sollten sie idealerweise auch mobil erreichbar sein.

Als Geschäftsmodell würde sich das Jugendschutz Konzept für einen Mobilfunkanbieter eignen. Dieser könnte sich dadurch von anderen Mobilfunkanbietern absetzen und sich dem Kunden als ein Unternehmen präsentieren, das einen besonderen Wert auf Jugendschutz legt und weiterreichende Maßnahmen, als die in der Selbstverpflichtungserklärung angegebenen sind, unternimmt. Durch das Aussperren von Jugendlichen aus dem mobilen Internet gehen außerdem viele potentielle Kunden verloren. Die Erweiterung des Produktportfolios um eine individuell anpassbare Lösung für einen mobilen Jugendschutz kann dem entgegenwirken und zur Erschließung eines neuen Kundenkreises beitragen.

Es ist jedoch festzuhalten, dass das Konzept allein kein Garant für einen vollkommenden Jugendschutz im mobilen Kontext sein kann. Es ist vielmehr als ein technisches Puzzleteil zu verstehen, welches nur im Zusammenhang mit ausgereiften regulatorischen und pädagogischen Konzepten wirkungsvoll ist. Es bietet den Eltern die Möglichkeit, die pädagogischen Maßnahmen mit einer technischen Infrastruktur gezielt zu unterstützen.

ISBN 978-3-88579-286-4

Literaturverzeichnis

[BF07] Bundesministeriums für Familie, Senioren, Frauen und Jugend: Handy ohne Risiko? Mit Sicherheit mobil - ein Ratgeber für Eltern, http://www.bmfsfj.de/BMFSFJ/Service/Publikationen/publikationen,did=101196.html, 2007 (aufgerufen am 10.04.2011)

[BW09] Bundesministerium für Wirtschaft und Technologie Pressestelle: Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Technologie (9. Ausschluss) http://www.bmwi.de/BMWi/Redaktion/PDF/Gesetz/entwurf-gesetzes-zur-bekaempfung-der-kinderpornographie-in-kommunikationsnetzen,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf, 2009 (aufgerufen am 09.04.2011)

[CI03] Childnet International. Annual Review: http://www.childnet-int.org/downloads/annualreview03.pdf, 2003 (aufgerufen am 09.04.2011)

[FB09] Pressemitteilung des FoeBuD e.V. vom 17.4.2009: http://www.foebud.org/aboutus/gegen-internetsperren-in-einer-freien-gesellschaft-foebud-richtet-anti-zensur-dns-server-ein/, 2009 (aufgerufen am 21.04.2011)

[FSM05] http://www.fsm.de/de/subkodex_mobilfunk,2005 (aufgerufen am 23.04.2011)

[FSM07] http://www.fsm.de/inhalt.doc/Selbstverpflichtung_Mobilfunk.pdf, 2007

[GR08] Grimm, Petra, et.al.: Gewalt 2.0, Berlin 2008

[HO11] Honegger, Döbeli Beat., Das iPhone-Projekt: http://www.projektschule-goldau.ch/das-iphone-projekt, o.J. (aufgerufen am 09.04.2011)

[JIM10] Medienpädagogischer Forschungsverbund Südwest (Hrsg.): JIM-Studie 2010 - Jugend, Information, (Multi-) Media., 2010

[JMS10] Jugendmedienschutz-Staatsvertrag: http://www.kjm-online.de/files/pdf1/JMStV_Stand_14_RStV_Lesefassung-Endversion_1_7_20101.pdf, 2010

[JSN09] jugendschutz.net – Zentralstelle der Länder für Jugendschutz im Internet: Chatten ohne Risiko?, 4. Auflage, http://www.jugendschutz.net/pdf/chatten_ohne_Risiko.pdf, 2009 (aufgerufen am 10.04.2011)

[KA08] Kammerl, Rudolf: 14- 16-jährige Jugendliche im Chat In: Dittler U./Hoyer M. (Hrsg) Aufwachsen in virtuellen Medienwelten, München 2008

[KL08] Kleinz, Torsten: Bundesfamilienministerin fordert Netzsperren gegen Kinderpornographie: http://www.heise.de/newsticker/meldung/Bundesfamilienministerin-fordert-Netzsperren-gegen-Kinderpornographie-217598.html, 2008 (aufgerufen am 21.04.2011)

[KR11] Krempl, Stefan: Aus für "Zensursula" und Websperren: "Das Problem an der Wurzel packen" http://www.heise.de/newsticker/meldung/Aus-fuer-Zensursula-und-Websperren-Das-Problem-an-der-Wurzel-packen-1222817.html(aufgerufen am 09.04.2011)

[KR11b] Krempl, Stefan: Schwarz-Rot in Sachsen-Anhalt will neuen Jugendmedienschutz-Staatsvertrag http://www.heise.de/newsticker/meldung/Schwarz-Rot-in-Sachsen-Anhalt-will-neuen-Jugendmedienschutz-Staatsvertrag-1228153.html, 2011 (aufgerufen am 09.04.2011)

[Sch01] SchuelerVZ.net: Jugendschutz http://www.schuelervz.net/l/protectminor (aufgerufen am 10.04.2011)

[Sch02] SchuelerVZ.net: Informationen für Eltern und Lehrer http://www.schuelervz.net/l/parents/ (aufgerufen am 10.04.2011)

[SN08] Stadt Nürnberg, Jugendamt (Hrsg.): Jugendliche und Handys - Ein geniales Gerät?, 2008