Flavius Kehr, Tobias Rothmund, Mario Gollwitzer, Wendy Füllgraf

Prädiktoren sicherheitsrelevanten Verhaltens bei jugendlichen Computernutzern

Vor dem Hintergrund der stetig zunehmenden Fallzahlen von kriminellen Handlungen im Internet wird der Selbstschutz von Usern immer wichtiger. Gerade Jugendliche gelten als gefährdet, da sie sich häufig besonders sorglos im Netz bewegen. Der Beitrag präsentiert die Ergebnisse einer Befragung, die den Einfluss von fünf unterschiedlichen Faktoren auf das sicherheitsrelevante Verhalten von Jugendlichen untersucht hat. Besonderes Augenmerk wird dabei auf die Rolle von generalisiertem Vertrauen im Verhältnis zu anderen Faktoren gelegt.

Dipl.-Psych. Flavius Kehr

wissenschaftlicher Mitarbeiter am Institut für Technologiemanagement, Universität St. Gallen (HSG), sowie am Departement für Management, Technology and Economics (D-MTEC), ETH Zürich
E-Mail: flavius.kehr@unisg.ch

Dr. Tobias Rothmund

Jun. Prof. für Politische Psychologie am Institut für Kommunikationspsychologie und Medienpädagogik (IKM) im Fachbereich 8 Psychologie der Universität Koblenz-Landau.
E-Mail: rothmund@uni-landau.de

Prof. Dr. Mario Gollwitzer

Professor für Methodenlehre und Sozialpsychologie, Fachbereich Psychologie der Philipps-Universität Marburg.

E-Mail: mario.gollwitzer@staff.uni-marburg.de

Wendy Füllgraf

M.A. Pädagogik, M.A. Internationale Kriminologie, wissenschaftliche Mitarbeiterin in der Forschungs- und Beratungsstelle Cybercrime am Kriminalistischen Institut beim Bundeskriminalamt Wiesbaden
E-Mail: wendy.fuellgraf@bka.bund.de

1 Protektives Verhalten Jugendlicher

Mit der stetig steigenden Nutzung des Internets wird Internetkriminalität zu einem zunehmenden Problem. So stiegen gemäß Statistiken des Bundeskriminalamts Delikte, die „unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen wurden", zwischen 2009 und 2013 um 28% auf insgesamt 64.426 Taten, bei einem geschätzten Gesamtschaden von 42.6 Mio. € allein im Jahr 2013 [BKA 2013].

Neben der Verbesserung von IT-Sicherheit durch technische Maßnahmen nimmt die Aufklärung und Stärkung des Users mit Blick auf die Prävention von kriminellen Handlungen im Internet einen immer höheren Stellenwert ein. In der Tat können Endkonsumenten durch geeignete Maßnahmen verhindern, dass ihre Daten ausgespäht und missbräuchlich verwendet werden. Hierzu gehören beispielsweise das regelmäßige Aufspielen von Updates, die Einrichtung einer Firewall und eines Virenscanners, oder das Löschen unbekannter und potentiell gefährlicher EMails.

Es lässt sich annehmen, dass Personen sich darin unterscheiden, wie häufig und intensiv sie derartiges „protektives Verhalten" zeigen. So berichten frühere Untersuchungen, dass insbesondere Jugendliche sich angst- und sorgenfrei im Internet bewegen und häufiger riskantes Verhalten zeigen [Kie 2005]. Es kann daher angenommen werden, dass Heranwachsende besonders gefährdet sind, Opfer krimineller Handlungen im Internet zu werden.

Unklar bleibt indes, welche Faktoren gerade bei Jugendlichen dazu führen, dass diese sich durch geeignete Maßnahmen vor Fremdzugriffen schützen. Führt beispielsweise ein höheres Maß an Wissen um protektives Verhalten automatisch dazu, dass Jugendliche häufiger Updates installieren oder häufiger ihren Computer auf potentielle Schadsoftware untersuchen? Oder sind Jugendliche, die generell mehr Vertrauen in ihre Umwelt und Mitmenschen haben, auch nachlässiger mit dem Schutz ihres Computers vor Eingriffen durch Dritte?

Tab. 1 | Messeigenschaften der verwendeten Instrumente.

Konstrukt	Beispielfrage	Fragen	Antwortskala	M	SD	α
Vertrauen	Die meisten Menschen sind vertrauenswürdig.	6	1 (stimme überhaupt nicht zu) 5 (stimme vollständig zu)	3,07	0,84	.85
Risikoeinschätzung	Wie hoch schätzt du das Risiko ein, dass der Computer durch das Öffnen von Mailanhängen mit einem Computervirus infiziert wird?	8	0 (sehr geringes Risiko) 3 (sehr hohes Risiko)	1,54	0,71	.85
Wissen	Am sichersten ist…	9	☐ http://www.online-banking.de ☐ http://online-banking.de ☐ https://www.online-banking.de (*) ☐ Weiß nicht	3,05	2,20	
Computerexpertise	Wie schätzt du deine Kenntnisse im Umgang mit Computern selbst ein?	1	0 (Anfänger)3 (Experte)	1,54	0,83	
Elternkontrolle	Ich darf nicht so lange an den Computer, wie ich manchmal gerne möchte	6	0 (trifft überhaupt nicht zu) 3 (trifft vollständig zu)	1,67	0,65	.71
Protektives Verhalten	Ich lasse in regelmäßigen Abständen den Virenscanner die Festplatte komplett absuchen.	7	0 (trifft überhaupt nicht zu) 3 (trifft vollständig zu)	1,49	0,72	.79

Hinweis: Fragen = Anzahl der Fragen; M = Mittelwert über alle Fragen (und Personen);
SD = Standardabweichung (über Personen hinweg); α = Cronbachs Alpha; (*) = richtige Antwort.

Ziel dieses Beitrags ist es, anhand der Ergebnisse einer groß angelegten, repräsentativen Befragung unter jugendlichen Computernutzern relevante Prädiktoren protektiver Verhaltensweisen bei Jugendlichen zu identifizieren. Das heißt, es soll aufgezeigt werden, welche Faktoren dazu beitragen, dass Jugendliche mehr oder weniger protektives Verhalten bei der Computernutzung zeigen. Besonderes Augenmerk richtet sich dabei auf die Rolle von Vertrauen.

Im Folgenden werden zunächst eine Reihe potentieller Einflussfaktoren auf der Basis theoretischer Überlegungen eingeführt. Im Anschluss werden methodische Aspekte sowie die Ergebnisse der durchgeführten Studie erläutert und diskutiert.

2 Einflussfaktoren protektiven Verhaltens

Bei der Planung der Befragung wurden in einem ersten Schritt potentielle Prädiktoren ausgewählt, bei denen auf der Basis theoretischer Überlegungen und bisheriger Arbeiten davon auszugehen war, dass diese in Zusammenhang mit sicherheitsrelevantem Verhalten stehen könnten. Dies waren im Einzelnen:

► **Das generalisierte *Vertrauen* in Mitmenschen**

Personen unterscheiden sich darin, in welchem Ausmaß sie erwarten, dass sich ihre Mitmenschen im Allgemeinen vertrauenswürdig verhalten [May 1995; Rot 1967]. Diese generalisierte Erwartungshaltung spielt auch in der virtuellen Welt eine Rolle, wo Personen oft mit wenig durchschaubaren Strukturen konfrontiert sind. So haben vergangene Studien generalisiertes Vertrauen oft als einen Einflussfaktor beschrieben, wenn es z. B. darum geht, online Käufe zu tätigen oder Internet-Plattformen und Services zu nutzen [Din 2006a; Lee 2001].

Vor dem Hintergrund dieser Forschungsergebnisse kann davon ausgegangen werden, dass generalisiertes Vertrauen in andere Personen ebenfalls eine wichtige Rolle spielt, wenn Jugendliche z. B. durch Phishing-Mails dazu aufgefordert werden, private und sensible Daten einem potentiell gefährlichen Internetanbieter zur Verfügung zu stellen. Aufgrund der engen positiven Assoziation von generalisiertem Vertrauen mit risikoreichen Verhaltensweisen [May 1995] kann im vorliegenden Fall davon ausgegangen werden, dass ein höheres Maß an Vertrauen mit einer höheren Nachlässigkeit einhergeht. Für die Studie wurde also angenommen, dass das generalisierte Vertrauen in Mitmenschen protektive Verhaltensweisen von Jugendlichen eher negativ beeinflussen würde.

► **Die *Einschätzung des Risikos***

Neben dem grundsätzlichen Vertrauen in andere Personen zeigen frühere Forschungsarbeiten, dass die Risikowahrnehmung ein entscheidender Einflussfaktor bei Handlungen im Internet darstellt. Dabei ist die Risikowahrnehmung als subjektive Einschätzung zu betrachten, die vom objektiven Risiko abweichen kann. Zudem zeigen frühere Arbeiten, dass Personen sich bei ihren Handlungen stark von diesen Risikowahrnehmungen leiten lassen, z. B. wenn es darum geht, einem Online-Dienst persönliche sensitive Daten zur Verfügung zu stellen [Keh in press], oder Maßnahmen gegen potentiellen Identitätsdiebstahl zu ergreifen [Lai 2012].

Vor diesem Hintergrund lässt sich annehmen, dass das protektive Verhalten Jugendlicher von ihrer Risikowahrnehmung beeinflusst wird: Wer das Risiko als hoch einschätzt, online Opfer von kriminellen Handlungen zu werden, sollte auch entsprechend häufiger Gegenmaßnahmen ergreifen, d. h. mehr protektive Verhaltensweisen zeigen.

► **Die selbsteingeschätzte *Expertise* im Umgang mit dem Computer**

Ein weiterer, nahe liegender potentieller Prädiktor protektiver Verhaltensweisen stellt die Expertise im Umgang mit dem Computer dar. Es erscheint einleuchtend zu erwarten, dass ein höheres Maß an Erfahrung die Fähigkeiten erhöht, sicherheitsrelevante Maßnahmen überhaupt ergreifen zu können [Par 2011]. Daher wurde in dieser Studie angenommen, dass eine höhere Expertise im Umgang mit Computern in einem positiven Zusammenhang mit den Maßnahmen steht, die Nutzer ergreifen, um den eigenen Computern vor Fremdzugriffen zu schützen.

► **Das *Wissen* um sicherheitsrelevante Maßnahmen**

Trotz potentiell hoher Expertise im Umgang mit Computern könnten protektive Maßnahmen ausbleiben, wenn nicht ausreichende Kenntnisse zur Verfügung stehen, die das Ergreifen sicherheitsrelevanter Maßnahmen ermöglichen. Wie frühere Arbeiten zeigen, bedingt ein höheres Maß an Kenntnissen über zu ergreifende Maßnahmen z. B. die Wahrscheinlichkeit, dass Personen bestimmte Webseiten meiden oder sich für bestimmte Web-Dienste nicht registrieren [Par 2011]. Es liegt daher nahe anzunehmen, dass das Wissen um Themen der Computersicher-

heit ein wichtiger Prädiktor dafür ist, dass Jugendliche entsprechende Maßnahmen auch ergreifen.

► **Die *Kontrolle* durch die Eltern**
Insbesondere bei Jugendlichen, die meist noch bei den Eltern zuhause wohnen, kann angenommen werden, dass auch das Maß der elterlichen Kontrolle Auswirkung auf ihr Verhalten haben kann. So zeigen bisherige Studien, dass Regeln zur Internetnutzung, die von Eltern aufgestellt werden, das risikoreiche Verhalten von Jugendlichen im Internet drastisch reduzieren können [Kie 2005]. Es kann daher angenommen werden, dass ein höheres Maß an elterlicher Kontrolle einen positiven Einfluss auf das protektive Verhalten Jugendlicher ausüben kann.

3 Eine Befragung unter Jugendlichen

Ausgehend von diesen Annahmen wurde ein standardisierter (d. h. für alle Teilnehmer gleichlautender) Selbstauskunftsfragebogen erstellt, der die zu erfragenden Konstrukte abdeckte. Dieser wurde 2009 im Rahmen einer repräsentativen Befragung insgesamt 1.271 Jugendlichen vorgelegt. Bei der Auswahl der Teilnehmer wurde darauf geachtet, dass diese zu etwa gleichen Teilen aus verschiedenen Schultypen (Hauptschule, Realschule, Gymnasium) sowie Klassenstufen (7.-10. Klasse) stammten. Des Weiteren wurde pro Schultyp eine Schule aus einem großstädtischen (> 200.000 Einwohner), kleinstädtischen (80.000 – 100.000 Einwohner) sowie eher ländlichen Gebiet (< 30.000 Einwohner) ausgesucht, um die Gefahr einer Selektivität bei der Stichprobenziehung zu verringern.

Zur Messung des Computerwissens kam ein Multiple Choice Quiz zur Anwendung, bei dem die Anzahl der richtigen Antworten als Maß für das Computerwissen diente. Alle anderen Konstrukte wurden über Fragen und Aussagen erfasst, deren Ausprägung die Teilnehmer auf einer Ratingskala selbst einschätzen sollten. Mit Bezug auf das protektive Verhalten, beispielsweise, wurden sieben Aussagen formuliert, die relevante Dimensionen sicherheitsrelevanter Maßnahmen (z. B. Virenscanner nutzen, Firewall nutzen, Software updaten, fremde Mailanhänge nicht öffnen usw.) abbilden sollten. Einen Überblick über Anzahl und Art der verwendeten Fragen gibt Tabelle 1. Zusätzlich enthielt der Fragebogen Fragen zu soziodemographischen Merkmalen, also z. B. zu Alter, Geschlecht und täglicher Internet-Nutzungsdauer.

Als Schätzer für die Messgenauigkeit der verwendeten Skalen wurde, wo möglich, Cronbachs α bestimmt. Dieser Kennwert gibt an, in welchem Ausmaß Fragen, die das Gleiche messen sollen, miteinander korrelieren. Werte über 0,70 gelten als Richtwert für eine ausreichende Messgenauigkeit einer Skala. Wie aus Tabelle 1 ersichtlich ist, war dies für alle verwendeten Skalen der Fall.

4 Statistische Auswertung

Die Befragten waren im Durchschnitt 14,95 Jahre (SD = 1,73 Jahre) alt und verbrachten durchschnittlich 1,77 Stunden pro Tag vor dem Computer (SD = 1,95). Das Geschlechterverhältnis war mit 44,1% männlichen und 41,1% weiblichen Teilnehmern (14,7% keine Angabe) relativ ausgeglichen. Durchschnittlich fanden sich knapp vier Personen (M = 3,77; SD = 1,16) sowie 2,5 Computer (M = 2,47; SD = 1,51) pro Haushalt. Die überwiegende Mehrheit (87,3%) der Teilnehmer gab an, zuhause über einen Internetzugang zu verfügen, und 50% der Teilnehmer verfügten über ein eigenes Gerät, das exklusiv nur sie nutzten.

Insgesamt zeigte sich ein relativ geringes Wissen in Bezug auf sicherheitsrelevante Maßnahmen. So wussten lediglich 15,5% der Befragten, dass das das Hypertext Transfer Protocol Secure (https://) als sicherer zu bewerten ist als das entsprechende Standardprotokoll (http://), und weniger als die Hälfte der Befragten war in der Lage, eine Phishing-Mail von einer echten E-Mail zu unterscheiden (60,4% der Befragten antworteten falsch oder gaben an, die Antwort nicht zu kennen). Im Durchschnitt beantworteten die Teilnehmer damit lediglich drei der vorgegebenen neun Quizfragen richtig (vgl. Tabelle 1). Allerdings ließ sich bei den Antworten auch ein linearer Trend ermitteln, d. h. das Wissen stieg mit der Klassenstufe und Schulart linear an. So beantworteten Schüler in der 7. Klasse durchschnittlich 2,03 Fragen korrekt, während Teilnehmer der 10. Klasse im Schnitt 4,51 Quizfragen lösen konnten. ($F(1, 1229) = 206{,}41$; $p < 0{,}001$; $\eta^2 = 0{,}14$). Gleichzeitig unterschied sich das Wissen zwischen den Schultypen ($F(2, 1230) = 46{,}87$; $p < 0{,}001$; $\eta^2 = 0{,}07$): Wie Post-Hoc Analysen mit Bonferroni-Korrektur zeigten, konnten Hauptschüler mit 2,17 richtigen Antworten durchschnittlich weniger Fragen richtig beantworten als Realschüler ($M = 3{,}42$; $p < 0{,}001$) oder Gymnasiasten ($M = 3{,}54$; $p < 0{,}001$). Für Realschüler und Gymnasiasten fanden sich im direkten Vergleich jedoch keine signifikanten Unterschiede ($p = 0{,}99$).

Ebenfalls ausschlaggebend waren das Geschlecht sowie das Vorhandensein eines eigenen Computers: So gaben männliche Teilnehmer mehr richtige Antworten als weibliche ($M_{Männer} = 3{,}87$; $M_{Frauen} = 2{,}76$; $F(1, 1082) = 81{,}74$; $p < 0{,}001$; $\eta^2 = 0{,}07$), und Jugendliche mit eigenem Computer hatten ein höheres Wissen um sicherheitsrelevante Maßnahmen als Jugendliche ohne eigenen Computer ($M_{Mit} = 3{,}85$; $M_{Ohne} = 2{,}76$; $F(1, 1056) = 71{,}80$; $p < 0{,}001$; $\eta^2 = 0{,}06$).

Ähnliche Ergebnisse zeigten sich auch bei der Computerexpertise, wo männliche Befragte sowie Teilnehmer mit eigenem Computer angaben, über eine höhere Expertise zu verfügen ($M_{Männer} = 1{,}69$; $M_{Frauen} = 1{,}35$; $F(1, 1056) = 47{,}59$; $p < 0{,}001$; $\eta^2 = 0{,}04$; $M_{Mit} = 1{,}69$; $M_{Ohne} = 1{,}34$; $F(1, 1040) = 48{,}39$; $p < 0{,}001$; $\eta^2 = 0{,}04$).

Interessanterweise zeigten sich jedoch kaum Unterschiede in Bezug auf die anderen Konstrukte. Insbesondere das generalisierte Vertrauen sowie das protektive Verhalten unterschieden sich kaum zwischen Geschlechtern, Klassenstufen, Schultypen oder bei Vorhandensein/Nicht-Vorhandensein eines eigenen Computers. Während soziodemographische Merkmale also einen Einfluss auf das Wissen und die Expertise der Teilnehmer auszuüben scheinen, waren diese in unserem Datensatz nicht entscheidend

Tab. 2 | Ergebnisse der multiplen Regression.

Prädiktor	Koeffizient β (t)	R^2
Computerexpertise	0,43 (15,69)	
Risikoeinschätzung	0,29 (10,63)	
Wissen	0,13 (4,86)	
Elternkontrolle	0,11 (4,18)	
Vertrauen	0,10 (3,85)	
		0,39

Hinweis: Alle Regressionskoeffizienten signifikant mit $p < 0{,}0001$.

bei der Erklärung von Vertrauen oder protektiven Verhaltensweisen der teilnehmenden Schüler.

Um den Zusammenhang protektiven Verhaltens mit den angenommenen Einflussfaktoren zu untersuchen, wurde in einem nächsten Schritt eine multiple Regression durchgeführt. Bei diesem auf den Prinzipien der Korrelationsanalyse beruhenden Verfahren lassen sich die Regressionsgewichte mehrerer simultan untersuchter Prädiktorvariablen miteinander vergleichen. Positive Regressionsgewichte (sog. β-Koeffizienten) weisen dabei auf einen positiven Zusammenhang mit der Kriteriumsvariable (hier: protektives Verhalten) hin. Die Ergebnisse der Regressionsanalyse sind in Tabelle 2 dargestellt. Die Ergebnisse können wie folgt interpretiert werden: Das Ausmaß, in dem eine Person protektives Verhalten zeigt, steigt signifikant an, je größer ihre Computerexpertise, ihre Risikoeinschätzung und ihr Wissen ist, je stärker sie von den Eltern kontrolliert wird und je größer ihr generalisiertes Vertrauen ist. Die Expertise sowie die Einschätzung potentieller Risiken stellen dabei die bedeutsamsten Einflussfaktoren dar, während Vertrauen in andere Personen sowie elterliche Kontrolle eine kleinere Rolle zu spielen scheinen.

Insgesamt ließen sich mittels dieser fünf Prädiktoren knapp 40% der Varianz im protektiven Verhalten erklären ($R^2 = 0{,}39$). Dies lässt einerseits den Rückschluss zu, dass es weitere, in dieser Studie nicht beachtete Prädiktoren gibt, die das protektive Verhalten von Jugendlichen mitbestimmen. Gleichzeitig zeigt der relativ hohe Wert, dass in der vorliegenden Studie bereits einige der relevantesten Prädiktoren abgedeckt werden konnten.

5 Diskussion der Ergebnisse

Das Ziel der vorliegenden Studie war es, Prädiktoren sicherheitsrelevanten Verhaltens bei jugendlichen Computernutzern zu identifizieren. Es sollte also herausgefunden werden, welche Merkmale von Jugendlichen im Zusammenhang damit stehen, dass diese protektive Maßnahmen ergreifen, um den Computer vor Fremdzugriffen zu schützen. Aus der statistischen Auswertung der Befragung lassen sich folgende Implikationen ableiten:

▸ **Protektives Verhalten fördern**

Der höchste Zusammenhang mit protektivem Verhalten ergab sich für den Prädiktor Computerexpertise: Jugendliche, die sich selbst hohe Expertenkenntnisse im Umgang mit dem Computer zuschrieben, gaben gleichzeitig auch häufiger an, sicherheitsrelevante Maßnahmen am Computer zu ergreifen. Die Ergebnisse zeigten auch, dass computererfahrene Jugendliche in erster Linie männlich waren und über einen eigenen Computer verfügten. Diese Resultate bestätigen frühere Forschungsarbeiten, die wiederholt über einen positiven Zusammenhang zwischen Erfahrungswerten und datenschutzrelevanten Einstellungen oder Verhaltensweisen berichteten [Par 2011; You 2009]. Gleichzeitig deutet der starke Zusammenhang mit Computerexpertise auf die Wichtigkeit hin, Kinder und Jugendliche früh und in Eigenverantwortung an Informationstechnologie heranzuführen, um ihnen den Aufbau einer entsprechenden Expertise überhaupt zu ermöglichen.

Allerdings sollte dies nicht ohne die Vermittlung einer gesunden Risikoeinschätzung und eines ausreichenden Wissens über sicherheitsrelevante Maßnahmen geschehen, wie die Ergebnisse ebenfalls verdeutlichen. Vor dem Hintergrund des insgesamt eher gering ausgeprägten Wissens in der untersuchten Stichprobe erscheint die Vermittlung von Informationen über Computersicherheit als eine wichtige Aufgabe.

▸ **Die Rolle der Eltern**

Im Vergleich zu Computerexpertise und Risikoeinschätzung schien das Ausmaß der elterlichen Kontrolle in einem geringen Zusammenhang mit protektiven Verhaltensweisen zu stehen. Dies ist insofern überraschend, als frühere Arbeiten wiederholt auf erzieherische Einflussfaktoren von Seiten der Eltern verwiesen, um sicherheitsrelevante Einstellungen und Verhaltensweisen von Jugendlichen zu erklären. So zeigt etwa eine Befragung zu den Auswirkungen elterlicher Kontrolle unter 12-17jährigen Heranwachsenden, dass durch die Eltern aufgestellte Regeln die Häufigkeit potentiell gefahrvoller Treffen mit fremden Internetbekanntschaften signifikant reduzieren können [Kie 2005].

Allerdings weiß man auch, dass der Einfluss von elterlichen Ratschlägen auf das Verhalten Jugendlicher gerade in der Pubertät zurückgeht. Es ist daher möglich, dass die Umsetzung von computer- und sicherheitsbezogenen Geboten und Verboten in der Praxis nur schwer zu gewährleisten ist. Der geringe Zusammenhang zwischen elterlicher Kontrolle und protektiven Verhaltensweisen könnte also dadurch gegeben sein, dass Eltern trotz festgelegter Regeln wenige Möglichkeiten haben, die Ausübung dieser Regeln auch zu überwachen. Diese Erklärungsmöglichkeit deckt sich mit dem in Studien berichteten Gefühl vieler Eltern, zu wenig über die Internetaktivitäten ihrer Kinder zu wissen [Tel 2014]. Ein Weg, um trotz dieser Schwierigkeiten das Bewusstsein Jugendlicher zu schärfen, könnte daher über einen offenen und der Sache angemessenen Dialog führen, bei dem Eltern und Kinder auf Augenhöhe über Schutzmaßnahmen gegen Gefahren wie Phishing oder Computerviren diskutieren [You 2008].

▸ **Mehr Vertrauen schadet nicht**

Entgegen der Vorannahmen weisen die vorliegenden Ergebnisse auf einen geringen positiven Zusammenhang zwischen generalisiertem Vertrauen und protektiven Verhaltensweisen hin, d. h. Jugendliche mit höherem Vertrauen in andere Personen tendierten auch dazu, mehr Maßnahmen zum Schutz des eigenen Computers zu ergreifen. Dies ist insofern überraschend, als generalisiertes Vertrauen in vergangenen Studien häufig mit einer gewissen „Nachlässigkeit" assoziiert wurde, die eher risikoreicheres Verhalten erwarten ließ [May 1995]. Die vorliegenden Befunde stehen jedoch im Einklang mit der Annahme, dass generalisiertes Vertrauen und Leichtgläubigkeit unterschieden werden können und müssen [Yam 2001]. Es könnte also angenommen werden, dass generalisiertes Vertrauen in einem positiven Zusammenhang mit protektiven Verhaltensweisen steht, während Leichtgläubigkeit negativ mit sicherheitsrelevanten Maßnahmen korreliert.

Es erscheint daher aussichtsreich, die Rolle von Vertrauen und Leichtgläubigkeit als Prädiktoren von sicherheitsrelevantem Verhalten weiter zu studieren. An der Stelle sollte auch betont werden, dass im vorliegenden Artikel ***generalisiertes Vertrauen*** in andere Menschen und nicht ***Vertrauen in konkrete technische Geräte, Infrastrukturen oder ITDienstleister*** erfasst wurde. Es wäre plausibel anzunehmen, dass Vertrauen z. B. in die Funktionsweise des Internet, in die Seriosität von Anbieter von Antivirensoftware oder in die Sicherheitsausstattung des eigenen Rechners in einem höheren Zusammenhang mit der Ausführung sicherheitsrelevanter Maßnahmen bei Jugendlichen stehen könn-

ten. In der Tat zeigen frühere Arbeiten, dass z. B. das „Vertrauen in das Internet“ ein guter Indikator für die Bereitschaft von Personen ist, private Daten über das Internet preis zu geben [Din 2006b]. Offen bleibt allerdings die Frage, ob die Stärkung der (vertrauensbildenden) Akzeptanz von nutzerorientierten Tools wie Trackerfiltern und Scriptblockern zu ähnlich positiven Effekten führen könnte wie infrastrukturelle Maßnahmen.

Fazit

Ob und wie häufig Jugendliche Maßnahmen ergreifen, um ihren Computer vor Fremdzugriffen zu schützen, ist von vielfältigen Faktoren abhängig. Folgt man der oben beschriebenen Studie, so sind eine hohe Erfahrung im Umgang mit dem Computer und eine hohe Risikoeinschätzung in dieser Hinsicht besonders entscheidend, das Aufstellen und Überwachen von Geboten und Verboten durch die Eltern dagegen nicht. Zugleich jedoch scheinen vertrauensbildende Maßnahmen zumindest keine schädliche Auswirkung auf das protektive Verhalten von Jugendlichen haben. Insgesamt betont die vorliegende Studie damit die Bedeutung früher computerbezogener Erfahrungen und partizipativer, auf Vertrauen aufbauender Erziehungsmaßnahmen, um Jugendliche früh zu verantwortungs- und gefahrenbewussten Usern zu machen.

Literatur

[BKA 2013] Bundeskriminalamt: *Cybercrime Bundeslagebild 2013*. Wiesbaden: Bundeskriminalamt.

[Din 2006a] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, C. Colautti: *Privacy calculus model in e-commerce–a study of Italy and the United States*. European Journal of Information Systems 4/2006a, 389-402.

[Din 2006b] T. Dinev, P. Hart: *An Extended Privacy Calculus Model for E-Commerce Transactions*. Information Systems Research 1/2006b, 61-80.

[Keh in press] F. Kehr, T. Kowatsch, D. Wentzel, E. Fleisch: Blissfully ignorant: *The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus*. Information Systems Journal Special Issue on: Reframing Privacy in a Networked World in press,

[Kie 2005] L. A. Kienfie, A. Khoo, Ang, P. H.: *Factors influencing Adolescents Engagement in Risky Internet Behavior.* CyberPsychology & Behavior 6/2005, 513-520.

[Lai 2012] F. Lai, D. Li, C.-T. Hsieh: Fighting Identity Theft: *The coping perspective*. Decision Support Systems 2/2012, 353-363.

[Lee 2001] M. K. O. Lee, E. Turban: *A Trust Model for Consumer Internet Shopping*. International Journal of Electronic Commerce 2001, 75-92.

[May 1995] R. C. Mayer, J. H. Davis, D. Schoorman: *An Integrative Model of Organizational Trust*. The Academy of Management Review 3/1995, 709-734.

[Par 2011] Y. J. Park: *Digital Literacy and Privacy Behavior Online*. Communication Research 2/2011, 215-236.

[Rot 1967] J. B. Rotter: *A new scale for the measurement of interpersonal trust*. Journal of Personality 1967, 651-665.

[Tel 2014] Telekom: *Sicherheitsreport 2014*. Deutsche Telekom AG.

[Yam 2001]T. Yamagishi: *Trust as a form of social intelligence*. In: K. S. Cook (Ed.): *Trust in Society*, New York, Russell Sage Foundation, 121-147.

[You 2008] S. Youn: *Parental Influence and Teens' Attitude toward Online Privacy Protection*. Journal of Consumer Affairs 3/2008, 362-388.

[You 2009] S. Youn: *Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents*. Journal of Consumer Affairs 3/2009, 389-418.