Voruntersuchungen und erste Ergebnisse zur Webseitengestaltung für die situationsbewusste Unterstützung von Kindern in IT-Sicherheitsfragen

Sven Kuhlmann, Tobias Hoppe, Jana Dittmann, Jana Fruth
Fakultät für Informatik (FIN) / ITI
Otto-von-Guericke-Universität Magdeburg
Universitätsplatz 2, 39106 Magdeburg
stuchsch@ovgu.de, choppe@ovgu.de, jana.dittmann@iti.cs.uni-magdeburg.de,
jana.fruth@iti.cs.uni-magdeburg.de

Abstract: Kinder und Jugendliche treten heutzutage immer häufiger und früher als Nutzer von Computersystemen und des Internets auf - und das oft ohne die Gefahren zu kennen, die im Kontext von deren Nutzung vielerorts sowie auf vielfältige Weise drohen. Ausgehend von beispielhaften IT-seitigen Gefahren, mit denen besonders auch Kinder in Kontakt kommen können, stellt dieser Beitrag Ergebnisse einer Untersuchung vor, in der das Schutzbedürfnis speziell von Kindern beim Umgang mit dem Internet erfragt wurde, um einen Ansatz zur verbesserten Gestaltung dieser Systeme / Internetangebote für Kinder zu erarbeiten. Dafür werden analysierte beispielhafte Webseiten anhand von Sicherheitsaspekten und deren Umsetzung bewertet. Auch die Ergebnisse des Fragebogens zur Ermittlung des Schutzbedürfnisses von Kindern werden vorgestellt. Als Rückschlüsse auf die bestehenden Gefahren und Probleme werden abschließend Ansätze für sichere Systeme gezeigt, die die Sicherheit im Internet für Kinder und Jugendliche in besserer Weise adressieren sollen, so zum Beispiel ein metaphorischer Ansatz dem ein natural Mapping des Kinderzimmers zugrunde liegt.

1 Einleitung

Laut einer Studie [Zi2] nutzen ca. 68 Prozent aller Deutschen regelmäßig das Internet. Dabei ist die Tendenz steigend, wobei mit etwa 80% die deutschen Jugendlichen (10 - 13 Jahre) besonders ins Gewicht fallen [Ih1]. Sie nutzen diesen Dienst in immer früherem Alter und häufiger. Dies geht zusätzlich mit einer raschen Weiterentwicklung des Internets einher, das mittlerweile nahezu überall verfügbar ist. Teilweise nutzen es Kinder bereits im Alter von 6 Jahren regelmäßig, falls ihre Eltern dies zulassen [Ih1]. Doch wie sicher ist der Umgang mit den Internetinhalten und deren Bedrohungen? Kinder und Jugendliche werden diesbezüglich häufig nicht ausreichend von den Eltern aufgeklärt. Wie wichtig sind Datenschutz, Privatsphäre, Vorsicht vor Viren und Schadsoftware? Wie viel wissen die Kinder und Jugendliche darüber und wie gut kennen sie sich allgemein im Internet aus? Wozu nutzen sie es und wie können Webseiten für Kinder und Jugendliche sicherer gestaltet werden? Diese Fragen konnten bislang wissenschaftlich nicht oder nur unzureichend beantwortet werden. Aus diesem Grund werden diese Fragen im vorliegenden Beitrag im Kontext der Nutzung des Internets durch Kinder adressiert.

Zunächst werden Aspekte aufgezeigt, die im Zusammenhang mit der Sicherheit im Internet, speziell für Kinder, betrachtet werden sollten. Anschließend werden ausgewählte Webseiten verschiedener Kategorien (Chat, Soziale Netzwerke, Spiele, TV u.a.) bezüglich ihrer Kinderfreundlichkeit untersucht (siehe Abschnitt 3: Webseitenanalyse). Um die Analyse quantitativ untersuchen zu können, wurde ein

Fragebogen entworfen (siehe Abschnitt 4). Dieser wurde an eine Stichprobe von 18 (Grundschul-)Kindern verteilt und beantwortet. Der Fokus des Fragebogens liegt dabei auf der Erfassung des Verhaltens und der Kognition der Kinder im Internet bezüglich der IT-Sicherheit. Neben der quantitativen Auswertung des Fragebogens (deskriptive Statistik) und den sich daraus ergebenden Erkenntnissen wurden abschließend Vorschläge erarbeitet, wie die Sicherheit für Kinder und Jugendliche im Internet verbessert werden könnte (Abschnitt 5).

2 Sicherheit im Internet: Grundlagen und Stand der Forschung

Aus der Fachliteratur sind folgende fünf Sicherheitsaspekte bekannt, welche in Bezug auf die IT-Sicherheit informationstechnischer Systeme eine Rolle spielen: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit [Eck7]. Im Kontext der Vertraulichkeit wird mittlerweile speziell auch der Datenschutz mit einbezogen. In den folgenden Unterabschnitten wird der Fokus – in Bezug auf die eingangs formulierten Fragestellungen – besonders auf drei Teilaspekte der Sicherheit gelegt, den Datenschutz, der Passwortschutz (betrifft u.a. Integrität und Vertraulichkeit) und das generelle Verhalten im Internet (betrifft u.a. Verbindlichkeit). Diese drei Aspekte fließen in die Bewertung der ausgewählten Webseiten ein. Dabei wurde besonders darauf Wert gelegt, ob diese kindgerecht [MTF5] thematisiert und umgesetzt wurden.

2.1 Datenschutz

Eine der zentralen Fragen, die zu beantworten sind, ist, wie sicher die Daten von Kindern im Internet sind und wie sicher Kinder mit dem Umgang persönlicher Daten im Internet agieren. Als erstes ist zu prüfen, ob die Webseiten Datenschutzerklärungen aufweisen (z.B. auch zur Information der Eltern kindlicher Nutzer): wird versichert, dass persönliche Daten nicht an Dritte weitergegeben werden? Welche Daten werden von den Kindern erhoben? Wird darauf hingewiesen, welche Daten Kinder generell im Internet bzw. auf keinen Fall preisgeben sollten? Gibt es Barrieren beim Eingeben oder Hinweise vom System, wenn Zugriff von Außen auf die eigenen Daten (z.B. Synchronisierung) genommen wird?

2.2 Passwortschutz

Ein weiteres Kriterium, welches betrachtet wurde ist der Passwortschutz [Eck7]. Gibt es Hinweise zu diesem Thema auf der Webseite oder dazu, wie ein sicheres Passwort erstellt werden kann? Gibt es eine interaktive Unterstützung während der Passworterstellung, beispielweise indem sie den Anmeldevorgang unterbrechen, wenn das Passwort nicht ausreichend sicher ist? Gibt es spezielle Hinweise zum Umgang mit Passwörtern, z.B. sein Passwort niemandem zu verraten?

2.3 Verhalten im Internet

Ergänzend, zu den oben genannten Aspekten wurde betrachtet, ob und wie auf der Webseite erklärt wird, wie gutes und sicheres Verhalten im Internet aussieht, bzw. hierzu Empfehlungen gegeben und wie diese vermittelt werden. Dies ist besonders beim Umgang mit Onlinechats wichtig, da es dort auch zum Kontakt mit unbekannten Personen kommen kann. Ein Beispiel wäre die Möglichkeit einer Instruktion mit anschließendem Test bezüglich des umsichtigen Verhaltens im Internet. In der

Instruktion sollten diesbezüglich wichtige Hinweise kindgerecht [MTF5] gegeben werden. Innerhalb des Chats wäre einer dieser Hinweise, sich nicht mit fremden Leuten zu unterhalten und im Falle einer unbekannten Kontaktaufnahme einen Erwachsenen herbeizuholen – vor allem dann, wenn anonyme, fremde Personen diskrete Fragen stellen. Ein weiteres Beispiel für einen verhaltensunterstützenden Hinweis wäre, dass eine völlige Anonymität im Internet nicht möglich ist und entsprechend darauf geachtet werden muss, welche persönlichen Informationen preisgegeben werden, sowie der dazugehörige Hinweis, im Zweifelsfall Erwachsene (Eltern) um Rat zu fragen. Eine weitere beispielhafte Frage, die bei der Untersuchung betrachtet wurde ist die, wie reagiert werden sollte, wenn es zu einer Belästigung über das Internet kommt. Auch der technische Aspekt wurde im Verhaltenskontext betrachtet und untersucht, wie eine angemessene Reaktion unterstützt wird, wenn ein Virus oder Trojanisches Pferd auf den Rechner gelangt ist oder zu gelangen droht. Die genannten Aspekte flossen ebenfalls in die inhaltliche Gestaltung des Fragebogens ein, um festzustellen, ob sich Kinder derer und den Gefahren, die sie mit sich bringen, bewusst sind.

3 Analyse existierender Webseiten

Unter Beachtung der oben erläuterten Teilaspekte für Sicherheit und der generellen kindgerechten Gestaltung [MTF5] (u.a. altersangepasster Inhalt, Ausdruck, Darstellung) der Webseiten wurden exemplarisch Webseiten ausgewählt und durch vier Studenten im Rahmen einer Informatikveranstaltung zur IT-Sicherheit analysiert. Im Anschluss wurden die Analyseergebnisse durch drei Experten geprüft und diskutiert. Es wurden Webseiten ausgewählt, die Kindern zum großen Teil bekannt sein sollten. Dabei wurden auch bewusst Webseiten ausgewählt, die nicht speziell für Kinder gestaltet wurden, jedoch Inhalte anbieten, die Kinder ansprechen, so z.B. Videobroadcast. Wie realitätsnah die Einschätzung der Studenten und der Experten ist, wird später im Abschnitt 5 diskutiert. Die Webseiten wurden den Kategorien „Chaträume und Messenger“, „soziale Netzwerke“, „Suchmaschinen“, Seiten zum Thema „Lifestyle“, „Fernsehsender“, „Videoplattformen“ und „Sonstiges“ zugeordnet. In letztere wurden u.a. auch „Emails“ eingruppiert. Die Skala der Bewertung der Webseiten entspricht der des deutschen Schulnotensystems (1 bis 6). Im Anschluss daran wurden diese Schulnoten auf Ampelfarben abstrahiert. Dies dient einer Visualisierung der Ergebnisse dieser Untersuchung an die relevante Zielgruppe (Kinder), z.B. durch deren Eltern oder Lehrer und wurde bereits in anderen Arbeiten [MTF5], [MTF6] als eine geeignete und intuitive Darstellung identifiziert. Dieses Farbsystem wurde ebenfalls auf eine erdachte Figur im Comicstil (vgl. Abb. 9) übertragen, die beispielweise im Sinne eines einheitlichen Symbols die Kinderfreundlichkeit von Webseiten in der Praxis visualisieren könnte. Dieser Ansatz wird in Abschnitt 6 weiter detailliert und diskutiert. Im Folgenden wird eine tabellarische Analyse und Bewertung (Abbildung 1) aller untersuchten Webseiten anhand der gewählten Kriterien gegeben. Die Farbe grün (+) kennzeichnet Seiten mit dem Status “sehr sicher”, gelb (o) mit “Achtung/Vorsicht” und rot (-) signalisiert “nicht sicher”. Zusätzlich wurde der durchschnittliche Sicherheitswert vergleichbar zum Schulnotensystem für jede Webseite errechnet.

Überprüfte Webseite in Kategorien	Kinder-eignung	Sicherheits-sichtbarkeit	Kindgerechte Themenaufarbeitung	Umfang der Sicherheitsthemen			Umsetzung auf der Seite		
				Datenschutz	Passwort-schutz	Internetverhalten	Datenschutz	Passwortschutz	Internetverhalten
Chaträume und Messenger									
Chat4Free (3,2)	+	o	+	+	-	+	+	-	o
Msn4Kids (3,6)	+	+	+	-	-	-	+	+	+
Knuddels (4,0)	o	o	-	+	+	+	-	-	o
Soziale Netzwerke									
MeinVZ/ StudiVZ (2,8)	o	o	+	+	+	+	+	-	+
Facebook (4,2)	-	o	o	+	+	+	-	-	-
Schueler.cc (4,4)	o	-	o	o	o	o	-	-	+
Twitter (5,4)	-	-	-	o	-	o	-	-	-
Suchmaschinen									
BlindeKuh (3,2)	+	+	o	+	o	o	o	o	o
FragFinn (4,2)	+	+	-	+	-	+	-	-	-
Google (4,6)	o	o	-	+	-	-	+	-	-
Lifestyle									
Bravo (5,8)	-	-	-	-	-	o	-	-	-
Fernsehwebseiten									
Kika (3,0)	+	o	+	+	+	o	-	+	o
Tivi (3,4)	+	-	o	+	o	+	+	-	+
Toggo (5,4)	o	-	-	o	o	-	-	-	-
Nick (5,6)	o	-	-	-	o	-	-	-	-
Videoplattformen									
Youtube (4,2)	-	o	-	+	-	+	o	o	o
Clipfish (5,6)	-	-	-	+	-	-	-	-	-
Myvideo (5,8)	-	-	-	o	-	-	-	-	-
Email und sonstiges									
Yahoo (4,2)	-	-	-	+	+	+	-	+	-
Hausarbeiten (5,8)	o	-	-	-	-	-	-	-	-

Abbildung 1: Gesamtübersicht der Webseitenanalyse und -bewertung.

3.1 Detaillierte Erläuterung der tabellarischen Ergebnisdarstellung

Abbildung 1 zeigt die Gesamtübersicht aller untersuchten Webseiten und deren Bewertung anhand der Eingangs dieses Beitrages vorgestellten Teilaspekte für die Sicherheit – speziell für Kinder. Im Folgenden wird nun die jeweils beste Seite jeweils für einen der Teilaspekte von Sicherheit genauer beschrieben. Auf die detaillierte Beschreibung aller Webseiten wird in diesem Beitrag aus Platzgründen verzichtet. Weiterhin liegt der Fokus hier auf der Identifikation von angemessenen Umsetzungsmöglichkeiten der IT-Sicherheitsfragen (vgl. Titel).

Erläuterung der Tabellenköpfe

Neben den untersuchten Webseiten fließen die bereits erläuterten Sicherheitsteilaspekte als Bewertungskriterien ein (Erläuterung der Spalten in Abbildung 1 im Folgenden von links nach rechts).

Es wurde untersucht und bewertet, ob und wie sich die Seiten für Kinder im Allgemeinen eignen. Dazu zählt beispielsweise, wie viel Werbung verschiedenster Art sich auf den Seiten befindet (z.B. erotische / pornographische Anzeigen, Werbung für Onlinespiele oder Automobile), oder ob andere, für Kinder unangebrachte Inhalte dargestellt werden.

Unter dem Aspekt der „Sicherheitssichtbarkeit“ wurde bewertet, wie sichtbar oder auffällig Informationen zu Sicherheitsaspekten platziert und dargestellt sind - es dem Kind also leicht fällt diese zu ekennen und als Kriterium für sich zu nutzen. Ein Kriterium hierbeit ist z.B. die Frage: Ist ein Link zum Thema Sicherheit deutlich sichtbar

platziert und auffallend gestaltet, oder ist er zu klein und unauffällig angelegt und es muss danach gesucht werden?

Unter dem Aspekt „kindgerechte Themenaufarbeitung“ wurde die Art und Weise, wie Informationen über Sicherheitsaspekte aufbereitet werden bewertet und ob diese für Kinder verständlich und nachvollziehbar dargestellt sind [MTF5]. Besonders auf Webseiten für Kinder sollte darauf geachtet werden, dass für wichtige Sicherheitsaspekte keine langen Fließtexte genutzt werden sollten, um für Kinder verständlich zu sein [MTF5]. Die Ergebnisse dieser Analyse schwanken zwischen schlechten Bewertungen für seitenlange Texte in zu kleiner Schriftgröße, bürokratisch verfassten Inhalten, über prägnante, konkrete und für Kinder verständliche Stichpunkte, bis hin zur vollständigen Gestaltung durch Bildercomics und Videos, die Kinder für die IT-Sicherheitsaspekte sensibilisieren sollen.

Der nächste, größere Bereich der IT-Sicherheitsaspekte beinhaltet die – in Abschnitt 2 - vorgestellten Themen Daten- und Passwortschutz und das generelle Verhalten im Internet. Es wurde bewertet, inwiefern die Webseiten explizit auf diese Themen eingehen. So sollte zum Beispiel speziell die Internetseiten, die einen Chat anbieten Verhaltensregeln in Bezug auf die Kontaktaufnahme durch unbekannte/fremde Personen vermitteln. Auch Datenschutzerklärungen sollten weder fehlen, noch so dargestellt werden, dass sie für Kinder unverständlich sind. Dies gilt insbesondere auch für Suchmaschinen, die zum Teil die Anfragen speichern, verarbeiten und (an Dritte) weitervermitteln. Ein angemessener Passwortschutz (vgl. 2.2) ist generell auf anmeldepflichtigen Seiten wichtig und es sollten präzise Informationen und Hinweise (vgl.2.2) zu diesem Kriterium gegeben werden.

Im Bereich zur Bewertung der Umsetzung der IT-Sicherheitskriterien (vgl. Abschnitt 2) wurde bewertet, ob und wie stringent die altersangemessenen IT-Sicherheitskriterien umgesetzt wurden. Wenn Kinder beispielsweise eigene Daten, wie ihre Adresse, Telefonnummer oder ähnlich persönliche Daten in ein Formular eingeben, sollte beispielsweise – dem Eingabefeld direkt zugehörig – ein entsprechender Hinweis bzw. eine Warnung erscheinen (vgl. hierzu [MTF5], um darauf hinzuweisen, dass die eingegebenen Daten gespeichert (und gegebenenfalls an Dritte weitergegeben) werden. Als weiteres Beispiel kann ein kindergeeigneter Passwortschutz umgesetzt werden, indem neben den Hinweisen, wie ein Passwort aussehen sollte, auch bei der Passworterstellung interaktiv darauf hingewiesen wird. Um die Stufe der Sicherheit eines Passwortes darzustellen, kann eine Analogie zu einer Fußgängerampel verwendet werden (rot (nicht geeignet/unsicher) vs. grün (geeignet / sicher). Weiterhin sollte stets eine Mindestlänge für ein Passwort und eine Kombination aus Groß- und Kleinbuchstaben, Ziffern und eventuell auch Sonderzeichen gefordert werden. Eine weitere Möglichkeit bietet die Sperrung der Fortsetzung des Anmeldevorgangs solange, bis das Passwort ausreichend sicher ist.

3.2 Abschließende Bewertung

Wie in Abbildung 1 ersichtlich, gibt es innerhalb der thematischen Zuordnung (Zeilen) von Webseiten („Chaträume und Messenger“, „soziale Netzwerke“, „Suchmaschinen“, Seiten zum Thema „Lifestyle“, „Fernsehsender“, „Videoplattformen“ und „Sonstiges“) teils hohe Diskrepanzen. Teilweise wurden IT-Sicherheitsaspekte angemessen ausgewählt und in die Praxis umgesetzt. Jedoch erreichten auch die – am besten bewerteten – Webseiten eine Durchschnittsbewertung von 3 (Schulnotenskala von 1 bis 6). Auch bei diesen Internetauftritten besteht somit noch Potential bezüglich der Verbesserung der IT-Sicherheitsaspekte, vor allem darin, wie diese altersgerecht an Kinder vermittelt werden.

Betrachtet man die Spalten in Tabelle 1, so fällt auf, dass die kindgerechte Aufarbeitung (Spalte 3) sowie die altersgerechte Umsetzung des Passwortschutzes durch die meisten untersuchten Webseiten mangelhaft umgesetzt werden. Auch an dieser Stelle besteht bezüglich der Umsetzung und (sehr wahrscheinlich) auch bezüglich der zugrundeliegenden Konzepte ein enormes Verbesserungspotential.

Nach der Analyse der Webseiten erfolgte eine Befragung von Kindern zum Thema IT-Sicherheit. Der Fragebogen und die entsprechenden Ergebnisse werden in den folgenden Abschnitten 4 und 5 vorgestellt.

4 Fragebogenkonzept, Entwicklung und Methode

Innerhalb der Untersuchung wurde der grundlegenden Fragestellungen nachgegangen, welche Seiten Kinder im Internet häufig aufsuchen, wofür sie das Internet aus persönlicher Sicht nutzen und wie sicher sie sich beim Umgang damit fühlen.

4.1 Fragebogenkonstruktion und Methode

Die Konstruktion des Fragebogens wurde in folgenden Schritten realisiert: Aus einem anfangs gesammelten Pool von 20 potentiellen Fragen mit Bezug auf das Untersuchungsziel wurde für die Erstellung des Fragebogens anschließend eine Auswahl von 10 Fragen getroffen. Bei der Selektion der Fragen wurde auch bewusst auf Fragestellungen verzichtet, die z.B. die Privatsphäre der Familie betreffen – mit Ausnahme der Frage, ob dem Kind (seitens der Eltern) weitere Regeln für den Umgang mit dem Internet (als die im Fragebogen abgefragten) auferlegt sind. Anhand einer Vorabstichprobe (5 Kinder) wurde getestet, ob die Fragen für die Zielgruppe (Kinder) verständlich formuliert sind und anschließend teil reformuliert Deutungsinterferenzen zu minimieren. Ergebnis war ein Fragebogen, der – in der zu untersuchenden Altersgruppe – die Einschätzungen zu folgenden Themen erfasst: Wie lange und oft bewegen sich Kinder im Internet und wozu nutzen sie es? Wie sicher fühlen sie sich dabei? Können Erkenntnisse aus einer möglichen Dauernutzung entnommen werden? Zur Ermittlung, wie relevant die im Voraus analysierten Webseiten für Kinder wirklich sind, wurde zusätzlich erhoben, ob Kinder diese besuchen oder überhaupt kennen. Um einschätzen zu können, wie ausgeprägt der Kontakt von Kindern mit den Gefahren des Internets ist, wurde ebenfalls erhoben, ob es bereits Erfahrungen bezüglich Belästigungen durch Fremde gab, oder ob bereits Viren oder Trojanische Pferde wissentlich auf den Rechner gelangt sind. Außerdem wurde dabei jeweils die Reaktion auf die Gefahr erfragt. Im Folgenden werden die 10 Fragen inklusive ihrer Antwortmöglichkeiten aufgeführt:

1. Wie lange nutzt du schon das Internet? Antwort: Angabe in Jahren.
2. Wie oft bist du im Internet? Vier Antwortalternativen: weniger als einmal pro Woche – einmal pro Woche – einmal täglich – mehr als einmal täglich.
3. Wie sicher fühlst du dich im Internet? Vier Antwortmöglichkeiten: grundsätzlich sicher – sicher, aber nicht immer – unsicher, aber nicht immer – grundsätzlich unsicher.
4. Macht es für dich einen Unterschied, ob du an Deinem eigenen oder an einem öffentlichen Computer im Internet bist? (z.B. Schule / Internetcafé) Antwort: ja – nein.
5. Gibt es für dich Regeln für das Surfen im Internet? Auswahl mehrerer Antworten: technische Regeln (Firewalls / Antivirenprogramme...) – zeitliche Regeln (Fristen / Tageszeiten...) – nur bestimmte Seiten besuchen dürfen. Zusätzlich besteht die Möglichkeit eigene Regeln hin zuzufügen.
6. Wozu nutzt du das Internet hauptsächlich? Auswahl mehrerer Antworten: Spiele (Onlinespiele) – Email – Videos schauen / Musik hören – Chatten (z.B. Chat4Free) – Schularbeiten – Soziale Netzwerke (z.B. Facebook) – Informationssuche (z.B. Wikipedia). Zugeordnet jeweils: Wie sicher fühlst du dich dabei? Drei Alternativen: sehr sicher - geht so - nicht sicher.
7. Hat dich im Internet schon einmal jemand beobachtet oder belästigt? Vier Antwortmöglichkeiten: nein, noch nicht - ja, aber ich habe es ignoriert - ja und ich habe eine andere Person um Rat gefragt / hinzu geholt - ja und ich habe selber aktiv etwas getan / darauf reagiert.

8. Was hilft dir im Internet, damit du dich sicherer fühlst? Auswahl mehrerer Alternativen: Passwörter – Sicherheitssymbole – viel Text/Erklärungen – wenig Text/Erklärungen, dafür mehr Bilder – Virenscanner / Firewalls – spezielle Schutzsoftware für Kinder – regelmäßige Hilfe durch eine andere Person.
9. Denkst du, es ist möglich, im Internet völlig anonym / unsichtbar zu sein? Drei Antwortalternativen: ja – ja, aber mit besonderen Vorkehrungen – nein, nie.
10. Welche der folgenden Seiten benutzt du regelmäßig? Wie hoch schätzt du die Gefahr ein, dass man dich dort beobachten / belästigen könnte? Hier wurden die 20 zuvor analysierten Webseiten aufgelistet und eine Tabelle daneben platziert, in der die Kinder angeben konnten, wie sicher sie sich auf der Seite fühlen: sehr sicher – geht so – nicht sicher. Im Anschluss daran bestand noch die Möglichkeit bis zu drei weitere Webseiten zu nennen, die ihnen sehr wichtig erscheinen, aber in der vorangegangen Analyse nicht beachtet wurden.

4.2 Stichprobe und Durchführung

Der oben beschriebene Fragebogen wurde an 18 Kinder der 6. Klasse einer Sekundarschule verteilt. Die Beantwortung dauerte im Mittel ca. 10 - 20 Minuten. Es folgt nun die deskriptive Auswertung der Antworten aus Fragebögen. Im Anschluss werden aus den gewonnenen Erkenntnissen Schlussfolgerungen gezogen und Vorschläge gegeben, wie zukünftig Webseiten gestaltet werden sollten, um die Sicherheit für Kinder im Internet zu verbessern. Durch die geringe Stichprobengröße liegt der Fokus auf einer deskriptiven Betrachtung. Weiterhin ist die Generalisierbarkeit der Ergebnisse stark eingeschränkt. Eine inferenztatistische Auswertung (Signifikanzen, Effektstärken) wurde insofern nicht durchgeführt, da das Ziel der Untersuchung auf der Gewinnung qualitativer Ergebnisse lag.

4.3 Ergebnisse der Auswertung des Fragebogens

Auf die Frage, seit wann die Kinder und Jugendlichen das Internet nutzen, antworteten die befragten Kinder im Mittel mit einem Zeitraum von knapp vier Jahren. Im Umkehrschluss bedeutet dies, dass viele Kinder bereits seit der Grundschule das Internet nutzen. Dabei gibt es auch Ausreißer: zwei der Kinder nutzen das Internet bereits seit 9 Jahren. Zu beachten ist dabei, dass manche Kinder stark überaltert in einer Klassenstufe sind, wobei eine Abweichung von 5 Jahren vom Mittelwert dennoch nicht außer Acht gelassen werden sollte. Ein Kind scheint noch keinerlei oder sehr wenig Kontakt mit dem Internet gehabt zu haben, denn es gab eine Nutzung von 0 Jahren an. 3 Kinder haben keine Angabe bei dieser Frage gemacht. Eine Visualisierung der gegebenen Antworten ist in Abbildung 2 zu sehen, in der die rote Linie den Durchschnittswert von ca. 4 Jahren anzeigt.

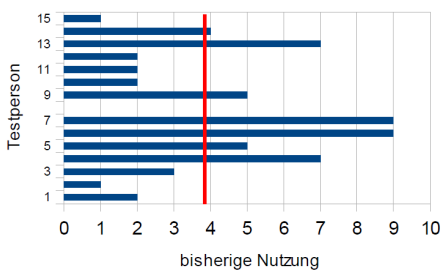

Abbildung 2: Nutzung des Internets von Kindern in Jahren.

Als nächstes wurde nach der Häufigkeit gefragt, mit der Kinder das Internet nutzen. Etwa 30% antworteten mit „weniger als einmal pro Woche“, Eines der 18 Kinder gibt „durchschnittlich einmal pro Woche“ an und ca. 20% geben an, „einmal am Tag“ das Internet zu nutzen. Die verbleibenden etwa 40% der Kinder sind sogar mehr als einmal am Tag online (vgl. Abbildung 3).

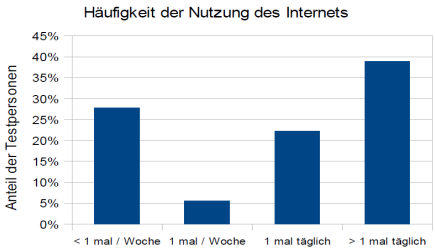

Abbildung 3: Nutzungshäufigkeit

Interessante Ergebnisse sind bei der Frage nach dem Sicherheitsgefühl der Kinder im Internet zu erkennen: keines der Kinder fühlt sich generell unsicher im Internet. Zu jeweils ca. 40% gaben die Kinder an, sich generell oder meist sicher zu fühlen. Die restlichen etwa 20% beantworteten die Frage mit relativ unsicher (Abbildung 4).

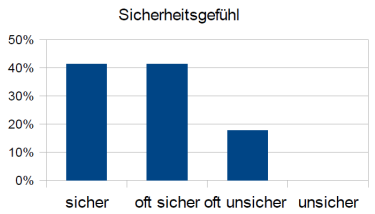

Abbildung 4: Sicherheitsgefühl der Kinder im Internet

Bei der Frage, ob es für die Kinder einen Unterschied darstellt, mit einem fremden oder dem eigenen Rechner zu surfen gaben 60 % die Antwort „ja“ und 40 % „nein“. Auch bezüglich dieses Punktes sollten Kinder zukünftig verstärkt sensibilisiert werden.

Bei der Frage zu den Regeln, nach denen sich Kinder beim Umgang mit dem Internet richten, antworteten ca. 65% der Befragten unter Beachtung technischer Regeln, also unter Nutzung von z.B. Firewalls oder Virenscannern (vgl. Abb. 5). Zwei weitere Regeln wurden von den Kindern selbst angegeben: zum einen nur kostenlose Computerspiele zu spielen und zum anderen generell keine eigenen Daten im Internet preiszugeben.

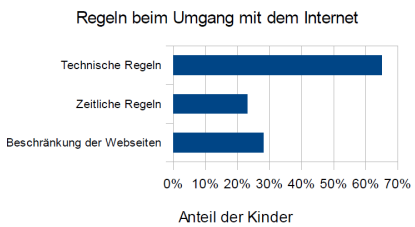

Abbildung 5: Aufteilung der Antworten bez. der Regeln bei Nutzung des Internets

Auf die Frage, wozu die Kinder das Internet nutzen und wie sicher sie sich dabei fühlen, zeigt sich, dass die am häufigsten (72%) genutzte Anwendung das Schauen von Videos und Hören von Musik ist. Bei dieser Aktivität fühlen sich die Kinder zudem am sichersten. Darauf folgt das Spielen von Onlinegames (68%). Platz drei belegen die Besuche von Chats und Sozialen Netzwerken (je 60%). Chats weisen den höchsten Anteil an Unsicherheit während der Nutzung auf. Wenig Verwendung findet das Internet für Informationssuche, Schulthemen und Emails. Die hohe Unsicherheit beim Chatten geht vermutlich mit dem Umgang mit persönlichen Daten, die man vielleicht preisgibt, einher. Auch die drohende Belästigung durch andere, fremde Personen kommt hier zum Tragen. Neben den Sozialen Netzwerken rufen auch Emails bei Kindern eine gewisse Unsicherheit hervor. Die anderen Kategorien wurden nicht mit „unsicher“ bewertet (vgl. Abbildung 6, bei der die Farbe grün für „sehr sicher“ und Rot für „unsicher“ steht).

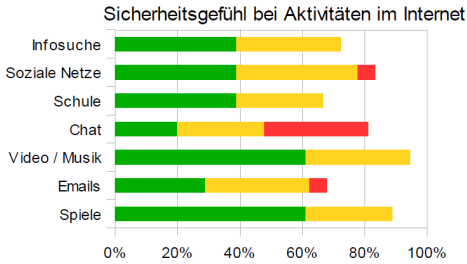

Abbildung 6: Aktivitäten der Kinder im Internet und Sicherheitsempfinden

Auch die Frage nach Erfahrungen mit Belästigung oder Beobachtung gaben fast 80% der Kinder an, dass ihnen so etwas noch nie widerfahren sei, 20% beantworteten die Frage mit „Ja“. Diese verteilen sich mit jeweils ca. 10% auf das Ignorieren von solchen Vorfällen und das aktive Reagieren. Keines der Kinder gab an, in einem solchen Fall Hilfe geholt zu haben.

Auf die Frage, was die Sicherheit im Internet für Kinder erhöhen könnte ergab sich folgende Verteilung; Während laut der Antworten eine spezielle Schutzsoftware für Kinder (zum Beispiel K9 [K94]) und die regelmäßige Hilfe durch andere Personen, genauso wie viel Text, nur wenig dazu beitragen würden, scheinen Virenscanner und mehr Bilder für Erklärungen eher bei Kindern Anklang zu finden. Wider Erwarten haben Passwörter nur einen niedrigen Rang im Sicherheitsgefühl erhalten, wohingegen die Einführung, Verbreitung und sichtbarere Platzierung von Sicherheitssymbolen mit 82% positiv bewertet wurde (vgl. Abb. 7).

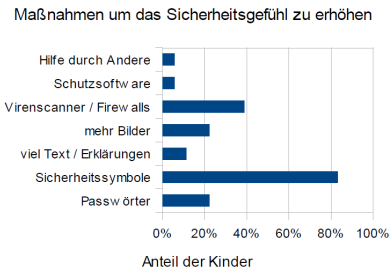

Abbildung 7: Verteilung der Antworten zu Sicherheitserhöhenden Maßnahmen

Zum Abschluss dieses Kapitels wird im Folgenden die Webseitenanalyse aus Abschnitt 3 mit der Bewertung durch die Kinder verglichen. Nur vier Webseiten wurden von keinem der Kinder besucht oder häufiger benutzt. Dies zeigt, dass die Analyse und Bewertungen zu Beginn des Projektes vergleichsweise realitätsnah sind und die Interessen der Kinder gut eingeschätzt wurden.

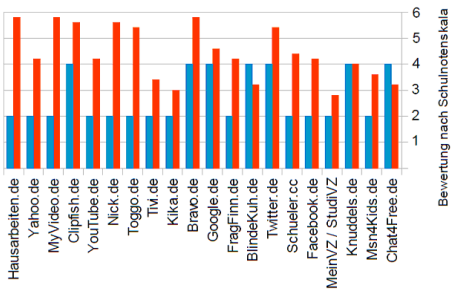

Abbildung 8: Gefahreneinschätzung der Webseiten nach Schulnotenskala - Vergleich der Vorabanalyse (rot) und der Bewertung durch die Kinder (blau)

Eine Gegenüberstellung der Gefahreneinschätzung durch die Vorabanalyse und durch die Bewertung der Kinder ist in Abbildung 8 zu sehen. Auf die Frage nach weiteren Webseiten antworteten die Kinder mit sechs Spieleseiten (dabei tauchte mehrfach Spielaffe auf, des Mailingdienstes Web.de und weiteren Webseiten wie Scoyo und Girlsgogames. Weiterhin wurden die großen Onlineshops Amazon und Ebay genannt, die im Rahmen der Analyse weniger in Zusammenhang mit Kindern gebracht wurden, da dort Kaufverträge die Grundlage der Aktivitäten bilden.

Betrachtung des Zusammenhangs

Es zeigt sich, dass Kinder, die bei Frage 3 angegeben haben, dass sie sich grundsätzlich oder oft sicher im Internet fühlen, auch mehr der vorgestellten Webseiten kennen und diese auch oft positiv bewertet haben. Ebenfalls haben diese bei Frage 2 angegeben, dass sie häufiger im Internet sind (also ein- oder mehrmals täglich) und haben bei Frage 8 weniger Vorschläge für Hilfe im Internet angegeben. Im Gegensatz dazu haben Kinder, die sich Frage 3 zufolge im Internet nicht immer sicher fühlen, sehr wenige der präsentierten Webseiten als bekannt markiert. Diese Kinder sind auch seltener im Internet, als die erste beschriebene Gruppe und haben auch bei Frage 8 mehr hilfreiche Aspekte beim Umgang mit dem Internet gewählt.

5 Verbesserungsvorschläge für die IT-Sicherheit der Webseitengestaltung

Nach Abschluss der Untersuchungen, welche Kriterien eine Webseite erfüllen sollte, um als kinderfreundlich und -sicher eingestuft werden zu können, wurde als ein wesentlicher Mangel identifiziert, dass zwar prinzipiell Informationen zum Thema Sicherheit vorhanden sind, diese jedoch versteckt und unauffällig platziert sind und teilweise nicht gefunden wurden. Darauf aufbauend wäre ein grundlegender Verbesserungsvorschlag die Sicherheitshinweise sichtbar und auffällig auf der Seite zu platzieren. Seiten, die in erster Linie von Kindern besucht werden, sollten zudem die Art der Darstellung der Informationen kinderfreundlicher aufbereiten: es sollten keine langen Texte und dafür mehr Bilder verwendet werden.

Eine weitere wichtige Erkenntnis lieferte die Auswertung der Gefahreneinschätzung: zu oft stimmen die Gefahreneinschätzungen der Vorabanalyse und die der Kinder nicht überein (vgl. Abb. 8). Deshalb sollte eine Möglichkeit geboten werden, sehr deutlich zu kennzeichnen, wie sicher eine Webseite für Kinder anhand der Sicherheitsaspekte wirklich ist. Aus diesem Grund wird im Folgenden ein einheitliches Sicherheitssymbol vorgeschlagen. Dieses 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 und bei Bedarf zusätzliche Sicherheitsmaßnahmen ergreifen (z.B. keine Informationen über sich selbst geben) oder entsprechend die Eltern hinzuzuziehen. Im Folgenden werden nun Vorschläge für Sicherheitssymbole bzw. Sicherheitsmetaphern gegeben.

5.1 Sicherheitssymbol

Diese Figur ist als Beispiel für ein allgemeines Symbol angedacht, das auf Webseiten platziert werden sollte, um sichtbar zu kennzeichnen, wie kinderfreundlich die entsprechende Seite ist. Hierbei wurde die Analogie zur Fußgängerampel durch die Farbkodierung verwendet. Die Farbe gelb wurde hinzugefügt, um entsprechende Webseiten, die entweder nicht beurteilt wurden oder IT-Sicherheitsaspekte in einzelnen Punkten nicht vollständig kinderfreundlich umgesetzt haben, ebenfalls in das Konzept

mit aufzunehmen. Zusätzlich wird das Sicherheitssymbol durch die Mimik der Comicfigur unterstützt. In Abbildung 9 sind jeweils zwei unterschiedliche grafische Repräsentationen abgebildet.

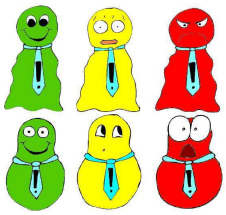

Abbildung 9: Entworfene Figur als Sicherheitssymbol

5.2 Metaphorisches Konzept zur Visualisierung der IT-Sicherheitsaspekte

Da heute die Datenübertragungsraten im Mittel sehr hoch sind, können zukünftig neben den herkömmlichen informationsvermittelnden Repräsentationstechniken, wie Text oder kleine Bilder auch Medien wie Audio, Video und/oder spielerisch aufbereitete Inhalte übertragen werden. Unter dieser Voraussetzung soll hier ein Vorschlag gemacht werden, wie das Thema IT-Sicherheit in seinen Aspekten den Kindern altersgerecht vermittelt werden kann. Zu Beginn sei vorangestellt, dass eine multimediale Darstellung die Aufmerksamkeitsselektion sowie -fokussierung besser adressiert als eine rein textuelle oder grafische Darstellung.

Ziel der metaphorischen Darstellung ist, ein sogenanntes „natural mapping“ herzustellen. Dies bedeutet, dass die IT-Sicherheitsaspekte auf ein natürliches, möglichst allen Kindern bekanntes Szenario übertragen werden und die Kinder entsprechend den Zusammenhang zwischen den abstrakten IT-Sicherheitsaspekten und der natürlichen Situation herstellen und somit die Bedeutung der IT-Sicherheitsaspekte erfassen und verstehen. Eine Möglichkeit wäre die Übertragung des Computers auf das eigene Kinderzimmer. Hier könnte bezüglich der Vertraulichkeit eine Visualisierung im Kontext des „offenen Liegenlassens von geheimen Sachen“ oder durch ein „Spähen durch das Fenster“ im Video oder bildlich, mit entsprechenden Audiokommentaren realisiert werden. Bezüglich der Passwortsicherheit wäre das Abschließen der Kinderzimmertür bzw. des geheimen Tagebuchs eine denkbare Metapher. Zusätzlich könnte hier ebenfalls visualisiert werden, dass es auch wichtig ist, wer für welches der beiden genannten Beispiele einen Schlüssel hat. So sollten natürlich die Eltern einen Schlüssel für die Kinderzimmertür haben, Freunde jedoch nicht und die beste Freundin möglicherweise einen Schlüssel für das Tagebuch, aber nicht für die Kinderzimmertür. Dies soll beispielhaft illustrieren, dass eine Übertragung der abstrakten IT-Sicherheitsaspekte in reale Szenarien durchaus möglich ist und evtl. ein entsprechendes Potential bieten. Neben der Darstellung durch ein Video könnte ebenfalls ein sogenanntes Browserspiel entwickelt werden, mit dem Ziel, innerhalb der Metapher (hier: das Kinderzimmer) die IT-Sicherheitsaspekte umzusetzen. Durch den interaktiven Charakter würde sowohl die Aufmerksamkeitsfokussierung als auch die Motivation des Kindes gefördert und evtl. die Beachtung der IT-Sicherheitsaspekte nicht als Last oder notwendiges Übel, sondern als meisterbare Herausforderung wahrgenommen. Diese Annahmen sollten zukünftig alternativ zu den bisherigen Ansätzen durch Webseitenbetreiber aufgegriffen und untersucht werden.

6 Zusammenfassung und Ausblick

In der Untersuchung wurde gezeigt, dass an vielen Stellen noch akuter Aufholbedarf bezüglich der IT-Sicherheit und deren Repräsentation für Kinder im Internet besteht. Es ist zu erkennen, dass sich Kinder zwar mit diesen Themen befassen, aber dennoch treten zu viele Lücken im sicheren Umgang mit dem Internet auf. Es gibt bereits Webseiten, die speziell für Kinder entworfen wurden. Jedoch sind diese oftmals nicht bekannt [KI3] und/oder behandeln das Thema IT-Sicherheit nicht explizit. Vielerorts ließen sich keine Informationen zu Sicherheitsaspekten auf Webseiten finden. Weiterhin bietet die Qualität der Aufbereitung der Sicherheitsthemen besonders im Bereich des Datenschutzes und des Schutzes der Privatsphäre noch enormes Potential. Hierzu sollten vermehrt multimediale Techniken verwendet werden. Besonders für Kinder eignet sich Wissensvermittlung durch Videos oder spielerisches Lernen mehr als eine rein textuelle Darstellung. Es sollte ein einheitliches Symbol gefunden werden, das die Sicherheit von Webseiten charakterisiert. Wichtig ist, dass Kinder Unterstützung und Hilfe beim Erlernen des korrekten Umgangs mit dem Internet benötigen und sie sollten verstärkt darüber aufgeklärt werden, was mit den Daten geschieht, die sie im Internet preisgeben.

Der Ansatz der Metapher und deren Umsetzung soll in weiteren Projekten vorangetrieben werden. Hierzu sollen auch verstärkt Kinder im entsprechenden Alter eingebunden werden, um eine auf das Kind abgestimmte multimediale Repräsentation zu ermöglichen.

Quellenangaben

[Ih1] Klassisches wird von elektronischem Spielzeug verdrängt: Kinder stehen auf Computer, Handy und Fernsehen, http://www.golem.de/0708/53966.html, 7.8.2007, Jens Ihlenfeld, letzter Zugriff 26.01.2012

[Zi2] Studie: 68 Prozent der erwachsenen Deutschen sind online, http://heise.de/-135011, 16.01.2007, Peter-Michael Ziegler, letzter Zugriff 26.01.2012

[KI3] KINDERSICHERHEIT.NET, http://kinderseiten.net/tag/kindersicherheit, letzter Zugriff 26.01.2012

[K94] K9 Web Protection, http://www1.k9webprotection.co, letzter Zugriff 26.01.2012

[MTF5] Wiebke Menzel, Sven Tuchscheerer, Jana Fruth, Christian Krätzer, Jana Dittmann: *Designansatz und Evaluation von kindgerechten Securitywarnungen für Smartphones*. Proc. Sicherheit 2012: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI). Neeraj Suri, Michael Waidner (eds.), Gesellschaft für Informatik e.V. (GI), Darmstadt, 7.-9. März 2012, LNI 195 GI 2012, Köllen Druck+Verlag GmbH, Bonn, pp. 211-223, 2012.

[MTF6] Wiebke Menzel, Sven Tuchscheerer, Jana Fruth, Christian Kraetzer, and Jana Dittmann: *Design and evaluation of security multimedia warnings for children's smartphones*. In Reiner Creutzburg, David Akopian, Cees G. M. Snoek, Nicu Sebe, Lyndon Kennedy (Eds.): Multimedia on Mobile Devices 2012, Proc. SPIE 8304, 83040B

[Eck7] Claudia Eckert: *IT-Sicherheit. Konzepte - Verfahren - Protokolle*. 7., überarbeitete und erweiterte Auflage, Oldenbourg, München, 2012

Acknowledgements

S. Kuhlmann and J. Fruth are funded by the German Ministry of Education and Science (BMBF), project 01IM10002A. The presented work is part of the ViERforES II Project.

Wir danken den Studierenden S. Lehmann, M. Schulze, M. Mikuteit und L. Osten für die Unterstützung bei der Analyse und der Erstellung dieses Beitrags.