Erster Konzeptansatz von Sicherheitstypen: Sicherheitsbewusstsein von Kindern und Jugendlichen im Umgang mit dem Internet

Jana Fruth, Marcel Beskau, Matthias Volk, Anneke Meyer, Robin Richter, Jana Dittmann
Otto-von-Guericke-Universität Magdeburg
Fakultät für Informatik
Arbeitsgruppe Multimedia and Security
PO Box 4120, D-39016 Magdeburg
fruth@ovgu.de, dittmann@ovgu.de

Abstract: Bereits jüngere Kinder im Grundschulalter verwenden heute Computer, Tablet-PCs und Smartphones bzw. das Internet. Laut aktuellen Studien ist dabei das Sicherheitsbewusstsein von Kindern weniger gut ausgeprägt. So sind Kinder aufgrund ihrer Aktivitäten im Internet teilweise zahlreichen Bedrohungen im Internet ausgesetzt. Beispielsweise gehen viele Kinder sehr nachlässig mit ihren persönlichen Daten um. Diese könnten aber von Fremden und Kriminellen missbraucht werden. In diesem Artikel wird der Konzeptansatz der „Sicherheitstypen" basierend auf dem theoretischen Konstrukt der „Sicherheitsmentalitäten" bezüglich Kriminaliätsrisiken von D. Klimke für das Sicherheitsbewusstsein (IT-Security) von Kindern und Jugendlichen adaptiert. Der in diesem Artikel beschriebene Konzeptansatz stützt sich dabei auf eine umfangreiche Nutzerstudie (Fragebogenbefragung) von 157 Schülern/innen im Alter zwischen 10-15 Jahren eines Gymnasiums. Basierend auf dem Konzeptansatz sollen zukünftig Sensibilisierungsmaßnahmen (z.B. Sicherheitswarnmeldungen) zugeschnitten auf den jeweiligen Sicherheitstyp realisiert werden.

1 Einführung und Motivation

Heutzutage benutzen bereits Kinder im Grundschulalter (ab 6 Jahren) Computer, Tablet-PCs und Smartphones bzw. das Internet. Diese Technologien bieten Kindern und Jugendlichen[1] einerseits Chancen ihren Horizont zu erweitern. So wird ihnen beispielsweise durch die Nutzung sozialer Netzwerke (SN) ermöglicht, Kontakt zu Bekannten zu halten bzw. neue Menschen kennenzulernen. Andererseits sind aber auch Risiken durch die Benutzung der Informationstechnologie (IT) und Internetaktivitäten der Kinder zu bedenken. Laut [Liv11] haben beispielsweise ca. ein Drittel aller Kinder zwischen 9 und 16 Jahren, die ein Profil bei einem Sozialen Netzwerk haben, diese teils sehr persönlichen Profilinformationen (z.B. Familienname, Adresse, Telefonnummer) veröffentlicht. Nur weniger als die Hälfte setzt das SN-Profil auf privat, so dass nur als Freunde betitelte Personen des Profils dieses einsehen können. Dabei gibt es signifikante Unterschiede je nach Geschlecht, Alter und sozio-ökomomischem Status. So halten laut [Liv11] vor allem Mädchen und

[1] In diesem Artikel werden der Einfachheit halber Kinder und Jugendliche allgemein als Kinder bezeichnet.

Kinder aus Familien mit höherem sozio-ökomomischem Status ihre SNS-Profile eher privat, als Kinder aus anderen Gruppen. Die Veröffentlichung persönlicher Informationen in Sozialen Netzwerken könnten aber Dritte für ihre Zwecke (z.B. Ausspionieren, Kontaktierung des Kindes) missbrauchen. Um Kinder adäquat vor Onlinegefahren schützen zu können, müssen ihre Onlineaktivitäten betrachtet werden, durch die sie in Gefahr geraten können. Dazu wird in diesem Artikel der Konzeptansatz der „Sicherheitstypen" für das Sicherheitsbewusstsein (IT-Security) von Kindern und Jugendlichen vorgestellt. Der Ansatz basiert auf dem theoretischen Konstrukt der „Sicherheitsmentalitäten" von D. Klimke [Kli08], der Standpunkte von Personengruppen zu Kriminalitätsrisiken ausdrückt (siehe Kapitel 2). Der in diesem Beitrag beschriebene Konzeptansatz der Sicherheitstypen stützt sich dabei auf Vorarbeiten des Netzwerkes EU Kids Online[2] und auf eine eigene Nutzerstudie (Fragebogenbefragung) von 158 Schülern/innen im Alter zwischen 10-15 Jahren eines Gymnasiums in Nordrhein-Westfalen. Basierend auf dem Konzept der Sicherheitstypen sollen zukünftig Sensibilisierungsmaßnahmen (z.B. Sicherheitswarnmeldungen) zugeschnitten auf den jeweiligen Nutzer (Sicherheitstyp) realisiert werden.

Folgende **Forschungsfragen** sollten mit der Nutzerstudie (s. Kap. 4) beantwortet werden:

1. Lassen sich bestimmte Klassen von Sicherheitstypen für das Sicherheitsbewusstsein von Kindern und Jugendlichen bestimmen (kurz: *Klassen von Sicherheitstypen*)?

2. Wenn ja, was zeichnet eine bestimmte Klasse eines Sicherheitstyps aus (kurz: *Besonderheiten des Sicherheitstyps*)?

3. Gibt es einen Unterschied zwischen erfahrenen Kindern (IT, Internetnutzung) und unerfahrenen Kindern (kurz: *Erfahrungsunterschiede*)?

4. Wie wirken sich Belehrungen und Regeln von Eltern und Lehrern auf das Sicherheitsbewusstsein von Kindern und Jugendlichen aus (kurz: *Belehrungen und Regeln*)?

Der Beitrag gliedert sich wie folgt: In Kapitel 2 wird das Konzept der „Sicherheitsmentalitäten" und der *Stand der Technik* hinsichtlich der Ermittlung und Schulung des Sicherheitsbewusstsein (IT-Security) näher vorgestellt. Im darauf folgenden Kapitel 3 werden die *Methodik* zur Ermittlung des Sicherheitsbewusstsein von Kindern und Jugendlichen mittels eines Fragebogens erläutert, sowie Hypothesen zu den Ergebnissen der Befragung thematisiert. Die Durchführung, sowie Testergebnisse der eigentlichen *Nutzerstudie* und das daraus entwickelte Konzept der Sicherheitstypen werden in Kapitel 4 vorgestellt. Dieser Beitrag schließt mit der *Zusammenfassung* der Ergebnisse dieses Artikels und einem *Ausblick* über zukünftige Forschungsarbeiten.

[2] www.eukidsonline.net, letzter Zugriff: 22. April 2013

2 State of the art: Sicherheitsmentalitäten, Ermittlung und Schulung des IT-Sicherheitsbewusstseins von Kindern

Im folgenden Kapitel wird zum Einen der Stand der Forschung zum Konzept der Sicherheitsmentalitäten bezüglich Kriminalitätsrisiken auf Grundlage von [Kli08] dargelegt. Zum anderen wird der Stand der Forschung zum Sicherheitsbewusstsein von Kindern und Jugendlichen bezüglich potentieller Gefahren beim Surfen im Internet kurz erläutert.

2.1 Konzept der Sicherheitsmentalitäten

In diesem Kapitel soll das Konzept der „Sicherheitsmentalitäten“, wie es in [Kli08] definiert ist, näher beschrieben werden. Das Konzept ist Grundlage, des in diesem Artikel in Kapitel 4 beschriebenen Konzepts der „Sicherheitstypen“.

Laut Klimke [Kli08] werden „Sicherheitsmentalitäten“ wie folgt definiert:
”*Mit Sicherheitsmentalitäten soll die systematische Verknüpfung von Sicherheitsdenken, Gefahrenwahrnehmungen und Praktiken, mit Risiken umzugehen, bezeichnet werden. Die Handlungsebene der Schutzmaßnahmen, die Meinungen zur Inneren Sicherheit, die wahrgenommenen Bedrohungen und Erwartungen an die Sicherheitsinstitutionen umfassen dessen Dimensionen. Mit den Sicherheitsmentalitäten wird zusammengebracht, was zusammen gehört: Die Schemata des Denkens, Handelns und Wahrnehmens in Bezug auf Kriminalitätsrisiken. ...*“

Das Konzept soll laut der Autorin als Alternative zur „Erfassung und Erklärung von Unsicherheit“ zu gängigen Konzepten der Kriminalitätsforschung dienen, um eine komplexere Analyse von Einstellungen zu Kriminalitätsrisiken zu ermöglichen. Die Autorin schlägt dazu fünf Typen von Sicherheitsmentaliäten vor. Jedem einzelnen Typen werden bestimmte Merkmalsausprägungen in bestimmten Dimensionen zugeordnet (siehe Tab. 1, ausgewählte Dimensionen). Die in Tabelle 1 ausgewählten Dimensionen der verschiedenen Sicherheitsmentalitäten bilden das eigene Sicherheitsgefühl, Schutzmaßnahmen im öffentlichen und privaten Bereich, sowie deren Wirkung ab. Diese Dimensionen wurden ausgewählt, da sie unserer Meinung nach etwas über das Sicherheitsbewusstsein der untersuchten Zielgruppe aussagen. Die ermittelten Dimensionen von Klimke ähneln den Kriterien zur Ermittlung des Sicherheitsbewusstseins von Kindern und Jugendlichen in Kapitel 4.2. Es wurde ebenso wie in der Studie von Klimke versucht, Aussagen zum Sicherheitsgefühl und zu den verwendeten Schutzmassnahmen der Befragten zu gewinnen. Im Unterschied dazu wurden aber in unserer Studie nicht die Einstellungen von Erwachsenen zu Kriminalitätsrisiken, sondern das Sicherheitsbewusstsein von Kindern und Jugendlichen bei ihrer Internetnutzung untersucht.

Tabelle 1: Typen von Sicherheitsmentaliäten (ausgewählte Dimensionen nach [Kli08])

Dimension	**Pragmatischer**	**Ängstlicher**	**Eingreifer**	**Anklagender**	**Responsibilisierter**
Sicherheitsgefühl	Zu einem gelassenen, sicheren Gefühl gemahnt man sich	Generell ängstlich	Selbstsicher und wehrhaft	Hohe Unsicherheit und Hilflosigkeit wird appellativ bekundet	Hohes Sicherheitsgefühl, schließlich weiß man sich auch gut zu schützen
Schutzmaßnahmen im öffentlichen Raum	Sorgfältiges Abwägen von Notwendigkeit und Beeinträchtigung, Wachsame und vermeidende Strategien	Ausufernde Vermeidungsstrategien und höchste Alarmbereitschaft	Selbstsicheres Auftreten, Wachsamkeit und Wehrhaftigkeit sowie schlichte Intervention	Vermeidung gefährlicher Viertel, ansonsten eher leichtsinnige Verhaltensweisen	Wachsamkeit und Wehrhaftigkeit
Schutzmaßnahmen für die Wohnung	Minimal, man will sich nicht verbarrikadieren	Wenig, denn in der Wohnung fühlt man sich recht sicher	Man sorgt für Sicherheit und Ordnung auch für die Nachbarschaft	Wenig, denn der Nahraum wird als sicher und angenehm empfunden	Wenige effiktive, eher technische Vorkehrungen
Wirkung persönlicher Schutzpraktiken	Ausreichend, bis etwas passiert	Eigene Schutzpraktiken können prinzipiell nie ausreichen	Mit dem eigenen Sicherheitsengagement ist man sehr zufrieden	Klage über die beeinträchtigenden und überdies kaum wirksamen Schutzmaßnahmen	Schutzmaßnahmen können wirksam abschrecken

2.2 IT-Security-Sicherheitsbewusstsein von Kindern und Jugendlichen

Unter ***Sicherheitsbewusstsein***[3] bezüglich Gefahren der IT-Security wird in diesem Artikel das Erkennen, das Voraussehen und vorbeugende Maßnahmen gegen Gefahren bezüglich der Nutzung von IT und dem Internet verstanden.

Die ***Forschung auf dem Gebiet des IT-Securitybewusstsein von Kindern und Jugendlichen*** ist relativ jung. Ergebnisse wissenschaftlicher Studien[4] [Bra10, Byr08, O'B09, Has06, LH09, LHGO11] zu diesem Forschungsbereich sind erst vor ein paar Jahren veröffentlicht worden. Die wohl umfangreichsten sind die „EU Kids Online" Studien [LH09, LHGO11]. Diese fassen Ergebnisse von Studien aus 25 Ländern zum IT-Securitybewusst-

[3] In der Literatur (siehe [Lim95] und [Cop85]) wird auch oft von Gefahrenbewusstsein gesprochen. Darunter wird das Bewusstsein für gefährliche und sichere Situationen verstanden. Der von uns verwendete Begriff des IT-Security-Bewusstseins beinhaltet beide Kategorien.

[4] In Deutschland wird vom Medienpädagogischer Forschungsverbund Südwest in einer Langzeitstudie der Medienumgang von Kindern und Jugendlichen untersucht [BSKR10, BR11]. Schwerpunkt ist die Untersuchung des Medienkonsums, dabei werden auch einige wenige Fragen zum Sicherheitsbewusstsein von Kindern und Jugendlichen gestellt.

sein von ca. 25000 Kindern und Jugendlichen zwischen 6 und 17 Jahren in der gesamten EU über einen längeren Zeitraum (2006-2011) zusammen und vergleichen diese. Aus diesen Studien geht hervor, dass Kinder kaum für Bedrohungen aus der Welt der IT-Security sensibilisiert sind. Im Vergleich zur EU Kids Online Studie [LHGO11] mit ca. 25000 Teilnehmer/innen, ist die im Kapitel 4 beschriebene Studie mit 158 Schüler/innen relativ klein angelegt. Die Stichprobengröße ist aber ausreichend, um einige Aussagen zum Sicherheitsbewusstsein von Kindern und Jugendlichen treffen zu können. Beide Studien haben teilweise ähnliche Fragestellungen, aber es gibt auch Unterschiede. Beide Studien erheben Informationen zum soziodemographischen Hintergrund, der Nutzung von IT, des Internets und sozialer Netzwerke durch Kinder. Weiterhin werden Fragen zu Hilfestellungen bei der Internetnutzung und Sicherheitsschulung durch die Eltern und Lehrer gestellt, wobei in der EU Kids Online Studie detaillierter Fragen an die Eltern mit einem extra Fragebogen erhoben werden. In unserer, in Kapitel 4 beschriebenen Studie, werden genauere Fragen zu den Themen sichere Nutzung sozialer Netzwerke und Handys/Smartphones, sowie schlechte Erfahrungen im Internet (Angabe der Webseite und Freitext für eigene Beschreibung und eigene Gegenmaßnahmen) gestellt. Weiterhin wird den Kindern die Möglichkeit geboten, eigene Ideen zur sicheren Internetgestaltung anzugeben (eine Seite dafür reserviert).

Wie kann nun das Sicherheitsbewusstsein von Kindern erhoben werden? Gängige ***Methoden zur Ermittlung des IT-Securitybewusstseins*** sind *Umfragen* in Form von Interviews und Fragebögen (oft auch in Kombination miteinander gerade für jüngere Kinder geeignet, wie in [LHGO11]). Die in diesem Artikel beschriebene Umfrage ist eine reine Fragebogenbefragung ohne Interviewcharakter, da ältere Kinder zwischen 10 und 15 Jahren befragt wurden. Eine weitere Methode zur Ermittlung des IT-Security-Sicherheitsbewusstseins sind *situationsspezifische Tests*. Beispielsweise könnten Kinder die Aufgabe bekommen, sich bei einem Sozialen Netzwerk anzumelden und ein eigenes Profil zu erstellen (inklusive des Festlegen eines Passwortes). In diesem Szenario könnten direkt die Aktivitäten der Kinder hinsichtlich der Umsetzung von Sicherheitsmechanismen und Sicherheitsmaßnahmen (IT-Security) überprüft werden [BVMR13].

Präventiv- und Sensibilisierungsmaßnahmen zur Stärkung des IT-Security Bewusstseins von Kindern und Jugendlichen: Im Vergleich zur Sicherheitsschulung für alltägliche Gefahren (z.B. im Straßenverkehr, im Haushalt) [Cop85, Lim97] gibt es derzeit noch relativ wenige Konzepte zur Sensibilisierung von Kindern und Jugendlichen vor Gefahren aus dem Bereich der IT-Security. Dieser Abschnitts basiert zum größten Teil auf [BVMR13]. Kinder (vor allem ältere Kinder in der Sekundarstufe) werden teilweise im ***Schulunterricht*** auf Gefahren bei der Internetnutzung hingewiesen, wobei diese Sensibilisierungsmaßnahmen nicht immer detailliert im Lehrplan stehen müssen. Gerade für jüngere Kinder im Grundschulalter gibt es hier seitens der Schule[5] eher wenige Angebote. Eine weitere Möglichkeit der Sensibilisierung von Kindern und Jugendlichen ist das sogenannte ***peer-to-peer-teaching*** [LH09]. Kinder unterrichten sich in diesem Fall gegenseitig. Grundlage des Konzeptes ist die Beobachtung, dass Kinder sehr oft von Gleichaltrigen, Freunden oder Gleichgesinnten lernen. Das ermöglicht es Kindern und Jugendlichen,

[5]Diese Aussage stützt sich auf Gesprächen mit Lehrern aus dem Grundschul- und Sekundarbereich in Sachsen-Anhalt. Dabei können innerhalb eines Bundeslandes und einer Stadt die Unterrichtsangebote in einer Klassenstufe je nach Schulträger stark variieren, z.B. bieten einige Grundschulen schon ab der ersten Klasse Computerunterricht an, wärend an anderen Schulen dieser Unterricht erst in höheren Klassenstufen möglich ist.

sich in ihrer eigenen Sprache für Gefahren zu sensibilisieren. Wichtige Partner bei der Sicherheitssensibilisierung sind auch die ***Eltern und Sorgeberechtigten*** der Kindern. Durch ***Initiativen*** werden Eltern darauf hingewiesen, ihre Kinder auch im Internet zu schützen. Ein Beispiel ist die EU-Initiative "klicksafe"[6], die z.B. mittels TV-Werbung Eltern auffordert, auch ihre Kinder im IT-Bereich nicht zu vernachlässigen.
Um Kinder vor den Gefahren des Internet zu schützen, gibt es restriktive Methoden, wie z.B. ***sichere Surfräume***. Dazu zählen u.a. sichere Suchmaschinen für Kinder (z.B. FragFinn.de[7]), sowie Jugendschutzsoftware (z.B. JuSProg[8]). Diese Software filtert und sperrt auf Grundlage von Listen Webseiten mit nicht kindgerechten Inhalten. In [KHFD12] haben wir bereits ein ***allgemeines Sicherheitssymbol*** für Kinder vorgestellt, das auf Webseiten platziert werden könnte. Das Symbol ist in den Farben einer Fußgängerampel kodiert, was Kinder aus ihrem Alltag kennen. „*Dieses* [das einheitliche Sicherheitssymbol] *soll in der praktischen Umsetzung mehr Schutz für die Kinder bieten, indem Kinder bereits beim ersten Besuch der Webseite das Sicherheitsniveau dieser Seite einschätzen können [...]* " [KHFD12]. Dieses Sicherheitssymbol sollte kindgerecht Kinder vor nicht kindgerechten und sicherheitsgefährdenden Inhalten warnen und Kinder ermutigen bei Bedarf Sicherheitsmaßnahmen zu ergreifen (z.B. Hilfe einholen). Ein weiteres Konzept wäre die Nutzung von ***Metaphern*** [KHFD12] aus der kindlichen Erfahrungswelt zur Erklärung von Sicherheitsgefahren und Sicherheitsmaßnahmen im Internet. So könnte beispielsweise IT-Sicherheitsbegriffe (z.B. Vertraulichkeit) auf ein für Kinder bekanntes Szenario übertragen werden (z.B. könnten Passwörter metaphorisch als Schlüssel des Kinderzimmers oder Tagebuches symbolisiert werden).
Entwicklungspsychologische Forschungen bestätigen, das Kinder oft spielerisch lernen [Ber11]. Diese Eigenschaft könnte auch für die IT-Erziehung genutzt werden [Sac04]. Eingesetzt werden könnten geeignete Computerspiele die als ***Lernsoftware*** dienen. Beispiele dafür finden sich auf der Schweizer Homepage „Security4Kids"[9]. Hier können Kinder anhand interaktiven Geschichten die Funktionsweise des Internets mit seinen Gefahren erfahren.

3 Methodik

Ziel des Artikels war es, erste Ergebnisse aus der umfangreichen Studie mit 160 Teilnehmern vorzustellen. Der Fokus lag auf der Ermittlung des Sicherheitsbewusstseins der befragten Kinder und Jugendlichen und der Ableitung von Sicherheitsklassen. In diesem Kapitel wird die Methodik zur Berechnung beider Ergebnisse erläutert. Grundlage bildet ein selbst entworfenen Fragebogen[10]. Dieser wurde unter Beachtung aktueller Datenschutzgesetze [Bun09] erstellt, sodass die anonymen Antworten keine Rückschlüsse auf das ausfüllende Kind bzw. Jugendliche geben. Um sicherzustellen, dass die Fragen auch richtig verstanden werden, wurden viele Fragen als Aussage formuliert, z.B. "Ich bin ...

[6] www.klicksafe.de, letzter Zugriff 24. 4. 2013
[7] www.fragfinn.de, letzter Zugriff 24. 4. 2013
[8] www.jugendschutzprogramm.de, letzter Zugriff 24. 4. 2013
[9] www.security4kids.ch, letzter Zugriff 24. 4. 2013
[10] Hinweis: Vor der Befragung der Kinder und Jugendlichen wurde das Einverständnis der Eltern eingeholt.

Jahre alt". So mussten die Kinder nur noch eine Lücke in dem Aussage-Satz ausfüllen oder konnten die jeweiligen Antwortmöglichkeiten ankreuzen [BVMR13]. Es wurden 23 Fragen mit Blick auf die zu untersuchenden Themen gestellt. Dabei wurde zunächst nach *sozio-demographischen Eigenschaften* (Alter und Geschlecht der Kinder) und *Vorerfahrungen* (Nutzung internetfähiger Geräte, erste Internetnutzung und der Nutzungshäufigkeit des Internets) gefragt. Weiterhin wurden Informationen zu *sozialen Netzwerken (SN)* (Nutzer von bestimmten SN, Sicherheitseinstellungen - Passwörter, Profil) erfasst. Ebenfalls wurde die *Handy/Smartphone*-Nutzung (genutzte Apps und Wissen über Nutzung privater Daten) erhoben. Zusätzlich wurde gefragt, ob und von wem sie bereits *Informationen und Grundregeln zum sicheren Umgang mit dem Internet* erhalten haben und von wem sie sich *weitere Informationen und Hilfen* wünschen würden. Abschließend wurde ermittelt, mit welchen *Hilfen* sich Kinder sicherer im Internet fühlen, welche *schlechten Erfahrungen* sie bereits beim Surfen im Internet erlebt haben (einschließlich der eigenen Gegenmaßnahmen) und welche *eigenen Ideen* sie für eine Gestaltung eines sicheren Internets haben.

Methodik zur Berechnung der Sicherheitstypen: Das *Sicherheitsbewusstsein* der Kinder wurde aus bewerteten Antworten der Befragten errechnet. In diesem Zusammenhang wurde sich Methoden der deskriptiven/beschreibenden Statistik bedient. Zur Berechnung des Sicherheitsbewusstseins wurden ausgewählte Antworten auf Fragen benutzt, die unserer Meinung nach Hinweise auf einen sicherheitsbewussten Internetumgang der Befragten geben könnten (siehe Tab. 2, Kriterium). Zunächst wurden die Antworten der ausgewählten Fragen mit Punkten auf einer Skala von 0 (nicht sicherheitskritisch) bis 4 (sicherheitskritisch) bewertet. Da die Fragen heterogene Antwortmöglichkeiten boten (Mischung aus Ja-Nein-Antworten und Mehrfachantworten) wurde im nächsten Schritt das Ergebnis jeder Frage gewichtet (siehe Tab. 2, Wichtungsfaktor). Die aus unserer Sicht aussagekräftigsten Kriterien zu Beurteilung des Sicherheitsbewusstseins von Kindern ein höheres Gewicht (z.B. Angabe privater Daten im Internet) als weniger aussagekräftige Kriterien (z.B. Kenntnis ungefragten Versendens personenbezogener Daten der Apps). Alle gewichteten Ergebnisse wurden danach aufsummiert. Die dadurch ermittelte Punktzahl symbolisiert das Sicherheitsbewusstsein der Kinder.

Tabelle 2: Berechnung des Sicherheitsbewusstseins aus ausgewählten gewichteten Antworten

Kriterium	**Max.Punkt-zahl**	**Wichtungs-faktor**	**gewichteter Max.wert**
Angabe privater Daten im Internet	19	2	38
Mitglied bei einem / mehreren SN	28	1	28
Schlechte Erfahrungen im Internet	7	2,5	17,5
Handy mit Internetzugang	11	1	11
Nutzung von Apps	18	0,5	9
"privat"-Stellen des SN-Profils	3	2,5	7,5
Mitglied bei mehreren SN und Passwortverwendung	4	1,5	6
Wissen ungefragtes Versenden von Daten an App-Ersteller	2	2	4

Ausgehend von den Antwortmöglichkeiten des Fragebogens wurden *drei Klassen von Sicherheitstypen*, die das Sicherheitsbewusstsein der befragten Kinder ausdrücken, festgelegt (Clusteranalyse). Ziel war es, schnell ohne großen Aufwand erste Ergebnisse aus der

Fragebogenbefragung zu ziehen. Daher wurde sich einfacher Mittel bedient und aufwändige automatisierte Clusterverfahren (hierarchische und partitionierende Clusteranalysen) gemieden [Bor05]. Die Clustereinteilung wurde durch visuelles Klassieren in einem Histogramm, der alle Punktzahlen des Sicherheitsbewusstseins der Kinder darstellt, durchgeführt. Dabei wurde die Position des ersten Trennwertes und die Anzahl der Trennwerte vorgegeben. Das Statistikanalyseprogramm SPSS[11] berechnete dann automatisch die Breite des folgenden Clusters und damit die zweite Clustergrenze. Die Clustergrenzen wurden so gesetzt, dass sich die meisten Kinder in der Klasse des Sicherheitstyps 2 (mittleres Sicherheitsbewusstsein) befinden. Da die Klasse des Sicherheitstyps 1 (hohes Sicherheitsbewusstsein) und Sicherheitstyps 3 (niedriges Sicherheitsbewusstsein) eher als Ausnahme betrachtet wurden. Es sollte evaluiert werden, warum gerade diese "Ausreißer" sich in diesen Klassen befinden. Um zusätzlichen Wissen über die Eigenschaften der einzelnen Sicherheitsklassen aus den Ergebnissen zu ziehen, wurden Kontingenztafeln/Kreuztabellen verwendet. Mit diesem Verfahren kann anhand der Häufigkeiten ermittelt werden, ob zwei Merkmale gleichzeitig auftreten (z.B. Alter und Sicherheitsklasse) [Bor05].

Im Folgenden werden die **Hypothesen** vorgestellt, die durch die Nutzerstudie in Kap. 4 zu beweisen oder zu widerlegen sind:

1. Es lassen sich bestimmte Klassen von Sicherheitstypen für das Sicherheitsbewusstsein von Kindern bestimmen (zu Frage 1 - *Klassen von Sicherheitstypen*).
2. Im Vergleich zu unerfahrenen und jüngeren Kindern scheinen erfahrene und ältere Kinder ein ausgeprägteres Sicherheitsbewusstsein aufgrund ihrer Erfahrung zu haben (zu Frage 3 - *Erfahrungsunterschiede*).
3. Ein Kriterium das einen Sicherheitstyp vom anderen unterscheidet, ist die Erfahrung beim Umgang mit IT, Smartphones und dem Internet (zu Frage 2 - *Besonderheiten des Sicherheitstyps*).
4. Kinder, denen weniger Regeln bei der Internetnutzung vorgeschrieben werden, scheinen ein geringeres Sicherheitsbewusstsein zu haben (zu Frage 4 - *Regeln*).
5. Kinder, die öfter an Belehrungen teilgenommen haben, scheinen ein ausgeprägteres Sicherheitsbewusstsein zu haben (zu Frage 4 - *Belehrungen*).
6. Unerfahrene und jüngere Kinder wünschen eher *persönliche Hilfestellungen* (z.B. durch Eltern und Lehrer), aufgrund des Unsicherheitsgefühls im Internet (zu Frage 3 - *Erfahrungsunterschiede*).

4 Nutzerstudie

Mit Hilfe des in Kapitel 3 beschriebenen Fragebogens wurde im Dezember 2012 in den Klassenstufen 5 bis 8 an einem Gymnasium in Nordrhein-Westfalen eine Befragung von

[11] http://www-01.ibm.com/software/de/analytics/spss/, letzter Zugriff: 27. Juni 2013

157 Kindern durchgeführt. Die teilnehmenden Kinder haben den Fragebogen selbst (ohne weiteres Interview) ausgefüllt. Die Beantwortung der Fragen dauerte ca. 10 bis 15 Minuten. Das Ziel der durchgeführten Umfrage war die Ermittlung des Sicherheitsbewusstseins von Kindern und Jugendlichen im Bereich der IT-Security. In den folgenden Abschnitten werden nun die Ergebnisse und die dazugehörigen Auswertungen präsentiert. Da die Stichprobengröße sehr gering ist, wurde eine deskriptive Betrachtung der Ergebnisse vorgenommen [BVMR13].

4.1 Testergebnisse

Der Fokus der Umfrage lag auf der Ermittlung des Sicherheitsbewusstseins von Kindern und Jugendlichen. Die befragten Kinder waren im Alter zwischen 10 und 15 Jahren. Die große Mehrheit (70%) der Kinder war zwischen 11 und 13 Jahre alt. Ca. 60% der Befragten waren Mädchen, ca. 40% waren Jungen. Alle Kinder nutzen das Internet, davon gaben 60% an, es täglich bzw. mehr als einmal täglich zu nutzen. Die Kinder scheinen schon sehr früh mit dem Internet in Berührung zu kommen. So gaben mehr als die Hälfte der Probanden an, mit der Internetnutzung schon vor ihrem zehnten Lebensjahr begonnen zu haben.

Das Sicherheitsbewusstsein für jedes befragte Kind wurde nach der in Kapitel 3 beschriebenen Methodik ermittelt. Anschliessend wurden drei Klassen von ***Sicherheitstypen*** aus einer Punktzahl, die das Sicherheitsbewusstsein symbolisiert, berechnet. In Abhängigkeit von den Ergebnissen, wurden die Kinder den einzelnen Sicherheitstypklassen zugeordnet: Sicherheitstypklasse 1 (hohes Sicherheitsbewusstsein) - geringe Punkzahl (bis 6,5), Sicherheitstypklasse 2 (mittleres Sicherheitsbewusstsein) - mittelwertige Punkzahl (zwischen 6,5 und 44,5), Sicherheitstypklasse 3 (niedriges Sicherheitsbewusstsein) - hohe Punkzahl (ab 44,5). Wesentliche Eigenschaften, die die Klassen von Sicherheitstypen kennzeichnen sind in Tabelle 3 aufgelistet.

In der Klasse des ***Sicherheitstyp 1*** sind eher jüngere Kinder (zw. 10 und 13 Jahren) und anteilig gleich viel Mädchen wie Jungen. Im Vergleich zu den Kindern der beiden anderen Sicherheitstypklassen, haben diese Kinder weniger technische Vorerfahrungen: nur knapp die Hälfte nutzt das Internet täglich (ca. 45%) und nur wenige sind in SN angemeldet (4%). Einige Kinder haben schon an Sicherheitsbelehrungen für die Internetnutzung teilgenommen bzw. ihre Eltern haben ihnen bestimmte Regeln zur Internetnutzung vorgeschrieben. Von diesen Kindern geben alle an, keine persönlichen Daten im Internet preiszugeben. Von den wenigen Kindern die in SN angemeldet sind, haben alle ihr Profil auf privat gestellt. Nur wenige der Kinder des Sicherheitstyps 1 haben schlechte Erfahrungen im Internet gemacht. Um das Sicherheitsgefühl im Internet zu erhöhen wünschen sich mehr als die Hälfte dieser Kinder eine Begleitperson an ihrer Seite. Weiterhin wünscht sich die Mehrzahl der Kinder dieses Sicherheitstyps mehr Informationen zur sicheren Internetnutzung von ihren Eltern (100%) und ihrer Schule (ca. 70%).

Zum ***Sicherheitstyp 3*** gehören eher ältere Kinder (zwischen 12 und 14 Jahren) und etwas mehr Jungen (57%) als Mädchen. Diese Kinder haben im Vergleich zu den beiden anderen Sicherheitsklassen mehr Erfahrungen mit IT und dem Internet gesammelt. So nutzen laut

Tabelle 3: Eigenschaften von Sicherheitstypen nach [BVMR13] (Gerundete prozentualen Angaben.)

Eigenschaften der Sicherheitstyp-Klassen	**Sicherheitstyp 1**	**Sicherheitstyp 2**	**Sicherheitstyp 3**
Anteile der Befragten	14,6%	77,7%	7,6%
Sozio-demographische Eigenschaften			
Alter	10 - 13 Jahre	10 - 15 Jahre	12 - 14 Jahre
Geschlechterverteilung	gleich	mehr Mädchen (60%)	mehr Jungen (57%)
Vorerfahrungen			
tägliche Internetnutzung	45%	60%	100%
Teilnehmer in SN	4% bei Twitter, 95% keins	in mehreren: u.a. 35% Facebook, 34% ICQ, 33% keins	in mehreren: u.a. 83% Facebook, 75% ICQ, 0% keins
Nutzung eines Smartphones mit Internetzugang	eher wenige (40%)	mehr als die Hälfte (60%)	jeder (100%)
Nutzung von Apps	50% Google+	40% Facebook u. andere	92% Facebook u. andere
Teilnahme an Sicherheitsbelehrungen	11% Informatik, 42% Belehrung, 16% Info.material, 37% keine	15% Informatik, 56% Belehrung, 13% Info.material, 23% keine	17% Informatik, 67% Belehrung, 25% Info.material, 25% keine
Beurteilung des Sicherheitsbewusstseins			
persönliche Angaben im Internet	keine	30% Name und E-Mail-Adresse, 1% Adresse und Telefonnummer	80% Name, 90% E-Mail-Adresse, 17% Adresse und Telefonnummer
Gleiche Logindaten in verschiedenen SN:	keine Angabe	25% gleiche, 30% verschiedene	60% gleiche, 40% verschiedene
SN: privates Profil	96% keine Angabe, 4% ja	32% keine Angabe, 48% ja, 8% nein, 12% nicht bekannt	50% ja, 17% nein, 33% nicht bekannt
Versenden von Daten an App-Ersteller	48% bekannt	53% bekannt	83% bekannt
Verhaltensregeln der Eltern für das Internet	5% keine Regeln, 36% Virenscanner aktiv, 50% unbekannte Mails nicht öffnen, 36% Erstellung sicheres Passwort	8% keine Regeln, 39% Virenscanner aktiv, 41% unbekannte Mails nicht öffnen, 31% Erstellung sicheres Passwort	0% keine Regeln, 50% Virenscanner aktiv, 17% unbekannte Mails nicht öffnen, 17% Erstellung sicheres Passwort
Hilfen zur Erhöhung des Sicherheitsgefühls im Internet	Begleitung durch erfahrenen Internetbenutzer (mehr als 50%) und erklärende Texte auf Internetseiten	Begleitung durch erfahrenen Internetbenutzer (mehr als 14%) und mehr Bilder zur Erklärung (15%)	mehr Bilder zur Erklärung (35%)
Schlechte Erfahrungen im Internet	5% ungewollte Fotoveröffentlichung	5% ungewollte Fotoveröffentlichung, 3% Virus in E-Mail Anhang, 5% fremdes Einloggen in Webaccount	27% ungewollte Fotoveröffentlichung, 27% Virus in E-Mail Anhang, 36% fremdes Einloggen in Webaccount
Sicherheitsbewusstsein	eher hohes	eher mittleres	eher niedriges

ihrer eigenen Angaben, alle Kinder des Sicherheitstyp 3 täglich das Internet, besitzen ein Handy mit Internetzugang und sind in mindestens einem sozialen Netzwerk angemeldet. Obwohl sie mehr für Sicherheitsgefahren im Internet sensibilisiert scheinen (z.B. Teilnahme an Sicherheitsbelehrungen, Wissen um Appgefahren, schlechte Erfahrungen im Internet), veröffentlichen sie vergleichsweise mehr persönliche Informationen über sich im

Internet (z.B. Adresse, Telefonnummer) als Kinder aus den beiden anderen Sicherheitstypklassen (siehe Abb. 1). Weiterhin verwenden 60% der Nutzer mehrerer SN den gleichen Benutzernamen, das gleiche Passwort oder identische Logindaten, wie sie auch in anderen SN verwenden. 67% der Kinder dieses Sicherheitstyps wünschen sich hauptsächlich mehr Informationen zur sicheren Internetnutzung von ihren Eltern und nur ca. 17% von ihrer Schule.

Kinder des ***Sicherheitstyps 2***: gehören zu allen befragten Altersklassen (zw. 10 und 15 Jahren), dazu zählen mehr Mädchen (60%) als Jungen. Diese Sicherheitstypklasse stellt ein Mittel zwischen den beiden anderen Klassen dar und wird hier nicht näher erklärt (s. Tab. 3).

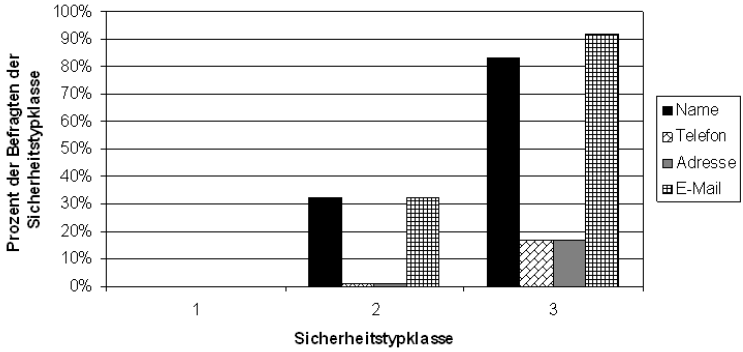

Abbildung 1: Persönliche Angaben im Internet in Zusammenhang mit der Sicherheitstypklasse

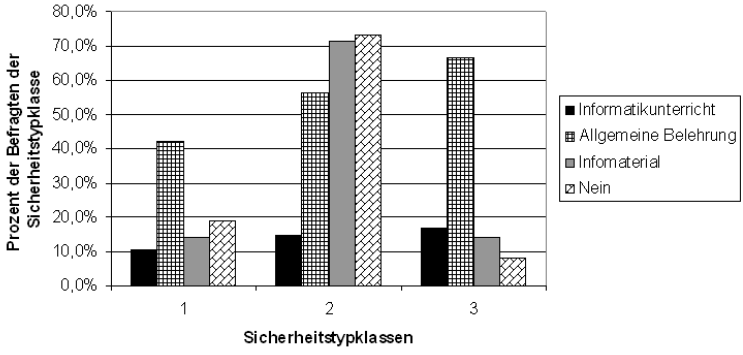

Abbildung 2: Bereits erhaltende IT-Security Belehrung pro Sicherheitstypklasse

4.2 Diskussion

Die im Kapitel 1 genannten Forschungsfragen und in Kapitel 3 genannten Hypothesen werden in diesem Abschnitt diskutiert. Um Zusammenhänge zwischen verschiedenen Ergebnissen der Umfrage ermitteln zu kön-nen, wurden Kreuztabellen erstellt (s. Kap. 3).

Es konnte eine ***Klassifizierung von Sicherheitstypen*** auf Grundlage einer Punktebewertung vorgenommen werden, was Hypothese 1 bestätigt. Die Einteilung in Clustern wurde allerdings nicht vollautomatisiert durchgeführt (s. Kap. 3) und ist daher anfechtbar. Das Ziel der Umfrage war es, das Verhalten der Kinder in diesen verschiedenen Klassen von Sicherheitstypen zu untersuchen und Aufschluss darüber zu geben, welches die ausschlaggebenden Punkte für dieses Verhalten sind.

Scheinbar geringes Sicherheitsbewusstsein älterer Kinder: Ein wichtiges Kriterium scheint das Alter zu sein. Es wurde festgestellt, dass *ältere Kinder* mehr persönliche Daten im Internet preisgeben als ihre jüngeren Schulkollegen. Das kann auf ein niedriges Sicherheitsbewusstsein hindeuten, was Hypothese 2 (Erfahrungsunterschiede) widerlegen würde. Im Kontrast dazu steht die These von Coppens Stufen des Sicherheitsbewusstseins, die aussagt, dass das Sicherheitsbewusstsein mit höherem Alter ansteigt [Cop85]. Dies deutet darauf hin, dass die Stufeneinteilung für die Entwicklung des Bewusstseins von Kindern für Gefahren für ihr Leib und Leben (Safety) nicht für das Bewusstsein für IT-Security Gefahren übernommen werden kann. Eine mögliche Erklärung wäre, dass die potentiellen Safety-Gefahren für Kinder realer sind (z.B. im Straßenverkehr). Die Gefahren, die vom Internet ausgehen, seien es Hacker oder Spyware, sind für die meisten jungen Nutzer möglicherweise schwer vorstellbar.

Ein möglicher ***Zusammenhang zwischen Smartphone-Nutzung und dem Sicherheitsbewusstsein*** könnte anhand der Umfrageergebnisse interpretiert werden. Das würde Hypothese 3 (Besonderheiten des Sicherheitstyps) bestätigen. Alle Kinder des Sicherheitstyps 3 benutzen ein Handy mit Internetzugang. Auch in Sicherheitstyp 2 ist der Anteil deutlich höher als in Sicherheitstyp 1, das ein höheres Sicherheitsbewusstsein repräsentiert. Es könnte damit erklärt werden, dass Kinder durch ihr Smartphone jederzeit Zugriff auf das Internet haben und teilweise nicht genug über die Datenschutzbedingungen der App-Anbieter wissen, obwohl ihnen scheinbar generell bewusst ist, das viele Appanbieter ihre Daten sammeln. Anhand der Umfrageergebnisse kann vermutet werden, dass Kinder über 12 Jahre und/ oder die ein Smartphone besitzen, zu einer Risikogruppe gehören, die zu offen mit ihren Daten im Internet umgeht und wenig Aspekte der IT-Security berücksichtigt. Viele fühlen sich vielleicht gerade auch wegen der bereits längeren Nutzung des Internets ohne schlechte Erfahrungen (Zwei Drittel) sicher und geben daher vermehrt persönliche Daten im Internet an.

Ein weiteres, wichtiges Ergebnis der Umfrage ist, dass ***Belehrungen scheinbar das Sicherheitsbewusstsein nicht erhöhen.*** Was Hypothese 2 (Erfahrungsunterschiede) und Hypothese 5 (Belehrungen) widerlegen würde. Die bisher durchgeführten Belehrungen in der Schule und von den Eltern scheinen demzufolge nicht ausreichend wirksam. Das muss aber in zukünftigen Studien zusammen mit Pädagogen noch detaillierter evaluiert werden. Dies könnte am Inhalt und der Qualität der vermittelten Informationen oder an der Form

der Belehrung liegen. So könnte möglicherweise Respektpersonen (z.B. ein Polizist) oder Gleichaltrige Kinder für Onlinegefahren sensibilisieren.

Laut unserer Umfrageergebnisse haben ***Kinder mit wenigen Regeln beim Surfen im Internet ein scheinbar höheres Sicherheitsbewusstsein***, als Kinder denen von ihren Eltern mehr Regeln bei der Internetnutzung vorgeschrieben werden. Was gegen unsere Hypothese 4 (Regeln) spricht. Dies könnte daran liegen, dass die Kinder sich aufgrund der fehlenden Regeln sehr vorsichtig und insgesamt zeitlich weniger im Internet bewegen, als die Kinder, denen Regeln vorgeschrieben wurden. Die Eltern legen laut Aussage ihrer Kinder mehr Wert darauf, dass die Kinder nur kostenlose Spiele spielen, als dass sie ein sicheres Passwort erstellen können. Dies lässt vermuten, dass viele Eltern selbst nicht gut im Bereich IT-Security aufgeklärt sind und viele IT-Security Gefahren gar nicht kennen. Die Sensibilisierungsmaßnahmen durch die Eltern scheinen daher unzureichend. Deshalb müssten nicht nur die Kinder über Themen der IT-Security belehrt werden, sondern gerade auch die Eltern, die zudem darauf hingewiesen werden sollten, dass sie den Umgang ihrer Kinder mit dem Internet besser beobachten sollten.

Jüngere Kinder haben scheinbar einen größeren Wunsch nach persönlichen Hilfestellungen als ältere Kinder: Besonders viele Kinder des Sicherheitstyps 1, denen vorwiegend jüngere Kinder zw. 10 und 13 Jahren angehören, wünschen eher persönliche Hilfestellungen. Das würde unsere Hypothese 4 (persönliche Hilfestellungen) bestätigen. Es zeigt sich aber generell bei Kindern aller Sicherheitstypklassen ein *Verlangen nach mehr Informationen durch die Eltern (ca. 83%) und durch die Schule (ca. 43%) zum sicheren Umgang mit dem Internet*. Daher sollten in naher Zukunft auch vermehrt Informationsveranstaltungen für Eltern, aber auch Lehrer angeboten werden, in denen sie sich zum Thema IT-Sicherheit weiterbilden können.

5 Zusammenfassung und Ausblick

In diesem Beitrag wurde ein erster Konzeptansatz vorgestellt, der das Sicherheitsbewusstsein von Kindern und Jugendlichen ausdrücken soll. Er soll dazu beitragen, nutzerspezifische Präventiv- und Sensibilisierungsmaßnahmen im Bereich der IT-Security für Kinder und Jugendliche zu entwickeln. In diesem Zusammenhang wurden ***drei Klassen von Sicherheitstypen*** definiert, die eine Adaptation des Konstrukt der „Sicherheitsmentalitäten“ bezüglich Kriminaliätsrisiken von D. Klimke [Kli08] sind. Der in diesem Artikel vorgeschlagene Konzeptansatzes stützt sich auf eine umfangreiche Nutzerstudie (Fragebogenbefragung) mit 157 Schülern/innen im Alter zwischen 10-15 Jahren eines Gymnasiums.

Da bereits Kinder im Grundschulalter das Internet nutzen, sollten sie unserer Meinung nach für Onlinegefahren sensibilisiert werden. Die große Lernbereitschaft dieser Kindern [Ber11] könnte für Sensibilisierungsmaßnahmen im Bereich der IT-Security genutzt werden. Jüngere Kinder sollten vermehrt *persönlichen Hilfestellungen* von Eltern, Lehrern, aber auch Gleichaltrigen/Gleichgesinnten erhalten. Dabei besteht laut unserer Kenntnis vor allem Eltern die Notwendigkeit sich im Bereich der IT-Sicherheitsgefahren weiterzubilden, zumal die meisten Kinder unserer Studie die Hilfe ihrer Eltern hierbei wünschen.

Als zusätzliches Angebot könnten Grundschulkinder durch *kindgerechte technische Hilfestellungen* auf IT-Security-Gefahren im Internet hingewiesen werden. Diese könnte mittels eines Browser Plug-Ins (Sicherheitsguide) umgesetzt werden, welches jeweils eine Benutzersicht für Kinder und Eltern hat. Im Kindermodus könnten Hilfestellungen in textueller und/oder bildlicher Form, entsprechend des Sicherheitstyps, im Browser durch den Sicherheitsguide angezeigt werden. Somit könnten Kindern Hinweise zur IT-Sicherheit der Webseiten und Handlungsanweisungen zum sicheren Umgang mit dem Internet gegeben werden. Eine theoretische Vorarbeit wurde schon in [KHFD12] veröffentlicht. Hier wurden u.a. ein erster Designansatz für Sicherheitssymbole in Form von Comicfiguren zur Warnung von Kindern vor Onlinegefahren vorgestellt. Der Sicherheitsguide zur Verbesserung der IT-Sicherheit soll zukünftig in Zusammenarbeit mit Psychologen und Pädagogen weiterentwickelt und in weiteren Studien auf seine Eignung überprüft werden.

Die im Artikel vorgestellte Sicherheitstypklassen wurden mit einer teilautomatischen Clusteranalyse ermittelt. Die zugrundeliegenden Daten basieren auf einer Punktebewertung ausgewählter verschieden gewichteter Kriterien (z.B. Veröffentlichung persönlicher Daten im Internet, Verwendung gleicher Logindaten für verschiedene soziale Netzwerke). Um die Signifikanz der bisherigen Umfrageergebnisse zu evaluieren, soll zukünftig eine automatisierte Clusteranalyse genutzt werden. Weiterhin sollen in Kooperation mit Psychologen detailliertere Daten zum Sicherheitsbewusstsein von Kindern und Jugendlichen erhoben werden. So soll z.B. abgeklärt werden, in welchem Kontext Kinder persönliche Informationen im Internet angeben (z.B. Login, Kommunikation mit anderen). Als Grundlage für den Sicherheitsguide soll das Konzept der Sicherheitstypen weiterentwickelt werden. Dazu zählen unter anderem die weitere Auswertung der im Artikel beschriebenen Umfrage (z.B. eigene Ideen der Kinder für ein sicheres Internet) und der Abgleich mit den Ergebnissen der EU Kids Online Studien. Weiterhin soll vor allem an der kindgerechten Kommunikation von Sicherheitsbedürfnissen (Sicherheitsziele) und deren Umsetzung (Sicherheitsmaßnahmen und Mechanismen) in Form von Sicherheitswarnmeldungen weitergeforscht werden.

Danksagung

Wir danken dem Herder-Gymnasium der Stadt Minden (NRW), Dr. Sven Kuhlmann und Dr. Michael Knuth. Die Arbeit von Jana Fruth ist Teil des ViERforES[12] Projektes, welches vom Deutschen Ministerium für Bildung und Forschung (BMBF) (Projektnummer 01IM10002A) finanziert wird.

Literatur

[Ber11] L.E. Berk. *Entwicklungspsychologie (5. Aufl.).* Pearson Studium, Stuttgart, 2011.

[12] http://www.vierfores.de/, letzter Zugriff: 1. Juli.2013

[Bor05] Jürgen Bortz. Statistik für Human- und Sozialwissenschaftler. 2005.

[BR11] Peter Behrens und Thomas Rathgeb. *JIM-Studie 2011*. Medienpädagogischer Forschungverbund Südwest, Stuttgart, 2011.

[Bra10] Clara Brady. Security Awareness for Children. 2010.

[BSKR10] Peter Behrens, Thomas Schmid, Tina König und Thomas Rathgeb. *KIM-Studie 2010*. Medienpädagogischer Forschungverbund Südwest, Stuttgart, 2010.

[Bun09] Bundesministeriums der Justiz. Bundesdatenschutzgesetz (BDSG), August 2009.

[BVMR13] Marcel Beskau, Matthias Volk, Anneke Meyer und Robin Richter. Sicherheitsbewusstsein von Kindern und Jugendlichen im Umgang mit dem Internet. *Abschlussbericht des Seminars „Sicherheitsfragen eingebetteter Systeme“ im WS12\13 unter Leitung von Prof. Dr.-Ing. Jana Dittmann*, 2013.

[Byr08] Tanya Byron. *Safer children in a digital world: The report of the Byron Review*. DCSF Publications, Nottingham, 2008.

[Cop85] Nina M. Coppens. *Cognitive characteristics as predictors of children's understanding of safety and accident prevention*. 1985.

[Has06] Uwe Hasebrink. *Comparing children's online opportunities and risks across Europe: cross-national comparisons for EU Kids Online, 2nd edition*. EU Kids Online, 2009-06.

[KHFD12] Sven Kuhlmann, Tobias Hoppe, Jana Fruth und Jana Dittmann. Voruntersuchungen und erste Ergebnisse zur Webseitengestaltung für die Situationsbewusste Unterstützung von Kindern in IT-Sicherheitsfragen. In *Informatik 2012, 42. Jahrestagung der Gesellschaft für Informatik*, Braunschweig, 2012.

[Kli08] Daniela Klimke. *Wach- & Schließgesellschaft Deutschland: Sicherheitsmentalitäten in der Spätmoderne*. VS, Verl. für Sozialwissenschaften, Wiesbaden, 1. Auflage, 2008.

[LH09] Sonia Livingstone und Leslie Haddon. EU Kids Online - Final Report. 2009.

[LHGO11] Sonia Livingstone, Leslie Haddon, Anke Görzig und Kjartan Ólafsson. EU Kids Online II - Final Report. 2011.

[Lim95] Maria Limbourg. Entwicklungspsychologische Voraussetzungen für das sicherheitsorientierte Verhalten von Kindern. In *Kindersicherheit: Was wirkt?*, Seiten 46–58. 1995.

[Lim97] Maria Limbourg. Gefahrenkognition und Präventionsverständnis von 3- bis 15jährigen Kindern. In *Kindersicherheit: was wirkt?*, Seiten 313–326. 1997.

[Liv11] Sonia Livingstone. *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. EU Kids Online Network, 2011.

[O'B09] Emmet O'Briain. 2008 Survey of Children's Use of the Internet in Ireland: Report prepared by Ipsos MORI on behalf of the National Centre for Technology in Education. 2009.

[Sac04] Norbert Sachser. Neugier, Spiel und Lernen: Verhaltensbiologische Anmerkungen zur Kindheit. *Zeitschrift für Pädagogik*, 50(4):475–486, 2004.