KASTEL-Bürgerdialog

Ein Ergebnisbericht

12. & 13. Mai 2014

„Das Internet ist für uns alle Neuland“ – wer sich am 12. und 13. Mai 2014 in Karlsruhe aufhielt, wurde schnell eines Besseren belehrt. Knapp ein Jahr nach Beginn der NSA-Affäre durch die Enthüllungen Edward Snowdens ist das Thema IT-Sicherheit in aller Munde: Sowohl bei den Bürgerinnen und Bürgern, die eine Überwachung ihrer Kommunikation durch ausländische staatliche Stellen befürchten, als auch bei Unternehmen, deren wirtschaftlicher Erfolg maßgeblich vom erfolgreichen Schutz ihrer Firmengeheimnisse beeinflusst wird.

Im Rahmen des 19. Präventionstags, dem seit 1995 bestehenden, europaweit größten Kongress zum Thema Kriminalprävention, wurde vom CyberForum e. V., dem über 1000 Mitglieder starken Hightech-Unternehmer-Netzwerk, für die interessierte Öffentlichkeit eine Reihe von Veranstaltungen zum Thema Cyber-Sicherheit angeboten. Neben mit hochkarätigen Referenten wie dem Präsidenten des Bundeskriminalamts Jörg Ziercke besetzten Vorträgen bestand an beiden Tagen die Möglichkeit, an Ständen verschiedener Aussteller zu aktuellen Themen in Diskussion zu treten. Im Rahmen dieser Vortragsreihe hat das Kompetenzzentrum für angewandte Sicherheitstechnologie KASTEL des Karlsruher Instituts für Technologie (KIT) einen Bürgerdialog zum diesem Thema durchgeführt. Dieses vom Bundesministerium für Bildung und Forschung initiierte Format dient zur Kommunikation zwischen Bürgerinnen und Bürgern auf der einen und Verantwortlichen aus Wissenschaft, Politik und Wirtschaft auf der anderen Seite, an dessen Ende dieser Ergebnisbericht steht. Er reflektiert die Veranstaltung und wertet das in Form von Fragebögen und Diskussionen erhobene Meinungsbild aus.

1 Vorträge und anschließende Diskussionen

Die Vorträge im Rahmen des 19. Präventionstages beleuchteten gesellschaftlich hochaktuelle Themen der IT-Sicherheit. Einige werden hier exemplarisch angeführt. Jeder Vortrag wurde von 30 bis 50 Teilnehmern besucht – beim Abschlussvortrag waren es knapp über 100.

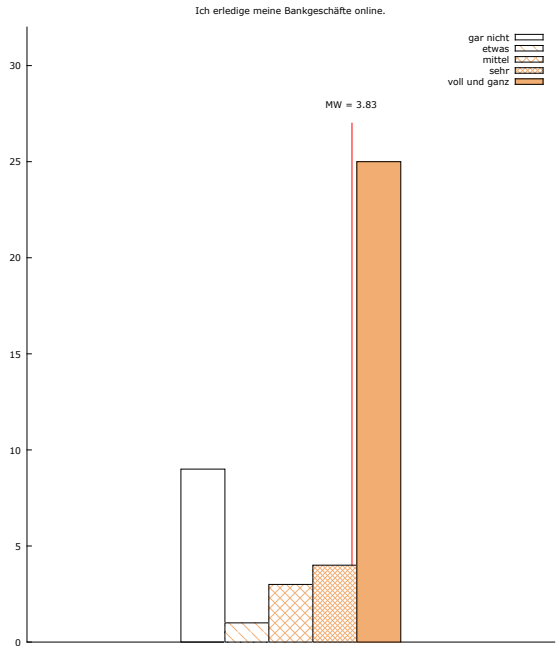


Abbildung 1: „Ich erledige meine Bankgeschäfte online.“

1.1 Cyberkriminalität – die Schattenseite der digitalen Gesellschaft

Referent: Jörg Ziercke, Präsident des Bundeskriminalamts

Von Facebook bis Online-Banking: Das Leben des 21. Jahrhunderts ist ohne Internet für viele schlicht nicht vorstellbar (siehe auch Abbildung 1). Jörg Ziercke, Präsident des Bundeskriminalamts, illustrierte, dass mit den vielen Vorteilen und Bequemlichkeiten, die aus der Verfügbarkeit der neuen Medien im Alltag resultieren, jedoch auch ein großes Gefahrenpotenzial einhergeht. Sei es der Diebstahl der digitalen Identität, der Missbrauch von personenbezogenen Daten oder schlicht Cybermobbing – für jede legitime und gewollte Nutzung des Cyberspaces gibt es eine Missbrauchsmöglichkeit. Ziercke sieht daher als wichtige Konsequenz, sich mit dieser Schattenseite der digitalen Gesellschaft auseinanderzusetzen und sowohl auf politischer als auch technischer Ebene Lösungsansätze zu entwickeln und Aufklärung zu betreiben.

Diskussion

In der an den Vortrag angeschlossenen Diskussion wurde unter anderem erörtert, in wie weit ein globales Netzwerk wie das Internet überhaupt durch einzelne Staaten beaufsichtigt bzw. reguliert werden kann. Thematisiert wurde vor diesem Hintergrund ebenfalls die Tatsache, dass viele bedeutende Internetunternehmen ihren Sitz in den Vereinigten Staaten haben und so beispielsweise europäisches Datenschutzrecht oftmals nur begrenzt anwendbar ist. In diesem Kontext wurde auch das Spannungsfeld zwischen Anonymität und Datenspeicherung für eine effektive Strafverfolgung beleuchtet. Tenor der Diskussion war, dass der Fokus nicht nur auf der Aufklärung von bereits geschehenen Verbrechen liegen darf, sondern dass durch technische Maßnahmen Missbrauchsmöglichkeiten soweit wie möglich eliminiert werden soll-

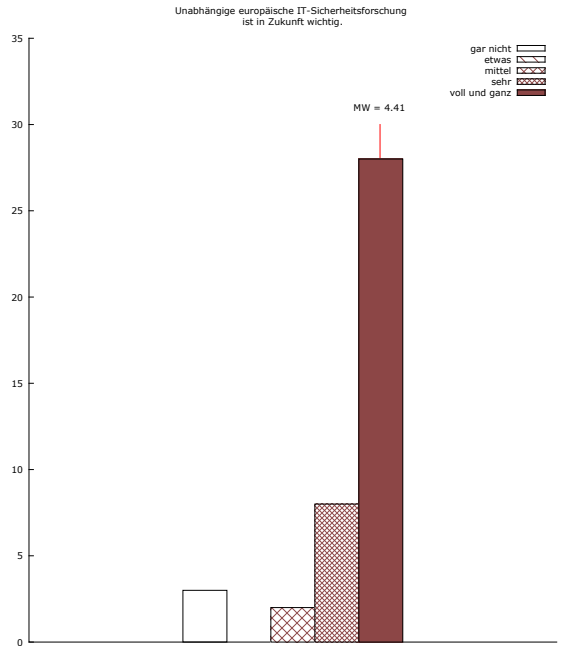


Abbildung 2: „Unabhängige europäische IT-Sicherheitsforschung ist in Zukunft wichtig.“

ten, wobei neben der Wirtschaft auch der Staat, beispielsweise im Rahmen der Förderung von IT-Sicherheitsforschung, in der Pflicht gesehen wird (siehe auch Abbildung 2).

1.2 Cybersicherheit – eine neue Herausforderung für Bund und Länder?

Referent: Herbert O. Zinell

Wer sich fragte, welche Maßnahmen Bund und Länder zur Sicherung der deutschen IT-Infrastruktur unternehmen, wurde in diesem Vortrag ausführlich von Ministerialdirektor im Innenministerium Baden-Württemberg Herbert Zinell informiert. Betrachtet wurde das Thema Cybersicherheit sowohl unter dem Gesichtspunkt, dass den Bürgerinnen und Bürgern vermehrt das Internet zur Erledigung von Behördengänge zu Verfügung steht, als auch unter dem allgemeinen Aspekt, dass das Internet mittlerweile zu einer kritischen Kommunikationsinfrastruktur geworden ist. Vorgestellt wurden verschiedene Behördenkonzepte, unter anderem zur Bewertung der momentanen Bedrohungslage und zur Entwicklung möglicher Reaktionen auf dieselbe.

Diskussion

Ein Punkt, der viele Zuhörerinnen und Zuhörer beschäftigte, war die Frage nach der Sicherheit bzw. Angreifbarkeit grundlegender Infrastruktur wie des Energie- oder Wassernetzes und wie stark die Bedrohung in diesem Bereich sei. Laut der Referenten besteht im Moment keine akute Bedrohung, zumal öffentliche Stellen die Etablierung von Sicherheitsmaßnahmen in kritischen Bereichen beobachtend und beratend begleiten.

Abbildung 3: KASTEL führte auf dem 19. Präventionstag in Karlsruhe einen Bürgerdialog zum Thema Cyber-Sicherheit durch.

1.3 Unternehmen in Sozialen Netzen – Wer hat die Kontrolle?

Referentin: Silvija Höger, Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB

Fast ebenso selbstverständlich wie eine eigene Hompepage ist für Unternehmen mittlerweile eine Präsenz in sozialen Netzwerken wie Facebook. Vorteile und Risiken wurden ausführlich von Silvija Hörner vom Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) vorgestellt, wobei auch konkrete Handlungsempfehlungen nicht zu kurz kamen. Thematisiert wurde weiterhin, welche Regeln Mitarbeiter im Umgang mit dem Web 2.0 beachten sollten, insbesondere bei wichtigen Geschäftsprozessen wie der Kundenakquise. Auch die andere Seite, nämlich die Nutzung von Informationen aus Netzwerken wie Facebook zur Bewerberauswahl, kam zur Sprache.

Diskussion

Besonderes Interesse fand das Themengebiet Marketing und was dabei erlaubt und verboten ist. Die Referentin teilte ihren Erfahrungsschatz mit dem Publikum und konnte ihre Zuhörer anhand des Beispiels eines Autohändlers, der eine empfindliche Strafe für wettbewerbswidrige Werbung zahlen musste, die ein angestellter Verkäufer ohne Wissen der Geschäftsführung auf seiner privaten Facebook-Seite veröffentlichte, sensibilisieren.

1.4 WLAN-Hacking

Referenten: Kai Jendrian und Jörg Völker, KA-IT-Si/Secorvo Security Consulting GmbH

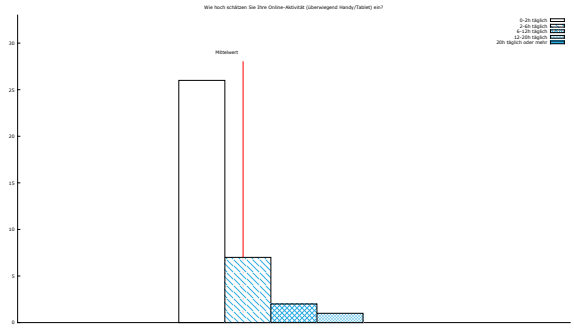


Abbildung 4: „Wie hoch schätzen Sie Ihre Online-Aktivitität (überwiegend Handy/Tablet) ein?“

Die Befragung der Besucher hat gezeigt, dass ein großer Teil des Internetzugriffs heutzutage kabellos stattfindet (siehe Abbildung 4). Dass eine sichere Übertragung der Daten dabei nicht selbstverständlich ist, wurde eindrucksvoll beim Vortrag zum Thema WLAN-Hacking demonstriert. Vor den Augen der Zuschauer wurde vorgeführt, wie einfach es für versierte Personen sein kann, in schlecht gesicherte Drahtlosnetzwerke einzudringen und die darüber laufende Kommunikation mitzuhören; Folgen reichen vom Beobachten des Surfverhaltens bis zum Ausspähen von Daten von vermeintlich gesicherten Webseiten. Abschließend wurde erklärt, woran schlecht gesicherte Netzwerke erkennbar sind und welche Maßnahmen man ergreifen kann, wenn eine Benutzung unumgänglich ist.

Diskussion

In der anschließenden Diskussion war es den Teilnehmerinnen und Teilnehmern wichtig zu erfahren, ob die WLAN-Router, die in der Regel vom Internetanbieter zur Verfügung gestellt werden, in ihrer Standardeinstellung sicher sind oder weitere Maßnahmen ergriffen werden müssen. Leider konnte diese Frage nicht pauschal beantwortet werden, da dies von Hersteller zu Hersteller unterschiedlich ist und es tatsächlich Modelle gibt, bei denen die Standard-Passwörter nicht ausreichend schützen. In jedem Fall wurde dazu geraten, regelmäßige Firmware-Updates durchzuführen, wobei auch ein gelegentliches Ändern des WLAN-Schlüssels nicht schaden kann.

1.5 Cybermobbing auch ein Problem bei Erwachsenen? Was verrät die Sprache der Täter/Opfer?

Referent: Uwe Leest, Bündnis gegen Cybermobbing e. V.

Während in den Medien vorallem über das traurige Phänomen des Facebook-Mobbings unter Jugendlichen berichtet wird, findet das Thema Cybermobbing unter Erwachsenen kaum Beachtung. Uwe Leest vom Bündnis gegen Cybermobbing e. V. klärte die Besucherinnen und Besucher der 19. Präventionstage darüber auf, dass sich auch im beruflichen und privaten Umfeld das Mobbing vom „echten Leben“ immer mehr in soziale Netzwerke verlagert. Neben dem potenziell größeren Adressatenkreis leiden Opfer vorallem unter der Tatsache, dass es durch die ständige Verfügbarkeit im Internet kein Entkommen mehr von den Beleidigungen und Verletzungen gibt, wie es sonst beispielsweise nach der Heimkehr von der Arbeit

der Fall ist. Untermauert wurden die Ausführungen des Referenten durch die Daten einer über 6000 Teilnehmer starken Studie, die vom Bündnis gegen Cybermobbing im Jahr 2002 durchgeführt wurde.

Diskussion

Was kann ich als Opfer von Cybermobbing tun? Um diese Frage drehte sich das Gespräch zwischen Vortragendem und Zuhörern. Herr Leest unterstrich wie wichtig es ist, sich konsequent (juristisch) zur Wehr zu setzen und verwies auf Anlaufstellen für Cybermobbing-Opfer.

1.6 juuuport – Die Selbstschutz-Plattform von Jugendlichen für Jugendliche im Netz

Referenten: Markus Brock, Karin Wunder, Niedersächsische Landesmedienanstalt (NLM)

Immer früher kommen Kinder heutzutage mit dem Internet in Berührung – sei es durch den elterlichen Computer oder über das eigene Smartphone, das zur Kommunikation mit Freunden genutzt wird. In diesem Vortrag wurde die Plattform juuuport vorgestellt, auf der sich Jugendliche mit Gleichaltrigen zu Themen wie Datenschutz, Cybermobbing oder Abzocke im Internet austauschen können. Die Berater sind zwischen 15 und 21 Jahre alt und speziell in einzelnen Themen geschult. Um mit den Scouts in Kontakt zu treten, gibt es sowohl ein Forum als auch die Möglichkeit, eine vertrauliche E-Mail zu schreiben. So kann in vielen Fällen direkt Hilfe geleistet werden, wobei komplizierte Fragen teilweise von Erwachsenen beantwortet werden.

Diskussion

Von großem Interesse war unter anderem die Frage, welche Erfahrungen während des mittlerweile vierjährigen Betriebs der Plattform gemacht wurden. Karin Wunder wusste zu berichten, dass das Angebot bei seiner Zielgruppe auf eine große Resonanz gestoßen ist und sowohl von den Nutzern als auch den Scouts äußerst positiv bewertet wird. Die Anerkennung für das Projekt drückt sich auch in vielen Auszeichnungen aus, die der Plattform im Laufe ihres Bestehens verliehen wurden.

1.7 Cybermobbing – auch bei uns? Implementierung von Prävention

Referent: Uli Gilles, Rhein-Sieg-Kreis

Passend zum Vortrag über Cybermobbing bei Erwachsenen fand am darauffolgenden Tag eine Veranstaltung statt, die sich diesem Phänomen nun bei Jugendlichen, vornehmlich unter dem Aspekt der Prävention, widmete. Die Besucher erfuhren, dass gute Erfahrungen mit regelmäßigen, im Schulprogramm verankerten Maßnahmen gemacht wurden. Ein weiterer Ansatz besteht darin, nicht nur Opfer und Täter, sondern auch den Rest der Klassengemeinschaft in Form von Zuschauern und Mitläufern einzubeziehen, anstatt sofort juristische Schritte zu unternehmen. Ergänzt wurde der Vortrag mit wissenschaftlichen Ergebnissen zur Wirksamkeit bestimmter Maßnahmen und zu aktuellen Zahlen zum Thema Cybermobbing.

Diskussion

Keine Einigkeit bestand bei den Zuhörern in der Frage, ob das Mobbing unter Jugendlichen im Laufe der Zeit zugenommen oder durch soziale Netzwerke einfach nur besser sichtbar geworden ist.

1.8 Online-Kinderschutz im Zeitalter des Digitalen Exhibitionismus – eine (un)lösbare Herausforderung

Referent: Julia von Weiler, Innocence in Danger e. V.

Die Teilnahme an sozialen Netzwerken bietet Kindern und Jugendlichen die Möglichkeit, ständig und oftmals ohne elterliche Kontrolle mit Menschen in Kontakt zu treten, deren Identität potenziell falsch bzw. nicht feststellbar ist. Thema dieses Vortrags war die äußerst besorgniserregende Folge, dass Pädokriminelle diese Plattformen vermehrt zur Kontaktaufnahme zu potenziellen Opfern nutzen, was auch vermehrt medial thematisiert wird. Als notwendige Prävention wurde nicht nur eine regelmäßige Kontrolle der Inhalte genannt, sondern auch eine verstärkte Kooperation zwischen Wirtschaft, Politik und Eltern.

Diskussion

Die Frage besorgter Eltern, was sie zum Schutz ihrer Kinder im Internet tun können, wurde unter anderem mit dem Hinweis auf die vom Verein angebotene App beantwortet, die sich sowohl an Eltern als auch an Kinder richtet. Kritisch hinterfragt wurde die Position von Innocence in Danger e. V., sich für Internetsperren einzusetzen.

1.9 Datenschutz bei notwendigen Veröffentlichungen privater Daten mit Beispielen aus dem Gesundheits- und Energiebereich

Referent: Stephan Kessler, Karlsruher Institut für Technologie (KIT)

In vielen Bereichen wie dem Gesundheitswesen oder der Energieversorgung ist ein Trend zur vermehrten elektronischen Erhebung und Verarbeitung personenbezogener Daten zu beobachten. Stephan Kessler umriss anhand des Beispiels von Gesundheitsdaten, deren Veröffentlichung einerseits im Interesse der medizinischen Forschung sein kann, andererseits aber auch einen Eingriff in die Privatsphäre der Betroffenen darstellt, das sich ergebende Spannungsfeld. Vorgestellt wurden Verfahren zur Anonymisierung von Datensätzen, die den

datenschutzrechtlichen Bedürfnissen entgegenkommen, aber trotzdem noch die Möglichkeit bieten, die modifizierten Daten nach interessanten Kriterien auszuwerten.

Diskussion

In der Diskussion wusste Stephan Kessler zu vermitteln, dass unzureichende Datenanonymisierung ein Problem ist, das viele Menschen in Deutschland direkt betrifft, wie sich vor einigen Monaten beim Skandal mit Rezeptdatenhandel zeigte, wo Patientendaten nur unzureichend pseudonymisiert wurden. Auch zum Thema Datenschutz im Zusammenhang mit Smart Metern, deren Verwendung bei Neubauten in Deutschland mittlerweile Pflicht ist, stand der Referent kompetent Rede und Antwort. Gerade bei der Verbrauchsdatenerfassung durch Smart Meter äußern die Bürger ein hohes Schutzbedürfnis (vgl. Abbildung 15, Frage 4).

1.10 Be Wiser – Ein europaweiter Ansatz zur Stärkung des IT-Security-Sektors

Referentin: Tamara Högler, CyberForum e. V.

Spätestens nach dem Beginn des NSA-Skandals wurde ersichtlich, dass Cybersicherheit nicht im nationalen Alleingang erfolgen kann, sondern internationale Kooperation erfordert. Ebenso hat sich gezeigt, dass ein niedriger Schutz vor staatlichen Datenzugriffen wie in den Vereinigten Staaten wirtschaftliche Nachteile für die dortigen Unternehmen mit sich bringen kann. Vor diesem Hintergrund stellte Tamara Högler vom CyberForum e. V. das EU-Forschungsprojekt FP7: „Be Wiser – Building Enterprises: Wireless and Internet Security in European Regions“ vor, das Wissenschaft, Wirtschaft und Entscheidungsträger zusammenbringt, um die europäische Wettbewerbsfähigkeit im Bereich der IT-Sicherheit zu stärken.

Diskussion

Ein Thema der an den Vortrag folgenden Diskussion war die Frage, ob öffentliche Initiativen zur Förderung von Alternativen zu US-amerikanischen Diensten wie Google oder Facebook, wie sie mehrmals von deutschen Politikern gefordert wurden, Sinn ergeben. Auch die Idee des “Schengen-Netzes”, also das Verhindern, dass innereuropäische Datenübertragung über Drittländer geführt wird, wurde kontrovers unter den Teilnehmerinnen und Teilnehmern diskutiert.

1.11 Gemeinsam gegen Cybercrime – Neue Ansätze in der Prävention

Referent: Peter Vahrenhorst, Landeskriminalamt Nordrhein-Westfalen

Am Beispiel des Landes Nordrhein-Westfalen wurde in diesem Vortrag erläutert, wie ein möglicher Ansatz der Bundesländer zur Bekämpfung von Cybercrime aussehen könnte. So wurde im Landeskriminalamt Nordrhein-Westfalen ein spezielles Kompetenzzentrum zu diesem Thema eingerichtet, um in dem schnell veränderlichen Umfeld der IT-Krimininalität erfolgreich präventiv tätig werden zu können. Ein besonderer Aspekt ist die enge Kooperation zwischen Landeskriminalamt und Wirtschaftsunternehmen, die sich unter anderem im

gegenseitigen Personalaustausch ausdrückt. Der Erfolg des NRW-Modells führte dazu, dass sich weitere Bundesländer an dieser Sicherheitskooperation beteiligen.

Diskussion

Für unterschiedliche Meinungen sorgte die Frage nach der Verantwortung des Staates für die IT-Sicherheit im privatwirtschaftlichen Bereich. Einerseits wurde die Meinung vertreten, dass es nicht verstärkte Anforderungen und Meldepflichten einen Eingriff in die unternehmerische Freiheit darstellten, andererseits wurde auf die Asymmetrie zwischen Diensteanbieter und Nutzer hingewiesen, wodurch bei letzteren eine besondere Schutzbedürftigkeit bestehe, die einen staatlichen Eingriff, beispielsweise zur Meldepflicht bei Datendiebstahl, rechtfertige.

1.12 Strategic Importance of Cyber Security

Referentin: Melissa Hathaway, Belfer Center for Science and International Affairs

Die Cyberangriffe auf Estland im Jahr 2007 oder zunehmende Angriffe auf US-amerikanische Regierungsstellen, die China zugerechnet werden, zeigen, dass die IT-Sicherheit längst Teil der nationalen Sicherheitsstrategien geworden ist. Die Referentin Melissa Hathaway, Leiterin der Abteilung Cyberspace im National Security Council, betrachtete in ihrem Vortrag vorallem die Lastenverteilung zwischen staatlichen Stellen und Firmen und unterstrich die enorme Wichtigkeit einer umfassenden IT-Sicherheits-Politik. Alleine für die Wirtschaft der USA sieht sie jährliche Verluste in Höhe von über 300 Milliarden US-Dollar durch den Diebstahl geistigen Eigentums, was ungefähr 1 % der jährlichen Wirtschaftsleistung entspricht.

Diskussion

Die anschließende Diskussion wurde vor allem unter dem Eindruck der Enthüllungen Edward Snowdens geführt. Die Vortragende erklärte, dass man gegenüber datensammelnden Unternehmen misstrauisch sein sollte und sich jeder über die Risiken, die mit einer elektronischen Preisgabe von sensiblen Daten einhergeht, bewusst werden müsse.

2 Bürgerbefragung

Sowohl an den Ständen als auch im Anschluss an die Vorträge hatten die Bürgerinnen und Bürger die Möglichkeit, in Fragebögen ihre Position zu verschiedenen Themen rund um die IT-Sicherheit anzugeben und frei zu kommentieren. Insgesamt zeigt sich eine überwiegend kritische Einstellung zum zunehmenden Verlust der Privatsphäre (Abbildung 5), die sich in dem Gefühl, sich bei der Internetnutzung beobachtet zu fühlen (Abbildung 6), ausdrückt. Gleichzeitig wird aus den Ergebnissen der Befragung deutlich, dass europäische Errungenschaften wie das im internationalen Vergleich hohe Datenschutzniveau Anklang finden (Abbildung 7) und eine europäische IT-Sicherheitsforschung und -Infrastruktur unbedingt notwendig ist (Abbildungen 2 und 8).

2.1 Fragen und detaillierte Ergebnisse

Der Fragebogen umfasste 31 Fragen aus sechs Themengebieten (siehe Abbildungen 9 und 10, Seite 13f). Insgesamt wurden 43 Bögen ausgefüllt und abgegeben. Die Ergebnisse der Befra-

gung sind im Anhang als Häufigkeitsdiagramme aufgeführt.

3 Fazit

Als Resümee des vom KASTEL durchgeführten Bürgerdialogs ist die positive Resonanz, auf die die vielfältigen Angebote getroffen sind, zu nennen. Gut besuchte Vorträge mit angeregten Diskussionen zeugten davon, dass sich die Bevölkerung nicht nur mit der Rolle des passiven Konsumenten begnügt, sondern sich vielmehr aktiv mit dem Thema IT-Sicherheit beschäftigt. Nachdem zur Zeit des Volkszählungsurteils 1983 der Datenschutz erstmals in den Fokus der breiten Öffentlichkeit rückte, ist mit dem Bekanntwerden der anlasslosen und globalen Massenüberwachung durch Geheimdienste und dem immer weiter zunehmenden Datenhunger von Unternehmen wie Facebook oder Google eine ähnliche Entwicklung für die Preisgabe von persönlichen Daten im Internet zu beobachten. Auch aus wirtschaftlicher Sicht lassen sich Folgen für Europa und insbesondere Deutschland beobachten, da Kriterien wie Datenschutz und staatlicher Zugriff immer größere Relevanz gewinnen. Die Konsequenz kann daher nur sein, gesamteuropäische Anstrengungen zu unternehmen, um diese Vorteile gegenüber der ausländischen Konkurrenz weiter auszubauen und vorhandene Kompetenzen in Wissenschaft und Wirtschaft weiter zu stärken.

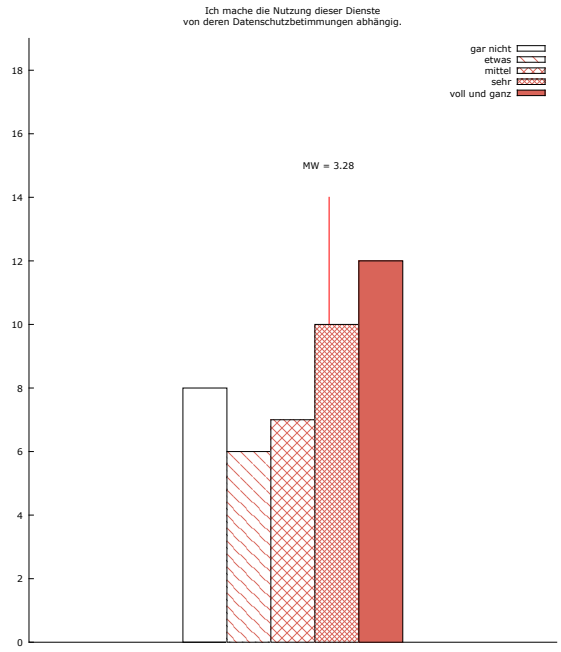


Abbildung 5: „Ich mache die Nutzung dieser Dienste von deren Datenschutzbestimmungen abhängig.“

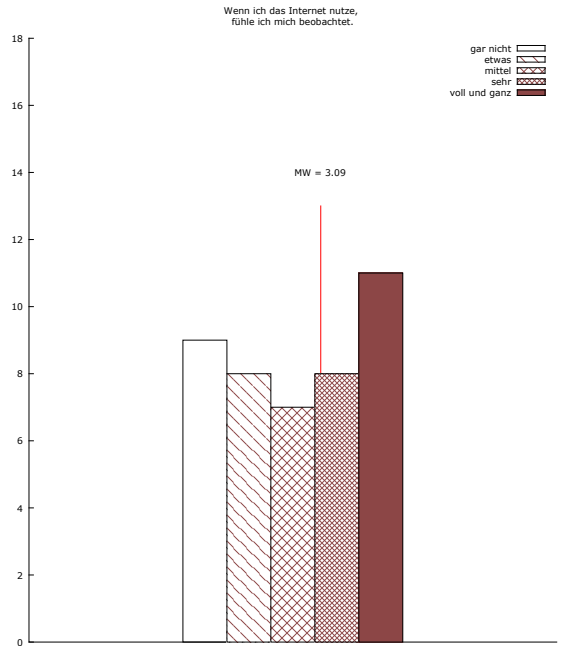


Abbildung 6: „Wenn ich das Internet nutze, fühle ich mich beobachtet.“

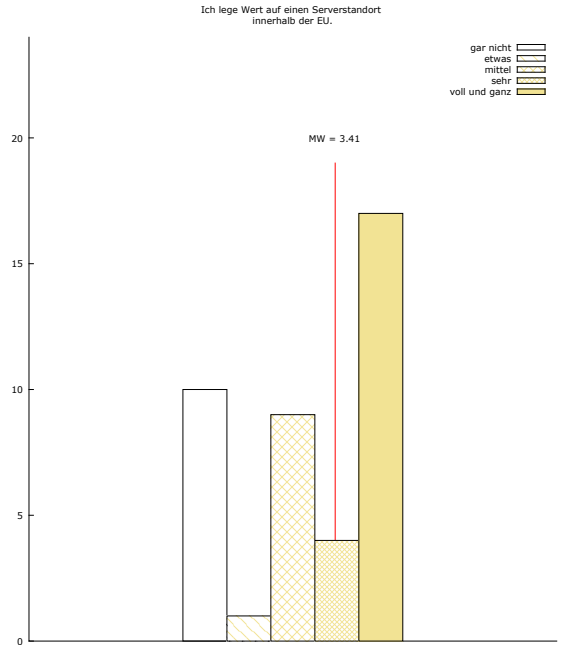


Abbildung 7: „Ich lege Wert auf einen Serverstandort innerhalb der EU.“

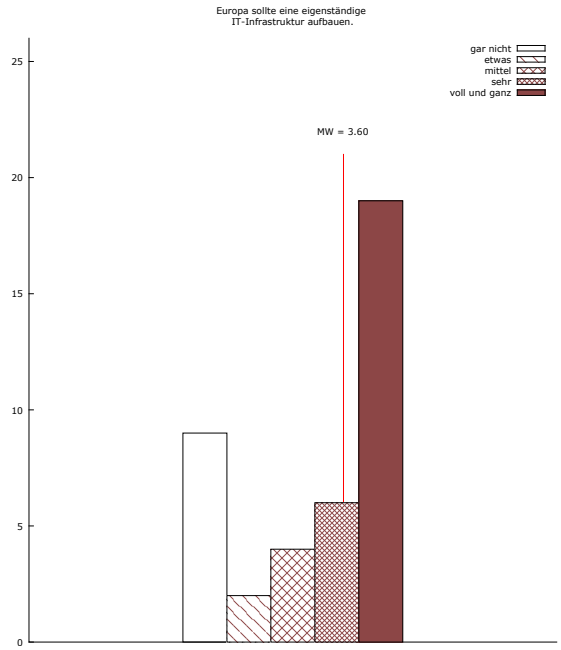
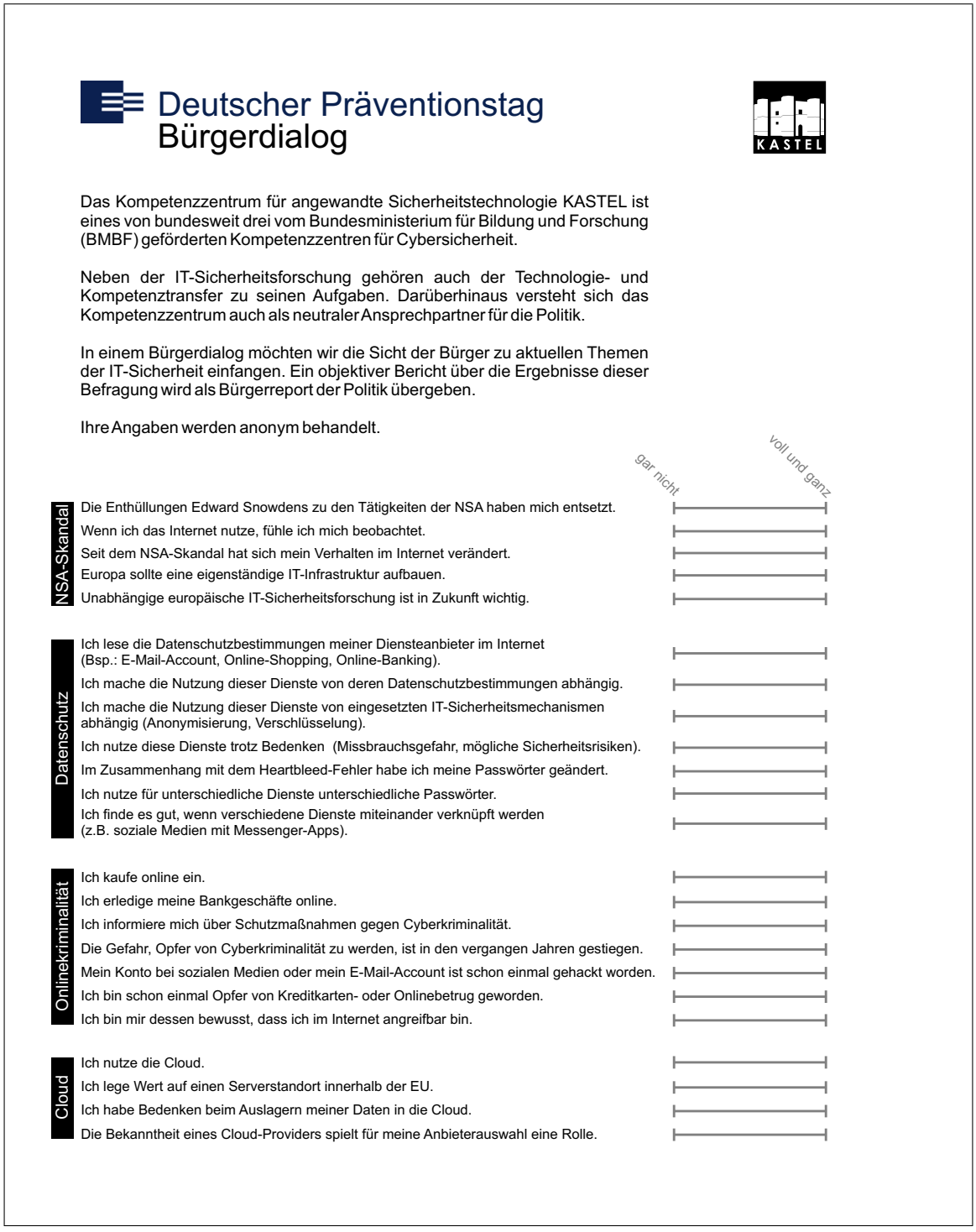


Abbildung 8: „Europa sollte eine eigenständige IT-Infrastruktur aufbauen.“

Anhang



Deutscher Präventionstag
Bürgerdialog

KASTEL

Das Kompetenzzentrum für angewandte Sicherheitstechnologie KASTEL ist eines von bundesweit drei vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Kompetenzzentren für Cybersicherheit.

Neben der IT-Sicherheitsforschung gehören auch der Technologie- und Kompetenztransfer zu seinen Aufgaben. Darüberhinaus versteht sich das Kompetenzzentrum auch als neutraler Ansprechpartner für die Politik.

In einem Bürgerdialog möchten wir die Sicht der Bürger zu aktuellen Themen der IT-Sicherheit einfangen. Ein objektiver Bericht über die Ergebnisse dieser Befragung wird als Bürgerreport der Politik übergeben.

Ihre Angaben werden anonym behandelt.

gar nicht — voll und ganz

NSA-Skandal
- Die Enthüllungen Edward Snowdens zu den Tätigkeiten der NSA haben mich entsetzt.
- Wenn ich das Internet nutze, fühle ich mich beobachtet.
- Seit dem NSA-Skandal hat sich mein Verhalten im Internet verändert.
- Europa sollte eine eigenständige IT-Infrastruktur aufbauen.
- Unabhängige europäische IT-Sicherheitsforschung ist in Zukunft wichtig.

Datenschutz
- Ich lese die Datenschutzbestimmungen meiner Diensteanbieter im Internet (Bsp.: E-Mail-Account, Online-Shopping, Online-Banking).
- Ich mache die Nutzung dieser Dienste von deren Datenschutzbestimmungen abhängig.
- Ich mache die Nutzung dieser Dienste von eingesetzten IT-Sicherheitsmechanismen abhängig (Anonymisierung, Verschlüsselung).
- Ich nutze diese Dienste trotz Bedenken (Missbrauchsgefahr, mögliche Sicherheitsrisiken).
- Im Zusammenhang mit dem Heartbleed-Fehler habe ich meine Passwörter geändert.
- Ich nutze für unterschiedliche Dienste unterschiedliche Passwörter.
- Ich finde es gut, wenn verschiedene Dienste miteinander verknüpft werden (z.B. soziale Medien mit Messenger-Apps).

Onlinekriminalität
- Ich kaufe online ein.
- Ich erledige meine Bankgeschäfte online.
- Ich informiere mich über Schutzmaßnahmen gegen Cyberkriminalität.
- Die Gefahr, Opfer von Cyberkriminalität zu werden, ist in den vergangen Jahren gestiegen.
- Mein Konto bei sozialen Medien oder mein E-Mail-Account ist schon einmal gehackt worden.
- Ich bin schon einmal Opfer von Kreditkarten- oder Onlinebetrug geworden.
- Ich bin mir dessen bewusst, dass ich im Internet angreifbar bin.

Cloud
- Ich nutze die Cloud.
- Ich lege Wert auf einen Serverstandort innerhalb der EU.
- Ich habe Bedenken beim Auslagern meiner Daten in die Cloud.
- Die Bekanntheit eines Cloud-Providers spielt für meine Anbieterauswahl eine Rolle.

Abbildung 9: Der Fragebogen zur Bürgerbefragung beim Bürgerdialog, Seite 1.

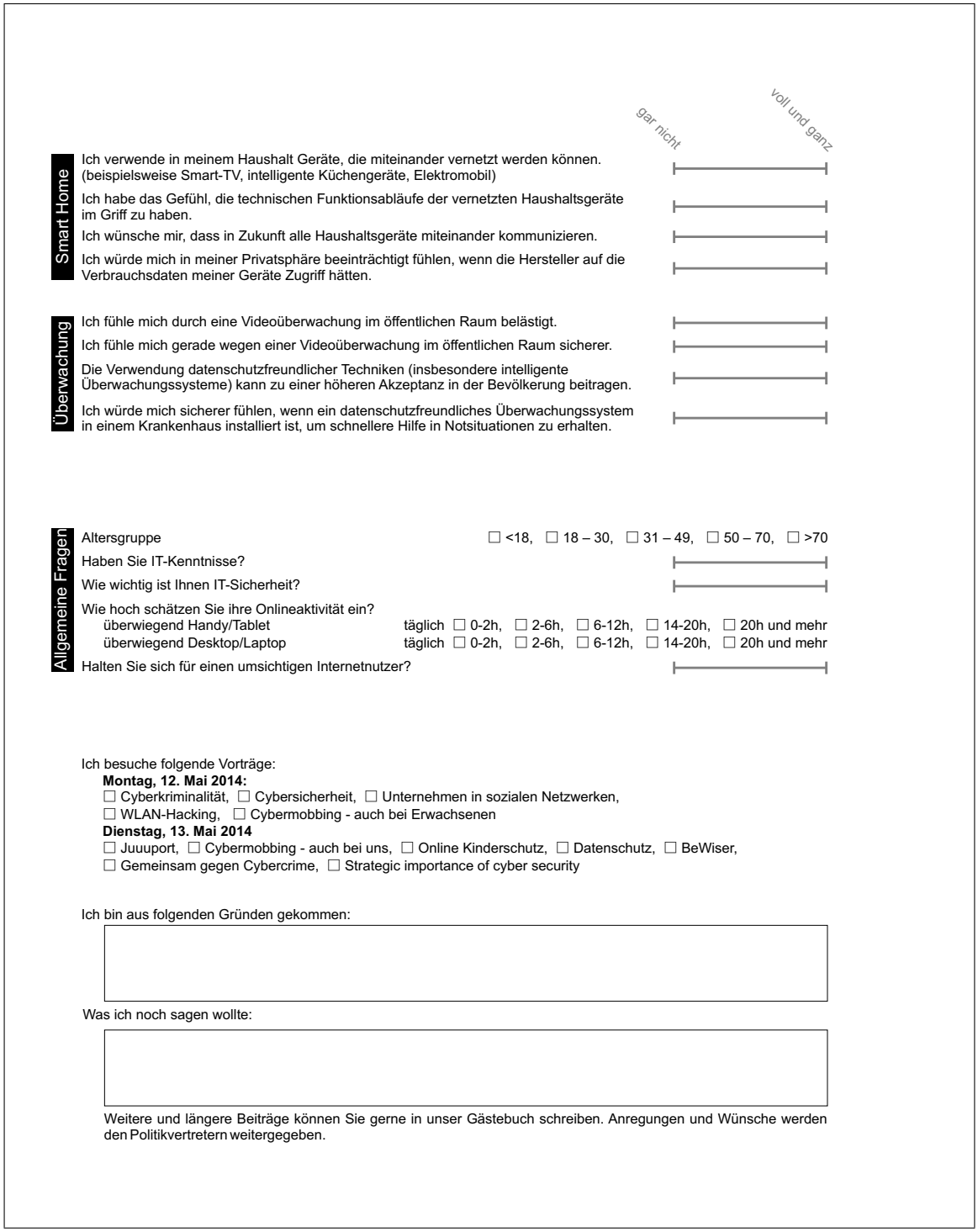


Abbildung 10: Der Fragebogen zur Bürgerbefragung beim Bürgerdialog, Seite 2.

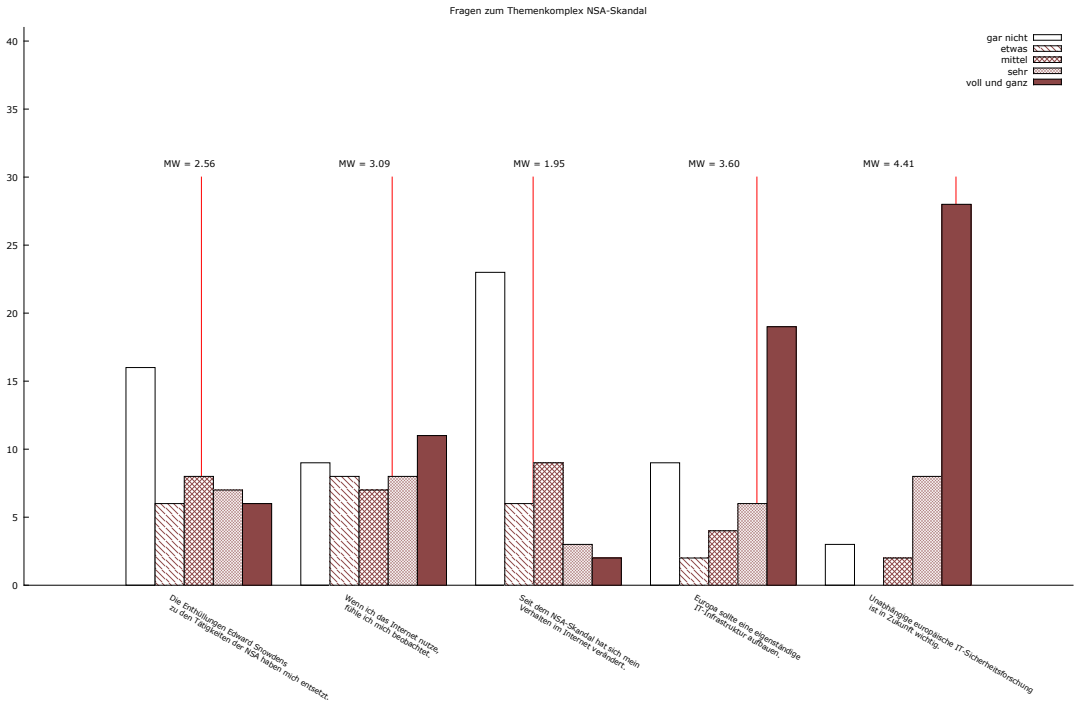


Abbildung 11: Fragen zum Themenkomplex NSA-Skandal.

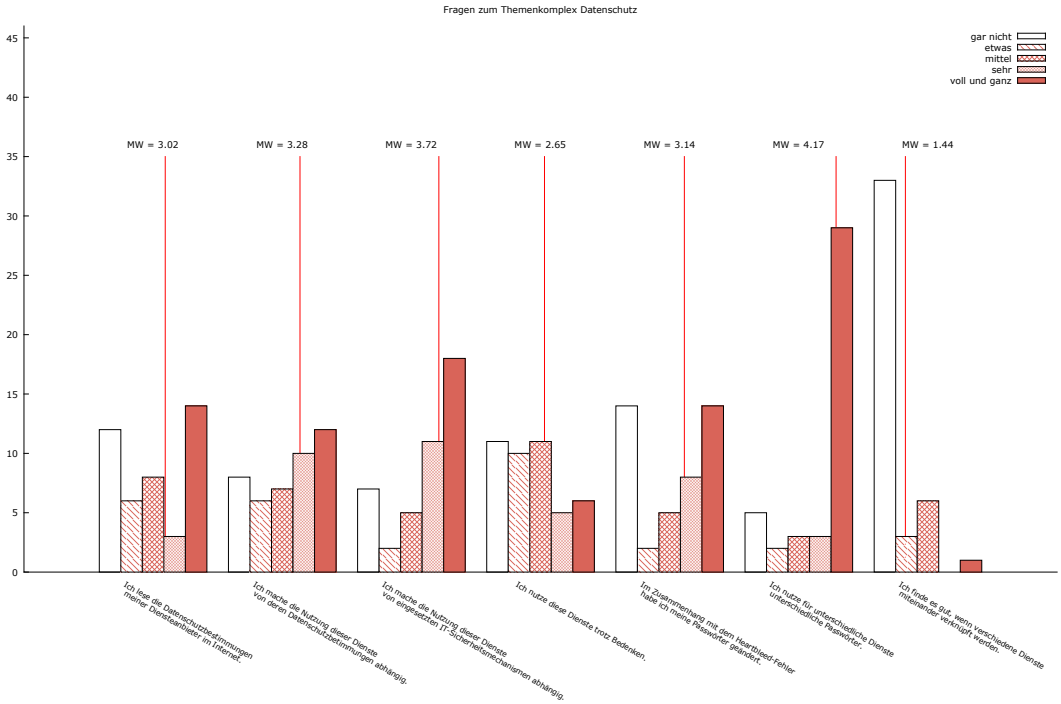


Abbildung 12: Fragen zum Themenkomplex Datenschutz.

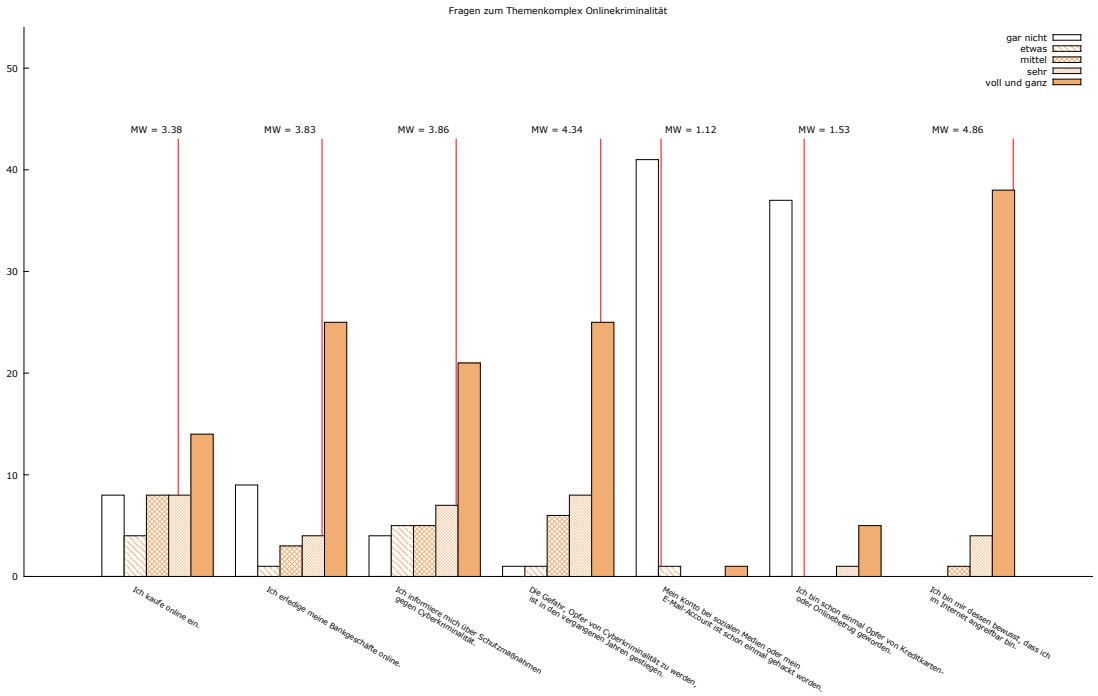


Abbildung 13: Fragen zum Themenkomplex Onlinekriminalität.

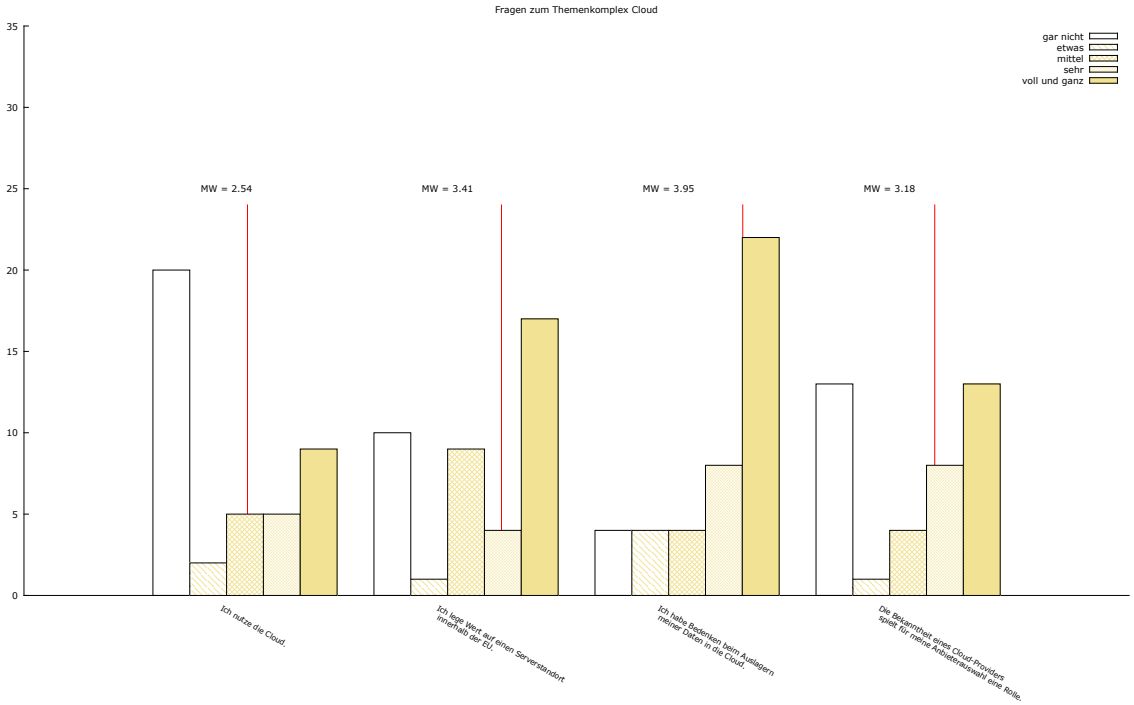


Abbildung 14: Fragen zum Themenkomplex Cloud.

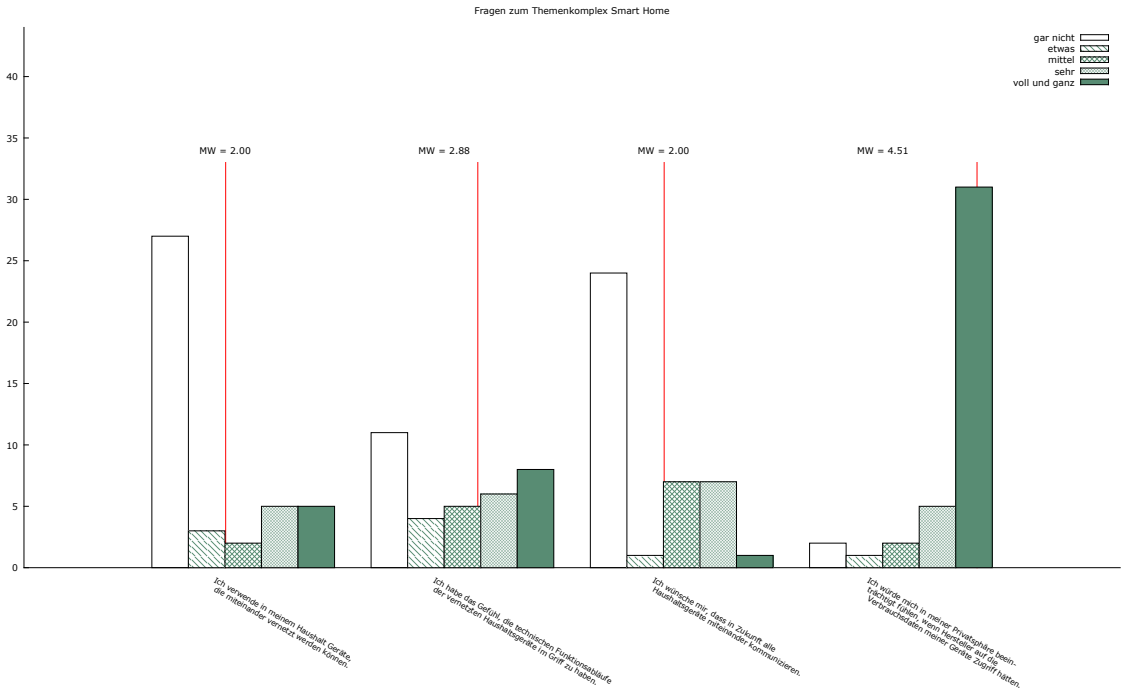


Abbildung 15: Fragen zum Themenkomplex Smart Home.

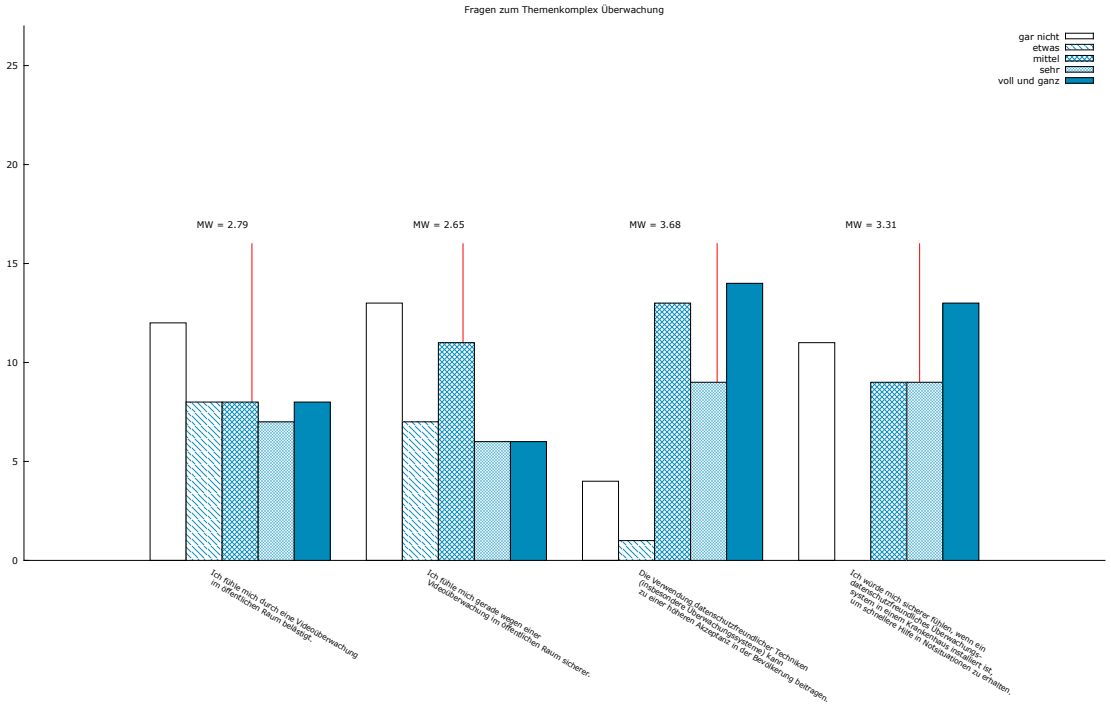


Abbildung 16: Fragen zum Themenkomplex Überwachung.

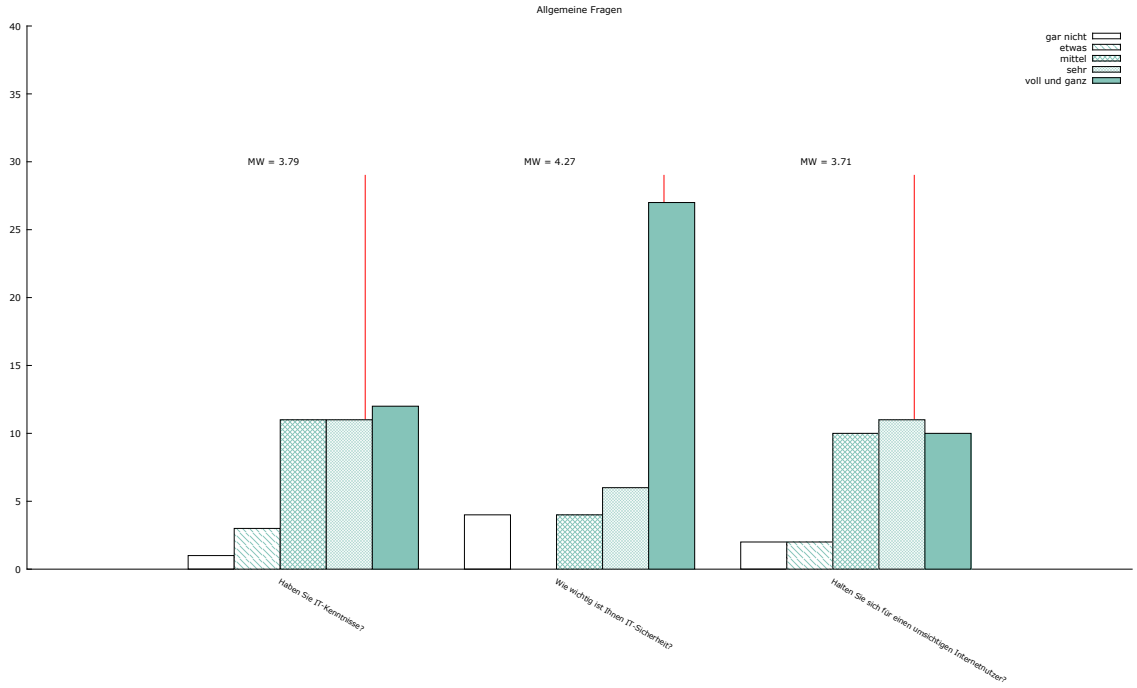


Abbildung 17: Allgemeine Fragen zum Umgang mit IT

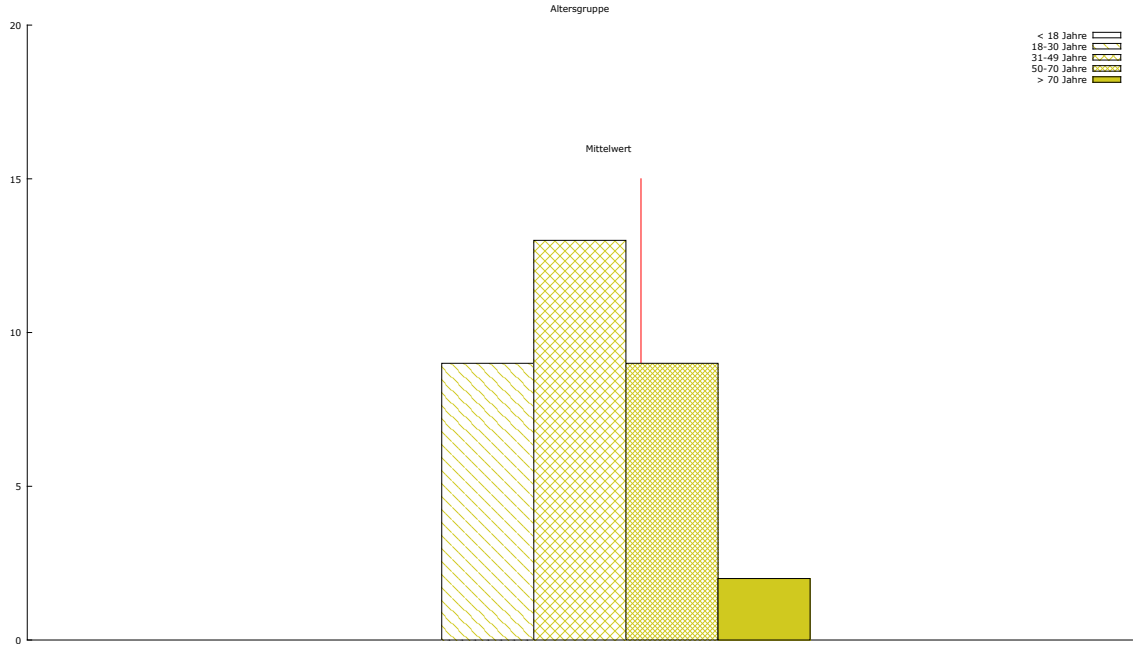


Abbildung 18: Altersgruppe

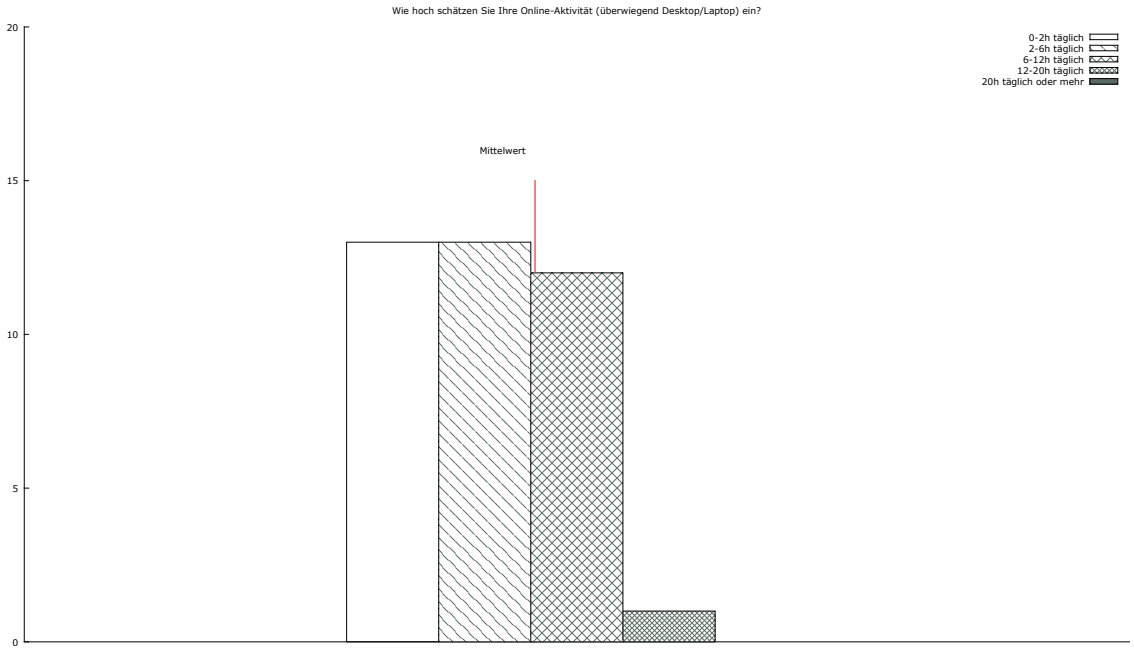


Abbildung 19: Internetnutzung am Desktop

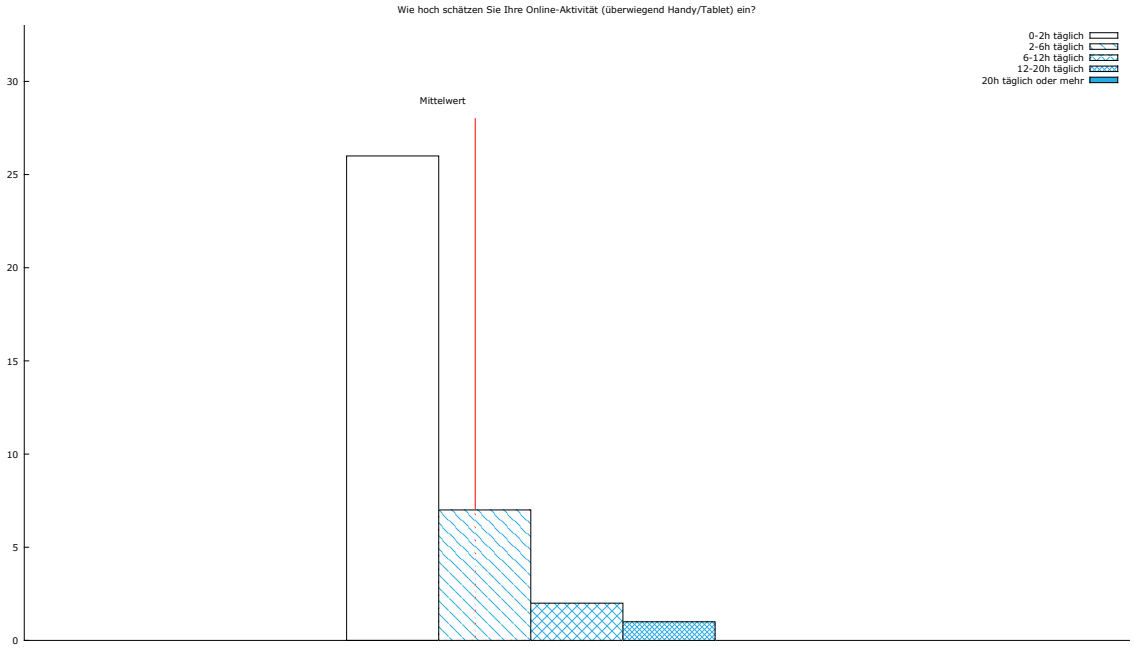


Abbildung 20: Internetnutzung auf dem Smartphone/Tablet