Ein erster Prototyp: Sicherheitsguide für Grundschulkinder beim Umgang mit dem Internet

Jana Fruth, Matthias Thimm, Sven Kuhlmann, Jana Dittmann
Otto-von-Guericke-Universität Magdeburg
Fakultät für Informatik
PO Box 4120, D-39016 Magdeburg
fruth@ovgu.de, matthias.thimm@st.ovgu.de, stuchsch@ovgu.de, jana.dittmann@ovgu.de

Abstract: Bereits Grundschulkinder nutzen das Internet regelmäßig. Dabei sind sie häufig Sicherheitsgefahren ausgesetzt, mit denen sie nicht umgehen können. In diesem Beitrag wird ein Konzept und Prototyp eines softwarebasierten Sicherheitsguides vorgestellt, der 6 bis 10 jährige Grundschulkinder für potentielle Sicherheitsgefahren im Internet sensibilisieren und ihnen Handlungskompetenzen für Sicherheitsmechanismen vermitteln soll. Der Prototyp wurde mit einer Nutzerstudie in einer Grundschule mit einer eigenen Methodik evaluiert. Die vermuteten Lerneffekte sind allerdings in Zukunft noch mit weiteren Tests zu belegen.

1 Einführung und Motivation

Das Internet nimmt in unserer Gesellschaft einen immer höheren Stellenwert ein. Internetnutzer sind in sämtlichen Altersgruppen zu finden. Diverse Studien belegen, dass vor allem der Anteil der Nutzer im Kindesalter stetig zunimmt. Laut [BR12] surfen ca. 40% der 6 bis 10-Jährigen mindestens einmal pro Woche im Internet. Dabei sind gerade Grundschulkinder wenig für Onlinegefahren sensibilisiert, wie verschiedene Studien [BR12][LHGO11][KHFD12] einstimmig belegen. Ursachen für das Eingehen von Sicherheitsrisiken im Internet von jungen Schulkindern sind u.a. das mangelnde Bewusstsein für Onlinegefahren und die mangelhafte Fähigkeit, kritische Situationen zu bewältigen oder abzuwehren [OEC11]. Beim Surfen im Internet können Kinder verschiedenen Sicherheitsgefahren ausgesetzt sein. Die häufigsten sicherheitskritischen Online-Aktivitäten von Kindern sind: das Veröffentlichen persönlicher Informationen, der Zugriff auf nicht vertrauenswürdige Webseiten oder Inhalte, das Herunterladen von Inhalten nicht vertrauenswürdiger Webseiten und das Chatten mit Fremden. Potentielle sicherheitskritische Konsequenzen können beispielsweise der Missbrauch persönlicher Informationen durch Fremde, Cybermobbing oder das Installieren von Schadsoftware sein [FSRD13].

Für die spätere Entwicklung im Umgang mit dem Internet ist es daher förderlich, Kindern schon im frühen Alter das Bewusstsein über die Gefahren des Internets zu vermitteln. Weiterhin sollten ihnen Hilfestellungen für die Handhabung von Sicherheitsmechanismen gegeben werden. Diese Arbeit ist nicht allein von den Eltern oder Lehrern zu bewerkstelligen, die sich oft im Hinblick auf die medienerzieherische Sicherheit im Internet, nicht

genügend informiert fühlen [KHFD12]. Derzeit gibt es nur wenige medienpädagogischen Angebote zur Sensibilisierung und dem Vermeiden von Onlinegefahren in Grundschulen. Lehrer und Medienpädagogen bestätigten hier einen hohen Bedarf, der bisher nicht durch vereinzelte Projekte gedeckt werden kann. In diesem Beitrag wird daher ein zum Unterricht alternativer Ansatz vorgestellt. Mit Hilfe eines so genannten softwarebasierten Sicherheitsguides[1], sollen Kinder im Grundschulalter für den sicheren Umgang mit dem Internet sensibilisiert werden und den Umgang mit Sicherheitsmechanismen erlernen. Der Sicherheitsguide soll hierbei Lehrer nicht ersetzen, sondern ist als zusätzliches Hilfsmittel für den Unterricht zu verstehen.

Folgende **Forschungsfragen** sollen dabei beantwortet werden: Welches neue Wissen und welche Handlungskompetenzen von Sicherheitsmechanismen bei Internettätigkeiten konnten Kinder mit Hilfe des Sicherheitsguides erwerben? Wie wird das multimediale Design des Sicherheitsguides von den Kindern bewertet? Eignet sich die kreierte Evaluationsmethodik, um Lerneffekte bei der Handhabung des Sicherheitsguides messen zu können?

2 State of the art: Sensibilisierung von Grundschulkindern für Onlinegefahren und Vermittlung sicherheitsbewussten Verhaltens

Im Folgenden werden verschiedene Konzepte und eigene Vorarbeiten vorgestellt, die Grundschulkinder für Onlinegefahren sensibilisieren sollen bzw. ihnen sicherheitsbewusstes Verhalten vermitteln helfen.

Es existieren zahlreiche Konzepte zur **Sicherheitssensibilisierung/-schulung von Grundschulkindern**[2]. Zum Einen wird ***Informationsmaterial*** von verschiedenen Initiativen zur Verfügung gestellt, z.B. vom deutschen Kinderhilfswerk [FO09]. Diese Ratgeber enthalten kindgerecht aufgearbeitete Informationen für Kinder zu Sicherheitsgefahren im Internet und Tipps für ein sicheres Verhalten im Netz. Weiterhin gibt es eine Vielzahl von ***Onlineangeboten***, die Kindern spielerisch Onlinegefahren und Sicherheitsmechanismen vermitteln, z.B. die Trickfilme des EU-Projekts "Sheeplive"[3]. Es gibt zum Thema auch vereinzelte ***Lernangebote*** in Grundschulen, die aber abhängig vom Bundesland bzw. Bildungsträger sind. Weiterhin bieten auch außerschulische Einrichtungen, wie die Polizei und Medienpädagogen Schulungen für Kinder an. Besonders die Polizei offeriert hier ein umfassendes Lehrangebot zur Internetsicherheit [Pol10]. Diese Angebote sind allerdings nicht für Grundschüler, sondern für ältere Kinder (ab ca. 12 Jahren) konzipiert. Die bisher vorgestellten Konzepte haben aus psychologischer Perspektive einen Nachteil: Die Informationen werden abstrakt, also getrennt von der eigentlichen Internetaktivität vermittelt. Es wird so genanntes Faktenwissen [And76] gelehrt. Unserer Ansicht können bessere Reaktionen erzielt werden, wenn Kindern in der aktuellen Situation im Internet, Hilfestellung zu aktuellen Sicherheitsbedrohungen gegeben und somit Handlungswissen vermittelt wird. Der in diesem Beitrag in Kap. 4 vorgestellte Sicherheitsguide ist ein erster

[1] Der in diesem Beitrag beschriebene softwarebasierte Sicherheitsguide basiert auf der Bachelorarbeit von Matthias Thimm [Thi13].

[2] Hinweis: Aufgrund des begrenzten Platzes können nur einige ausgewählte Konzepte erwähnt werden!

[3] de.sheeplive.eu, letzter Zugriff: 5. Mai 2014

Prototyp, der dieses Konzept umsetzt. Ein weiterer Ansatz ist das ***Konzept des sicheren Surfraums*** [Kal13]. Ziel ist es, Kinder erst gar nicht Onlinegefahren auszusetzen. Dieser Ansatz verhindert den Aufbau von Handlungswissen. Technische Lösungen zur Umsetzung des Surfraums sind kindgerechte Suchmaschinen im Internet, wie fragFINN[4], und Jugendschutzsoftware, wie JusProg[5]. Die Verwendung eines freien Ansatzes könnte Kindern die Möglichkeit geben, sich mit Onlinegefahren auseinanderzusetzen und so direkt am Beispiel nach dem Ursache-Wirkungs-Prinzip zu lernen und Handlungskompetenzen aufzubauen. Der in Kap. 4 vorgestellte Prototyp setzt diesen Lösungsansatz des Sicherheitsguides um.

Eigene Vorarbeiten: In [KHFD12] wird eine eigene *Studie zum Sicherheitsbewusstsein von Kindern* bezüglich ausgewählter Webseiten beschrieben. Evaluationsziele sind die Thematisierung ausgewählter Sicherheitsthemen auf den untersuchten Webseiten und die kinderfreundliche Umsetzung der Inhalte. Die Studie ergab, dass Kinder ein gemindertes Sicherheitsbewusstsein bezüglich der von ihnen oft genutzten Webseiten haben und computererfahrene Kinder Webseiten hinsichtlich ihrer Gefährlichkeit positiver bewerten, als weniger computererfahrene Kinder. [MTF+12] beschreibt ein Konzept *multimedialer Sicherheitswarnungen für Smartphones für Grundschulkinder*, welches exemplarisch für ausgewählte Angriffsszenarien umgesetzt, prototypisch auf einem Smartphone implementiert und in einer Nutzerstudie getestet und evaluiert wurde. Der multimediale kindgerechte Designansatz dient als Basis für die softwareseitige Unterstützung für Kinder beim sicheren Surfen im Internet, wie sie in diesem Beitrag beschrieben wird.

3 Designkonzept: Sicherheitsguide für Grundschulkinder

Im folgenden Kapitel wird das Designkonzept des Sicherheitsguides für Grundschulkinder beschrieben. Zunächst wird auf verschiedene Informationsstufen und Einsatzmodi des Sicherheitsguides eingegangen.

Informationsstufen und Einsatzmodi: Die Bewertung der auf einer Webseite getätigten Aktion des Kindes, erfolgt über die Einstufung in verschiedene ***Informationsstufen***, die zugehörige Ereignisse auslösen. Diese Stufen sind an den Bedrohungsstufen des BSI-Standards 100-2 angelehnt [Bun08]. Diese ereignisbasierten Aktionen werden je nach Informationsstufe vom Sicherheitsguide dem Nutzer auf unterschiedliche Art und Weise zurückgemeldet, zum Beispiel als Information (Hinweise, positives Feedback) oder Warnung (Bedrohungen). Kindern soll dadurch eine schnelle Einschätzung der aktuellen Bedrohungslage ermöglicht werden. Folgende vier Informationsstufen wurden umgesetzt: Die *Hinweisstufe* hat rein informative und unterstützende Funktion. Den Kindern werden nähere Informationen zur Funktionsweise einer Webseite und Sicherheitsmechanismen gegen bestimmte Onlinegefahren erläutert. Die *Schutzstufe* erzeugt positives Feedback, z.B. bei Eingabe eines als sicher eingestuften Passwortes. Die *Bedrohungsstufe mittel* meldet dem Nutzer mittels Warnmeldungen eine Verletzung von einzelnen oder mehreren Sicherheitsaspekten zurück, z.B. im Fall des Betretens eines Anmeldebereiches einer

[4] www.fragfinn.de, letzter Zugriff: 5. Mai 2014
[5] www.jugendschutzprogramm.de, letzter Zugriff: 5. Mai 2014

Webseite eines sozialen Netzwerks, welche als sicherheitsgefährdend gewertet wird. Die *Bedrohungsstufe hoch* weist auf ein erhöhtes Sicherheitsrisiko hin, z.B. bei Offenlegung persönlicher Informationen.
Die Aktivierung der vier genannten Informationsstufen basiert auf häufig durchgeführten Internettätigkeiten [BR12] (s. Tab. 1). Die ersten fünf in Tab. 1 angeführten Aktionen, be-

Tabelle 1: Oft getätigte Aktionen im Internet [BR12].

Tätigkeit	Prozentzahl der Befragten	Altersrahmen der Befragten
Nutzung einer Community-Seite	44%	6-13 Jahre
Nutzung einer Online-Anmeldung	>44%	6-13 Jahre
Nutzung einer E-Mail-Seite	40%	10-11 Jahre
Nutzung einer Chat-Seite	30%	10-11 Jahre
Nutzung einer Suchmaschine	99%	6-13 Jahre
Eingabe eines Passwortes	>44%	6-13 Jahre
Herunterladen einer Datei	36%	10-11 Jahre

schreiben das Betreten einer Internetseite. Der Sicherheitsguide soll die jeweilige Seite erkennen und für den identifizierten Webseitentyp neue eventbasierte Aktivierungen für die verschiedenen Informationsstufen zur Verfügung stellen. Eine Ausnahme bilden die letzten beiden in Tab. 1 aufgelisteten Internetaktionen. Über diese Ereignisse wird permanent, also unabhängig von der aufgerufenen Webseite, gewacht.
Die Informationsstufen ermöglichen es, an die Tätigkeiten des Nutzers angepasste Rückmeldung zu geben. Allerdings sind wiederholt eingeblendete Warnhinweisen zu meiden, um bei den Kindern Frustration und Ablehnung des Sicherheitsguides zu verhindern [Jür03]. Eine Lösung der Problematik wäre die Verwendung verschiedener ***Einsatzmodi***. Eine Aufteilung in einen Betriebsmodus und einen Lernmodus wäre denkbar. Der *Betriebsmodus* soll auf eine weitestgehend unterbrechungsfreie Nutzung des Internets ausgelegt sein. Es sollen nur Warnmeldungen der beiden Bedrohungsstufen angezeigt werden. Zur Gewährleistung eines unterbrechungsfreien Betriebs sollte weiterhin in diesem Modus die Wiederholung einer Nachricht zeitweise blockiert werden können. Der *Lernmodus* hingegen, ist dazu konzipiert, Kindern ihre Handlungen zu erklären und ihnen diese besser zu verdeutlichen. Daher sollten in diesem Modus Meldungen aller Informationsstufen angezeigt werden.

Multimediales Designkonzept: Der in diesem Beitrag beschriebene Sicherheitsguide für Grundschulkinder ist mittels multimedialer Mittel durch visuelle und akustische Designelemente kindgerecht gestaltet worden (s. Abb. 1). Das ***visuelle Design*** ist das primäre Designkriterium, da Informationen auf Rechnern im Allgemeinen visuell vorliegen und im Gegensatz zu akustischen und haptischen Designelementen, permanent verfügbar sind. Das visuelle Feedback des Sicherheitsguides besteht vor allem aus der Einblendung von (Warn-)Hinweisen und einer Helferfigur, die das Kind unterstützend begleitet, sowie einer Informationsansicht, die die derzeitige Gefahrensituation dem Kind rückmeldet. Eine *Helferfigur* wurde gewählt, da Kinder häufig dazu tendieren, Formen eine Seele zuzuordnen. Diese abstrahierte, comichafte Art der Darstellung ist Kindern auch bereits aus Computerspielen und Trickfilmen bekannt und wird dort gut angenommen [MTF+12]. Die Mimik des Helfers eignet sich sehr gut, um dem Kind eine schnelle visuelle Rückmeldung über den aktuellen Bedrohungsgrad zu geben. Die Farbe des Gesichts soll zudem eine von drei

verschiedenen Informationsstufen (s. Abb. 1(a), Helferfigur nach [6]) ausdrücken. Hier bieten sich die Farben der Ampel an, die jedes Grundschulkind bereits kennt und denen es somit automatisch eine Bedeutung zuordnen kann [MTF+12].
Neben der Änderung der Mimik und Hintergrundfarbe soll eine so genannte *Informationsansicht* die aktuelle Sicherheitsgefahrenlage und die Art der Bedrohung Kindern leicht verständlich visualisieren. Falls der Nutzer nähere Informationen wünscht, wird zur Informationsansicht gewechselt. Diese ist als Baum gestaltet (s. Abb. 1(b)). Sie soll Kindern vermitteln, dass analog zum Lebewesen Baum auch der Umgang mit dem Internet eine gewisse Sorgfalt bedarf. Die Blätter des Baumes stellen die sechs Sicherheitsaspekte (Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, Nichtabstreitbarkeit und Privatspäre) und deren derzeitigen Gefährdungszustand dar. Um diese Aspekte für Kinder verständlicher zu halten, werden hierbei abstrahierte Symbole genutzt, wie zum Beispiel ein Briefumschlag für die Vertraulichkeit. Ist ein Sicherheitsaspekt gefährdet, wird dies durch Anfärbung des entsprechenden Blattes des Baums visualisiert. Durch Klick auf das Symbol des jeweiligen Sicherheitsaspekts werden dem Nutzer nähere Informationen zum derzeitigen Zustand dieses Bereiches angezeigt. Die *Textgestaltung* ist an die Fähigkeiten

(a) Rückmeldung der Informationsstufe mittels Mimik und Farben (links oben: Bedrohungsstufe hoch (rot), rechts oben: Bedrohungsstufe mittel (gelb), unten: Schutzstufe (grün))

(b) Informationsansicht

Abbildung 1: Visuelles Design des Sicherheitsguides

von Grundschülern angepasst. Dazu gehört eine leicht verständliche Sprache und die Verwendung kinderfreundlicher Synonyme und Metaphern [FSRD13]. Es werden lineare, serifenlose Schriftarten verwendet, da sie auf digitalen Ausgabegeräten einfacher lesbar und besser verständlicher sind [Jür03]. Weiterhin wird eine ausreichend große Schriftgröße verwendet, um die Lesbarkeit zu gewährleisten, da Kinder im Grundschulalter noch nicht so viel Routine im Lesen haben wie ältere Kinder.
Das ***akustische Design*** soll das visuelle Design unterstützen. Die Stimmung der Helferfigur spiegelt eine *abstrahierte Sprache aus verschiedenen Tonfolgen* wider, welche aus Videospielen für Kinder bekannt sind und dort gut angenommen werden. Weiterhin werden diverse *Warnsignale* verwendet, die sich je nach der von einer Aktion ausgelösten

[6] http://www.deviantart.com/art/Expression-Chart-Pandora-258457532, letzter Zugriff: 17. Juni 2014

Informationsstufe, in ihrem Klang, ihrer Länge und der Anzahl ihrer Wiederholungen unterscheiden. In der Schutzstufe wird ein belohnendes akustisches Feedback durch eine höhere, kurze, nicht wiederholte Tonreihenfolge zurückgegeben. Das akustische Feedback der beiden Bedrohungsstufen ist im Gegensatz dazu um einiges tiefer und in die Länge gezogen, welches in der Bedrohungsstufe hoch zusätzlich noch wiederholt wird.

4 Prototypische Implementierung des Sicherheitsguides

Im Folgendem werden der Sicherheitsguide für Grundschulkinder und die Testumgebung beschrieben.

Aufbau des Sicherheitsguides: Der Prototyp wurde als browserbasiertes Firefox-Addon realisiert, welcher von den Probanden innerhalb einer geschlossenen Umgebung, in Form eines Offline-HTML-Szenarios, genutzt wird. Die geschlossene Testumgebung war aufgrund datenschutzrechtlicher Anforderungen notwendig geworden. Diese fasst verschiedene Testszenarien auf drei HTML-Seiten zusammen. Während die Probanden in dieser Testumgebung bestimmte Aufgaben erledigen, überwacht der Prototyp die getätigten Aktionen und gibt diesen Feedback. Bei sicherheitskritischen oder sicherheitskonformen Aktionen in der Testumgebung gibt der Sicherheitsguide Rückmeldung in Form von (Warn-) Meldungen. Die Funktionsfähigkeit des Addons ist dennoch außerhalb dieser Testumgebung gewährleistet.

Für die Implementierung des Sicherheitsguides wurden die in Kap. 3 gewählten Designkriterien realisiert. Umgesetzt wurde nur der *Lernmodus*, um Hinweise zu Lerneffekte zu evaluieren. Die Programmstruktur des Sicherheitsguides unterliegt einem modularen Aufbau, welcher eine schnelle Erweiterung und kompletten Austausch von Textinformationen, Validationslisten und Helferfiguren innerhalb weniger Minuten ermöglicht. Innerhalb der Startform werden separat hinterlegte *Validationslisten* geladen. Diese können entweder ganze Internetadressen oder Teilzeichenketten enthalten und können aktuell besuchte Seiten mit Hilfe regulärer Ausdrücke klassifizieren. Es wird validiert, welche Rückmeldung auf der besuchten Seite zu geben ist und welche seitenspezifischen Inhaltsskripte aktiviert werden müssen. Je nach Informationsstufe ändern sich der Text der angezeigten Hinweis- und Warnmeldungen und das optische Erscheinungsbild der Helferfigur. Die Meldungen bieten dem Nutzer zwei Auswahlmöglichkeiten an. Mit einem Klick auf “Okay” schließt sich das Fenster. Mit dem Klick auf “weitere Informationen” öffnet sich die Informationsansicht (s. Abb. 1(b)), welche die derzeitige Sicherheitsgefahrenlage beschreibt.

Die virtuelle **Testumgebung** ist in drei verschiedene, selbst erstellte Webseiten aufgeteilt, um datenschutzrechtlichen Anforderungen zu genügen. Den Probanden werden ausgewählte Abbildungen realer Szenarien präsentiert[7]. Die Aufgabe der Probanden ist es, die auf der Seite geforderten Eingaben zu tätigen. Dabei wird das Kind vom Sicherheitsguide je nach Einhaltung der Sicherheitsanforderungen ein positives oder negatives Feedback auf seine getätigten Eingaben erhalten. Generell gibt der Sicherheitsguides zunächst Ratschläge über das Verhalten auf einer bestimmten Seite. Der Aufbau der Testseiten ge-

[7] Hinweis: Der Sicherheitsguide funktioniert auch für reale Webseiten.

staltet sich folgendermaßen:

Die Testseite der *Registrierung* dient der Vermittlung der Erstellung eines sicheren Passwortes und dem Umgang mit privaten Daten. Die Webseite enthält mit Sternchen gekennzeichnete Pflichtfelder, die ausgefüllt werden sollen, Zusatzfelder und die Verlinkung auf AGBs. Zudem soll der Proband ein Passwort eintragen. Je nach Stärke des Passwortes wird ein passendes Feedback mit Ratschlägen für Verbesserungen angezeigt (s. Abb. 1(a)). Weiterhin erhält das Kind vor dem Absenden der eingegebenen Daten einen Hinweis, seine Eingaben noch einmal zu kontrollieren.

Die *E-Mail*-Testumgebung soll adäquates Verhalten gegenüber unbekannten Absendern von E-Mails vermitteln sowie über die nicht immer gegebene Unverfälschtheit des Inhalts der E-Mail aufklären. Der Proband hat zuerst die Aufgabe eine E-Mail zu verfassen und diese zu versenden. Diese landet dann im eigenen Postfach. Beim Öffnen des Postfachs wird das Kind noch einmal ermahnt nur E-Mails von bekannten Absendern anzunehmen und darauf hingewiesen, dass empfangene E-Mails nicht immer so ankommen müssen, wie sie abgeschickt wurden. So ist unter seinem abgeschickten Text der Spruch: “Hier könnte auch Werbung stehen” zu lesen.

Die *Chat*-Testseite soll den sensiblen Umgang mit persönlichen Informationen vermitteln und über die Anonymität des Chatpartners aufklären. Der Sicherheitsguide kontrolliert während des Programmablaufs die Eingaben der Probanden und die Ausgabe des Gegenübers. Im Chat werden zuerst zwei typische Chatnachrichten gesendet. Die dritte Nachricht fragt nach dem Alter des Probanden. Der Sicherheitsguide warnt hierbei den Probanden, keine allzu persönlichen Informationen (z.B. Adresse, Telefonnummer) an Unbekannte preiszugeben.

5 Evaluationsmethodik

Der softwarebasierte Prototyp (s. Kap. 4) des Sicherheitsguides wird in einem Testszenario von Probanden getestet und evaluiert. Dazu stehen verschiedene **Werkzeuge** zur Auswahl [LE11]. Eine Möglichkeit ist die ***Beobachtung*** der Probanden während der Nutzung des Prototyps. Anhand der Reaktionen der Probanden in bestimmten Situationen, können Rückschlüsse zur *Usability* des Prototyps gewonnen werden. Diese Reaktionen werden vom zuständigen Versuchsleiter in ein Protokoll schriftlich aufgenommen und im Nachhinein ausgewertet. Bei der ***Methode des lauten Denkens*** [LE11] verbalisiert die Testperson ihre Gedankengänge während sie den Prototypen testet. Sie kann in kleinen Gruppen und für ältere Kinder verwendet werden, um das Textverständnis und die Akzeptanz des Designkonzeptes zu ermitteln.

Um einen Wissenszuwachs und letztendlich *Lerneffekte* nachzuweisen zu können, wurde eine ***Fragebogenbefragung*** in Form eines Online-Quizzes durchgeführt [EW12]. Dazu werden mindestens drei Befragungen benötigt. Während der ersten Befragung, wird das technische Vorwissen der Probanden gemessen. Die zweite Befragung erfolgt unmittelbar nach dem Testen des Prototyps, um den direkten Lerneffekt ableiten zu können. Eine dritte Befragung sollte um einige Tage zeitversetzt erfolgen und evaluieren, über welche Zeit-

spanne das gelernte Wissen im Gedächtnis bleibt. Da keine standardisierten Fragebögen für die Evaluation geeignet waren, wurde ein eigener Fragebogen entwickelt. Er setzt sich aus einführenden Fragen zur Person des Testers und vier großen Fragebereichen mit je vier Fragen zu den Themen aus dem Bereich der Internetsicherheit zusammen (s. Abb. 2). Während es bei den persönlichen Fragen verschiedene Antwortarten gibt, hat der zweite Fragebogenteil eine festgelegte Anzahl an Antwortmöglichkeiten in Form einer Ratingskala. Diese wurden mit einem Psychologen erarbeitet. Wenn sich Probanden unsicher bei der Beantwortung einer Frage sind, tendieren sie dazu eine mittlere Antwort zu wählen. Um dies zu umgehen ist es besser, eine gerade Anzahl an Antwortmöglichkeiten vorzugeben (hier: völlig richtig, meistens richtig, meistens falsch, völlig falsch)[8].

Tabelle 2: Inhalte des Fragebogens

Bereich	Inhalte
Persönliches	Geschlecht, Alter, Einschätzung der Internetkenntnisse
Allgemein	Vertrauen in Suchmaschinenergebnisse, Gefahreneinschätzung von Downloads
Anmeldung	Vollständigkeit, Korrektheit und Vertraulichkeit der Eingaben, Handhabung der AGBs
Passwort	Länge, Zusammensetzung des Passwortes
E-Mail	Vertraulichkeit, Integrität der E-Mail-Nachrichten, technische Details
Chat	Authentizität des Chatpartners, Vertraulichkeit und Handhabung von Chatinhalten

6 Nutzerstudie: Durchführung und Testergebnisse

Im Folgendem werden die durchgeführte Nutzerstudie in einer Grundschule zur Evaluation des Sicherheitsguide-Prototypen beschrieben und die Testergebnisse erläutert und interpretiert. Die **Nutzerstudie** fand in der Dreisprachigen Internationalen Grundschule Magdeburg mit den Schülern einer 4. Klasse statt. Die Kinder hatten bereits gute technische Vorkenntnisse, da sie seit der 2. Klasse eigene Laptops im Unterricht nutzen. Die Nutzertests wurden auf vier verschiedene Tage und in drei verschiedene Phasen aufgeteilt. Es wurde ein Vortest (Fragebogen), ein Haupttest (Test Prototyp, Fragebogen) und ein Nachtest (Fragebogen) durchgeführt. Nach dem Einholen der Einverständniserklärung war es 12 Schüler/innen möglich, an den Testdurchläufen teilzunehmen. Beim *Vortest* wurde ein Online-Fragebogen von den Kindern in ca. 30 Minuten in ihrem Klassenzimmer selbständig an ihren persönlichen Rechnern ausgefüllt. Ziel war es, das technische Vorwissen der Kinder zu ermitteln, um einen Vergleichswert für spätere Befragungen zu bekommen. Der *Haupttest* wurde ca. eine Woche später an zwei Tagen nachmittags in Gruppen mit vier Kindern durchgeführt. Diese wurden im Werkraum platziert und jeweils in Zweiergruppen von einem Versuchsleiter betreut. Es herrschten für die Kinder bekannte Bedingungen zur Durchführung der Testläufe, was dem Angstabbau diente und eine entspannte Atmosphäre schuf. Schwerpunkt des Haupttests war der Test des Prototyps und die Fragebogenbefragung. Den Probanden wurden, die von ihnen zu bewältigenden Aufgaben

[8]Die mittleren Werte erhielten den Präfix “meistens”, um größere Verwirrungen bei den Kindern zu vermeiden, da die Distanz zwischen “meistens falsch” und “meistens richtig” größer wirkt und somit weniger verwirrt als die einfache Nutzung von richtig und falsch.

schriftlich ausgehändigt. Weiterhin wurde den ihnen erklärt, dass es schwerpunktmäßig nicht auf die Lösung der gestellten Aufgabe, sondern auf die Beobachtung des Helfers ankam. Der Test dauerte ca. 30 Minuten. Es folgte die Beantwortung des bereits bekannten Fragebogens, was ca. 10 Minuten beanspruchte. Anschließend wurden Fragen zur Usability des Sicherheitsguides und der Helferfigur gestellt. Abschließend fand ca. eine Woche später ein viertelstündiger *Nachtest* statt, bei welchem evaluiert wurde, inwiefern sich das erlangte Wissen eingeprägt hat. Hierzu wurde der Fragebogen ein letztes Mal von den Grundschulkindern ausgefüllt.

Testergebnisse: Die in der Grundschule durchgeführte Nutzerstudie sollte, Daten zur Evaluation von Lerneffekten und der Usability des Prototypen erheben.

Der eingetretene *Lerneffekt* wurde mit einem Online-Fragebogen (s. Tab. 2) evaluiert. Um die Antworten beurteilen zu können, war es nötig den Fragen eine gewisse Wertigkeit zu geben. In Zusammenarbeit mit IT-Security-Experten wurden den einzelnen Antwortmöglichkeiten die Werte von 1 (ganz falsch) bis 4 (absolut korrekt) zugewiesen. Den dazwischen liegenden Antworten wurde je nach ihrer Tendenz zur Korrektheit der Antwort, der Wert 2 oder 3 zugewiesen. Es konnten maximal 192 Punkte pro Fragenkomplex und 960 Punkte insgesamt erreicht werden. Den Antworten der anonymisierten Probanden wurde die zugehörige Punktzahl für jede Testphase zugewiesen. Anhand der erreichten Punktzahlen war es möglich das Feedback des Sicherheitsguides zu evaluieren. Eine steigende Punktzahl zwischen dem Vor- und dem Haupttest könnte auf einen Wissenszuwachs hindeuteten. Eine höhere Punktzahl des Nachtests im Vergleich zum Vortest könnte ein Hinweis auf einen eingetretenen, beständigen Lerneffekt sein. Um einen Überblick über die Bewertung des Sicherheitsguides als Ganzes zu bekommen, wurden die einzelnen Fragen innerhalb einer Testphase aufsummiert (s. Abb. 2). Die Zahlen deuten auf einen Wissenszuwachs vom Vor- zum Haupttest hin. Weiterhin weisen die vom Helfer abgedeckten Fragebereiche einen höheren Punktestand zwischen Haupt- und Nachtest auf, was auf Lerneffekte hinweisen könnte. Die statistische Untersuchung der Testergebnisse mittels multivariater Varianzanalyse konnte allerdings keine signifikante Steigerung des Wissens- und Lernzuwachses belegen. Daher wurde die Effektstärke nach Cohen [Bor05] jeweils für die Ausprägungen innerhalb der fünf Kategorien zwischen Vortest und Nachbzw. Langzeittest ermittelt als Indikator für die praktische Relevanz der Ergebnisse bei nicht signifikanten Unterschieden in kleinen Stichprobengrößen. Der Konvention [Bor05] folgend werden diese als: 0,2 kleiner, 0,4 bis 0,5 mittlerer und 0,8 starker Effekt definiert. Hierbei wurden zwei mittlere Effekte gefunden. Der “Passwortschutz” (d=0,46) und in der Kategorie “Chat” (d=0,41). Demnach profitieren die Kinder vor allem in diesen beiden Kategorien am stärksten von den Funktionen des Sicherheitsguides, was hierbei auf ein hohes Lernpotential schließen lässt.

Die erzielten Ergebnisse sind allerdings kritisch zu sehen. Der Erfolg der Wissensvermittlung des Sicherheitsguides hätte durch eine Nutzerstudie mit mehreren Kontrollgruppen besser eingeordnet werden können. Während die Probanden der ersten Kontrollgruppe in keinerlei Hinsicht für Onlinegefahren sensibilisiert worden wären, hätte einer zweiten Kontrollgruppe klassisches Informationsmaterial zu IT-Securitygefahren im Internet ausgehändigt werden können.

Aussagen zur *Usability* des Sicherheitsguides wurden mit der Methode des lauten Denkens, der Beobachtung sowie der Befragung der Grundschulkinder erhoben. Nach Aus-

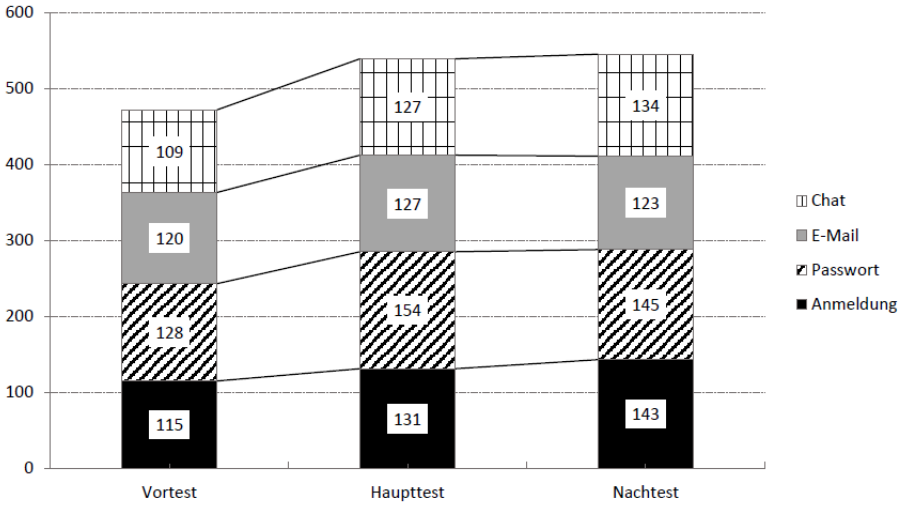

Abbildung 2: Punkteverteilung der vom Helfer behandelten Themengebiete über den Testzeitraum

sagen der Kinder war der Sicherheitsguide problemlos bedienbar. Gute Bewertungen erhielten auch das optische Design, einschließlich der Helferfiguren und der Informationsansicht. Wobei letztere von den Kindern selten angeklickt wurde. Als Lösungsalternative wäre eine Verschmelzung von Helfer und Informationsansicht denkbar.

7 Zusammenfassung und Ausblick

Ziel dieser Arbeit war es, Kinder im Grundschulalter von 6 bis 10 Jahren für den sicheren Umgang mit dem Internet zu sensibilisieren und ihnen Handlungskompetenzen für Sicherheitsmechanismen vermitteln. Restriktive Ansätze bieten hier jedoch keine Lösungen. In dieser Arbeit wurde ein alternativer Ansatz vorgestellt, der diese Ziele mittels eines softwarebasierten Sicherheitsguides umsetzt. Der Prototyp wurde mit einer Nutzerstudie in einer Grundschule evaluiert. Aus Datenschutzgründen wurde dazu ein virtuelles Testszenario mit realen Anwendungsfeldern aus dem Internet realisiert, in welchem die Kinder verschiedene Aufgaben zu lösen hatten (z.B. Anmeldung in einem fiktiven Portal). Die Evaluierung ergab, dass Grundschulkinder für Internetgefahren sensibilisiert werden sollten. Die Testergebnisse lassen vermuten, dass der Einsatz eines softwarebasierten Sicherheitsguides als Ergänzung zum Unterricht sinnvoll sein könnte, was allerdings mit weiteren Studien zu belegen ist.

In **Zukunft** ist das Design des Sicherheitsguides noch zu erweitern bzw. anzupassen. Beispiele sind die eindeutigere Formulierung von Informationstexten, die Nutzung mehrerer Helferfiguren und die Optimierung der Interaktion zwischen der Helferfigur und der Informationsansicht. Weiterhin sollten die Sicherheitsbegriffe, wie Vertraulichkeit, expliziter

vermittelt werden. Nähere Erläuterungen der Begriffe sind bisher nur in der Informationsansicht durch Anklicken der Symbole abrufbar. Die bisherige Nutzerstudie fand nur in einem kleinen Rahmen mit 12 Probanden an einer eher technisch-orientierten Schule statt. Um die Evaluationsergebnisse aussagekräftiger zu gestalten, wären Studien mit einer größeren Anzahl an Personen und verschiedenen Bildungshintergründen empfehlenswert. Der Prototyp ist bisher im Lernmodus implementiert und könnte um einen Betriebsmodus erweitert werden. Weiterhin soll der Sicherheitsguide auf andere Geräte (z.B. Mobiltelefone, Roboter) portiert werden. So könnte er Nutzer nicht nur für potentielle Security-Gefahren, sondern auch für Wechselwirkungen zwischen Vorfällen der Security und Safety sensibilisieren und ihnen Handlungskompetenzen für Sicherheitsmechanismen vermitteln.

Wie in anderen Warndomänen (z.B. Automobil, Produktion) spielt auch im Bereich der IT Sicherheit die Resilienz[9] des Adressaten eine vermittelnde Rolle in Bezug auf die Umsetzung der gelernten Inhalte. Hierfür sollten in folgenden Untersuchungen gezielt die Resilienzfaktoren: Emotionale Intelligenz (Problemfixierung vs. Problemlösungsorientierung) oder Kontrollüberzeugungen betrachtet werden. Je nach Ausprägung führen diese besonders auf der Verhaltensebene zur stabilen oder instabilen Anwendung von gelernten Inhalten. Darüber hinaus lassen sich diese psychologischen Prädispositionen aus den Reaktionen auf Warnungen ableiten und somit in die Gestaltung der Warnungen und Hilfestellungen integrieren. Auf diese Weise ließen sich sowohl besonders reaktive Anwendertypen identifizieren und entsprechend eine eher restriktive Umsetzung des Sicherheitsguides realisieren. Dagegen sind besonders vulnerable Anwender durch massive Warnungen schnell verunsichert. Diese sollten durch möglichst sensible Hilfe unterstützt werden. Darüber hinaus sollten gezielt Ressourcen vermittelt werden, die der Problemlösung hilfreich sind. Das bedeutet in erster Instanz eine Ableitung der Kontrollüberzeugung des Kindes in den jeweiligen Bedrohungsszenarien und eine aktive Vermittlung an soziale Ressourcen für Kinder mit sehr geringen Kontrollüberzeugungen. Für Kinder mit (zu) hohen Kontrollüberzeugungen sollten gezielt technische Ressourcen angeboten werden, die in der jeweiligen Situation Hilfestellung beinhalten. Für diese situations- und individuumsadaptive Gestaltung der Unterstützung sollte im Lernmodus eine entsprechende Reaktions- und Bewertungserfassung realisiert werden, aus der dann die oben genannten Informationen erfasst werden.

Danksagung

Wir danken der Dreisprachigen Internationalen Grundschule Magdeburg und Dr. Michael Knuth. Teile der Arbeit von Jana Fruth sind während des ViERforES[10]-Projektes entstanden, welches vom Deutschen Ministerium für Bildung und Forschung (Projektnummer 01IM10002A) finanziert wurde. Die vorliegende Arbeit wurde in Teilen durch die Deutsche Forschungsgemeinschaft unterstützt (Projekt ORCHideas, DFG GZ: 863/4-1).

[9] Unter Resilienz wird die psychische Widerstandskraft verstanden, die es ermöglicht schwierige Lebenssituationen unbeschadet zu überstehen [WW13].

[10] http://www.vierfores.de/, letzter Zugriff: 5. Mai 2014

Literatur

[And76] J. R. Anderson. *Language, memory, and thought*. The Experimental psychology series. L. Erlbaum Associates and Distributed by the Halsted Press Division of Wiley, Hillsdale and N.J and New York, 1976.

[Bor05] J. Bortz. *Statistik für Human- und Sozialwissenschaftler*. Heidelberg : Springer Medizin, 6. Auflage, 2005.

[BR12] P. Behrens und T. Rathgeb. *KIM-Studie 2012: Kinder + Medien, Computer + Internet: Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland*. Medienpädagogischer Forschungverbund Südwest, 2012.

[Bun08] Bundesamt für Sicherheit in der Informationstechnik (BSI). Standard 100-2: IT-Grundschutz Methodology, 2008.

[EW12] W. Edelmann und S. Wittmann. *Lernspychologie*. Weinheim, Beltz, 2012.

[FO09] S. Frank und S. Ostermann. *Kindersache: Der Internet-Guide für Kids*. Dt. Kinderhilfswerk, Berlin, 3. Auflage, 2009.

[FSRD13] J. Fruth, C. Schulze, M. Rohde und J. Dittmann. E-Learning of IT Security Threats: A Game Prototype for Children. In *Communications and Multimedia Security*, Lecture Notes in Computer Science, Seiten 162–172. Springer, 2013.

[Jür03] S. Jürgens. *Diplomarbeit: Evaluation von world-wide-web basierten Benutzungsschnittstellen für Kinder*. Universitat Hamburg, Fachbereich Informatik, 2003.

[Kal13] A. Kallweit. *Ein Netz für Kinder - Surfen ohne Risiko? Ein praktischer Leitfaden für Eltern und Pädagogen*. Service Kinder und Jugend. Bundesministerium für Familie Senioren Frauen und Jugend, Berlin, 10. Auflage, 2013.

[KHFD12] S. Kuhlmann, T. Hoppe, J. Fruth und J. Dittmann. Voruntersuchungen und erste Ergebnisse zur Webseitengestaltung für die Situationsbewusste Unterstützung von Kindern in IT-Sicherheitsfragen. In *Informatik 2012*, Braunschweig, 2012.

[LE11] J. Liebal und M. Exner. *Usability fuer Kids*. Vieweg+Teubner Verlag, Springer Fachmedien Wiesbaden GmbH, 2011.

[LHGO11] S. Livingstone, L. Haddon, A. Görzig und K. Ólafsson. EU Kids Online II - Final Report. 2011.

[MTF+12] W. Menzel, S. Tuchscheerer, J. Fruth, C. Krätzer und J. Dittmann. Design and evaluation of security multimedia warnings for children's smartphones. In *SPIE, Conference Multimedia on Mobile Devices*, Burlingame, Calif., 2012.

[OEC11] OECD. *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them*. 2011.

[Pol10] *Im Netz der neuen Medien: Internet, Handy und Computerspiele - Chancen und Risiken für Kinder und Jugendliche*. Polizeiliche Kriminalprävention, Stuttgart, 2010.

[Thi13] M. Thimm. *Bachelorarbeit: Konzeption und prototypische Implementierung eines Sicherheitsguides für Kinder für den Umgang mit dem Internet*. Uni. Magdeburg, 2013.

[WW13] A. Wieland und C.M. Wallenburg. The influence of relational competencies on supply chain resilience: a relational view. In *International Journal of Physical Distribution & Logistics Management*, Jgg. 43, Seiten 300–320, 2013.