Bundeskriminalamt

Gemeinsamer Abschlussbericht zum Projekt

Sicherheitsrisiken für Computeranwender im häuslichen Umfeld durch kindliche und jugendliche PC-Nutzer (SirUP)

des Methodenzentrums der Universität Landau
und des Bundeskriminalamtes

Stand: 09. August 2010

Ansprechpartner: Bundeskriminalamt
Fachbereich KI 13
Forschungsstelle für Schwere Gewaltkriminalität und IuK-Kriminalität
65173 Wiesbaden
eMail: KI13IuK@bka.bund.de

Inhaltsverzeichnis

Vorwort

Das Methodenzentrum der Universität Koblenz-Landau wurde am 17.11.2008 vom Bundeskriminalamt mit der Durchführung einer empirischen Untersuchung zum Thema „Sicherheitsrisiken für Computeranwender im häuslichen Umfeld durch kindliche und jugendliche PC-Nutzer“ (SirUP) beauftragt. Die Durchführung des Projektes erfolgte unter enger Einbindung und Beteiligung des im Bundeskriminalamt phänomenologisch verantwortlichen Fachreferates für IuK-Kriminalität und des Fachbereiches für IuK-Forschung. Das Bundeskriminalamt konnte insbesondere bezüglich fachlicher Fragestellungen zur IuK-Kriminalität im Rahmen der Projektdurchführung unterstützen. Überdies erfolgten eine enge Abstimmung zu den Studieninhalten und den Auswerteschritten zwischen der Universität Koblenz-Landau und dem Bundeskriminalamt sowie die gemeinsame Durchführung der Schülerbefragung an den verschiedenen Schulen in Rheinland-Pfalz.

An dieser Stelle möchten wir uns nochmals bei allen Beteiligten für die Unterstützung bedanken, welche diese Studie ermöglichte.

1 Einleitung

Die rasante Verbreitung der neuen Medien hat das Informations- und Kommunikationsverhalten vieler Menschen grundlegend verändert, insbesondere durch die Möglichkeiten, welche die Mobilfunktelefonie, das Internet sowie die E-Mail-Korrespondenz bieten. Waren es in der Anfangszeit des Internet vor allem die von den Websitebetreibern bereitgestellten und abrufbaren Inhalte, die das Interesse der Internetnutzer geweckt haben, so bietet heute das sogenannte Web 2.0 mit seinen Angeboten zur Mitgestaltung dieser Inhalte nahezu unbegrenzte Möglichkeiten der Wissensgenerierung und -verbreitung über jegliche Sprach- und Ländergrenzen hinweg. Darüber hinaus können im Internet u. a. Filme, Musik, Spiele oder Software nicht nur heruntergeladen, sondern auch selbst eingestellt und mit anderen Nutzern ausgetauscht werden. Dass das Internet mittlerweile zu einer grundlegenden Kommunikationsplattform geworden ist, zeigt auch die rege Nutzung von sozialen Netzwerken wie StudiVZ oder Facebook, bei denen sich die User eine persönliche Internetpräsenz aufbauen und in regen Austausch mit anderen Internetnutzern treten können.

Doch die technischen Weiterentwicklungen im Bereich des World Wide Web bieten nicht nur eine Vielzahl an Nutzungsmöglichkeiten. Sie bergen auch das Risiko, Opfer einer über das Internet verübten Straftat zu werden. Die Polizeiliche Kriminalstatistik weist für das Jahr 2008 bundesweit (ohne Bayern) 167.451 Straftaten aus, die mit dem Tatmittel Internet verübt worden sind, 2009 sind es bereits 206.909 Straftaten bundesweit (ohne Bayern). Bei den statistisch erfassten Straftaten handelt es sich hauptsächlich um die Verbreitung pornografischer Schriften, Urheberrechtsverletzungen und um verschiedene Betrugsstraftaten. Darüber hinaus sind weitere Strafrechtsnormen durch das Tatmittel „Internet“ tangiert, hierbei handelt es sich exemplarisch um Beleidigungen, Verleumdungen, Bedrohungen (z. B. Stalking) oder die Verbreitung verfassungsfeindlicher Inhalte. Auch die Veräußerung gestohlener Waren sowie der Handel mit Betäubungsmitteln und Waffen haben Einkehr in das In-

ternet gefunden.[1] Daneben wird das Internet zur Verabredung von inkriminierten Handlungen jedweder Art genutzt.

Darüber hinaus stehen auch elektronische Angriffe auf die Soft- oder Hardware des Computers oder Netzwerks, von dem aus ein Nutzer auf das Internet zugreift, im Fokus einer Vielzahl von Tätern. Ziel dieser elektronischen Angriffe, die mit Hilfe von Schadprogrammen (Malware wie z. B. Viren, Trojanische Pferde, Spy- und Adware) erfolgen, welche unbemerkt von außen in den Computer des Nutzers eingeschleust werden, sind oftmals die Veränderung oder Löschung gespeicherter Daten sowie das Ausspähen von persönlichen Daten des Nutzers oder die Kontrollgewinnung über dessen Rechner bzw. Rechnerverbund. Eine Fremd- und Fernsteuerung zielt häufig darauf ab, den Computer ohne Wissen des Nutzers zusammen mit anderen weltweit gekaperten Computern zu einem Netzwerk (Botnetz) zusammenzuschließen, um damit z. B. massenweise sogenannte Spam-Mails zu versenden oder andere Rechner (z. B. von Behörden oder Unternehmen) derart mit automatischen Anfragen zu überlasten, bis sie zusammenbrechen (Distributed-Denial-of-Service-Attacke). Dagegen ist das Ausspähen von persönlichen Daten oftmals auf die Erlangung von Zugangskennungen zu Konten oder Onlinediensten zum Zwecke deren missbräuchlicher Verwendung durch den Täter (Identitätsdiebstahl) ausgerichtet. Das Ausspähen solcher Daten kann ebenso mit Hilfe manipulierter Websites oder Links erfolgen, indem der Nutzer auf diese zugreift und anschließend sensible Informationen über sich preisgibt (Phishing).

[1] Die statistische Erfassung erfolgt über die Zuordnung der Sonderkennung „Tatmittel Internet“ zu dem jeweiligen Straftatbestand, wobei einschränkend bedacht werden muss, dass diese nicht auf Plausibilität geprüft wird.

2 Forschungsansatz

2.1 Hintergrund der Studie

Das Hauptaugenmerk bisheriger kriminologischer Studien lag insbesondere auf den Gefährdungsaspekten für Kinder und Jugendliche, die sich aus der Internetnutzung durch diese Zielgruppe ergeben können und sich z. B. durch gewaltverherrlichende, pornografische oder verfassungsfeindliche Inhalte äußern.
In Abgrenzung zu dieser Zielsetzung wird im vorliegenden Projekt untersucht, inwieweit Kinder und Jugendliche durch ihr eigenes Nutzungsverhalten eine Gefährdung der digitalen Sicherheit des von ihnen verwendeten Computers herbeiführen oder erhöhen. Auch die Wechselwirkungen zwischen dem Nutzungsverhalten der Kinder und Jugendlichen und der Kontrolle der Eltern über die Mediennutzung ihrer Kinder sowie die damit einhergehenden Gefährdungsaspekte für die elektronische Sicherheit dieses „Nutzerverbundes“ werden in der vorliegenden Studie untersucht. Die Relevanz dieses Betrachtungswinkels ergibt sich aus dem Umstand, dass in Deutschland praktisch alle Kinder und Jugendlichen Internetnutzer sind: 96,1 % der 14 bis 29-Jährigen nutzen inzwischen das Internet regelmäßig[2], in der Altersgruppe der 6 bis 13-Jährigen sind es 60 %[3].

Dem Projekt liegt dabei die Hypothese zugrunde, dass die Opferwerdung durch die zuvor beschriebenen Phänomene der Internetkriminalität, insbesondere Phishing, Botnetze und Identitätsdiebstahl, mitunter selbstbereitete Probleme sein könnten: Aus mangelnder Vorsicht auf Seiten der Kinder und Jugendlichen im Umgang mit den Risiken des Internets sowie durch fehlende Kenntnisse bezüglich der möglichen Folgen ihres Nutzungsverhaltens könnten Gefahren für sie selbst und andere Nutzer im häuslichen Umfeld entstehen. Beispielsweise könnten die Kinder und Jugendlichen mit ihrem Nutzungsverhalten den Computer (unbewusst) mit Schadprogrammen infizieren, welche in der Folge sensible Daten zugriffsberechtigter Nutzer manipulieren und ausspähen können. Exemplarisch können hier die Kontodaten der Eltern angeführt werden. Besonders gefährdet scheinen der Hypothese zufolge also solche Rechner zu sein, die von Kindern und Jugendlichen gemeinsam mit ihren Eltern oder anderen Hauhaltsmitgliedern genutzt werden.

[2] ARD/ZDF-Onlinestudie 2009.
[3] Kids-Verbraucher-Analyse 2009 (KidsVA) Egmont Ehapa Verlag.

2.2 Ziele und Fragestellungen der Studie

Die Ziele des Projekts gliedern sich wie folgt:

- Eine umfassende Untersuchung des Computer- und Internetnutzungsverhaltens von Kindern und Jugendlichen mit besonderer Berücksichtigung potenzieller Gefahrenquellen aufgrund dieses Verhaltens für andere Nutzer der entsprechenden Computer;
- Feststellung des Ausmaßes und der Intensität der Sicherungsmaßnahmen, die von den Kindern und Jugendlichen selbst oder von deren Umfeld (Eltern) zur Abwehr von Gefahren durch Internetkriminalität ergriffen werden;
- Überprüfung von Zusammenhängen zwischen dem Verhalten von Kindern und Jugendlichen im Internet und entsprechenden realen Erfahrungen mit Internetkriminalität.

Ausgehend von diesen Projektzielen soll die vorliegende Studie mit den erlangten Erkenntnissen Handlungsempfehlungen für Präventionsmaßnahmen im Bereich der Internetkriminalität generieren.

Aufgrund der Formulierung der Projektziele wurde der Schwerpunkt der Studie auf folgende Fragestellungen gelegt:

- Wie verhalten sich Computernutzer vor allem an gemeinsam genutzten Computern und wie risikoreich ist dieses Verhalten für die anderen Nutzer dieses Computers? Als gemeinsam genutzter Computer wird dabei ein internetfähiger Computer definiert, auf den mehrere Mitglieder des Haushaltes (z. B. Eltern und Kinder) gleichermaßen Zugriff haben.

- Wie viel wissen Kinder und Jugendliche über mögliche Sicherheitsrisiken und über geeignete Möglichkeiten diese einzudämmen? Wie sehr werden sie von ihren Eltern im Umgang mit dem Computer kontrolliert?

- Wie risikoreich verhalten sich die Kinder und Jugendlichen, die mehr über die Gefahren im Umgang mit dem Internet wissen und diese adäquat einschätzen können? Wie beeinflusst das Kontrollverhalten der Eltern das Verhalten von Kinder und Jugendlichen im Umgang mit dem Internet?

- Sind im entsprechenden Haushalt schon einmal Probleme in Verbindung mit Computer- und Datensicherheit aufgetreten? Welche Erfahrungen haben die Befragten mit eigener Viktimisierung gemacht?

- Welche Zusammenhänge zwischen oben genannten Faktoren lassen sich erkennen? In welchen Konstellationen kommt es besonders häufig zu Problemen mit der Computer- und Datensicherheit?

2.3 Untersuchungsmethode

Zur Beantwortung der Fragestellungen wurde ein sechsteiliger Fragebogen konstruiert, mit dem quantitativ, d. h. anhand auszuwählender Antwortkategorien, die Aussagen der Befragten über verschiedene Items erhoben wurden. Im Frühjahr 2009 wurde dieser Fragebogen den Schülerinnen und Schülern der 7. bis 10. Klassen von neun zufällig ausgewählten Schulen in Rheinland-Pfalz vorgelegt. Unter diesen Schulen befanden sich insgesamt drei Hauptschulen, drei Realschulen und drei Gymnasien, jeweils im ländlichen Raum, im städtischen Raum (ca. 100.000 Einwohner) und in einer Großstadt (ca. 200.000 Einwohner). Anschließend wurden die Daten mit Hilfe eines Statistikprogramms ausgewertet.

3 Ergebnisse

3.1 Stichprobenbeschreibung

Es wurden insgesamt 1.271 Schülerinnen und Schüler aus 56 Klassen befragt, von denen 1.171 auswertbare Daten lieferten. Die Stichprobe umfasste ca. zur Hälfte Jungen bzw. Mädchen, die zwischen 12 und 20 Jahren alt waren (Durchschnittsalter 14,7 Jahre) (Grafik 1).

Grafik 1: Altersverteilung

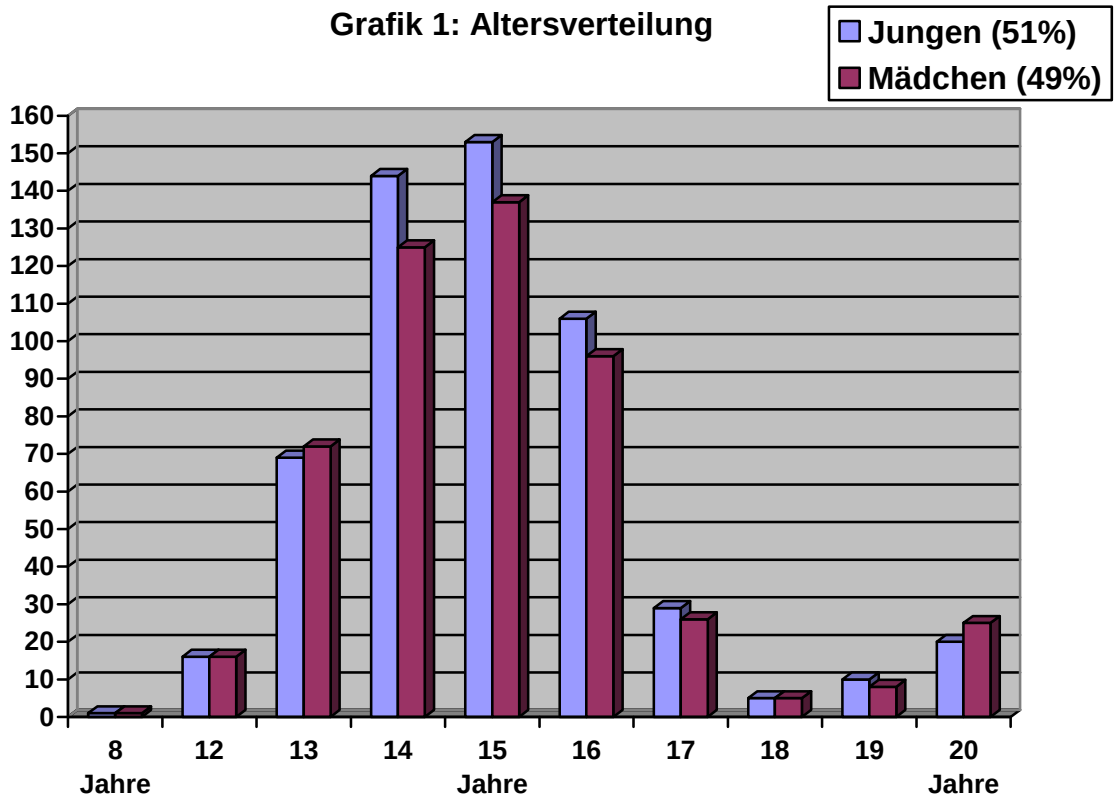


Tabelle 1a bis 1c geben einen Überblick über die Verteilung der Schülerinnen und Schüler auf die Schultypen, die Regionen und Klassenstufen.

Anteil Schülerinnen und Schüler (%) je Schultyp, Region und Klassenstufe
(N = 1.171)

Tabelle 1a:

Schultyp

Hauptschule	25 %
Realschule	36 %
Gymnasium	39 %

Tabelle 2b:

Region

ländlicher Raum	43 %
städtischer Raum (ca. 100.000 Einw.)	20 %
Großstadt (ca. 200.000 Einw.)	37 %

Tabelle 3c:

Klassenstufe

7. Klasse	26 %
8. Klasse	28 %
9. Klasse	26 %
10. Klasse	20 %

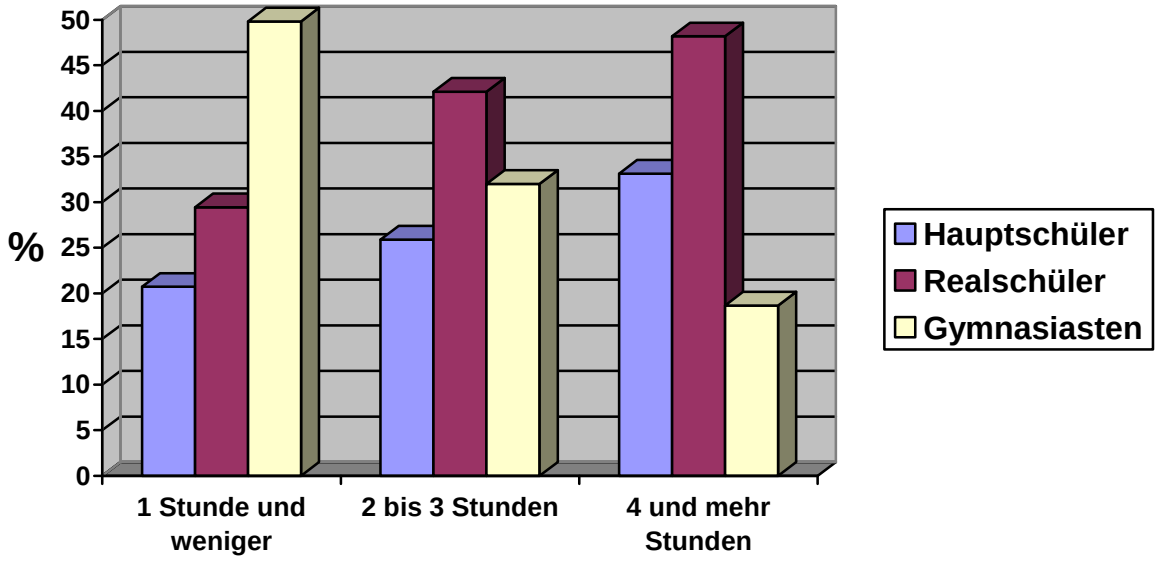
3.2 Computer- und Internetnutzung

3.2.1 Nutzungsverhalten

Von den befragten Kindern und Jugendlichen sagen mehr als die Hälfte (57 %), dass sie weniger als 1 Stunde im Durchschnitt pro Tag privat am Computer verbringen; mehr als 15 % geben eine durchschnittliche tägliche Nutzungsdauer des Computers von 4 und mehr Stunden an. Von den Befragten, die das Internet nutzen, geben 64 % an, pro Tag bis zu einer Stunde im Internet zu surfen und knapp 14 % verbringen vier Stunden und mehr im Internet.

Tendenziell verbringen Haupt- und Realschüler mehr Zeit vor dem Computer und auch im Internet als Gymnasiasten, und zwar in allen Klassenstufen (Grafik 2).

Grafik 2: Am Rechner verbrachte Zeit



Die Nutzungshäufigkeit nimmt bei den Schultypen Haupt- und Realschule über die Klassenstufen hinweg, d. h. mit zunehmendem Alter, zu.

90 % aller befragten Schülerinnen und Schüler geben an, dass mindestens ein einsatzfähiger Computer in ihrem Hauhalt vorhanden ist; gut die Hälfte von ihnen (54 %) besitzt einen eigenen Computer, also einen, der ausschließlich von ihnen selbst genutzt wird. Der Anteil der Nutzer mit eigenem Computer ist in der Altersgruppe der 14 bis 17 Jährigen am höchsten. Jungen nutzen dabei häufiger einen ei-

genen Computer als Mädchen. Die große Mehrheit (80 %) sagt jedoch, dass sie (zusätzlich zum eigenen oder ausschließlich) einen Rechner gemeinsam mit anderen Personen aus ihrem Haushalt nutzt; 71 % aller Befragten verfügen über einen gemeinsam genutzten Computer, der zusätzlich an das Internet angeschlossen ist. Die gemeinsame Nutzung eines internetfähigen Rechners in der Familie scheint also die dominierende Form zu sein, in der Kinder und Jugendliche Zugriff auf einen Computer haben. Dies unterstreicht die Relevanz des eingangs skizzierten Bedrohungsszenarios für die digitale Sicherheit heimischer PCs.

Die nachfolgenden Ergebnisdarstellungen beziehen sich nur noch auf die insgesamt 832 Schülerinnen und Schüler, die angegeben haben, über einen gemeinsam genutzten Computer mit Internetanschluss verfügen zu können.

3.2.2 Risikoverhalten

Risikoreiches Computer- und Internetnutzungsverhalten von Kindern und Jugendlichen wurde in Bezug auf *3 Bereiche (Risikoverhaltensweisen)* erfasst, und zwar mit Hilfe von insgesamt 17 Aussagen, die auf einer vierstufigen Ratingskala von 0 („trifft überhaupt nicht zu“) bis 3 („trifft voll und ganz zu“) zu bewerten waren. Diese 3 Bereiche waren:

- *Sorgfalt und Gründlichkeit im Umgang mit dem Computer* (Beispiele für Aussagen dazu: „Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.“, „Ich bin stets darum bemüht, meine Software auf dem neuesten Stand zu halten.“). Befragte, die in diesem Merkmal hohe Werte erhalten, gehen also eher sorgfältig und gründlich mit dem PC um.

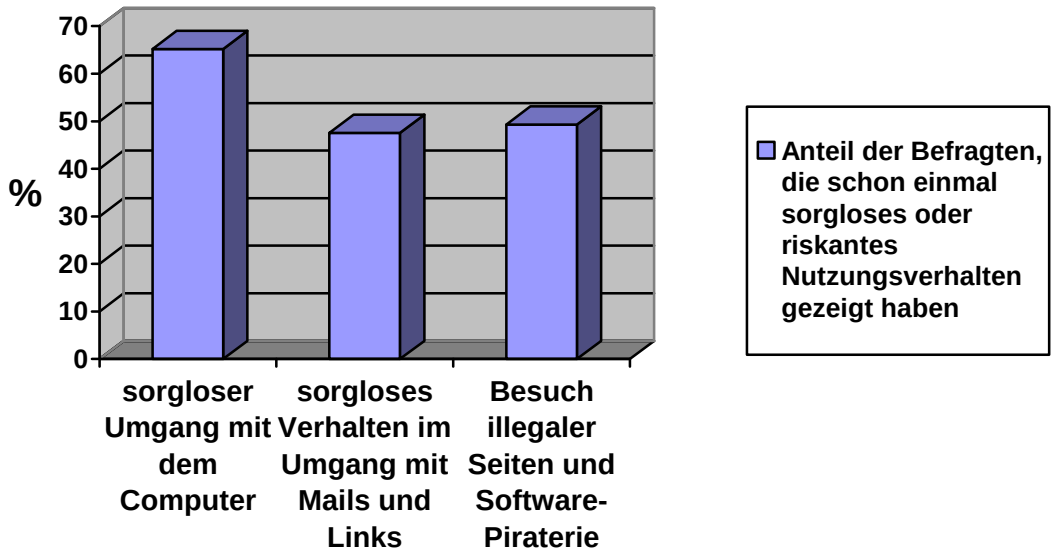
- *Sorgloses oder riskantes Verhalten im Umgang mit Mails und Links* (z. B. „Ich denke nicht lange darüber nach, einen E-Mail-Anhang zu öffnen; ich tue es einfach.“, „Es kommt schon mal vor, dass ich Werbebanner, die reizvoll klingen, anklicke.“). Wer diesen Aussagen stärker zustimmt und somit in diesem Merkmal einen höheren Wert erhält, geht also eher sorglos und riskant mit Mails und Links um.

- *Besuch illegaler Seiten und Software-Piraterie* (z. B. „Ich weiß genau, wie ich an gefälschte Seriennummern für meine Software gelange.“, „Ich habe mich schon einmal dabei erwischt, wie ich im Internet gezielt nach Seiten mit illegalen Inhalten gesucht habe.“). Wer in diesem Merkmal hohe Werte erhält, neigt eher zu illegalem Verhalten im Internet und damit zu risikoreicherem Nutzungsverhalten.

Die Analyse der Antworten der 832 Schülerinnen und Schüler mit gemeinsam genutzten Computern hat ergeben, dass im Durchschnitt vor allem im Bereich des Umgangs mit dem Computer eine mittlere Ausprägung riskanten und sorglosen Verhaltens erkennbar ist. Knapp darunter liegt die Ausprägung des Risikoverhaltens in Abhängigkeit mit dem Besuch illegaler Seiten und Software-Piraterie. Im Bereich des sorglosen Verhaltens im Umgang mit Mails und Links ist die Ausprägung riskanten Verhaltens vergleichsweise gering.

Auch wenn Ausprägungen der Risikoverhaltensweisen nur gering bzw. mittelmäßig sind, gibt nahezu die Hälfte der befragten Schüler und Schülerinnen an, schon einmal sorgloses Verhalten in mindestens einem der drei Bereiche gezeigt zu haben (Grafik 3).

Grafik 3: Anteil der Schüler und Schülerinnen mit riskantem Computer- und Internetnutzungsverhalten



In einer differenzierteren Betrachtung der Risikoverhaltensweisen hat sich gezeigt, dass sich Jungen im Umgang mit dem Computer weniger sorgfältig verhalten als

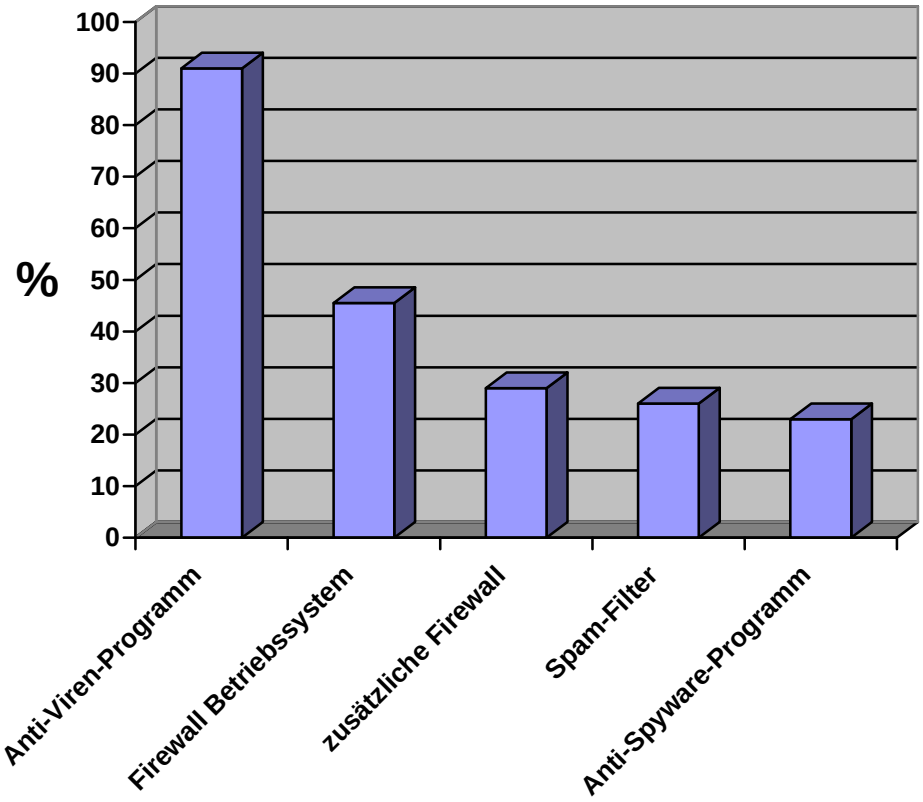
Mädchen und auch häufiger illegale Seiten besuchen und sich an Software-Piraterie beteiligen. Letztgenanntes Verhalten tritt insbesondere bei Befragten aus dem städtischen Raum (ab 100.000 Einwohner) auf. Im direkten Vergleich zeigen diejenigen Befragten, die Haupt- und Realschulen besuchen, häufiger ein riskantes Verhalten im Umgang mit Mails oder Internetlinks als Gymnasiastinnen und Gymnasiasten.

3.3 Sicherungsmaßnahmen

3.3.1 Technische Sicherungsmaßnahmen

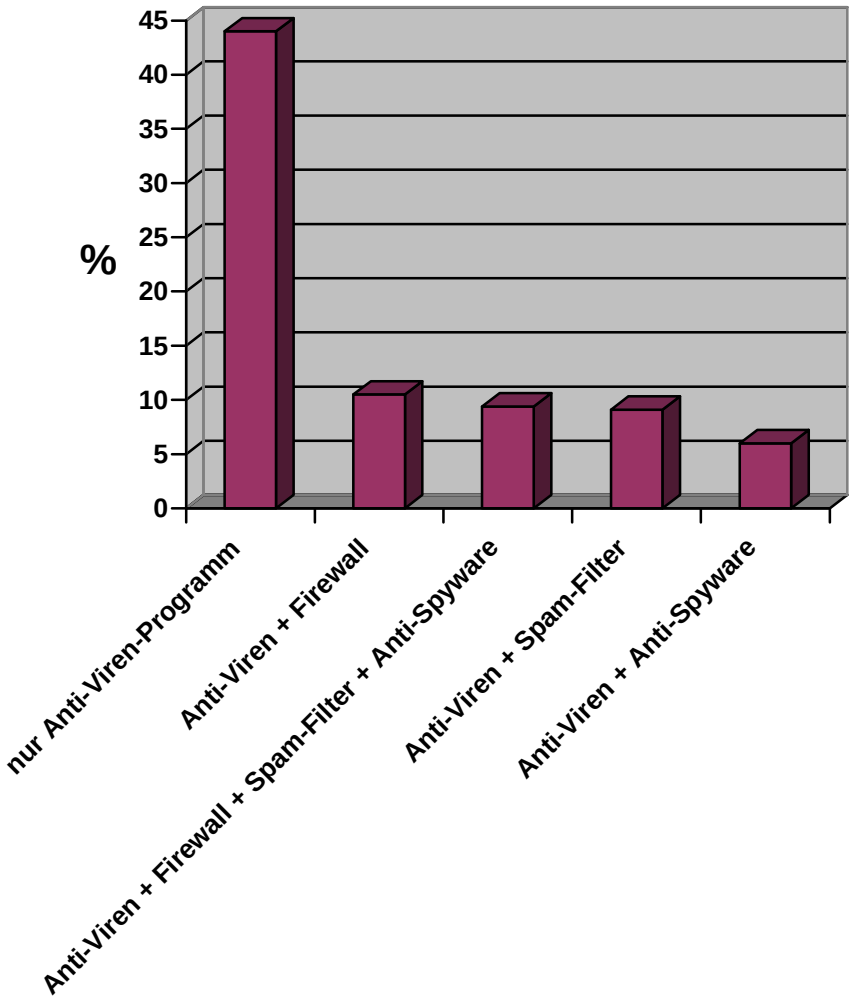
Die häufigsten Betriebssysteme, die auf gemeinsam genutzten, internetfähigen Computern installiert sind, sind Windows XP und Windows Vista; die am häufigsten verwendeten Browser sind Internet Explorer und Mozilla Firefox. 70 % der befragten Schüler und Schülerinnen geben an, dass bei ihnen zu Hause eine kabellose Verbindung zum Internet (WLAN-Verbindung) hergestellt werden kann, die zumeist passwortgeschützt ist und nie oder nur selten für Gäste freigegeben wird. Praktisch alle Computer verfügen über mindestens eine bzw. über eine Kombination von Sicherungsmaßnahmen: Die im Betriebssystem integrierte Firewall wird von ca. 45 % der Befragten benutzt. Daneben nutzen viele zusätzliche Sicherungsprogramme, die nicht im Betriebssystem integriert sind. Es handelt sich dabei um Firewalls, Anti-Spy-Software, Spam-Filter und insbesondere Anti-Viren-Programme (Grafik 4).

Grafik 4: Sicherungsmaßnahmen am gemeinsam genutzten Computer



Die zusätzlichen Sicherungsmaßnahmen werden von den Befragten in verschiedenen Kombinationen verwendet. Die meisten (44 %) geben an, nur ein Anti-Viren-Programm zu verwenden (Grafik 5).

Grafik 5: Kombinationen verschiedener Sicherungsmaßnahmen



In gut der Hälfte der Haushalte sind die befragten Schülerinnen und Schüler entweder alleine oder zusammen mit anderen Familienangehörigen für die Pflege und Verwaltung des gemeinsam genutzten PCs und der entsprechenden Sicherungsmaßnahmen verantwortlich.

Knapp zwei Drittel von ihnen haben für den gemeinsam genutzten Computer alle Rechte, können also Software installieren oder Systemeinstellungen ändern. Die Hälfte der Befragten sagt zwar, es gäbe für den Computer ein passwortgeschütztes Administratorenkonto, doch von denen wiederum hat nur knapp die Hälfte (40 %) Kenntnis von diesem Passwort.

3.3.2 Sicherheitsrelevantes Wissen

Das sicherheitsrelevante Wissen der Kinder und Jugendlichen wurde mit Hilfe eines Wissenstests erfasst, der aus 9 Fragen bestand (z. B. „Welche Aufgabe hat eine Firewall?").

Es zeigen sich große Unterschiede im Wissen, d. h. es gibt sowohl Schülerinnen und Schüler, die nur wenige oder gar keine der Fragen beantworten können, und solche, die auf viele Fragen die korrekte Antwort geben können. Vergleichsweise gering ausgeprägt ist das sicherheitsrelevante Wissen bei Mädchen aller Klassenstufen, jungen Schülerinnen und Schülern der 7. Klasse und bei Befragten, die eine Hauptschule besuchen.

3.3.3 Elternkontrolle

Den Befragten wurden 6 Aussagen zur elterlichen Kontrolle der Computer- und Internetnutzung vorgegeben (z. B. „Was ich wann und wie lange am Computer tue, ist meinen Eltern egal.", „Meine Eltern haben mich noch nie danach gefragt, was ich tue, wenn ich im Internet bin."), die sie auf einer vierstufigen Ratingskala von 0 („trifft überhaupt nicht zu") bis 3 („trifft voll und ganz zu") bewertet haben.

Die elterliche Kontrolle der Computernutzung ist bei jungen Schülerinnen und Schülern (7. und 8. Klasse) größer als bei älteren (9. und 10. Klasse). Ebenso ist sie bei Gymnasiastinnen und Gymnasiasten größer, verglichen mit Schülerinnen und Schülern, die eine Haupt- oder Realschule besuchen. Die Ausprägung elterlicher Kontrolle des Verhaltens nach Geschlecht differenziert unterscheidet sich nur minimal: Die Mädchen geben an, in ihrem Verhalten von den Eltern etwas stärker kontrolliert zu werden, als ihre Mitschüler.

Ca. 50 % der befragten Schüler und Schülerinnen geben an, dass die Aussagen zur Elternkontrolle „überhaupt nicht" oder „eher nicht" zuträfen, d. h. dass ca. 50 % gar nicht bis kaum in ihrem Nutzungsverhalten am Rechner und im Internet von den Eltern beaufsichtigt werden.

3.4 Gefährdung der Computer- und Datensicherheit

3.4.1 Viktimisierungserfahrungen

In den nachfolgend berichteten Zusammenhangsanalysen sollen die persönlichen Erfahrungen, die die Schülerinnen und Schüler, die den heimischen Rechner zusammen mit anderen Familienangehörigen nutzen, tatsächlich mit Internetkriminalität gemacht haben (Viktimisierungserfahrung), behandelt werden. Diese Erfahrungen wurden mit der Frage: „Ist dir oder jemandem aus deinem Umfeld schon einmal einer der folgenden Vorfälle passiert?“ erfasst. Den Befragten wurden vier konkrete Ereignisse vorgegeben (Virusmeldung, Rechnungseingang über nicht bestellte Waren oder Dienstleistungen, Geldverlust beim Online-Banking, Zugriff auf ein eBay-Konto), für die sie dann angeben mussten, ob diese Ereignisse schon einmal bei ihnen selbst, bei ihren Familienangehörigen oder bei ihren Freunden oder Bekannten aufgetreten sind.

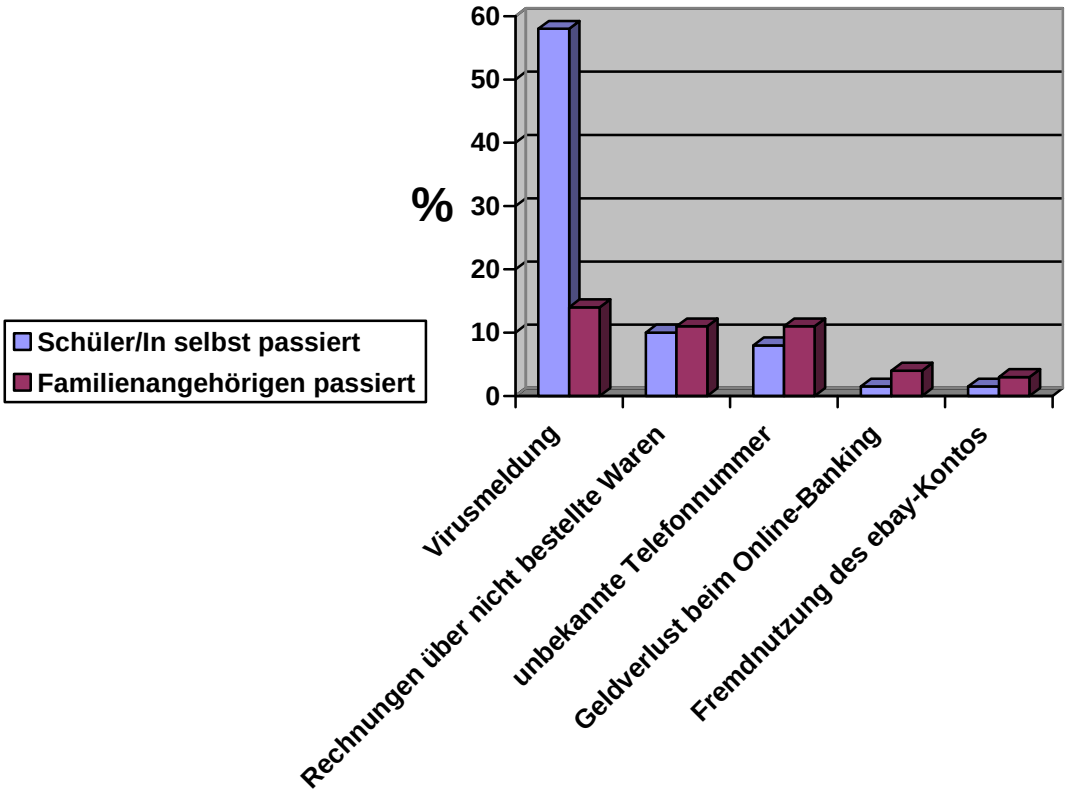
Einschränkend muss jedoch gesagt werden, dass im Bereich der Internetkriminalität die Viktimisierungserfahrungen keinen empirisch gesicherten Indikator für die tatsächliche Belastung der Befragten durch Straftaten über das Internet darstellen, da etliche Angriffe und unbefugte Zugriffe auf den Rechner nicht bemerkt werden (können). Das Ausspähen von Daten, Abgreifen digitaler Identitäten und das Anbinden des Rechners an ein Bot-Netz werden von den Geschädigten häufig nicht wahrgenommen.

58 % der befragten Schüler berichten, dass bei ihnen der Virenscanner schon einmal einen Virus gemeldet hat, 14 % können den Vorfall dieses Ereignisses für Familienangehörige angeben. 10 % berichten davon, selbst einmal Rechnungen über nicht bestellte Waren oder Dienstleistungen erhalten zu haben und 11 % geben dies für Angehörige ihrer Familie an.

8 % der befragten Schüler und Schülerinnen ist es schon einmal passiert, dass Gebühren für den Anruf unbekannter Nummern auf der Telefonrechnung verzeichnet waren (11 % geben dies für Familienangehörige an), lediglich 1,5 % teilen jeweils mit, dass von einem im Online-Banking verwalteten Konto Geld abhanden gekommen ist (4 % für Familienangehörige) und dass Fremde ebay-Kontodaten zu ihrem

Nutzen und auf Kosten des eigentlichen Besitzers missbraucht haben (3 % für Familienangehörige) (Grafik 6).

Grafik 6: Viktimisierungserfahrungen



Mit Ausnahme des Vorfalls einer Virusmeldung berichten jüngere Schülerinnen und Schüler (7. und 8. Klasse) häufiger von Viktimisierungserfahrungen durch Internetkriminalität als die älteren Jugendlichen (9. und 10. Klasse). Mit steigender Klassenstufe sinkt der Anteil der Schüler und Schülerinnen, die angeben, dass sie Viktimisierungserfahrungen in den Bereichen Rechnungseingang über nicht bestellte Waren oder Dienstleistungen, Geldverlust beim Online-Banking und fremder Zugriff auf ein eBay-Konto gemacht haben. Dies könnte sich aus dem Umstand erklären, dass jüngere Schüler und Schülerinnen über weniger sicherheitsrelevantes Wissen im Umgang mit dem Computer verfügen und demnach einem Missbrauch über das Internet eher erliegen als die älteren Schüler und Schülerinnen (Kapitel 3.3.2).

Sieht man vom Ereignis der Virusmeldung ab, erscheint die Grundrate des Auftretens der übrigen wahrgenommenen Viktimisierungsphänomene eher gering. Sowohl

bei den Angaben zu eigenen Viktimisierungserfahrungen als auch bei den Angaben zu Ereignissen, die Familienangehörige betreffen, ist es wahrscheinlich, dass die befragten Schüler und Schülerinnen mit einem Durchschnittsalter von 14,7 Jahren die entsprechenden Kompetenzen und Interessen zur Verwaltung von Telefonrechnungen und Online-Banking Konten (noch) nicht mitbringen und demnach die Aufmerksamkeitsspanne bzgl. der Vorgänge und Veränderungen in diesen Bereichen eher geringer ausgeprägt ist als bei Erwachsenen. Wie oben in Grafik 6 ersichtlich ist, geben die befragten Schüler und Schülerinnen für ihre Familienangehörigen eine höhere Auftretensrate an als für sich selbst. Zu beachten ist, dass die zu beurteilenden Ereignisse aus der Handlungswelt der Erwachsenen stammen und deren Vorkommen von den befragten Schüler und Schülerinnen möglicherweise gar nicht angemessen beurteilt werden können oder die Schüler und Schülerinnen sind über deren Eintreten nicht notwendigerweise präzise informiert. Außerdem mögen sich anfänglich unerklärliche Rechnungen bei späterer Betrachtung als durchaus erklärbar dargestellt haben, ohne dass die Betroffenen (Eltern) ihren Kindern (hier die Befragten) dies mitgeteilt haben.

3.4.2 Risikowahrnehmung

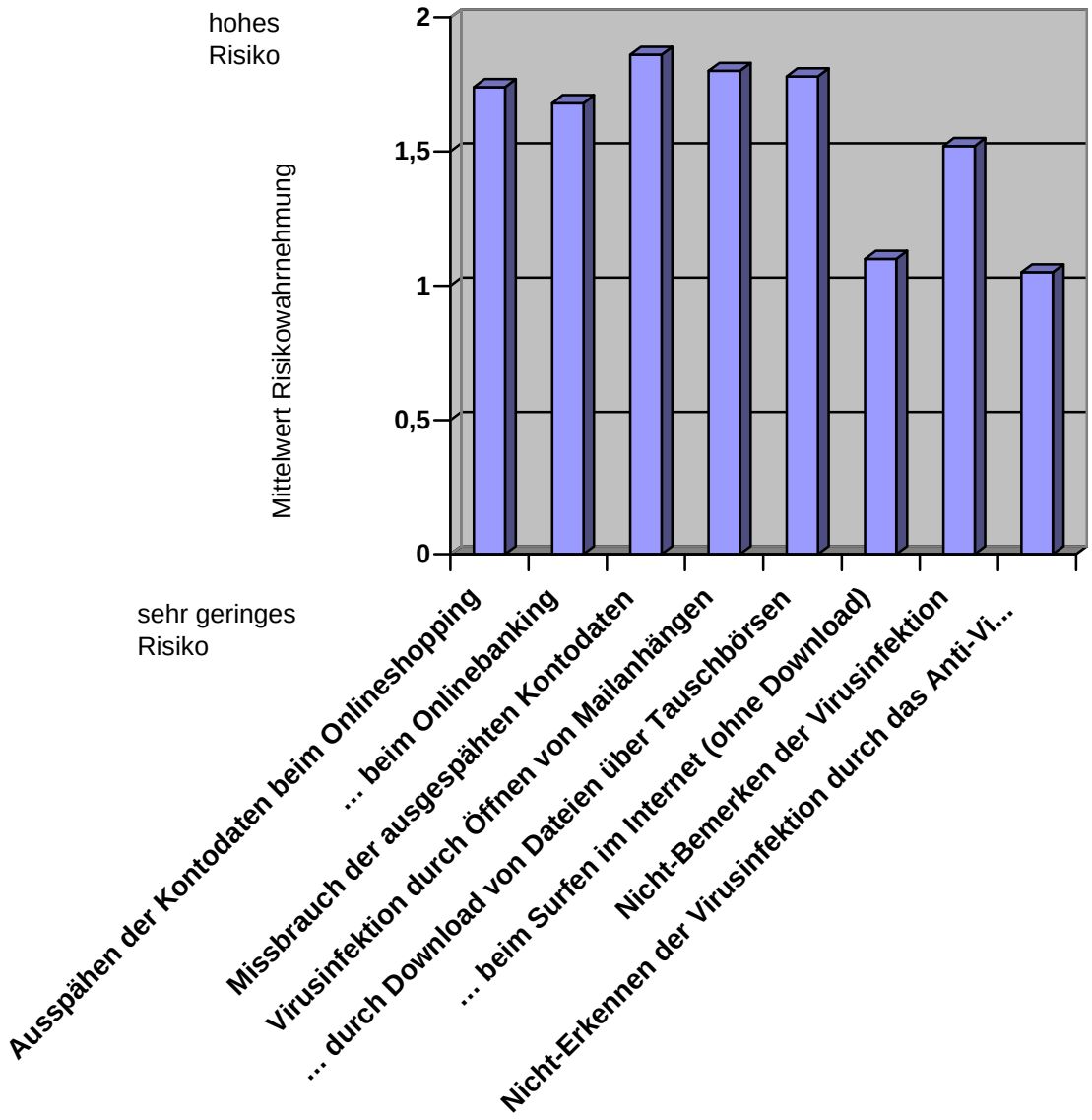
Das wahrgenommene Viktimisierungsrisiko, also das subjektiv empfundene Risiko, Opfer einer über das Internet begangenen Straftat zu werden, wurde über Fragen dieser Art erfasst: „Wie hoch ist deiner Meinung nach das Risiko, dass beim Onlineshopping die Kontodaten ausgespäht werden?". Die Antwortskala reichte von 0 („sehr geringes Risiko") bis 3 („sehr hohes Risiko").

Jeweils die Hälfte der Befragten gibt an, dass sie solche Risiken für im Durchschnitt hoch bis sehr hoch bzw. für gering bis sehr gering einschätzen. Vor allem junge Schülerinnen und Schüler (7. Klasse) halten das Viktimisierungsrisiko für hoch.

Das Risiko, dass ausgespähte Kontodaten dazu genutzt werden, Geld vom eigenen Konto abzuheben, wird von den Befragten am höchsten eingeschätzt, gefolgt von den Risiken, dass der Computer durch das Öffnen von Mailanhängen und durch den Download von Dateien über Tauschbörsen mit Viren infiziert wird (Grafik 7). Am geringsten wird das Risiko eingeschätzt, dass der Computer beim Surfen im Internet

(ohne Dateien herunter zu laden) mit einem Virus infiziert wird und dass ein Computervirus von der Anti-Viren-Software nicht erkannt wird.

Grafik 7: Ausprägung der Risikowahrnehmung



4 Sicherheitsrisiken für Computeranwender

4.1 Risiko- bzw. Schutzfaktoren

Insgesamt wurden im Fragebogen vier mögliche Faktoren untersucht, von denen angenommen wurde, dass sie das Risiko der Sicherheitsgefährdung des gemeinsam genutzten Rechners und zum anderen das Risiko, Opfer von Internetkriminalität zu werden, erhöhen bzw. im Sinne einer Schutzwirkung verringern. Diese vier Risikofaktoren sind: das Risikoverhalten (3.2.2), das sicherheitsrelevante Wissen (3.3.2), die Elternkontrolle (3.3.3), und die Risikowahrnehmung (3.4.2).

Hinter der Einbeziehung dieser Faktoren in die Untersuchung steht die Annahme, dass Kinder und Jugendliche umso leichter und öfter Opfer von Internetkriminalität werden, je gefährdeter der gemeinsam genutzte Rechner ist. Dies ist dann der Fall,

a) je riskanter das Nutzungsverhalten der Schüler und Schülerinnen am PC ist,

b) je weniger sicherheitsrelevantes Wissen die Schülerinnen und Schüler vorzuweisen haben,

c) je weniger sie von ihren Eltern bei der Computernutzung beaufsichtigt oder kontrolliert werden und

d) je geringer ihr subjektiv wahrgenommenes Risiko Opfer zu werden ist.

4.2 Zusammenhänge zwischen Risikofaktoren und Viktimisierungserfahrungen

In diesem Abschnitt sollen die Zusammenhänge zwischen den Viktimisierungserfahrungen der Befragten und den genannten Risiko- bzw. Schutzfaktoren analysiert und diskutiert werden. Die Ergebnisse dieser Analyse könnten Ansätze für präventive Maßnahmen nicht nur zum Schutz von Kindern und Jugendlichen sondern auch für die Computeranwender im häuslichen Umfeld vor Internetkriminalität bieten.

a) Risikoverhalten

Das Risikoverhalten wurde in Kapitel 3.2.2 über drei Bereiche definiert: *Sorgfalt und Gründlichkeit im Umgang mit dem Computer*, *Sorgloses oder riskantes Verhalten im Umgang mit Mails und Links* und *Besuch illegaler Seiten und Software-Piraterie.*

Die beiden Risikoverhaltensweisen *Sorgloses oder riskantes Verhalten im Umgang mit Mails und Links* und *Besuch illegaler Seiten und Software-Piraterie* korrelieren positiv miteinander, d. h. sie stehen miteinander im Zusammenhang, i. d. S., dass mit einem ausgeprägten riskanten Verhalten im Umgang mit Mails und Links auch ein vermehrter Besuch illegaler Seiten und ausgeprägte Software-Piraterie einhergeht. In der Praxis ist durch diese Verhaltensweisen die Sicherheit des Computers gefährdet und dies zeigt sich auch in der Studie:
Zwischen den Risikoverhaltensweisen *Sorgloses oder riskantes Verhalten im Umgang mit Mails und Links* sowie *Besuch illegaler Seiten und Software-Piraterie* und den Viktimisierungserfahrungen bestehen statistisch signifikante Zusammenhänge in positiver Richtung. D. h. je stärker die Verhaltensweise *Sorgloses oder riskantes Verhalten im Umgang mit Mails und Links* ausgeprägt ist, desto wahrscheinlicher ist das Auftreten von Viktimisierungserfahrungen. Der gleiche Zusammenhang besteht für den Bereich *Besuch illegaler Seiten und Software-Piraterie* und Viktimisierungserfahrungen.

Dagegen lässt sich zwischen der Sorgfalt und Gründlichkeit, die die Befragten im Umgang mit dem Computer angeben, und den angegebenen Viktimisierungserfahrungen kein Zusammenhang feststellen. Scheinbar paradoxerweise gehen ausgeprägte Sorgfalt und Gründlichkeit im Umgang mit dem Computer mit dem zunehmenden Besuch illegaler Seiten und mit Software-Piraterie einher.

Gleichzeitig steht der sorgfältige und gründliche Umgang mit dem Computer in positivem Zusammenhang mit den Schutzfaktoren sicherheitsrelevantes Wissen und wahrgenommenes Risiko der Viktimisierung. Dies erscheint plausibel, denn zunehmendes Wissen um Sicherheitsgefahren und Sicherungsmaßnahmen bei der Computer- und Internetnutzung und eine entsprechende Wahrnehmung des Risikos sollten sich auch in entsprechendem sorgfältigem Verhalten äußern.

b) Sicherheitsrelevantes Wissen

Auch das sicherheitsrelevante Wissen hängt mit dem Besuch illegaler Seiten und Software-Piraterie zusammen, so dass diejenigen, die mehr wissen im Vergleich zu Befragten mit weniger Wissen, stärker zu illegalem Verhalten im Internet neigen (Besuch illegaler Seiten und Software-Piraterie). Der Computer, der von den Betroffenen mit mehr Wissen genutzt wird, ist demnach durch damit einhergehende Sicherheitsrisiken potenziell gefährdet.
Aufgrund der Komplexität der hier untersuchten Merkmale und ihrer Wechselwirkungen untereinander ist eine Auflösung dieser paradoxen Zusammenhänge schwierig. Es ist aber zu vermuten, dass mit steigendem sicherheitsrelevanten Wissen und mit zunehmender Risikowahrnehmung der Umgang mit dem PC zwar, wie gezeigt, sorgfältiger wird, dass andererseits das wachsende Wissen aber auch dafür genutzt wird, neue Verhaltensweisen, die potenziell sicherheitsgefährdend sind, auszuprobieren (z. B. zwielichtige Websites zu besuchen, gezielt nach illegalen Inhalten zu suchen, Shoppingportale oder Tauschbörsen zu nutzen, die Rechnerkonfiguration zu verändern usw.).

Eine andere Erklärung des Zusammenhangs zwischen sicherheitsrelevantem Wissen und riskantem Verhalten (Besuch illegaler Seiten und Software-Piraterie) könnte lauten, dass die Kinder und Jugendlichen gerade deswegen über das abgefragte Wissen verfügen, weil sie sich explorativ verhalten und im Internet vieles ausprobieren, was diese Studie als riskantes Verhalten einstuft.

Wenn diese Verhaltensweisen dann das tatsächliche Sicherheitsrisiko für den PC negativ beeinflussen, wird dies fast zwangsläufig zu einer Erhöhung der Viktimisierungserfahrungen führen. Diese Annahme wird unterstützt durch die Tatsache, dass das sicherheitsrelevante Wissen mit steigender Klassenstufe der Schülerinnen und Schüler, also mit wachsendem Lebensalter, zunimmt (vgl. Kapitel 3.3.2). Mit zunehmendem Alter nimmt bei Kindern und Jugendlichen naturgemäß aber auch der individuelle Spielraum zur Gestaltung des eigenen Lebens zu, was sich auch auf die Computer- und Internetnutzung auswirken dürfte und die Sicherheitsgefährdung des Computers und damit einhergehende Viktimisierungserfahrungen erhöht.

Daneben hat die Studie gezeigt, dass nicht nur der sorgfältige und gründliche Umgang mit dem Computer mit vorhandenem sicherheitsrelevantem Wissen einhergeht, sondern auch das Verhalten in Bezug auf die Weitergabe der Bankverbindung beim Online-Shopping: So neigen die Schüler und Schülerinnen mit ausgeprägtem Sicherheitswissen dazu, genau zu prüfen, wem sie ihre Bankverbindung angeben. Sicherheitsrelevantes Wissen besitzt demnach neben den explorationsfördernden auch protektive Eigenschaften.

c) Elternkontrolle

Obwohl keine direkte Beziehung zur Viktimisierungserfahrung festgestellt werden konnte, kommt der elterlichen Kontrolle der Computernutzung möglicherweise doch eine wichtige Rolle im Beziehungsgeflecht zwischen den hier untersuchten Merkmalen zu: Je stärker die Elternkontrolle ist, umso größer ist die Risikowahrnehmung ihrer Kinder, umso weniger zeigen die Befragten sorgloses oder riskantes Verhalten im Umgang mit Mails und Links und umso weniger besuchen sie illegale Seiten oder betreiben Software-Piraterie. Auch das Online-Banking und der Download von Musik und Filmen sind bei zunehmender Elternkontrolle geringer ausgeprägt. Damit lässt sich auch die Gefährdung des Computers durch Internetkriminalität als niedrig einstufen.

Das bedeutet, dass die Elternkontrolle eine schützende Wirkung hat und damit in einer indirekten Beziehung zu den tatsächlich gemachten Viktimisierungserfahrungen steht, da sie genau die Merkmale beeinflusst, von denen die Viktimisierungserfahrungen abhängen: Je weniger also sorgloses, riskantes oder illegales Verhalten am Computer gezeigt wird, z. B. weil die Eltern ihre Kinder bei der Computernutzung intensiver beaufsichtigen, desto geringer ist die Gefährdung des Rechners und desto weniger (schwere) Viktimisierungserfahrungen machen die Kinder und Jugendlichen.

Wie bereits gezeigt wurde, geben ca. 50 % der Kinder und Jugendlichen an, von ihren Eltern kaum bis gar nicht bei der Computer- und Internetnutzung beaufsichtigt oder hinterfragt zu werden. Dies ist bemerkenswert, bedenkt man, dass vor dem Hintergrund der Gefährdung des gemeinsam genutzten Rechners durch riskantes Verhalten der Kinder und Jugendlichen, auch die Eltern und deren Datensicherheit von Internetkriminalität betroffen sein können. Zum Schutz ihrer Kinder und im eigenen

Interesse sollten auch die Eltern ein nachdrückliches Bewusstsein und Interesse an dem entwickeln, was an dem gemeinsam genutzten Rechner geschieht.

d) Risikowahrnehmung

Die vorliegende Studie hat gezeigt, dass das Merkmal der Risikowahrnehmung in engem Zusammenhang mit dem sorgfältigen und gründlichen PC-Umgang steht, d. h. ausgeprägte Gründlichkeit und Sorgfalt gehen mit einer erhöhten Risikowahrnehmung bzgl. der eigenen Internetnutzung einher.

Schüler und Schülerinnen, die gründlich und sorgfältig mit dem Computer umgehen, verfügen auch über mehr sicherheitsrelevantes Wissen zum Thema „Internet und Gefahren“. Darüber hinaus bestehen zwischen der Risikowahrnehmung und dem sicherheitsrelevanten Wissen keine Zusammenhänge[4] und auch zu anderen Faktoren hat das Merkmal Risikowahrnehmung keine weiteren Beziehungen, bis auf die Elternkontrolle: Mit einer ausgeprägten Elternkontrolle schärft sich auch das Bewusstsein möglicher Risiken und Gefahren bei der Internetnutzung.

Die meisten Kinder und Jugendlichen haben noch keine vertiefte Risikowahrnehmung für den Bereich der Internetgefährdung entwickelt und schätzen im Durchschnitt das Risiko von Internetkriminalität getroffen zu werden als mittel ein (Punktwerte: 1,5 bis 1,8 von min. 0 bis max. 3) (vgl. Kapitel 3.4.2). Es ist zu vermuten, dass eine ausgeprägte Risikowahrnehmung Einfluss auf das Risikoverhalten ausübt und bei entsprechender Schärfung des Bewusstseins der Kinder und Jugendlichen für die Gefahren, die mit dem sorglosen und riskanten Umgang mit Mails und Links sowie dem Besuch illegaler Seiten und der Software-Piraterie einhergehen, sich auch Verhaltensänderungen in diesen zwei Verhaltensbereichen einstellen.

[4] Dies entspricht auch dem wissenschaftlichen Kenntnisstand der Sozialpsychologie, dass Wissen kaum Einfluss auf die Risikowahrnehmung hat, da für die Wahrnehmung von Risiken vorhandenes oder vermitteltes Wissen wenig ausschlaggebend ist.

5 Fazit und Handlungsempfehlung

In allen Haushalten werden technische und in den meisten auch nutzerseitige bzw. verhaltensorientierte Maßnahmen zur Gewährleistung der digitalen Sicherheit eines gemeinsam genutzten Computers ergriffen (eingeschränkte Rechtevergabe zur Änderung von Systemeinstellungen, passwortgeschütztes Administratorenkonto usw.). Diese Maßnahmen erzielen im Sinne von Schutzfaktoren (s. Kapitel 3.3) eine reduzierende Wirkung hinsichtlich der Viktimisierungserfahrungen.
Dabei zeigt sich, dass das Nutzungsverhalten der Kinder und Jugendlichen durchaus einen Risikofaktor für die digitale Sicherheit des PCs darstellt, denn die eingesetzten Sicherungsmaßnahmen sind z. T. für die Kinder und Jugendlichen steuer- oder umgehbar. Je stärker der gemeinsam genutzte PC durch Internetkriminalität gefährdet ist, umso mehr machen die befragten Kinder und Jugendlichen Viktimisierungserfahrungen und umgekehrt.

Das Bewusstsein für Risiken bei der Internetnutzung hat Einfluss auf das Nutzungsverhalten. So geht mit einer ausgeprägten Risikowahrnehmung tendenziell eine erhöhte Sorgfalt und Gründlichkeit im Umgang mit dem Computer einher. Darüber hinaus kann das Bewusstsein für die Konsequenzen des riskanten Umgangs mit Mails und Links sowie dem Besuch illegaler Seiten und der Software-Piraterie bei den Kindern z. B. über elterliche Kontrolle dahingehend geschärft werden, dass sich auch in diesen Verhaltensbereichen Änderungen einstellen.

Insbesondere der Grad an elterlicher Kontrolle hat Einfluss auf die Risikowahrnehmung und auf das Risikoverhalten der Kinder und Jugendlichen am Rechner und im Internet. Die Elternkontrolle beeinflusst genau die Risikoverhaltensweisen, von denen die Gefährdung des gemeinsam genutzten Rechners und die Viktimisierungserfahrungen abhängen. Demnach ist es möglich, dass ausgeprägte Elternkontrolle präventive Wirkung entfaltet, im Sinne einer Reduzierung der Gefährdung des Rechners und der Wahrscheinlichkeit, Viktimisierungserfahrungen zu machen. Vor diesem Hintergrund geht mit der Kontrolle des Computer- und Internetnutzungsverhalten der Kinder durch die Eltern auch der Schutz der Eltern einher. Trotzdem wird die Hälfte der befragten Kinder und Jugendlichen von ihren Eltern kaum bis gar nicht beaufsichtigt, so dass es ratsam ist, auch das Risikobewusstsein der Eltern zu schärfen.

Wie durch die Studie aufgezeigt wurde, steht das sicherheitsrelevante Wissen in Zusammenhang mit dem Risikoverhalten, insbesondere dem Besuch illegaler Seiten und Software-Piraterie sowie mit der technisch und nutzerseitig bedingten Gefährdung des gemeinsam genutzten Computers. Schüler und Schülerinnen die über mehr sicherheitsrelevantes Wissen verfügen, neigen erstaunlicherweise stärker zu illegalem Verhalten im Internet und nutzen eher einen Computer, der potenzielle Sicherheitsrisiken birgt, obwohl ihr Umgang mit dem PC dabei durchaus sorgfältiger und gründlicher sein kann. In welche Richtung dieser Zusammenhang funktioniert, ist nicht geklärt: Einerseits ist es möglich, dass trotz des sorgfältigeren Umgangs mit dem PC das wachsende Wissen auch dafür genutzt wird, neue Verhaltensweisen, die potenziell sicherheitsgefährdend sind, auszuprobieren. Andererseits könnten sich die Kinder und Jugendlichen durch das explorative und illegale Verhalten im Internet das entsprechende Wissen angeeignet haben.

Fasst man die in dieser Studie untersuchten nutzerseitigen, bzw. verhaltensorientierten und technischen Merkmale *Risikoverhalten, Elternkontrolle* und *technische Sicherungsmaßnahmen* als potenzielle Sicherheitsrisiken für den Computer zusammen, dann zeigt sich, dass sie das Aufkommen von Viktimisierungserfahrungen zusammen besser erklären können, als nur ein Merkmal allein, wie z. B. nur das Risikoverhalten.

Die Studie hat gezeigt, dass das Nutzungsverhalten am Rechner und im Internet darüber entscheidet, ob und in welcher Ausprägung Viktimisierungserfahrungen gemacht werden.
Da davon ausgegangen werden kann, dass mit einer Veränderung der Risikowahrnehmung auch eine Verhaltensänderung einhergeht[5], ist die Schärfung des Gefahrenbewusstseins bei Kindern und Jugendlichen, aber auch bei Eltern, ein wichtiger Ansatzpunkt für Präventionsmaßnahmen.

[5] So testen z. B. Reisig et al. in einer Studie (*Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity* Criminal Justice and Behavior 2009. 36. S. 369) das Risikointerpretationsmodell von Ferraro anhand der Viktimisierungsgefährdung über Online-Kreditkartenmissbrauch und kommen zu dem Ergebnis, dass die Ausprägung der Wahrnehmung des Viktimisierungsrisikos Einfluss auf den Grad der Verhaltensänderung bei der Nutzung von Online-Diensten hat. Die Leute, die das Risiko, Opfer von Internetkriminalität zu werden, hoch einschätzen, passen ihr Verhalten an, um einer Viktimisierung zu entgehen.

Auch in der Sozialpsychologie, wo u. a. das Verhalten des Menschen und die Prozesse und Einflussfaktoren der Verhaltensänderung untersucht werden, spielt die Risikowahrnehmung eine Rolle. Es besteht Einigkeit darüber, dass sich über eine bloße Wissensvermittlung keine Verhaltensänderung bewirken lässt. Der Grund hierfür liegt in dem simplen Umstand, dass der Empfänger häufig nicht versteht, was ihm vermittelt wird: Da Wissen oft standardisiert und einheitlich vermittelt wird, trifft es auf unterschiedliche intellektuelle Verstehenskompetenzen bei den Empfängern und kann somit nicht von jedem zur Gänze verstanden werden.

Größeren Einfluss auf die Änderung von Verhalten hat jedoch die Risikowahrnehmung. Doch auch hierfür müssen bestimmte Rahmenbedingungen gewährleistet sein: Der Betroffene muss in erster Linie an das antizipierte Risiko affektiv gebunden sein. Diese Affektivbindung ist umso stärker, je mehr sich der Betroffene mit seiner Lebensgestaltung an dem Risiko und seinen Konsequenzen orientiert, d. h. der Einfluss der Risiken auf den eigenen Lebensbereich muss ersichtlich und nachvollziehbar sein. Dies ist umso ausgeprägter, je lokaler der Bezug zum Risiko ist und je öfter der Betroffene mit dem Risiko und den Konsequenzen frequentiert wird.

Eine besondere Bedeutung bei der Wahrnehmung und Einschätzung des Risikos einer Sache oder eines Verhaltens, hat der Nutzen, den der Betroffene aus dieser Sache oder dem Verhalten zieht.

Obwohl der Nutzen und das Risiko reell positiv miteinander korrelieren, besteht in der Wahrnehmung der Betroffenen zwischen den beiden Komponenten ein negativer Zusammenhang: Ist der Nutzen einer Sache unverzichtbar, so wird das Risiko bei der Ausübung oder dem Eintreten dieser Sache, als niedrig eingeschätzt und umgekehrt. Dieser negative Zusammenhang wird von der affektiven Komponente moderiert: Fühlt sich die betroffene Person mit einer Sache oder einem Verhalten, in diesem Falle das Nutzungsverhalten am Rechner und im Internet, wohl, schätzt sie den Nutzen hoch ein und das Risiko gering. Fühlt sie sich mit einer Sache unwohl, werden der Nutzen gering und das Risiko eher hoch eingestuft.[6] Diese Kosten-Nutzen-Abwägungen ist für eine Verhaltensänderung entscheidend und wird durch eine af-

[6] Finucane, M.L., Alhakami, A., Slovic, P., & Johnson, S.M. (2000). *The affect heuristic in judgments of risks and benefits*. Journal of Behavioral Decision Making, 13, 1–17.

fektiv gebundene Risikowahrnehmung beeinflusst (das Risiko tangiert den eigenen Lebensbereich).

Auch wenn das Wissen aufgrund der o. g. Probleme kaum Einfluss auf die Risikowahrnehmung hat, so lässt sich die Wahrnehmung dann beeinflussen, wenn trotz fehlendem Verständnis eine gewisse Glaubwürdigkeit zum Sender, d. h. dem der Wissen über Risiken vermittelt, hergestellt werden kann. Der Glaube des Betroffenen an den Sender bewirkt, dass dieser das vom Sender dargestellte Risiko glaubt (ohne es verstehen zu müssen) und daraufhin eine eigene Risikowahrnehmung entwickelt. Welche Sender besonders glaubwürdig sind, ist individuell abhängig vom Betroffenen. Allgemein gute Chancen haben Autoritätspersonen, Experten und populäre Charaktere.

Darüber hinaus kann ein glaubwürdiger Sender versuchen, die Risikowahrnehmung und damit einhergehende Verhaltensänderungen zu stimulieren, indem er Angst beim Empfänger auslöst. Diese Strategie funktioniert hingegen nur begrenzt: Die betroffene Person muss bereits über entsprechende Bewältigungsstrategien verfügen, um mit dem Risiko umgehen zu können. Andernfalls ist die vermittelte Angst zu überwältigend und das Risiko wird aus der Wahrnehmung zum Selbstschutz verdrängt. Die affektive Vermittlung des Risikos (im Sinne von „Angst machen“) muss der Zielgruppe und deren affektiven, kognitiven und Verhaltens-Kompetenzen angepasst sein. Zudem müssen Bewältigungsstrategien aufgezeigt werden, damit Verhalten geändert werden kann, und dies wiederum geschieht am besten über eine angepasste Wissensvermittlung.

Während der sorgfältige Umgang mit dem Computer mit Risikowahrnehmung positiv zusammenhängt, steht die Risikowahrnehmung laut dieser Studie (s. o.) in keinem Zusammenhang zu den riskanten Verhaltensweisen im Umgang mit Mails und Links sowie dem Besuch illegaler Seiten und der Software-Piraterie. Möglicherweise muss erst noch die Risikowahrnehmung in diesen zwei Verhaltensbereichen geweckt werden.

Beim Einsatz präventiver Maßnahmen zur Schärfung des Bewusstseins für Gefahren im und durch das Internet ist zu bedenken, dass die Wahrnehmung des Nutzens ei-

nes Verhaltens oder einer Sache zentral ist. Vor allem Kinder und Jugendliche überhöhen oft den zu erwartenden Nutzen im Vergleich zu den möglichen Risiken.[7]

Eine besonders wichtige Nutzendimension nimmt für Kinder und Jugendliche die soziale Bewunderung durch Freunde ein: Die soziale Dynamik beeinflusst, wie Risiken wahrgenommen und bewertet werden.[8] Kinder und Jugendliche gehen Risiken insbesondere dann verstärkt ein, wenn sie dafür Anerkennung erhalten. Im Falle des Internetnutzungsverhaltens könnte der Besitz besonders vieler Musiktitel, Spiele oder Filme, die illegal heruntergeladen wurden, Bewunderung und Anerkennung auslösen.

Nicht nur soziale Netzwerke, auch Medien vermitteln Stellenwert und Größe des Risikos, indem sie den Bezug zu öffentlichen, aber auch individuellen Sorgen und Interessen aufzeigen und verdeutlichen.[9] Das Bewusstsein für Gefahren im Internet kann z. B. durch Aufklärungskampagnen geschult werden. Denkbar wären u. a. an der Zielgruppe orientierte Werbespots in Form von Kurzfilmen, wie sie z. B. für die Anti-Alkohol-Kampagnen oder die Safer-Sex-Kampagnen genutzt werden. Der Vorteil dieser Werbespots liegt in der affektiven Einbindung der Zielgruppe in die dargestellte Thematik über situationsorientierte Modelle, die soziales Mimikry in Form der Nachahmung von Verhaltensvorbildern hervorrufen. Neben der Herstellung der Affektivbindung ist die Glaubwürdigkeit des Senders entscheidend. Wie bereits aufgezeigt wurde, kämen hierfür insbesondere medial populäre Persönlichkeiten in Frage, aber auch Gleichaltrige aus der Zielgruppe.
Darüber hinaus lassen sich Risiken bei der Internetnutzung auch in Form von Broschüren und Faltblättern vermitteln. In jedem Falle ist es wichtig, dass jegliche Vermittlungsformen an die affektiven, kognitiven und Verhaltens-Kompetenzen der Zielgruppe angepasst sind und ergänzend Wissen, Handlungsalternativen und Bewältigungsstrategien aufzeigen. Bei der präventiven Vermittlung und Kommunikation von Risiken bei der Internetnutzung sollte versucht werden, den wahrgenommenen Nutzen eines Risikoverhaltens zu reduzieren und den Nutzen Alternativverhaltens zu erhöhen.

---

[7] Kurzenhäuser, S. (2009). *Das Kind als Verbraucher*. BfR-Forum 29.06.2009. Bundesinstitut für Risikobewertung.
[8] Kasperson, R.E., Ortwin, R., Slovic, P., Brown, H., Emel, J., Goble, R.L., Kasperson, J.X., & Ratick, S.J. (1988). *The social amplification of risk: A conceptual framework.* Risk Analysis, 8(2), 177–187.
[9] Kasperson, R.E., Ortwin, R., Slovic, P., Brown, H., Emel, J., Goble, R.L., Kasperson, J.X., & Ratick, S.J. (1988). a. a. O.

In jedem Fall bietet auch der schulische Unterricht eine konstante und dem jeweiligen Kompetenzstand der Zielgruppe angepasste Möglichkeit, Risiken bei der Internetnutzung und Wissen über Handlungsalternativen entsprechend zu vermitteln.

Neben dem Ansatzpunkt der präventiven Risikovermittlung, Einstellungs- und Verhaltensänderung sollte der Fokus vor allem auf externe Sicherheitsmaßnahmen gelegt werden. Hierzu zählen technische Sicherungsmaßnahmen in Form von Anti-Viren-Programmen, Firewalls und regelmäßige Updates der Schutzsoftware, aber auch verstärkte Elternkontrolle bei der Nutzung des Internets durch die Kinder und Jugendlichen. Die Motivation der Eltern zu intensiverer Beaufsichtigung der Nutzungsvorgänge am Rechner lässt sich ähnlich wie bei den Kindern und Jugendlichen über die Vermittlung der Gefahren des Internet erreichen, d. h., auch das Bewusstsein der Eltern muss geschärft werden, soll sich ihr Verhalten verändern. Denkbar wären hierfür Veranstaltungen ähnlich wie Elternabende, die sich mit der Medien- und Kontrollkompetenz der Eltern beschäftigen und diese ausbauen.