Bürgerdialog 2014

Eine Umfrage zum Thema Datenschutz und IT-Sicherheit

CISPA
Center for IT-Security, Privacy and Accountability

Titelbild:
Quelle: Gerd Altmann / all-silhouettes.com / pixelio.de
Bearbeitung: Magdalena Gadaj / gadaj.de

Inhaltsverzeichnis

1 Hintergrund

Das “Center for IT-Security, Privacy and Accountability” (CISPA) ist das 2011 gegründete Kompetenzzentrum für IT-Sicherheit an der Universität des Saarlandes. Es ist eines von drei Kompetenzzentren für IT-Sicherheit in Deutschland, die durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert werden.

Am CISPA erforschen wir aktuelle Themen der IT-Sicherheit, um Lösungen für die Kernprobleme der digitalen Gesellschaft zu entwickeln. Wir identifizieren dabei Sicherheitslücken in heute verwendeten IT-Systemen und arbeiten gleichzeitig daran, sichere Lösungen und Methoden sowohl für bereits existierende, als auch für zukünftige IT-Systeme zu entwickeln.

Ein besonderes Anliegen des CISPA ist es, die eigene Forschung im engen Kontakt mit der Bevölkerung durchzuführen. Darunter verstehen wir mehr als lediglich eine an den Bedürfnissen der Gesellschaft orientierte Forschung. Wir streben gezielt auch die Aufklärung der Bevölkerung (“Awareness”) hinsichtlich existierender Schwachstellen im Datenschutz und in der IT-Sicherheit an. Darüber hinaus möchten wir auch auf bereits existierende und zukünftige Schutzmöglichkeiten hinweisen.

Ziel unseres Bürgerdialogs ist ein Informationsaustausch mit den Bürgern. Dies ermöglicht es uns, die Bedürfnisse der Bevölkerung in unsere aktuelle Forschungsrichtung einfließen zu lassen.

Wir möchten hervorheben, dass es sich hierbei nicht um eine klassische, repräsentative Datenerhebung handelt. Vielmehr soll ein Überblick über das aktuelle Stimmungsbild der Bürger in Bezug auf das Thema IT-Sicherheit geschaffen werden. Darüber hinaus soll die Befragung einen deutlichen Lehrcharakter haben und die Befragten beispielsweise auf die verfügbaren Sicherheitstechnologien hinweisen und ihnen aufzeigen, wie sie sich sicherer durch das digitale Zeitalter bewegen können.

Wir legen besonderen Wert auf den persönlichen Dialog zwischen unseren Forschern und den Bürgern, in dem die Bürger ihre Bedenken, Wünsche und Anregungen ausdrücken können. Neben den Ergebnissen der Befragung schildern wir im Folgenden auch unsere persönlichen Eindrücke aus diesem Dialog.

2 Befragung

Im Rahmen unseres Bürgerdialogs haben wir anlässlich der Vorträge der CISPA Professoren Prof. Christian Hammer und Prof. Michael Backes zum Thema Datenschutz und IT-Sicherheit eine Befragung der Zuhörer durchgeführt. Eine weitere Befragung der Bürger wurde von uns in der Innenstadt von Saarbrücken organisiert. Bei beiden Gelegenheiten erhielten die Bürger die Möglichkeit, mit unseren Professoren und Forschern in persönlichen Dialog zu treten, sowie einen Fragebogen auszufüllen.

Insgesamt waren wir sehr positiv über das enorme Interesse der Bürger an unserer Forschung und unserem Kompetenzzentrum überrascht. Viele Bürger kamen proaktiv und interessiert an unseren Stand. Es bedurfte lediglich der Präsenz unserer Forscher in der Stadt mit einem Poster, welches die Kernthemen unserer Forschung, die beteiligten Institute und unseren Förderer BMBF präsentiert, um eine große Anziehungskraft zu entwickeln.

Im Folgenden geben wir eine Übersicht über die Inhalte des Fragebogens und erläutern die Ergebnisse und unsere persönlichen Eindrücke aus dem Dialog. Die Fragen entstammen

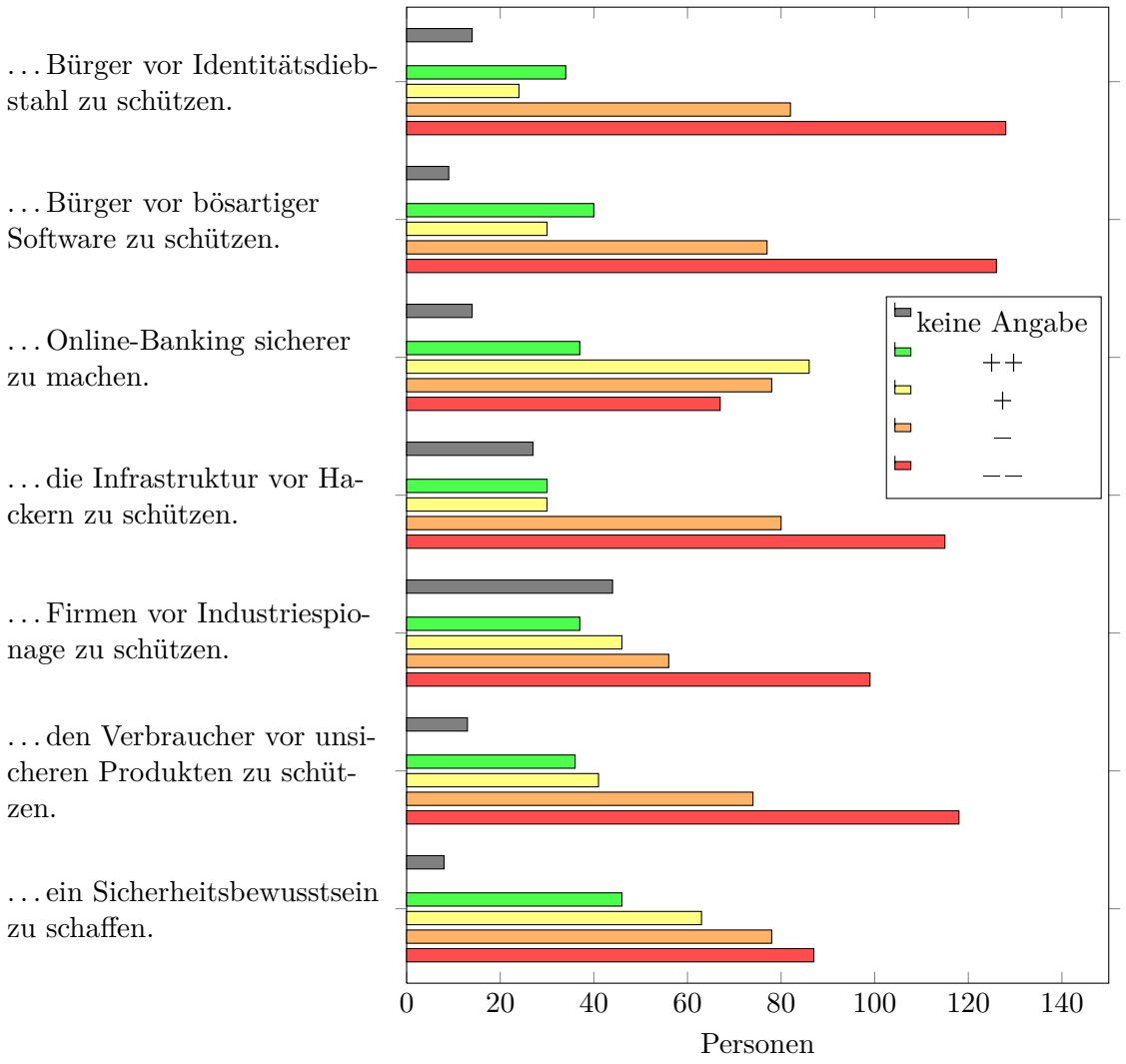

Abbildung 1: Antworten auf die Frage: “Ich finde, dass genug getan wird, um ... ”. Die Antwortmöglichkeiten reichen von “Stimme zu (++)” bis “Stimme nicht zu (−−)”.

hierbei folgenden Bereichen: 1. Einschätzung der aktuellen Lage, 2. Selbsteinschätzung, 3. Engagement zum Selbstschutz, 4. Umgang mit Daten im Web, 5. Anonymität und 6. Bezug zu neuen Technologien.

2.1 Einschätzung der aktuellen Lage

Uns ist es wichtig, zu verstehen, wo die Bürger derzeit Schwächen im Datenschutz und in der IT-Sicherheit sehen. Wir sprechen dabei eine Vielzahl von Themen an, von denen die Bürger entweder direkt betroffen sind, wie zum Beispiel bei Fragen zum Online-Banking, oder Themen von denen sie lediglich unmittelbar betroffen sind, zum Beispiel wenn es um Fragen der nationalen Sicherheit oder zur IT-Sicherheit in der Wirtschaft geht.

Mit der folgenden Frage fangen wir ein generelles Stimmungsbild ein und beginnen einen Dialog hinsichtlich der Zielsetzung moderner IT-Sicherheitsforschung.

Frage: “Ich finde, dass genug getan wird, um ...

a) ... Bürger vor Identitätsdiebstahl zu schützen.”

b) ... Bürger vor bösartiger Software zu schützen.”

c) ... Online-Banking sicherer zu machen.”

d) ... die Infrastruktur vor Hackern zu schützen.”

e) ... Firmen vor Industriespionage zu schützen.”

f) ... den Verbraucher vor unsicheren Produkten zu schützen.”

g) ... ein Sicherheitsbewusstsein zu schaffen.”

Die Umfrage zeigt, dass obwohl die Bürger starken Handlungsbedarf bei der Sicherheit von IT-Systemen sehen (siehe Abbildung 1), einige Systeme dennoch als relativ sicher angesehen werden. Dieses Sicherheitsgefühl basiert jedoch oft auf falschen Annahmen. Ein Beispiel ist die Annahme, ein bestimmtes Verfahren wie etwa SMS-TAN bei Online-Banking, sei absolut sicher. Wenn Online-Banking jedoch auf demselben Smartphone durchgeführt wird, welches auch die SMS empfängt, ist das SMS-TAN Verfahren nicht mehr unbedingt sicher.

Darüber hinaus zeigt der Dialog mit den Bürgern, dass vor allem seit dem Snowden-Vorfall ein neues Sicherheitsbewusstsein entstanden ist. Die Bürger beginnen, die Sicherheit von existierenden Systemen grundsätzlich zu hinterfragen.

Durch die Umfrage-Ergebnisse, aber auch durch den Dialog mit den Bürgern selbst zeigt sich, dass die Sicherheitsforschung (zum Beispiel durch das CISPA) als grundsätzlich wichtig erkannt wird. Es wird jedoch weiterhin ein gravierender Handlungsbedarf gesehen, der nicht nur die Forschung selbst betrifft, sondern auch die Umsetzung der von der Forschung vorgeschlagenen Methoden in die Praxis. Hier arbeitet das CISPA an mehreren Projekten, die unter dem Begriff der “Usable Security”, zu Deutsch “anwendbare Sicherheit”, auf Lösungen hinarbeiten, die leicht benutzbar sind und gleichzeitig effektiven Schutz bieten. Ein Beispiel hierfür ist die vom CISPA entwickelte App “AppGuard”, die es Benutzern ermöglicht, ihre Privatsphäre gegenüber neugierigen Apps zu schützen.

2.2 Selbsteinschätzung

Um die Bürger richtig aufklären zu können, ist es für uns von grundlegender Bedeutung zu erfahren, wie gut informiert die Bürger sich in Bezug auf Datenschutz und Datensicherheit fühlen. Die Antworten auf diese Fragen helfen uns, in den kommenden Gesprächen gezielt auf wahrgenommene Informationsmängel einzugehen. Des Weiteren zeigt uns diese Selbsteinschätzung, in welchen Bereichen generell Aufklärungsbedarf besteht.

Frage: “Ich fühle mich darüber informiert, ...

a) ... was Firmen mit meinen Daten tun.

b) ... was der Staat unternimmt, um meine Daten zu schützen.

c) ... auf welche meiner Daten Behörden Zugriff haben.

d) ... wie ich meine Daten auf meinem Computer schütze.

e) ... an wen ich mich im Falle eines Datendiebstahls wende.

Die Resultate zeigen, dass sich die Bürger grundsätzlich nicht ausreichend über die Verwendung ihrer persönlichen Daten informiert fühlen (siehe Abbildung 2). Den Bürgern fällt es

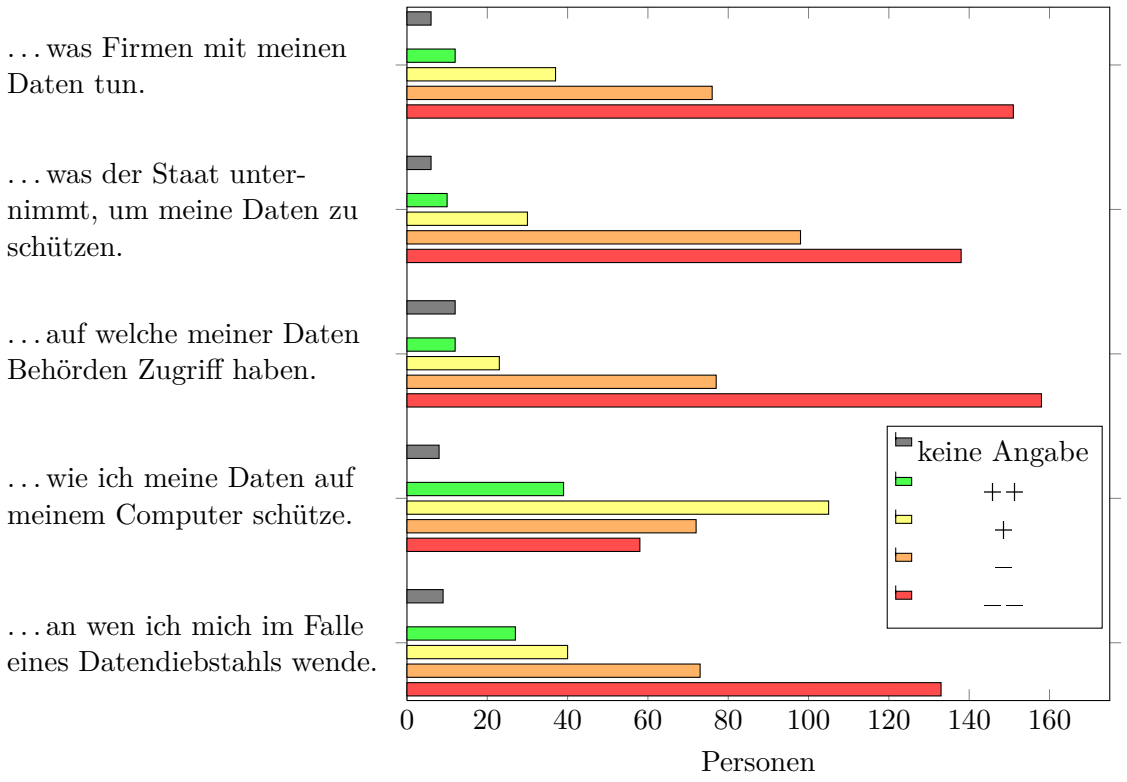

Abbildung 2: Antworten auf die Frage “Ich fühle mich darüber informiert, ...”. Die Antwortmöglichkeiten reichen von “Stimme zu (++)” bis “Stimme nicht zu (−−)”.

insbesondere schwer nachzuvollziehen, wie genau mit ihren Daten im Internet umgegangen wird und was letztens Endes mit ihren Daten geschieht.

Wir stellen fest, dass ein großes Interesse an genaueren Informationen vor allem in Bezug auf die Verwendung von persönlichen Daten durch Dienstleister vorhanden ist. Den Bürgern ist es wichtig zu verstehen, wie sich einzelne Datenerhebungen auf ihre Privatsphäre auswirken. Dies könnte möglicherweise durch striktere Auflagen zur Informationspflicht von Dienstleistern bei der Datenerfassung gelöst werden. Aber auch unabhängig von solchen Regulationen arbeiten wir am CISPA mit unserer Forschung daran, Lösungen zu finden, die nachvollziehbar machen, wie persönliche Daten im Internet verbreitet werden.

Viele der Befragten haben den Eindruck, dass ihre Daten zumindest auf dem eigenen PC sicher sind und erst durch die Herausgabe nach Außen in Gefahr geraten. Obgleich wir hier ebenfalls Handlungsbedarf sehen (viele PCs sind nicht ausreichend geschützt), stellen wir doch fest, dass die Mehrzahl der befragten Bürger die Gefahr der Herausgabe von Daten korrekt einschätzt.

Frage: “Wurden Ihre Daten schon einmal gegen Ihren Willen weitergegeben oder gestohlen?” Die Mehrheit der Befragten sieht die Gefahr, dass ihre Daten gegen den eigenen Willen weitergegeben wurden. Ein Großteil (fast jeder Vierte) gab sogar an, bereits Opfer von Datendiebstahl geworden zu sein (siehe Abbildung 3).

Unter den Befragten, die angaben, bereits Opfer von Datendiebstahl geworden zu sein, befanden sich überdurchschnittlich viele junge Bürger. Obwohl allgemein angenommen wird, dass jüngere Bürger tendenziell mehr Daten von sich veröffentlichen, zeigen unsere

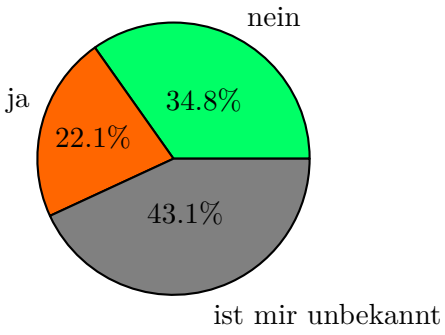

Abbildung 3: Antworten auf die Frage: “Wurden Ihre Daten schon einmal gegen Ihren Willen weitergegeben oder gestohlen?”

Gespräche, dass sie sich der Gefahren dieser Veröffentlichungen sehr bewusst sind. Des weiteren hatten wir aufgrund der Gespräche mit den Bürgern den Eindruck, dass junge Menschen einen Diebstahl ihrer persönlichen Daten früher erkennen.

2.3 Engagement zum Selbstschutz

Mit den folgenden Fragen möchten wir feststellen, wie häufig existierende Lösungen zur Verbesserung der eigenen Sicherheit genutzt werden. Hier geht es uns hauptsächlich darum, zu erfahren, ob weiterer Aufklärungsbedarf über existierende Lösungen und deren Benutzung bei den Bürgern besteht.

Diese Fragen haben zum einen den Charakter einer Stimmungserfühlung, zum anderen aber auch einen deutlichen Lehrcharakter. Es ist uns wichtig, die Bürger darauf hinzuweisen, welche sicherheitsverbessernden Möglichkeiten ihnen grundsätzlich zur Verfügung stehen.

Frage:“Verwenden Sie eine der folgenden Methoden, um sich und Ihre Daten zu schützen?”

a) ... Antivirus Software

b) ... Werbe-Blocker

c) ... Passwort-Manager

d) ... Verschlüsselte oder elektronisch signierte E-Mails

e) ... Festplattenverschlüsselung

f) ... Ignorieren unbekannter E-Mail Anhänge

g) ... Kein Anklicken verdächtiger Links

Erwartungsgemäß stellt sich heraus, dass Standard-Methoden wie Antivirus Software oder Werbe-Blocker von vielen Befragten benutzt werden (siehe Abbildung 4). Weniger beworbene Sicherheitsmethoden wie etwa Passwort-Manager, welche die Erstellung und Verwaltung sicherer Passwörter erlauben, oder Festplattenverschlüsselungen, die unbefugten Zugriff auf sensible Daten verhindern, werden hingegen weniger häufig genutzt. Insbesondere bei Passwort-Managern waren wir überrascht zu sehen, wie gering deren Verbreitung ist. Passwort-Manager erlauben es, ohne großen Aufwand sichere Passwörter für verschie-

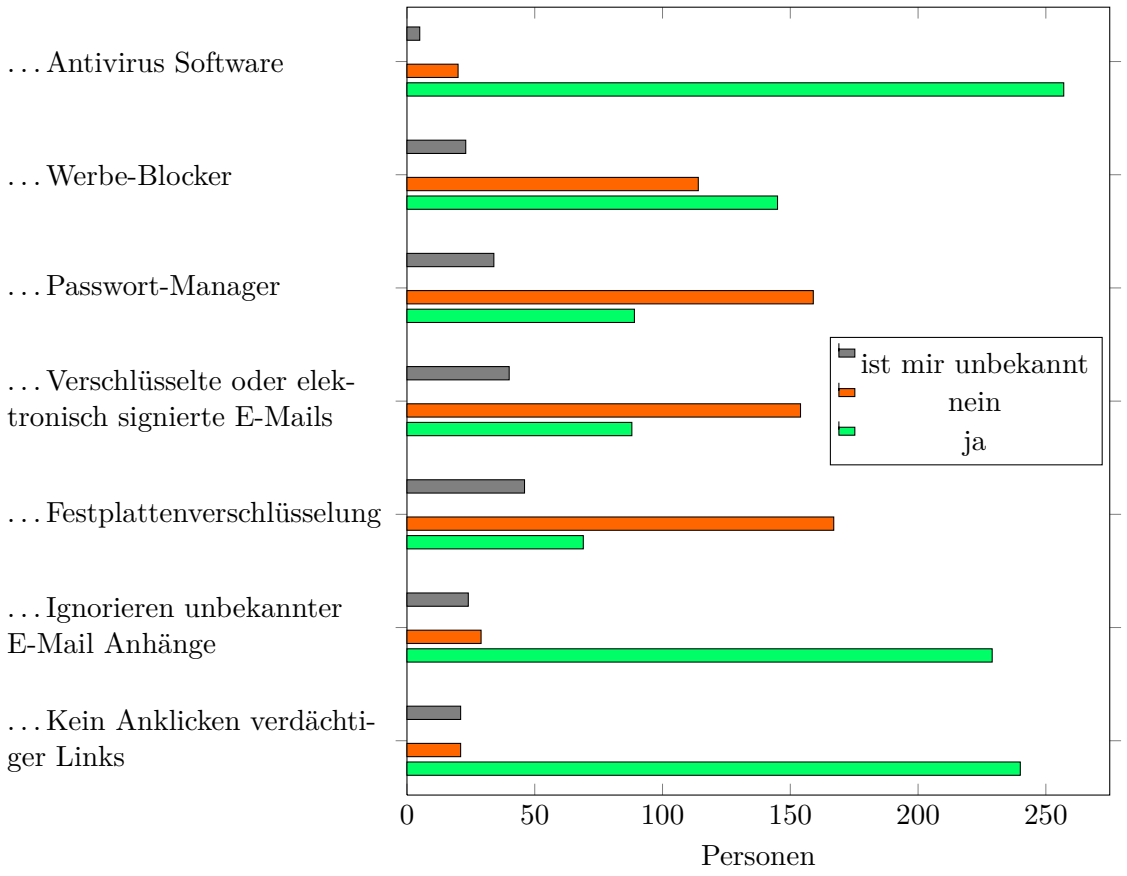

Abbildung 4: Antworten auf die Frage: “Verwenden Sie eine der folgenden Methoden, um sich und Ihre Daten zu schützen?”

dene Anwendungen zu generieren und mit einem so genannten Master-Passwort zu sichern. So muss sich ein Benutzer nur ein einziges sicheres Passwort überlegen und merken.

Im Gespräch mit den Bürgern zeigte sich, dass sich diese zwar für diese eher unbekannten Sicherheitsmethoden interessiere, aber ein großer Informationsbedarf dahingehend besteht, wie diese Methoden genutzt werden können.

Eine standardmäßige und benutzerfreundliche Integration bisher ungenutzter Sicherheitsmethoden in IT-Systeme, sowie eine breit angelegte Informationskampagne, wie sie in den letzten Jahren schon für Anti-Virus Software durchgeführt wurde, könnte hier das Nutzungsverhalten der Bürger deutlich verbessern.

Um dem hier offenbar gewordenen Bedarf nach Informationen gerecht zu werden, arbeitet das CISPA bereits mit der Saarbrücker Zeitung zusammen: wir werden gemeinsam eine Reihe von Artikeln veröffentlichen, in denen wir Begriffe und Technologien der IT-Sicherheit für Laien verständlich erklären. Insbesondere gehen wir hierbei auch auf bisher wenig genutzte Sicherheitsmethoden, wie die oben genannten Passwort-Manager oder die Festplattenverschlüsselung, ein.

2.4 Umgang mit Daten im Web

Mit den folgenden Fragen soll festgestellt werden, ob sich die Bürger Gedanken darüber machen, was mit ihren Daten passiert, wenn sie diese online mit verschiedenen Dienstanbietern teilen.

Der Hintergrund dieser Frage ist folgender: Der Schutz persönlicher Daten im Internet ist nur dann möglich, wenn verantwortungsvoll mit ihnen umgegangen wird. Wir raten in diesem Zusammenhang schon seit Jahren zur Datensparsamkeit: So sollten bei Anfragen im Internet beispielsweise nur die notwendigsten Daten angegeben werden. Dieses Verhalten ist eine einfache Methode, um den Schutz der persönlichen Daten gravierend zu erhöhen. Mit der folgenden Frage weisen wir die Bürger auf das Prinzip der Datensparsamkeit hin und erkundigen uns danach, ob sie dieses Prinzip bereits anwenden.

Frage: "Stellen Sie sich bitte folgendes Szenario vor: Sie wollen bei einem Ihnen bislang unbekannten Versandhaus online etwas bestellen und werden um die Eingabe von Informationen gebeten (zum Beispiel Adresse, Bankdaten, Geburtsdatum). Wie gehen Sie vor?"

a) ... Ich bestelle nie online.

b) ... Ich bestelle online nur bei wenigen, mir gut bekannten Anbietern.

c) ... Ich informiere mich eingehend über den Anbieter, ehe ich meine Daten eingebe.

d) ... Ich gebe meine Daten ein.

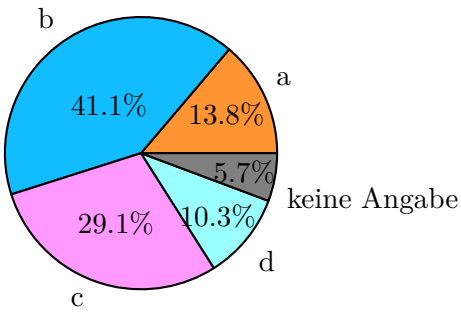

Abbildung 5: Antworten auf die Frage: "Stellen Sie sich bitte folgendes Szenario vor: ... Wie gehen Sie vor?"

Die Umfrage-Ergebnisse zeigen, dass sich die Bürger weitestgehend der Gefahren des Missbrauchs ihrer persönlichen Daten bewusst (siehe Abbildung 5) sind. Trotzdem handeln viele Befragte unvorsichtig, da sie dadurch bis dato keinen unmittelbaren Nachteil erfahren haben.

Auch diese Frage hat einen deutlichen Lehrcharakter. Bei der Beantwortung wird den Befragten klar, dass die Eingabe ihrer persönlichen Daten ein Sicherheitsrisiko darstellt, was mehrere Befragte ihre übliche Vorgehensweise hinterfragen ließ: Einige Befragte, die Antwort "d" ankreuzten, gaben an, dass ihnen bewusst war oder wurde, dass dies "eigentlich nicht die 'richtige' Antwort" sei.

2.5 Anonymität

Da unsere Forschung sich in Teilen auch mit der Möglichkeit befasst, online anonym zu sein, haben wir auch zu diesem Themenschwerpunkt Fragen eingebaut. Wir möchten erfahren, wie wichtig dies den Bürgern ist und welche Methoden sie üblicherweise verwenden, um ihre Anonymität zu verbessern.

Frage:"Finden Sie es wichtig anonym online sein zu können?" Obwohl heutzutage viele Menschen freizügig mit ihren Daten umgehen, zeigt die Umfrage überraschenderweise, dass die überwiegende Mehrzahl der Bürger es sehr wichtig findet, sich anonym im Internet bewegen zu können (siehe Abbildung 6). Hierbei zeigt sich kein großer Unterschied zwischen den verschiedenen Altersgruppen: Allen Altersgruppen war Anonymität ein wichtiges Grundbedürfnis.

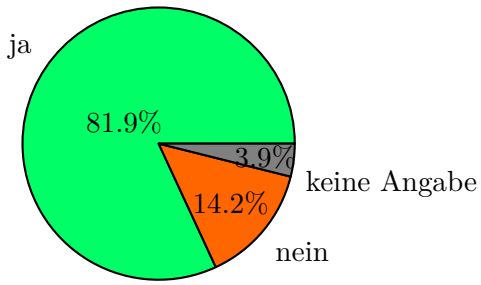

Abbildung 6: Antworten auf die Frage: "Finden Sie es wichtig anonym online sein zu können?"

Wir möchten nicht nur erfahren, ob die Bürger anonym sein wollen, sondern ebenfalls herausfinden, welche existierenden Methoden sie benutzen, um dies im Internet zu erreichen.

Mit der folgenden Frage gehen wir wieder implizit auf das Prinzip der Datensparsamkeit ein. Dieses Prinzip haben wir ebenfalls in unseren Gesprächen mit den Bürgern ausführlich diskutiert.

Frage:"Nutzen Sie eine der folgenden Methoden, um ihre Anonymität im Internet zu verbessern?"

a) ... Ich lasse optionale Angaben zu meiner Person weg, wenn ich Konten erstelle.

b) ... Ich nutze Pseudonyme statt meinen echten Namen und meine echten Daten anzugeben.

c) ... Ich benutze Anonymisierungsdienste (zum Beispiel Tor, Proxys, etc.).

Obwohl den Befragten Anonymität wichtig ist, zeigt sich hingegen, dass nur wenige Bürger aktiv versuchen, im Internet anonym zu bleiben (siehe Abbildung 7). Dies lässt sich unserer Erkenntnis nach darauf zurückführen, dass beispielsweise die Nutzung anonymisierender Dienste häufig einen Mehraufwand bedeutet, dem die Bürger sich im täglichen Umgang mit dem Internet nicht aussetzen wollen.

2.6 Bezug zu neuen Technologien

Neue Technologien bringen oft ein inhärentes Gefahrenpotential in Bezug auf die Sicherheit und die Privatsphäre ihrer Nutzer mit sich. Die Forschung am CISPA widmet sich daher unter anderem der Aufgabe, konkrete Probleme bei neuen Technologien zu identifizieren, diese Probleme zu lösen und dabei die Nutzbarkeit der neuen Technologien zu wahren.

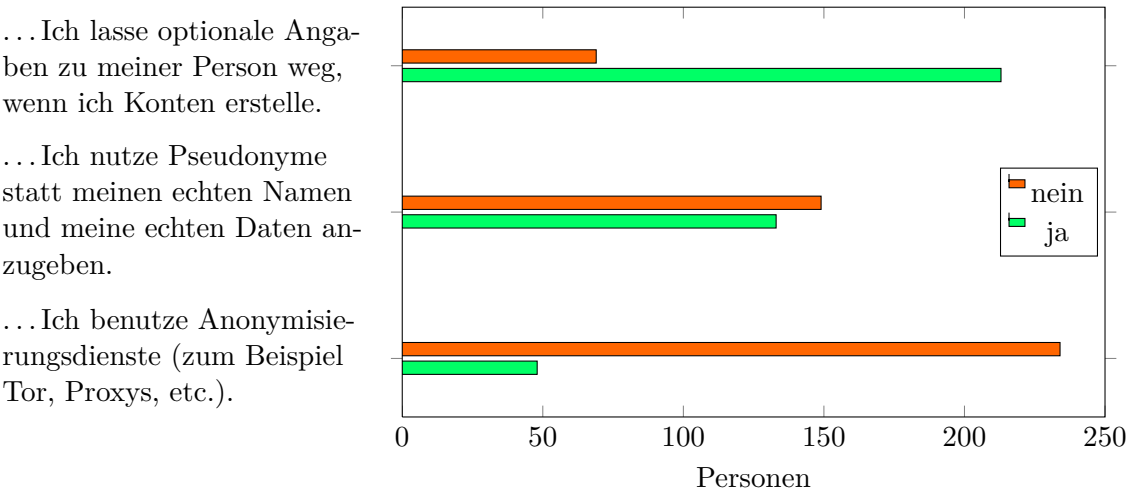

Abbildung 7: Antworten auf die Frage: “Nutzen Sie eine der folgenden Methoden, um ihre Anonymität im Internet zu verbessern?”

Wir möchten mit den folgenden Fragen feststellen, inwieweit sich die Bürger über die Relevanz neuer Technologien in Bezug auf Sicherheit und Privatsphäre im Klaren sind. Wir beziehen uns in den Fragen vor allem auf neue Technologien wie zum Beispiel Google Glass, die Smartphone-ähnliche Funktionalität in Alltagsgegenstände einbinden. Wir haben der Umfrage unter anderem ein Informationsblatt beigefügt, welches die Befragten über solche Technologien informierte.

Frage:“Wie stehen Sie zur Nutzung von neuen Technologien, insbesondere in Bezug auf Datensicherheit?”

a) ... Am Kopf getragene Minicomputer wie Google Glass gefährden meine Privatsphäre.

b) ... Am Kopf getragene Minicomputer wie Google Glass können der Datensicherheit (zum Beispiel bei Banking) im Alltag helfen.

c) ... Ich vertraue auf die Sicherheit von biometrischen Zugangsverfahren (zum Beispiel Fingerabdruck- und Iris-Scanner).

Diese Befragung zeigt (siehe Abbildung 8), dass sich die Bürger durchaus darüber bewusst sind, dass neue Technologien auch neue Gefahren mit sich bringen können. Auch wenn dies tendenziell eher von älteren Befragten angegeben wurde, zeigt sich doch, dass auch sehr viele junge Befragte Gefahren sehen.

Grundsätzlich besteht auch eine Skepsis gegenüber der Nutzbarkeit neuer Technologien (insb. Google Glass) zur Verbesserung der Sicherheit. Hier sehen wir großen Aufklärungsbedarf, da die aktuelle Forschung deutlich macht, dass diese neuen Technologien sehr wohl eingesetzt werden können, um die Sicherheit zu erhöhen. So zeigt die Arbeit des CISPA Forschers Prof. Dominique Schröder, wie Google Glass zur verbesserten Authentifikation gegenüber Bankautomaten genutzt werden kann.

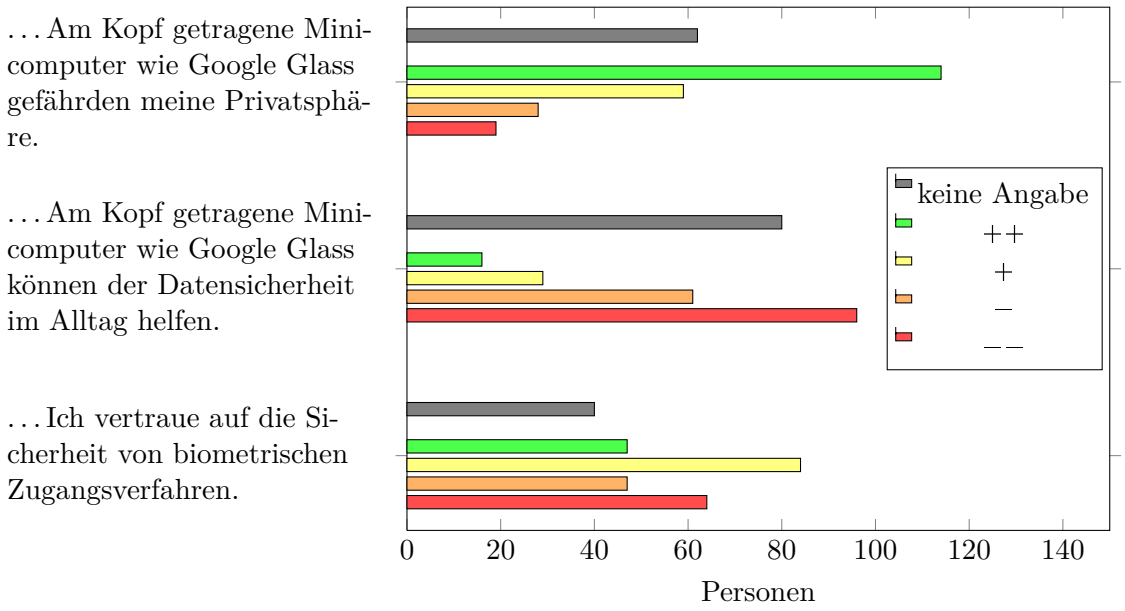

Abbildung 8: Antworten auf die Frage: “Wie stehen Sie zur Nutzung von neuen Technologien, insbesondere in Bezug auf Datensicherheit?”. Die Antwortmöglichkeiten reichen von “Stimme zu (++)” bis “Stimme nicht zu (−−)”.

3 Fazit

Wir betrachten den Bürgerdialog als großen Erfolg: Die Bürger waren sehr interessiert daran, sich mit uns auszutauschen und sind insbesondere auch aktiv auf uns zugegangen. Datenschutz und Anonymität ist ihnen ein wichtiges Grundbedürfnis, dessen Erfüllung bislang als unzureichend empfunden wird. Die Bürger sehen das CISPA und insbesondere auch die Unterstützung der Sicherheitsforschung durch das BMBF daher sehr positiv und als Schritt in die richtige Richtung.

Sie würden sich aber wünschen, dass die Forschung im Sicherheitsbereich, insbesondere im Bezug auf aktuelle Probleme, noch weiter ausgebaut wird. Viele Bürger hätten zum Beispiel gerne Lösungen gegen die Spionage durch andere Länder, sowie eine umfassendere Aufklärung über die bestehenden Risiken und die Möglichkeiten, sich gegen diese zu schützen.

4 Methodik

Die hier präsentierten Daten stammen aus Bürgerbefragungen, die zu verschiedenen Gelegenheiten durchgeführt wurden. Zum einen hatten Zuhörer der Vorträge über Datenschutz und IT-Sicherheit von Prof. Christian Hammer und Prof. Michael Backes die Möglichkeit, Fragebögen auszufüllen, zum anderen fand eine Online-Umfrage statt. Wir danken hierzu der Saarbrücker Zeitung für die Veröffentlichung des Links zur Umfrage. Darüber hinaus wurde von uns eine Befragung der Bürger in der Innenstadt von Saarbrücken durchgeführt. Wir verteilten dabei Umfragebögen mit den hier präsentierten Fragen an die Bürger und stellten uns den Bürgern auch zum persönlichen Dialog zur Verfügung. Der Hauptanteil der hier präsentierten Daten stammt aus dem direkten Kontakt mit den Bürgern.

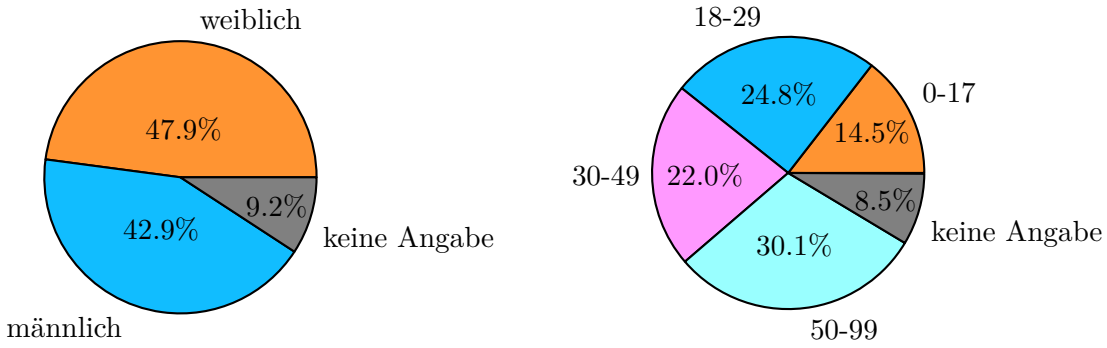

Abbildung 9: Geschlechterverteilung und Altersgruppen der Befragten

Das Spektrum der insgesamt 282 Befragten deckt alle Altersgruppen (siehe Abbildung 9) und eine Vielzahl an Berufen (akademischer und nicht akademischer Natur) ab. Unter den Befragten befanden sich insgesamt 135 Frauen und 121 Männer. 26 Befragte gaben ihr Geschlecht nicht an. Das Durchschnittsalter betrug etwa 38 Jahre.

UNIVERSITÄT DES SAARLANDES

Max Planck Institute for Software Systems

max planck institut informatik

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung