Digitale Gesellschaft: smart & sicher

Zusammenfassung der Studienergebnisse

IT-Sicherheit aus Sicht von Nutzer/innen und Expert/innen

Ansprechpartner für das Projekt:
Kerstin Franzl
nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung GmbH
Tel.: 030 318 054 64
E-Mail: franzl@nexusinstitut.de

Volker Tripp
Digitale Gesellschaft e.V.
Tel.: 030 68916575
E-Mail: volker.tripp@digitalegesellschaft.de

Ein Projekt im Auftrag des

Bundesamt für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

1 Einleitung 1
1.1 Projekthintergrund 1
1.2 Das Projekt „Digitale Gesellschaft: smart & sicher“ 1
2 Interviews mit Expertinnen und Experten 2
2.1 Erhebungskonzept 2
2.2 Zusammenfassung der Ergebnisse 2
2.3 Ergebnisse der Interviews 3
2.3.1 Aufgaben und Handlungsbedarfe der Informationssicherheit 3
2.3.2 Vertrauen 5
2.3.3 Herstellung von Sicherheit 7
2.3.4 Institutionalisierung von IT-Sicherheit 12
3 Umfrage unter Nutzerinnen und Nutzern 15
3.1 Erhebungskonzept 15
3.2 Zusammenfassung der Ergebnisse 15
3.3 Ergebnisse der Online-Befragung 16
3.3.1 Verständnis von Digitalisierung und digitaler Gesellschaft 16
3.3.2 Wahrnehmung von Risiken der Digitalisierung 17
3.4 Digitalisierung und Sicherheitsmaßnahmen 18
3.4.1 Was Nutzerinnen und Nutzer selbst für ihre Sicherheit im digitalen Raum tun 18
3.4.2 Maßnahmen zur Erhöhung der Informationssicherheit 21
3.5 Überblick über die Segmente 23
4 Fazit 25

Abbildungsverzeichnis

Abbildung 1: Welches der folgenden Szenarien einer Kennzeichnung von IT-Sicherheit (z.B. Siegelvergabe) könnten Sie sich im normalen User-Bereich vorstellen? 8
Abbildung 2: Wie sollte Haftung in der digitalen Welt geregelt sein? 11
Abbildung 3: Eine nationale Institution zur Herstellung von IT-Sicherheit sollte...? 13
Abbildung 5: Bitte denken Sie an den Begriff "Digitalisierung". Verbinden Sie damit...? 16
Abbildung 6: Wie groß ist Ihrer Meinung nach der Einfluss der Digitalisierung auf die folgenden Bereiche? 17
Abbildung 7: Inwieweit sehen Sie Risiken bei den folgenden Online-Aktivitäten? Bitte verwenden Sie für Ihre Antwort eine Skala von 1 bis 5, wobei die 1 für "große Risiken" und die 5 für "kleine Risiken" steht. 18
Abbildung 8: Sicherheit im digitalen Raum ist mir persönlich sehr wichtig. 19
Abbildung 9: Ich kenne mich persönlich sehr gut mit dem Thema Sicherheit im Internet aus. 19
Abbildung 10: Um die eigenen Daten zu schützen, gibt es eine Vielzahl an Möglichkeiten 20
Abbildung 11: Verantwortung vs. Vertrauen in die Akteure zur Sicherheit im Internet 21
Abbildung 12: Wie wichtig sind Ihnen dabei die folgenden Aspekte, um Ihr Vertrauen in die Sicherheit dieser Produkte und Services zu stärken? 22
Abbildung 13: Welche Voraussetzungen müssen für Sicherheit im digitalen Raum erfüllt sein? 23
Abbildung 13: Übersicht über die Segmente 24

1 Einleitung

1.1 Projekthintergrund

Informationssicherheit im digitalen Raum zu schaffen, ist ein gesamtgesellschaftliches Generationenprojekt. Nicht nur technische, sondern auch politische, ökonomische und kulturelle Entwicklungen wirken dabei in erheblichem Ausmaß auf die Rahmenbedingungen ein. Die vielen gesellschaftlichen und ganz unterschiedlichen Akteure in diesen Bereichen agieren jedoch kaum gemeinsam oder gar geschlossen. Dies hat viele verschiedene Gründe, nicht zuletzt ist die schnell fortschreitende technische Innovation hierbei eine der großen Herausforderungen. Zudem werden Technologien zur Absicherung der individuellen Informationssicherheit nicht hinreichend genutzt. Dies kann zum Teil auf fehlende Benutzerfreundlichkeit, mangelhaften Wissensstand und rechtliche sowie technische Vorgaben zurückgeführt werden, die dem entgegenstehen. Gleichwohl gibt es aber ein starkes gesamtgesellschaftliches Verlangen nach privater und sicherer Kommunikation, dass sich in einer breiten Debatte zur Überwachung im digitalen Raum widerspiegelt. Es ist zunehmend notwendig zu analysieren, welche Technologien bisher zur Verfügung stehen und was Menschen davon abhält, diese zu nutzen. Unter anderem stellt sich die Frage, inwiefern hier Veränderungen erreicht werden können und wo Verbesserungspotential besteht. Zudem muss eine gesamtgesellschaftliche Debatte angestoßen werden, die erörtert, wie Informationssicherheit, die die Interessen möglichst aller relevanter Akteure berücksichtigt, in der digitalen Gesellschaft realisiert und gewährleistet werden kann. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) engagiert sich in der Schaffung eines solchen gesamtgesellschaftlichen Diskurses durch die Bereitstellung von Informationen, wie auch mit partizipativen Formaten, die zur Diskussion der Grundfragen einer smarten und sicheren Gesellschaft einladen.

1.2 Das Projekt „Digitale Gesellschaft: smart & sicher“

Die „Denkwerkstatt sichere Informationsgesellschaft“ im April 2016 stellte einen wichtigen Schritt im Dialogprozess dar. Im Ergebnis der Veranstaltung entwickelten die Teilnehmerinnen und Teilnehmer aus Zivilgesellschaft, Kultur, Wissenschaft, Wirtschaft und Verwaltung „sieben Thesen für eine sichere Informationsgesellschaft“. Das Format war so erfolgreich, dass es 2017 im Projekt „Digitale Gesellschaft: smart & sicher“ vom nexus Institut und der Digitalen Gesellschaft e.V. sowie der Ipsos GmbH und Dr. Ben Wagner (Europa-Universität Viadrina) fortgeführt wurde. Die auf den Denkwerkstätten angestoßenen Diskussionen sollten dabei auf eine breitere Datenbasis gestellt werden. So wurden die aufgeworfenen Fragen zur Grundlage einer sozialwissenschaftlichen Untersuchung, deren Ergebnisse wiederum von den Diskutanten weiterverarbeitet wurden.

Das Projekt begann im Februar 2017 mit der „Denkwerkstatt sichere Informationsgesellschaft“ im World Café-Format, bei der knapp 30 Vertreterinnen und Vertreter aus Zivilgesellschaft, Kultur, Wissenschaft, Wirtschaft und Verwaltung relevante Fragestellungen entwickelten, die es auf dem Weg zu einer sicheren und smarten Informationsgesellschaft zu beantworten gilt. Den herausgearbeiteten Fragen und Problematiken wurde durch das nexus Institut im Rahmen von Experten-Interviews mit relevanten Akteuren, insbesondere Vertreterinnen und Vertretern der Zivilgesellschaft, nachgegangen. Zeitgleich befragte die Ipsos GmbH in einer repräsentativen Online-Umfrage insgesamt 2.000 Nutzerinnen und Nutzer zu ihren Gewohnheiten und Erfahrungen mit Informationssicherheit und organisierte eine zweitägige Online-Community.

Die empirischen Ergebnisse wurden durch Ipsos und das nexus Institut analysiert und ausgewertet und bildeten die Grundlage für eine weitere Denkwerkstatt im Juni 2017. Aufbauend auf den Untersuchungsergebnissen entwickelte die Denkwerkstatt gemeinsam Visionen, Handlungsempfehlungen und Forderungen und schrieb diese in einem konsensual erarbeiteten ***Impulspapier*** fest. Das Impulspapier bildet ein wesentliches Ergebnisdokument des bisherigen Prozesses und stellt zugleich einen nächsten Schritt dar, den angestrebten und fortzuführenden Dialog der unterschiedlichen gesellschaftlichen Akteure weiter miteinander zu beschreiten.

2 Interviews mit Expertinnen und Experten

2.1 Erhebungskonzept

Im Zeitraum April bis Juli 2017 führte das nexus Institut 36 teilstandardisierte qualitative Interviews mit Akteuren im weiteren Themenfeld der Informationssicherheit. Die Interviews erfolgten leitfadengestützt und beinhalteten neben offenen Fragen auch einzelne quantitative Abfragen. Der Entwicklung der Interviewfragen lagen die inhaltlichen Ergebnisse der „Denkwerkstatt sichere Informationsgesellschaft“ im Februar 2017 zugrunde. Die Auswertung der Interviews erfolgte mit der Methode der qualitativen Inhaltsanalyse nach Mayring (2010).

Interviewt wurden Akteure aus verschiedensten Bereichen, insbesondere der organisierten Zivilgesellschaft, aber auch der Wissenschaft, Wirtschaft, Medien, Kultur sowie staatlicher Organisationen. Die Interviewpartner/innen wurden anhand ihrer Expertise ausgewählt: Im Rahmen einer ***Stakeholder-Analyse*** wurden Veröffentlichungen zu den relevanten Themen der letzten drei Jahre quantitativ analysiert. Zudem wurde auf die Relevanz der Akteure in der öffentlichen Debatte zur sicheren Informationsgesellschaft im Hinblick auf eine nachhaltige Beschäftigung mit dem Thema geachtet. Drittens wurden nur deutschsprachige Akteure ausgewählt.

2.2 Zusammenfassung der Ergebnisse

Aufgaben und Handlungsbedarfe der Informationssicherheit

Die befragten Expertinnen und Experten waren gebeten, die derzeit größten Probleme in der Informationssicherheit zu benennen. Am häufigsten wurde dabei auf die mangelnde digitale Expertise verwiesen – sowohl bei privaten Nutzerinnen und Nutzern als auch bei politischen und staatlichen Akteuren. Daneben befanden sie den unverantwortlichen Umgang mit Daten durch privatwirtschaftliche Unternehmen und staatliche Akteure als größte Probleme. Die daraus entstehende Unsicherheit könnte zu verschiedenen digitalen Katastrophen führen. Am schlimmsten wäre nach Meinung der Befragten ein Ausfall Kritischer Infrastrukturen. Ebenso fürchten sie, dass in dem Bemühen, Sicherheit herzustellen, eine Totalüberwachung eingeführt würde – was die Befragten ebenfalls als Katastrophe ansahen.

Vertrauen in Akteure

Bevor die Schaffung neuer Strukturen zur Herstellung von Informationssicherheit diskutiert werden kann, muss zunächst die Ausgangslage geklärt werden. Zur Klärung der Frage, wer zukünftig welche Rolle einnehmen könnte wurde daher die Einschätzung abgefragt, wie kompetent und vertrauenswürdig die Akteure im Feld sind.

Als besonders kompetent und vertrauenswürdig wurden dabei die Datenschutzbeauftragten der Länder und des Bundes, die zivilgesellschaftlichen Organisationen und das BSI gesehen. Im restlichen Feld stehen sich – vereinfacht ausgedrückt – zwei Akteursgruppen gegenüber, die sich diametral voneinander unterscheiden: Die staatlichen Organisationen, denen zwar grundsätzlich Vertrauen, zugleich aber wenig Fachkompetenz zugesprochen werden. Daneben stehen wirtschaftliche Akteure, die zwar fachlich kompetent, aber wenig vertrauenswürdig seien. Private Nutzerinnen und Nutzer zeichnen sich aus Sicht der Expertinnen und Experten durch die geringste Fachkompetenz im Feld aus. Als vertrauensbildende Faktoren stellten sich heraus:

- Fachkompetenz und personelle Expertise
- Persönliche Kontakte zu Bürgern und Zivilgesellschaft (Workshops, Veranstaltungen etc.)
- Skandalfreiheit
- Gemeinwohlorientierte Zielausrichtung
- Transparentes, unabhängiges und eigenbestimmtes Handeln

Lösungswege zu einer sicheren Informationsgesellschaft

Die Teilnehmerinnen und Teilnehmer der Denkwerkstatt identifizierten drei Ansätze bzw. drängendste Fragen, die zur Diskussion an die Expertinnen und Experten weitergereicht wurden:

- Technologien, die Sicherheit herstellen
- Kennzeichnung (Zertifizierung und/oder Siegelvergabe) von Soft- und/oder Hardware
- Etablierung eines Haftungsregimes

Brauchen wir weitere Technologien, die Sicherheit herstellen?

Neue technische Lösungen spielten für die Befragten keine wichtige Rolle. Zwar nannten sie Gründe, die eine Weiterentwicklung der Technologie notwendig machen, doch sahen sie in der Entwicklung neuer Technologien keine wirkliche Lösung.

Kennzeichnung von IT-Sicherheit

Die Expertinnen und Experten begrüßten die Einführung einer Kennzeichnung von Produkten in Bezug auf ihre IT-Sicherheit. Politische, wirtschaftliche und technische Herausforderungen werden dabei die Ausgestaltung und Wirksamkeit der Kennzeichnung stark beeinflussen. Für die Definition einer effektiven Kennzeichnung werden vor allem zwei Akteure als vielversprechend angesehen: Das BSI und ein heterogen zusammengesetztes Experten-Gremium, das noch gegründet werden müsste.

Die Regelung von Haftung in der digitalen Welt

Die Diskussion der Kennzeichnung setzt sich in der Frage der Haftungsregelung fort. Die Expertinnen und Experten halten die Etablierung einer Haftungsregelung für sehr wichtig und sehen dafür die Kennzeichnung von IT-Sicherheit (Zertifizierung/Siegelvergabe) als vielversprechendste Grundlage.

Institutionalisierung von IT-Sicherheit

Eine nationale Institution zur Herstellung von IT-Sicherheit müsste laut der Expertinnen und Experten vor allem zwei Dinge tun: Zum einen sollte sie als fachliche Autorität das komplexe Thema für alle Akteure zugänglich und bewältigbar machen durch Informations-, Bildungs- und Beratungsangebote für Nutzerinnen und Nutzer, Wirtschaft und Politik. Zudem sollte sie eine neue Form der Kooperation mit der Zivilgesellschaft praktizieren und propagieren. Sie sollte daher selbst eng mit Expertinnen und Experten zusammenarbeiten, in gemeinsamen Gremien beraten und entscheiden und den Dialog darüber hinaus gesellschaftlich aktiv fördern.

2.3 Ergebnisse der Interviews

2.3.1 Aufgaben und Handlungsbedarfe der Informationssicherheit

Die Expertinnen und Experten wurden nach den *zwei drängendsten Problemen im Status Quo der Informationssicherheit* gefragt, die wiederum als mögliche Aufgabenfelder und Ansatzpunkte für Verbesserungen und Handlungsansätze interpretiert werden können.

Mangelnde digitale Expertise und mangelndes Sicherheitsbewusstsein: Viele Privatnutzerinnen und -nutzer von IT-Angeboten scheinen unzureichend über die Gefahren und entsprechende Sicherheitsmaßnahmen aufgeklärt. Sofern Bedrohungen wahrgenommen werden, schlagen sich diese nicht in einem angemessenen Sicherheitsbewusstsein nieder. Ein **mangelndes Sicherheitsbewusstsein** wurde zudem auch **öffentlichen Institutionen und privatwirtschaftlichen Akteuren attestiert**.

Auch hinsichtlich Politik und Staat wurde eine mangelnde digitale Expertise kritisiert. Die Politik würde der digitalen Entwicklung hinterherhinken. Auf der anderen Seite wurde allerdings auch eine **zunehmende Überwachung durch staatliche Organe** (z.B. Vorratsdatenspeicherung) als drängendes Problem angeführt, welche es schnellstmöglich einzudämmen gelte. Das „Ausspionieren“ von Nutzerinnen und Nutzern stelle dabei ein Eindringen in deren Privatsphäre und damit eine Sicherheitsverletzung und ein Sicherheitsrisiko dar.

Insbesondere für private Nutzerinnen und Nutzer bestehe demgegenüber insgesamt noch **zu wenig Transparenz** beim Umgang mit Informationssicherheit in der öffentlichen Verwaltung. Von staatlicher Seite (Bund, Länder, EU) gebe es zudem zu wenig finanzielle Projektförderung für Cyber-Sicherheitsforschung und Initiativen, die sich für Cyber-Sicherheit engagieren.

> *„[…] was mir gerade so ein bisschen Sorgen macht, welche Einschränkungen der Privatsphäre aus Sicherheitsdenken plötzlich passieren und zwar so nebenbei und auch mit relativ wenig Medienberichterstattung. […] Ich finde, dass sehr viele staatliche Akteure nicht verantwortlich damit umgehen. Das ist eigentlich nicht die Grundidee unserer Verfassung und unseres demokratischen Agreements in meinen Augen." (A6)*

Demgegenüber wurde **von den Anbietern von IT-Produkten implizit mehr Sicherheit ihrer IT-Produkte gefordert**, da momentan noch zu viele Produkte nicht sicher genug seien bzw. durch Updates ihre Sicherheit aufrechterhalten würden.

Datensammlung und unzureichender Datenschutz: Thematisiert wurde die Datensammlung durch privatwirtschaftliche Unternehmen, aber vor allem auch durch staatliche Autoritäten, wie z.B. die Polizei, Geheimdienste sowie Einschränkungen durch Gesetze (z.B. pentesting). Ein Hinweis erfolgte in Bezug auf Datenmonopole einzelner Anbieter bzw. Plattformanbieter (z.B. Facebook, Google), die aggregierte Daten, bzw. Daten, die ihnen durch Kunden zur Verfügung gestellt werden, in Form und Umfang nur sehr eingeschränkt wiederum den Kunden oder der Community zur Verfügung stellen.

Die Heterogenität der Nutzerinnen und Nutzer (private Nutzung, Unternehmen, öffentliche Einrichtungen) lasse überdies keine Einheitslösungen zur Informationssicherheit zu, was somit passgenaue Regelungen und Lösungsansätze erfordere. Ähnlich sei dies auch durch die Kurzlebigkeit und den ständigen Wandel der digitalen Welt bedingt, was ebenfalls kontinuierliche Anpassungen an die Sicherheitssituation erfordere. Andererseits bestünden zum Teil auch festgefahrene Strukturen, die Anpassungen und Veränderungen der IT-Welt nur schwer realisierbar machten. An die existierende Softwarebasis sei man bereits gewohnt und diese habe einen Bestandsschutz. Für manche Akteure und Nutzerinnen und Nutzer könne dies z.B. auch zu einer Art Fatalismus führen, die Situation einfach hinzunehmen, da man ja ohnehin nichts ändern könne.

Was wäre die größte digitale Katastrophe?

Die Expertinnen und Experten wurden gebeten, Negativszenarien für die Informationssicherheit zu skizzieren und die aus ihrer Sicht *„große digitale Katastrophe"* zu benennen, die z.B. einem Vulkanausbruch oder einer Jahrhundertflut gleichkäme. Die Häufigkeit der Nennung eines Szenarios kann als Orientierungspunkt für die Wahrscheinlichkeit ihres Eintretens interpretiert werden.

Angriffe auf Kritische Infrastrukturen: Genannt wurde z.B. die Unterbrechung der Energieversorgung, das außer Betrieb setzen des Internets, Angriffe auf die Wasserversorgung oder Verkehrsinfrastruktur, ein großflächiges Lahmlegen von Computern bzw. Erpressungsszenarien (vgl. Wannacry) oder der Cyber-Angriff auf ein Atomkraftwerk. Besonders Angriffe auf zentralisierte Systeme wurden als gefährlich eingestuft.

Überwachung: Formuliert wurde die Sorge einer umfassenden Totalüberwachung oder weitreichender Datenweitergabe und -zugänglichkeit, wie sie z.B. im „NSA-Skandal" öffentlich wurde.

Manipulation von Daten und Informationen: Neben der Datenmanipulation im Allgemeinen wurde konkret z.B. eine Manipulation bei Wahlen wie auch von Meinungen, z.B. innerhalb Sozialer Netzwerke oder auch auf Informationsplattformen/-diensten angeführt.

Schließlich wurde auch der Datenverlust durch einen Sicherheitsvorfall, namentlich bei Banken, in der Verwaltung und bei staatlichen Einrichtungen als „katastrophaler Zustand" bezeichnet.

> *„Wenn Kritische Infrastrukturen[…] zusammenbrechen würden, weil sie gehackt wurden und durchbrennen oder die Zugangsdaten verschlüsselt wurden, dass wirklich der Strom ausfällt, das Wasser nicht mehr läuft, wenn die Ampeln nicht mehr funktionieren, wenn die Supermarktregale leer bleiben, weil ein Hackerangriff von einem fremden Staat passiert ist, ich glaube das wäre ein wirklich absolutes Katastrophenszenario, was zeigen würde, wie stark die digitale mit der analogen Welt gesteuert wird und wo man sich auch fragen muss, ob man wirklich alles vernetzen muss, ob wirklich jeder Kühlschrank einen Chip braucht, ob alle Warenströme und Infrastrukturen an das Internet angeschlossen werden sollten.“ (T8)*

2.3.2 Vertrauen

Insbesondere in Fragen der Sicherheitsherstellung werden Akteuren weitreichende Kompetenzen und Verantwortung übertragen. Die Ausgestaltung der Sicherheitsarchitektur wird davon geprägt, wer mit der Ausführung damit einhergehender Aufgaben betraut ist. Das Verhalten von Nutzerinnen und Nutzern trägt dazu bei, Sicherheit herzustellen oder auch zu gefährden. Abhängig von dem Vertrauen gegenüber Nutzerinnen und Nutzern kann ihre Eigenverantwortung eingestuft werden. Gegebenenfalls werden auch Strukturen notwendig, die Nutzerinnen und Nutzern Verantwortung abnehmen und dafür mehr Schutz bieten. Das Vertrauen der Nutzerschaft entscheidet darüber, wer für sie Verantwortung tragen soll. Dies gilt z.B. auch in Bezug auf die Gewährleistung der Sicherheit bei der Ausübung von Geschäftsbeziehungen oder auf das sichere Funktionieren von Hard- und Software etc.

Welche Faktoren sind für eine Vertrauensbildung bezüglich Informationssicherheit wichtig? Wie funktioniert Vertrauen in der digitalen Welt?

2.3.2.1 Faktoren für Vertrauen in der digitalen Welt

Akteure, die erkennbar ihren **Arbeitsschwerpunkt** auf Fragen der Digitalisierung und IT-Sicherheit legen, genießen per se ein Grundvertrauen hinsichtlich ihrer Fachkompetenz. Einen zweiten wichtigen Faktor bildet entsprechend die Fachkompetenz, die **Mitarbeiterinnen und Mitarbeitern** zugesprochen wird. Organisationen, deren **gute Ausstattung mit qualifiziertem Fachpersonal** bekannt ist, gelten als kompetent.

Eng verbunden mit den Arbeitsinhalten ist die **offizielle Zielsetzung** der Akteure, welche ebenfalls mit dem ihnen entgegengebrachten Vertrauen in Verbindung gebracht wurde. Dies sowohl bezogen auf die Kompetenz, als auch und besonders in Bezug auf moralisch vertretbares Verhalten.

Vertrauen in **Fachexpertise** wird teilweise an den nach außen hin vermittelten Zielen festgemacht. Auf moralischer Ebene zeigt sich der Zusammenhang wiederum insbesondere, wenn Akteure eine tendenziell altruistische, **am Gemeinwohl orientierte Zielausrichtung** erkennen lassen, wohingegen (staats-)autoritäre oder wirtschaftliche Ziele und Aufgaben tendenziell negative Effekte auf die Vertrauensbildung nehmen. Ein zusätzlich verstärkender Effekt ergibt sich, wenn Akteure oder Institutionen in ihrer Arbeit und Zielsetzung als **unabhängig** gelten und eigenbestimmt, frei und weisungsungebunden agieren können.

Einen starken vertrauensbildenden bzw. -erhaltenden Effekt erfährt die **persönliche Begegnung**. Die Befragten äußerten in Bezug auf verschiedene Akteure, dass die persönliche Erfahrung im Rahmen von Veranstaltungen, bilateralen Gesprächen, Workshops, Podiumsdiskussionen, aber auch Statements in den Medien einen bedeutenden Einfluss auf ihre Einstellung gegenüber den Akteuren nehme. Eine Rolle spielte dabei das **Auftreten** bzw. die vermittelte **Authentizität** von Einzelpersonen, wie auch Organisationen in ihrer öffentlichen Präsenz.

Schließlich sei das für verschiedene Akteure zitierte **Staatsvertrauen** erwähnt, das für staatsnahe bzw. behördliche Institutionen eine wertvolle Grundlage für ihre Arbeit mit anderen Akteuren

darstellt. Der häufige Verweis auf das **Staatsvertrauen** erscheint vor dem Hintergrund einer in der Vergangenheit zum Teil ausgeprägten Kritik an Regierung, Politik und staatlichen Institutionen und dem Wunsch nach mehr Liberalität und Freiheit im Netz bemerkenswert; schließlich wurden in den Interviews zivilgesellschaftliche Akteure befragt, die z.T. Befürworter sind von Parallel- bzw. Alternativstrukturen, bis hin zu Ansätzen einer autarken, selbstverwalteten Internet-Community.

Als der schwerwiegendste **negativ wirkende Faktor** gelten öffentliche **Skandale** und Verfehlungen, wie aber auch bekannt gewordene **Versuche der Verschleierung** dieser. Hierzu zählen bekannt gewordene Fälle von Datenverlust und Datenlecks, Sicherheitslücken, Datenklau und Datenweitergabe, aber auch Überwachung von Nutzerinnen und Nutzern oder die Verletzung des Datenschutzes. Diese Aspekte schädigen zuvorderst das Vertrauen aus moralischer Sicht, aber auch in Hinblick auf die Kompetenz der Akteure, welche nicht kompetent genug scheinen, ihre bzw. die ihnen anvertrauten Daten ausreichend zu schützen. Institutionen und Akteure, für die keine Skandale oder Verfehlungen bekannt sind, genießen nicht zuletzt vor dem Hintergrund der Negativbeispiele ihrerseits größeres Vertrauen. So gelten auch Akteure, die mit einem mangelnden Problembewusstsein oder gar mutmaßlicher Untätigkeit bzw. Nachlässigkeit im Zusammenhang mit Datenschutz und Informationssicherheit in Verbindung gebracht werden, als wenig vertrauenserweckend.

Unter den **vertrauensbildenden** Faktoren, die von den Expertinnen und Experten im offenen Teil der Befragung ergänzt worden sind, nimmt die **Transparenz** den bei weitem am häufigsten und als am wichtigsten angeführten Aspekt ein. Dabei wird der Begriff der Transparenz sehr unterschiedlich interpretiert. In den Gesprächen deutete sich an, dass hierunter insbesondere die grundsätzliche Verfügbarkeit zu Informationen bezüglich der Tätigkeiten, Zielsetzungen, Geschäftsbedingungen und Rechtsgrundlagen, Datensicherheit- und Datenschutzbedingungen von Akteuren subsumiert wurde. Allerdings wurden auch Aspekte angeführt wie der Datenschutz, die Privatheit bzw. das sogenannte „Privacy on Demand“ und „Opt out“ sowie eine evidenzbasierte, d.h. auf empirische Belege gestützte Gesetzgebung. Eine Interviewpartnerin nannte auch das Offenlegen von Quellcodes als Variante der Transparenz.

Mehrere Befragte wiesen im Zusammenhang mit dem Begriff der Transparenz darauf hin, dass die Frage der **Verständlichkeit und Nachvollziehbarkeit** zur Verfügung gestellter **Informationen** eine wichtige Rolle spiele: Transparent vorgehaltene Allgemeine Geschäftsbedingungen (AGBs), die jedoch für Normalverbraucherinnen und -verbraucher bzw. -nutzerinnen und -nutzer unverständlich formuliert sind, fördern z.B. kein Vertrauen. In Kombination mit den Aussagen bezüglich des Vertrauens (siehe oben) füllt sich der an sich allgemeine und unspezifische Begriff der Transparenz weiter mit Inhalt. Demnach wird Transparenz offensichtlich vor allem als eine „**proaktive Transparenz**“ begrüßt und wirkt dann vertrauensbildend. Für Akteure bzw. Institutionen sollte nach außen hin einsehbar sein – und auch aktiv kommuniziert werden – wofür sie stehen, welche Ziele sie verfolgen, mit welchen Methoden, welchem Personal und welcher Technologie sie dabei konkret vorgehen. Die **Kommunikation** dieser Aspekte hat besonders im persönlichen Kontakt vertrauensbildende Wirksamkeit. Schließlich wird in diesem Moment Transparenz alltagssprachlich verständlich, ehrlich, persönlich und authentisch hergestellt. Somit bilden in den Ausführungen der Befragten das Empfinden von Ehrlichkeit und Authentizität, wie andererseits im Falle z.B. mutmaßlicher Überheblichkeit von Akteuren, ebenfalls Faktoren für Vertrauen. Hinter dem oft angeführten Begriff der Transparenz verbergen sich damit also mitnichten nur die oft darunter verstandene Möglichkeit des Zugriffs auf Dokumente und öffentlich einsehbare Entscheidungsprozesse, sondern die Möglichkeit zum Austausch mit konkreten Personen und dessen aktive Initiation.

Einzelne Interviewpartnerinnen und -partner wiesen auf klare Haftungsregelungen wie auch das Prinzip von Zertifikaten hin, worüber eine grundlegende Verlässlichkeit und damit auch Vertrauen erreicht werden könne. Ein weiteres Argument für Vertrauen ergebe sich in manchen Fällen zudem durch **Konsensmeinung**, das heißt mehrere Akteure (bzw. die Community) vertreten eine klare Meinung zu Sachverhalten, so dass somit eine Richtigkeit bzw. Gewissheit geschaffen wird, die

Mehrheit könne schließlich nicht ganz so falsch liegen, also kann einer Information bzw. einem Akteur vertraut werden.

2.3.3 Herstellung von Sicherheit

Als Lösungswege zur Steigerung der Informationssicherheit brachte die Denkwerkstatt hervor: ***Technologien, die Sicherheit herstellen***, die ***Kennzeichnung*** (Zertifizierung und/oder Siegelvergabe) von Soft- und/oder Hardware und die Etablierung eines ***Haftungsregimes***. Entsprechend wurden die Expertinnen und Experten in den Interviews zu diesen Ansätzen befragt.

2.3.3.1 Brauchen wir weitere Technologien, die Sicherheit herstellen?

Der Stellenwert der Entwicklung neuer Technologien als Lösungsansatz wurde von den Befragten insgesamt kritisch thematisiert. Technikentwicklung ziehe eine fortwährende Weiterentwicklung und Anpassung von Sicherheitstechnologie nach sich. Bestehende Lösungen erforderten fortlaufend Updates, um das Sicherheitsniveau aufrecht zu erhalten und neu entstehende Felder (z.B. Internet der Dinge) erfordern die Entwicklung neuer Technologien. Insgesamt bestehe weniger Bedarf an neuen Technologien, sondern bei der **konsequenten und korrekten Anwendung existierender Lösungen**.

Wichtige **Technologien zur Herstellung von IT-Sicherheit** könnten z.B. Kryptographie, Passwortverschlüsselung, Ende-zu-Ende-Verschlüsselung, redundante/parallele Strukturen oder Authentifizierung sein. Jenseits der Diskussion um Nutzerfreundlichkeit wurde vereinzelt angeregt, Sicherheitstechnologien, die derzeit nur im Hochsicherheitsbereich Anwendung finden, für die Allgemeinheit zugänglich zu machen, beispielsweise Kryptotelefone. Da mit Sicherheitstechnologien häufig eine verminderte Nutzerfreundlichkeit einhergehe, sprachen sich Interviewte mehrfach für die **Weiterentwicklung der Usability** von Sicherheitstechnologien aus. Einige Interviewte favorisieren in diesem Zusammenhang neue Technologien, die die Nutzerfreundlichkeit steigern, indem sie die Automatisierung eines Prozesses erhöhen und so die Mitarbeit der Nutzerschaft minimieren (security by design/security by default).

2.3.3.2 Kennzeichnung von IT-Sicherheit

Eine Kennzeichnung von Produkten und Services bezüglich ihrer IT-Sicherheit könnte vor allem für Verbraucherinnen und Verbraucher interessant sein, da sie eine gewisse Transparenz herstellen und die Eigenverantwortung bei Kaufentscheidungen unterstreichen würden. Den Interviewpartnerinnen und -partnern wurden drei archetypischen Szenarios zur Wahl gestellt, aus denen Sie das ihnen sinnvollste und wünschenswerteste benennen oder Mischformen und neue Szenarien entwerfen konnten:

- **Keine Kennzeichnung**: Digitale Produkte und Services sind nicht mit standardisierten Informationen zu digitaler Sicherheit zu versehen.
- **Freiwillige Kennzeichnung**: Es gibt z.B. Siegel zu digitaler Sicherheit, die Produkte und Dienstleistungen freiwillig erwerben können und den Verbrauchern Informationen zum Sicherheitsstand des Produkts oder der Dienstleistung liefern.
- **Verpflichtende Kennzeichnung**: Digitale Produkte und Dienstleistungen werden nur für den Markt zugelassen, wenn sie den Gütekriterien eines Sicherheitssiegels genügen.

Einige Interviewpartnerinnen und -partner kommentierten, der hohe Grad an Komplexität und die Schnelllebigkeit in der Technologieentwicklung mache es schwierig, politisch zugespitzte Lösungen zu favorisieren oder abzulehnen. Diese grundlegende Problematik macht bereits deutlich, weshalb sich eine gezielte und rasche Maßnahmenentwicklung so schwierig gestaltet. Folgende Einschätzung wurde von den Interviewpartnerinnen und -partnern gegeben:

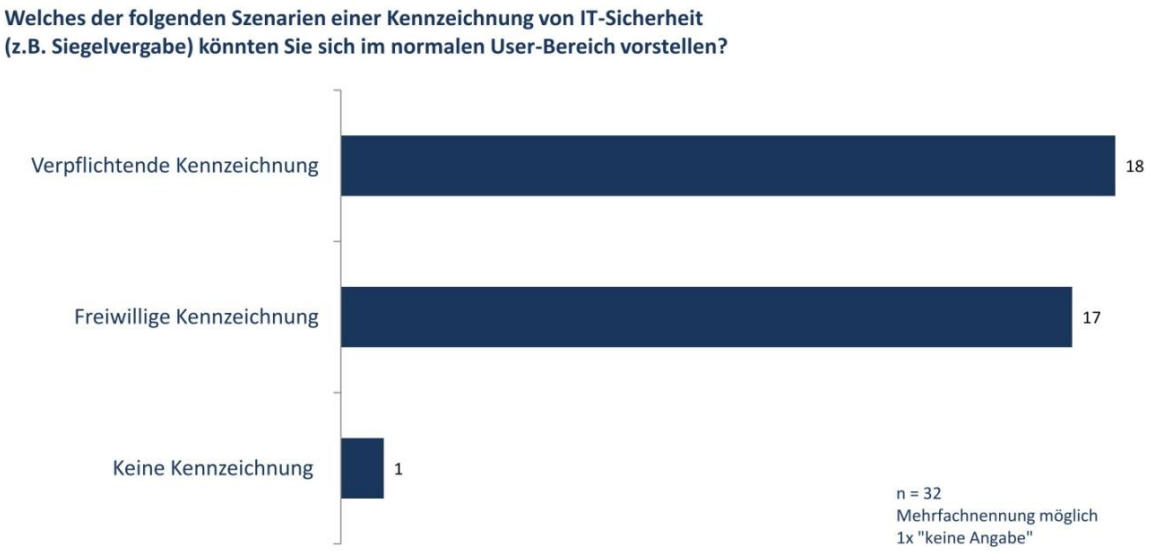


Abbildung 1: Welches der folgenden Szenarien einer Kennzeichnung von IT-Sicherheit (z.B. Siegelvergabe) könnten Sie sich im normalen User-Bereich vorstellen?

Eine Befürwortung von Kennzeichnung – sei sie nun freiwillig oder verpflichtend – kann also als eindeutig angesehen werden. Viele befürworteten die Vorteile der verpflichtenden Kennzeichnung, sahen aber auch große Probleme mit ihr einhergehen und wählten daher als Kompromisslösung die freiwillige oder eine Mischform aus freiwilliger und verpflichtender Kennzeichnung.

> *„Also Variante drei [die verpflichtende Kennzeichnung] finde ich äußerst erstrebenswert, aber ich bin auch realistisch und denke mir, das würde schon alleine aus wirtschaftlichen Gründen niemals gemacht." (A6)*

Grundlegende (Heraus-)Forderungen an eine Kennzeichnung

Die Einführung einer Kennzeichnung könne nach Ansicht der Interviewten nur dann erfolgreich sein, wenn folgende politische, wirtschaftliche und technische **Rahmenbedingungen** gemeistert werden:

- Der Prozess der Kriterienbestimmung/Definition und Vergabe einer Kennzeichnung sollte offen, transparent und nachprüfbar erfolgen. Allerdings wurde die politische Umsetzbarkeit dieser Bedingung von den Befragten in Frage gestellt.
- Grundlegend ist zu unterscheiden, ob Anbieter oder Produkte gekennzeichnet werden; die Interviewten tendierten zu Produkten. Zu klären bliebe, ob einzelne Komponenten oder das Gesamtprodukt der Kennzeichnung unterliegen sollten.
- Die Definition einer national geltenden Kennzeichnung in einem stark internationalisierten Markt (Software-, Hardware-Komponenten und Endprodukte) stellt eine Herausforderung dar. Die rechtliche Grundlage und deren Gültigkeitsbereich bedarf einer genauen rechtlichen Prüfung und Absicherung.
- Der als langwierig antizipierte Prozess der Kennzeichnung eines Produkts könnte neuen Produkten den Markteintritt erschweren und damit besonders kleinere Unternehmen behindern. Deutsche Produkte wären ggf. in der Lage, Kennzeichnungsprozesse schneller zu absolvieren, als ausländische.
- Die grundlegende Kurzlebigkeit von Softwareprodukten erfordert auch für gekennzeichnete Produkte regelmäßige Updates, um den Sicherheitsstatus aufrecht zu erhalten. Hieraus folgen viele Detailfragen, z.B. ob eine Kennzeichnung das Updaten beinhalten oder Produkten nach einem Update die Kennzeichnung entzogen werden sollte.
- Die Forderungen nach standardisierten Sicherheitsmaßnahmen stehen mit (derzeit angebotenen) individuellen Lösungsansätzen im Widerspruch; es folgt die Notwendigkeit von Sonderfallregelungen und Möglichkeiten der Abstufung.

Verpflichtende oder freiwillige Kennzeichnung – Idealismus versus Pragmatismus

Eine verpflichtende Kennzeichnung besitze den höchsten Informationsgehalt, biete den größten Schutz für Verbraucherinnen und Verbraucher und setze den stärksten Anreiz für Unternehmen, in Sicherheit zu investieren. Damit die verpflichtende Kennzeichnung ihren Anspruch erfüllen kann, müssten die genannten Herausforderungen überwunden werden, was viele Interviewte bezweifelten. Eine freiwillige Kennzeichnung sei weit weniger effektiv und stelle ohne eine klare Definition von Sicherheit keine solide Information dar; zudem ließen sich weiche Regelungen zu leicht umgehen. Eine freiwillige Variante erscheint den Interviewten allerdings realistischer und habe eine höhere Chance auf politische Realisierung. Auch Negativeffekte auf den Markt würden abgemildert, indem die Auditierungszeit verkürzt würde. Einige Interviewte wiesen explizit darauf hin, dass der Nutzerschaft in diesem Szenario eine größere Verantwortung zugesprochen werde, die durch Bildungs- und Informationsangebote bedient werden müsste. Auch stelle die freiwillige Kennzeichnung die Gewährleistung der Wahlfreiheit in den Vordergrund und sei besonders für Unternehmen von Vorteil, da sie weniger stark in den Markt eingreife.

Mischformen und Entwicklungsdynamiken

Viele Befragte erachteten eine Mischform von verpflichtender und freiwilliger Kennzeichnung als einen realisierbaren Mittelweg. Aufgrund der schwer umsetzbaren Regelungen, die starke Folgeeffekte zeitigen, solle eine Abstufung eingeführt werden, bei der nur Produkte in sicherheitsrelevanten Kontexten verpflichtend gekennzeichnet werden. Für Produkte im User-Bereich genüge eine freiwillige Kennzeichnung. Zudem komme bei der Einführung von freiwilliger Kennzeichnung eine Dynamik zu verpflichtender Kennzeichnung zum Tragen. Hier wurde das Beispiel der Lebensmittelauditierung angeführt, in der Unternehmen Druck auf Zulieferer ausübten, freiwillige Siegel zu erwerben. Dies führe in der Realität zu einer quasi-verpflichtenden Kennzeichnung und später zur Entwicklung verpflichtender Standards. Eine ähnliche Dynamik sei in der IT-Sicherheit denkbar.

Argumente gegen eine Kennzeichnung

Eine Kennzeichnung wurde mehrheitlich unter der Bedingung als sinnvoll angesehen, dass die oben genannten Schwierigkeiten ausgeräumt werden können. Unter anderem wurde kritisiert, dass Kennzeichnungen im IT-Bereich technisch nicht realisierbar seien. Wer sich mit IT-Sicherheit auskenne, würde eine Technologie niemals als vertrauenswürdig und sicher bezeichnen. Die Feststellung, ein Produkt sei sicher, wäre kontraproduktiv für die Sicherheitsdebatte und Betrug an der Verbraucherin und am Verbraucher. Zudem würden Verbraucherinnen und Verbraucher in ihrer Tendenz bestärkt, sich allgemein nicht intensiv mit dem Thema Informationssicherheit auseinanderzusetzen und sich aus ihrer Verantwortung entlassen zu fühlen.

> *„Und dabei muss man vermeiden, glaube ich, […] davon zu sprechen, dass eine Technologie auf jeden Fall sicher ist. Also das kann grundsätzlich sowieso nicht gewährleistet sein. Es geht also eher darum, einen Prozess zu gestalten, indem die größtmögliche Sicherheit erreicht werden kann und das ist auf jeden Fall ein Prozess, der offen gestaltet werden muss." (K1)*

Welche Akteure könnten die Definition einer Kennzeichnung übernehmen?

Die Einführung einer Kennzeichnung von Produkten bezüglich ihrer IT-Sicherheit wurde von den interviewten Expertinnen und Experten sehr begrüßt. Politische, wirtschaftliche und technische Herausforderungen werden dabei die Ausgestaltung sowie die Wirksamkeit der Kennzeichnung stark beeinflussen. Zwei Lösungsansätze werden in der Definition einer effektiven Kennzeichnung als besonders vielversprechend angesehen: Das BSI und ein heterogen zusammengesetztes Experten-Gremium, eine Art „IT-Rat" nach Vorbild des Ethikrates. Die Befragten verwiesen verschiedentlich auf die Kompetenzen des BSI und das ihm entgegengebrachte Vertrauen in Sicherheitsfragen. Mehrere Befragte sprachen sich explizit dafür aus, dass das BSI eigenständig und unabhängig vom BMI agieren solle, wenn es mit der Definition einer Kennzeichnung beauftragt werde.

In Hinblick auf die Schaffung eines Gremiums, Konsortiums oder „IT-Ethikrats“ begriffen einige der befragten Akteure sich oder Mitglieder aus ihrer Organisation als adäquate Mitglieder eines derartigen Gremiums. Darüber hinaus sahen die Befragten grundsätzlich staatliche und staatsnahe Akteure, wie z.B. die Datenschutzbeauftragten oder auch eine entsprechende EU-Behörde, als geeignete Varianten an.

Mehrere Interviewpartner präferierten demgegenüber formal unabhängige Institutionen, wie zuvorderst die Stiftung Warentest, den TÜV oder die Verbraucherzentralen. Im Kontrast wurden vereinzelt auch privatwirtschaftliche Lösungen, z.B. durch ein zertifizierendes IT-Unternehmen oder ein aus der Privatwirtschaft hervorgehendes Siegel (vgl. „trusted shops“) als zielführend eingestuft.

> *„Ich glaube, so etwas ist auch schwierig einem Akteur zu überlassen. Also, ich glaube, da müsste man alle an den großen runden Tisch holen […].“ (E7)*

Schließlich entfielen auch mehrere Vorschläge auf zivilgesellschaftliche Akteure, wie z.B. den Chaos Computer Club oder auch die Community, Sicherheitsbelange und damit auch die Basis einer Kennzeichnung zu definieren. Jedoch wurde von den Expertinnen und Experten aus der Zivilgesellschaft nur sehr selten eine alleinige oder auch nur zentrale Rolle der zivilgesellschaftlichen Organisationen angeboten, gefordert oder angemahnt.

2.3.3.3 Die Regelung von Haftung in der digitalen Welt

Derzeit existiert kein Haftungssystem für Schäden, die in Zusammenhang mit Informationssicherheit stehen. Es ist ungeklärt, in welchem Umfang Nutzerinnen und Nutzer, Anbieter, Software- oder Hardwarehersteller, Kommunikationsdienstleister, der Staat oder Aufsichtsbehörden und Aufsichtsinstitutionen etc. für die Schaffung von Sicherheit verantwortlich gemacht werden sollen.

> *„Haftung ist ein ganz wichtiger Punkt. Die ist an vielen Ecken diffus. Weil in einem Produkt so viele Teilkomponenten drin sind, da muss eben klar sein, dass einer für die Komposition insgesamt haftet.“ (A1)*

Die Expertinnen und Experten befanden die Klärung von Haftung als wichtig. Bezüglich einer möglichen Form der Haftungsregelung wurden den Befragten vier Szenarien zur Wahl gestellt:

- **Liberale digitale Welt**: Jede Nutzerin und jeder Nutzer ist für die Sicherheit eigener Daten verantwortlich, muss sich über Risiken und Lösungsmöglichkeiten informieren und ist haftbar für Schäden, die durch eigene Geräte und Software verursacht werden.
- **Zertifizierte digitale Welt**: Es gibt zertifizierte Anbieter und Geräte. Nutzerinnen und Nutzer zertifizierter Anbieter und Geräte sind nicht haftbar für Schäden durch eigene Geräte/Software.
- **Versicherte digitale Welt**: Nutzerinnen und Nutzer können eine Versicherung abschließen, die für Schäden durch eigene Geräte und Software aufkommt.
- **Fonds für Cyber-Risiken**: Wie bei anderen unkalkulierbarer Großrisiken sollte es eine Haftung durch den Staat geben. Ein „Fonds für Cyber-Risiken“ würde Nutzerinnen und Nutzer und Unternehmen im Schadensfalle entschädigen.

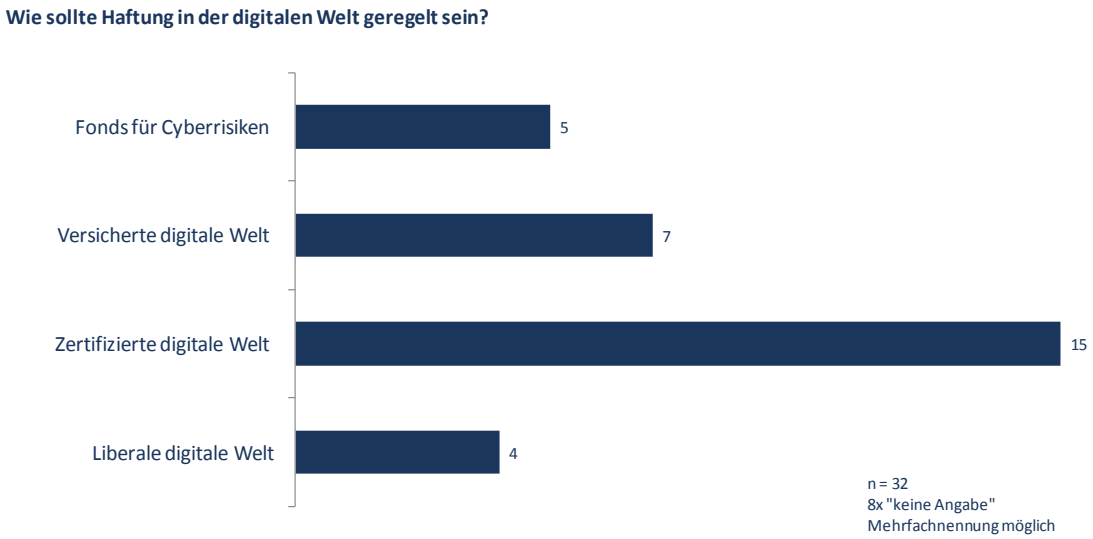


Abbildung 2: Wie sollte Haftung in der digitalen Welt geregelt sein?

Die Befragten kritisierten in den Interviews die (z.B. rechtliche) Umsetzbarkeit der Varianten. Bei der Schaffung von IT-Sicherheit ist es offenbar eine grundlegende Herausforderung, **Lösungen zu entwickeln, die auch unter komplexen rechtlichen, politischen und wirtschaftlichen Rahmenbedingungen wirksam sind.**

Unter den Antworten (Abbildung 2) erhielt die **Zertifizierung** den deutlich größten Zuspruch: Ein Zertifikat könne Orientierung bei der Produktwahl, wie auch Absicherung bieten, falls das Produkt seinem Sicherheitsversprechen nicht nachkommt oder gar Schäden entstehen.

Fonds für Cyberrisiken wurden von vielen Befragten als „Fass ohne Boden“ abgelehnt, da sie ggf. Schäden in sehr großem Maßstab ausgleichen müssten. Auch könne eine derart globale Absicherung, Nutzerinnen und Nutzer zu riskantem Verhalten oder Untätigkeit verführen. Dies erscheint bemerkenswert, da der Angriff auf Kritische Infrastrukturen die häufigste Antwort bezüglich potentieller Cyber-Katastrophen war (vgl. 2.3.1.); hier käme primär die öffentliche Hand als „Letztversicherer“ in Frage.

Die **Versicherung** wurde nur von wenigen Befragten als sinnvoller Ansatz gewählt und wurde u.a. als „reiner Betrug“ deklariert: Die Frage der Verantwortlichkeit sei derart komplex, dass Versicherungen sich zu einfach aus ihrer Verantwortung ziehen und Nutzerinnen und Nutzer auf Schäden sitzen lassen könnten. Auch würde die aktuelle Gesetzeslage eine Versicherungslösung nicht erlauben. Erneut wurde die Vermutung geäußert, eine Versicherung von Cyber-Risiken verführe zu Untätigkeit.

Die **liberale digitale Welt** kommt der aktuellen Realität wohl am nächsten und verkörpert die am weitesten gehende Freiheit bei zugleich größtem Risiko. Die Entscheidung über digitale Lösungen wird dabei den Nutzerinnen und Nutzern überlassen, die entsprechend mögliche Anwendungsrisiken der Sicherheitslücken selbst verantworten müssen. Als stärkstes Argument gegen eine vollkommen liberale digitale Welt wurde die Haftung der Endnutzerinnen und -nutzer angeführt, die letztlich zu einer vollkommenen Überforderung dieser führe.

Die eindeutige Stellungnahme der Expertinnen und Experten für eine generelle Kennzeichnung (s.o.) steht offenbar mit der Präferenz der Haftungsregelung auf Zertifikatbasis in Einklang. Ein besonderer Vorteil der Kennzeichnung (Zertifikat oder Siegel) sei, dass sie eine Grundlage für Anreize zur Steigerung der IT-Sicherheit böte.

Nutzerinnen und Nutzer zwischen Eigenverantwortung und Überforderung

Die **Rolle der Nutzerinnen und Nutzer** ist bei der Haftungsregelung offensichtlich zentral, konnte jedoch von den Expertinnen und Experten nicht eindeutig definiert werden: Die Hälfte der Interviewten sah die Nutzerinnen und Nutzer selbst dafür verantwortlich, sich zu informieren und

ihre Geräte möglichst sicher zu halten sowie verantwortungsbewusst mit ihren Daten umzugehen. Die andere Hälfte schätzte dies als Überforderung ein, da die Komplexität der mannigfaltigen Software- und Hardwareprodukte sowie eine häufig geringe Benutzerfreundlichkeit von Sicherheitslösungen die Kompetenz der Nutzerinnen und Nutzer übersteige. Oftmals müssen allerdings Anbieter- und Nutzeraktivitäten ineinandergreifen, um Sicherheitslücken zu vermeiden, wie z.B. bei der Installation von Updates. Es scheint demnach unvermeidbar, Nutzerinnen und Nutzer in Prozesse der Sicherheitsherstellung zu integrieren.

> *„Das ist ja ein ganz normaler Haftungsmechanismus, der jetzt mit einem Regime. Also nehmen wir mal an, das Produkt macht etwas, was der Nutzer gar nicht beeinflussen kann. An wen kann er sich dann halten? An den, der die Teilkomponente hergestellt hat, die kaputt gegangen ist oder an den, der das Produkt in Gänze ihm übergeben hat? Die Frage muss geklärt sein. Die ist teilweise ja nicht geklärt. Also ich meine, bei den Autos haben wir im Moment noch die Situation, dass der Hersteller des Autos, der es mir verkauft, auch für seine Leistungsfähigkeit haftet. Auch wenn er vielleicht die ganzen Komponenten, die da drin sind, gar nicht selbst beurteilen kann." (A1)*

Die Diskussion der Expertinnen und Experten lässt sich schließlich auf die Differenzierung zwischen verschiedenen Schadenslagen verkürzen: Ist der Verursacher eines Schadens eindeutig, muss dieser zur Verantwortung gezogen werden, ggf. auch Nutzerinnen und Nutzer. Sollte dies nicht möglich sein, sollten die Hersteller und Anbieter digitaler Produkte in der Verantwortung stehen.

2.3.4 Institutionalisierung von IT-Sicherheit

Das Format der *Denkwerkstatt sichere Informationsgesellschaft* befördert den Dialog zwischen zivilgesellschaftlichen, wirtschaftlichen und staatlichen Akteuren. Ein derartiger Dialog wäre grundsätzlich auch als institutionalisierte Form denkbar, sei es ergänzend oder auch als logische Weiterentwicklung des Dialogprozesses in einem Institutionalisierungsprozess. In den Interviews wurden daher mögliche Aufgaben und eine mögliche Struktur einer fiktiven nationalen Institution zur Herstellung von IT-Sicherheit thematisiert und dabei der Verantwortungsbereich der unterschiedlichen Akteure, speziell der Zivilgesellschaft, diskutiert.

2.3.4.1 Die Rolle des Staates

Den Expertinnen und Experten wurden mögliche Aufgabenfelder einer **nationalen Institution zur Herstellung von IT-Sicherheit** zur Diskussion gestellt (Abbildung 3, S. 13).

Bereitstellung von neutralen Bildungs- und Informationsangeboten

Die Interviewten sprachen sich dafür aus, dass eine staatliche Institution Beratungen für Privatwirtschaft sowie Privatnutzerinnen und -nutzer bieten sollte. Dabei wäre eine Zusammenarbeit mit einem Expertengremium wünschenswert, um Expertise, Neutralität und Vollständigkeit von Informationen zu sichern.

> *„Wahrscheinlich macht man es idealerweise im Dialog. Also wenn ich so Befindlichkeiten von Verwaltungen am besten einschätzen kann, dann ist es wahrscheinlich - sollte das schon teilkennzeichnend sein als behördeninterne Sache, aber wenn man sich da nicht externen Sachverstand dazu holt, dann wird es einfach inhaltlich nicht so gut. Deswegen sollte es auf jeden Fall nicht komplett autark geschehen." (K1)*

Definition und Vergabe von Kennzeichnung in Kooperation mit Expertinnen und Experten

Die Aufgabe und Verantwortung der Definition einer IT-Sicherheitskennzeichnung sehen die Befragten entweder bei einer staatlichen Institution (am geeignetsten das BSI) oder einem Expertengremium. Die Expertinnen und Experten befürworten mehrheitlich die Definition und Vergabe einer Kennzeichnung durch eine staatliche Institution. Bei der Definition von Gütekriterien erhielt die Variante, externe Experten als „fremde Werkstatt" mit der Erarbeitung zu beauftragen, den Vorzug vor der eigenen Definition von Gütekriterien. Eher noch konnten sich die Befragten die offizielle Vergabe der Kennzeichnung vorstellen, z.B. im Sinne eines „TÜV" für digitale Produkte.

> *„Man braucht für die Zertifizierung Fachleute, die wissen, worüber sie reden. Und die Zertifizierung braucht einen regulatorischen Rahmen, mit dem die Verbindlichkeit dieses Zertifikats irgendwie abgesichert wird und auch seine Bedeutung geklärt wird. Wofür oder wofür das Voraussetzung ist und was weiß ich. Und ich würde dann Zertifizierung immer in einen Kompetenzkontext stellen und es nicht von vornherein deswegen ausschließlich als staatliche Aufgabe organisieren." (A1)*

Eine neue Aufgabe: Der Staat als Aufsichtsbehörde für Unternehmen

Breiten Anklang fand die Idee, der Behörde die Rolle eines Aufsichtsrats zu übertragen, der für die Überprüfung der Einhaltung von Richtlinien zuständig wäre. Der Kundendienst für Bürgerinnen und Bürger und die Bereitstellung sicherer Produkte durch den Staat, wurde von den Interviewten hingegen tendenziell abgelehnt.

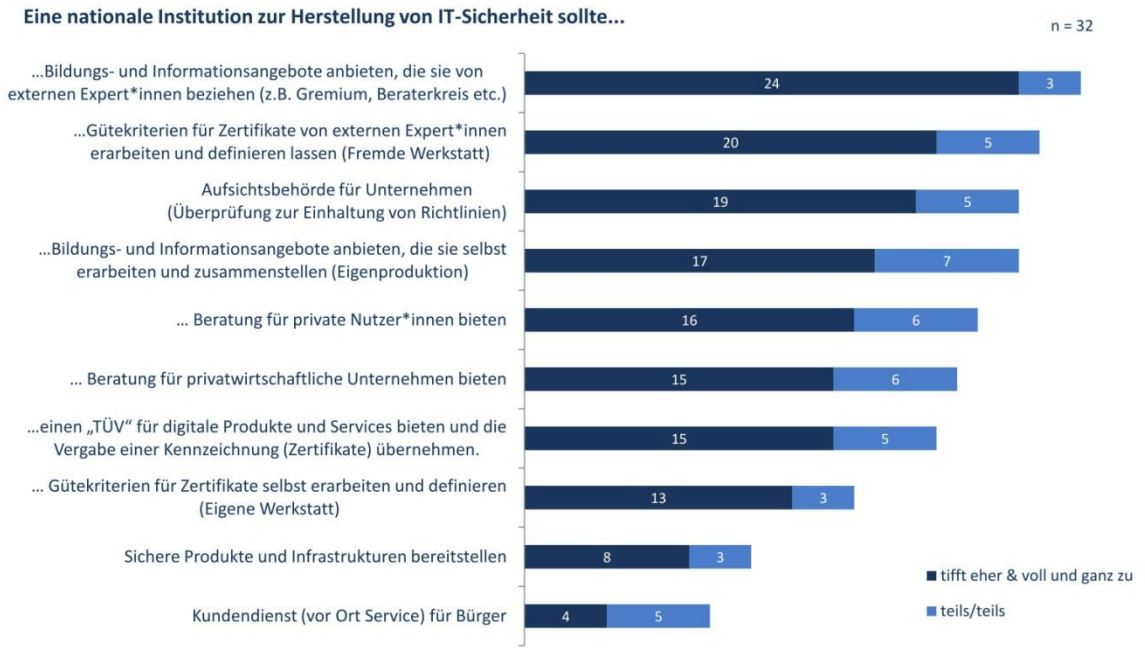


Abbildung 3: Eine nationale Institution zur Herstellung von IT-Sicherheit sollte...?

Weitere mögliche Aufgabenfelder

Die über die vorgegebenen Antworten hinaus genannten Aufgabenfelder lassen sich in vier Themenblöcken zusammenfassen:

Fachliche Autorität und Vermittlung von Expertise: Die Information, Bildung und Beratung von Privatnutzerinnen und -nutzern, Unternehmen und Verwaltung erscheint besonders sinnvoll vor dem Hintergrund der Diskussion über Kennzeichnung und Haftung (s.o.). Private Endnutzerinnen und -nutzer, wie auch Unternehmen und die Verwaltung müssten sich vermutlich weiterhin selbst für die Sicherheit ihrer Geräte und Software engagieren. Die Institution könne aber auch in größeren Zusammenhängen als Expertin tätig werden, z.B. durch Anreize für Unternehmen, Politikberatung

und die Mitdefinition rechtlicher Rahmenbedingungen. Ergänzend wurde die Aufgabe einer „Bedarfsanalyse“ formuliert. Dieser Vorschlag könnte programmatisch verstanden werden, in Richtung einer Institution, die wissenschaftlich fundiert, faktenbasiert und effektiv bzw. als Ratgeberin für handelnde Akteure agiert.

> *„Einiges hängt ja auch mit rechtlichen Regelungen zusammen, die müssen gestaltet werden, und das passiert halt nun mal in der Politik, und im Moment ist das ein Spiel aus Parlamentariern und Lobbyisten, und da bräuchten wir eine starke Vertretung, die auf neutraler Ebene und nicht wirtschaftlich orientiert ist, und der Politik Expertise bereitstellt, um die Entscheidungen überhaupt […] fällen zu können, wie man reguliert. Ich glaube das ist eine zentrale Aufgabe eines solchen Instituts.“ (A4)*

Förderung von vertrauensvollem Austausch: Die „(finanzielle) Förderung zivilgesellschaftlicher Akteure“ wurde mehrmals im Zusammenhang mit der Forderung nach einer stärkenden und vermittelnden Funktion für zivilgesellschaftliche Organisationen genannt. Hierzu passt auch die Idee eines „Vertrauensankers“ oder auch die Funktion als Bindeglied zwischen den Akteuren (z.B. Behörden, zivilgesellschaftlicher Organisationen, Anbietern, Nutzerinnen und Nutzern). Die Forderung nach vertrauensvollem Austausch stellt insgesamt eine Kernbotschaft dar, ohne deren Umsetzung eine nationale Institution deutlich weniger Akzeptanz erführe.

Schutz vor Angriffen: Kritische Infrastrukturen und Regierungsinstitutionen (bzw. deren IT-Infrastruktur) zu schützen, fällt nach Ansicht einiger Expertinnen und Experten ebenfalls in den Aufgabenbereich einer Institution zur Herstellung von IT-Sicherheit.

Kompetente und mit Kompetenzen ausgestattete Überprüfung von Vorgaben: Laut einiger Expertinnen und Experten sollte die Institution auch eine Meldestelle für Sicherheitsschäden betreiben und zur Sanktionierung bei der Nichteinhaltung von Vorgaben befähigt sein.

2.3.4.2 Die Rolle der Zivilgesellschaft

Die Expertinnen und Experten leiteten für die Zivilgesellschaft eine beratende und assistierende Stellung ab. **Die wesentliche Verantwortung solle weiterhin der Staat tragen**. Wenngleich Kritik an staatlicher Fachexpertise und staatlichem Handeln formuliert wurde, genießt der Staat ein stabiles Vertrauen. Um Schwachstellen staatlicher Institutionen (insb. mangelnde Expertise) auszugleichen, wurde eine **enge Verzahnung mit der Zivilgesellschaft** gefordert. Die staatlichen Institutionen sollten Teil eines Gefüges verschiedener Akteure mit unterschiedlichen Kompetenzen sein.

Die Rolle der Zivilgesellschaft wurde als Korrektiv gesehen, das als kritische, unabhängige Instanz ihre digitale Expertise einbringen und auf Missstände aufmerksam machen könne. Des Weiteren stehe sie für Bürgernähe und Nutzerorientierung ein. Viele Befragte sprachen sich daher für ein **Gremium oder Konsortium** aus, **um die Aufgabe(n) einer nationalen Institution für IT-Sicherheit zu organisieren** oder einer öffentlichen Instanz beratend zur Seite zu stehen. In diesem Gremium sollten Akteure aus der Zivilgesellschaft und Expertinnen und Experten der Privatwirtschaft, Wissenschaft, Bildung und ggf. weiterer Bereiche vertreten sein. Allerdings fanden sich unter den befragten Expertinnen und Experten vergleichsweise wenige, die sich für ihre Organisation eine Beteiligung an einem derartigen Gremium vorstellen könnten. Dies mag die Schaffung eines solchen Gremiums schwierig gestalten.

3 Umfrage unter Nutzerinnen und Nutzern

3.1 Erhebungskonzept

Im April 2017 führte die Ipsos GmbH im Projekt eine repräsentative Online-Befragung durch, an der 2.000 Personen im Alter von 14 bis 65 Jahren teilnahmen. Die Repräsentativität wurde durch entsprechende Quoten bei Geschlecht, Alter, Bildungsstand und Bundesland hergestellt. Die Ergebnisse erlaubten eine Klassifikation der Bevölkerung in Gruppen mit ähnlichen Werten und Einstellungen. Der Inhalt orientierte sich u.a. an den Ergebnissen der „Denkwerkstatt sichere Informationsgesellschaft“ im Februar 2017. Die Ergebnisse wurden durch eine zweitägige qualitative Online-Community[1] vertieft. Diese fand im Juni 2017 mit 20 Teilnehmenden im Alter zwischen 18 und 65 Jahren aus dem ganzen Bundesgebiet statt. Die Einladung strebte eine Durchmischung der Bildungsgrade, Erfahrungsgrade bei der Internetnutzung und eine Gleichverteilung der Geschlechter an.

3.2 Zusammenfassung der Ergebnisse

Der Begriff „Digitalisierung“

Die Bevölkerung verbindet mit dem Begriff Digitalisierung das Internet und den Fortschritt. Sie steht der Digitalisierung insgesamt aufgeschlossen gegenüber: Die Mehrheit (53 Prozent) verbindet damit etwas (sehr) Positives. Nur eine Minderheit (13 Prozent) etwas (sehr) Negatives.

Nutzen der Digitalisierung und ihr Einfluss

Die größten Vorteile der Digitalisierung werden in der Schnelligkeit und Effizienz sowie beim Zugriff auf Informationen gesehen. Die Preisgabe persönlicher Informationen und mangelnder Datenschutz werden hingegen als häufigste Nachteile genannt. Es wird deutlich, dass auch Datensicherheit für die Befragten eine große Rolle spielt. Der Einfluss von Digitalisierung auf verschiedene Lebensbereiche ist laut Angaben der Befragten bei Kommunikation und Konsumverhalten am größten. Mehr als drei Viertel geben an, dass hier ein (sehr) großer Einfluss besteht. In den Bereichen Wohnen und Gesundheitswesen wird der geringste Einfluss gesehen. Dennoch geben auch hier vier von zehn Befragten an, dass die Digitalisierung große Veränderung bewirkt.

Eingeschätzte Risiken von Online-Aktivitäten

Beim Thema Informationssicherheit, werden die größten Risiken von Online-Aktivitäten bei den sozialen Netzwerken und beim Online-Banking gesehen. Mehr als die Hälfte der Bevölkerung gibt an, dass diese genannten Aktivitäten risikoreich sind. Zudem haben elf Prozent der Befragten bereits negative Erfahrungen bei der Nutzung von Internetanwendungen (z.B. Online-Shopping oder Soziale Netzwerke) gemacht. Bei den smarten Geräten (z.B. Smartphone oder Tablet) sind es etwas weniger (sieben Prozent). Dabei beziehen sich die negativen Erfahrungen bei Internetanwendungen vor allem auf Spam E-Mails und Viren. Die Auswirkungen auf die Befragten durch diese negativen Erfahrungen äußern sich durch ein Vermeidungsverhalten, welches vor allem ein gesteigertes Misstrauen bei der Internetnutzung bzw. eine eingeschränkte Nutzung von smarten Geräten umfasst. Mehr als jeder Zehnte gibt jedoch auch an, dass es keine Auswirkungen auf das eigene Verhalten gab.

Maßnahmen zur Gewährleistung von Informationssicherheit

Es besteht bei vielen Personen eine **kognitive Dissonanz** bzw. ein Spannungszustand zwischen dem gefühlt wichtigen Thema der Sicherheit auf der einen und der Überforderung und Tatenlosigkeit auf der anderen Seite.

Als Vorkehrungen, sich im Internet zu schützen, werden vor allem Anti-Viren-Software, sichere Passwörter und Updates genannt. Zur Gewährleistung von Sicherheit im digitalen Raum sollten Inter-

[1] Eine Online-Community ist eine Art digitaler Treffpunkt, der Personen zur gemeinsamen Diskussion versammelt. Dieser steht den Teilnehmenden 24 Stunden am Tag zur Verfügung, um dort Fragen zu posten, sich gegenseitig zu kommentieren und somit in Dialog zu treten.

netanbieter, Technologie- und Social-Media-Unternehmen sowie nationale Behörden die größte Verantwortung innehaben. Nationalen Behörden wird dabei ein hohes Vertrauen entgegengebracht.

Bedienungsfreundlichkeit, Verständlichkeit und gesetzliche Mindeststandards sind die am häufigsten genannten Maßnahmen, um das Vertrauen in die Sicherheit von Produkten und Services zu stärken. Bei den zu erfüllenden Voraussetzungen für Sicherheit im digitalen Raum sind Sicherheitstests, Sicherheitsrichtlinien und klare Haftungsregelungen die am häufigsten genannten Antworten.

Sicherheit im digitalen Raum und die Schaffung von Mindeststandards für die Sicherheit von Anwendungen und Geräten, die auf das Internet zugreifen, sind den Befragten sehr wichtig. Zwei Drittel sind der Ansicht, der Staat habe einen Regulierungsauftrag für mehr Informationssicherheit. Weniger als die Hälfte der Bevölkerung (48 Prozent) kennt sich persönlich sehr gut mit dem Thema "Sicherheit im Internet" aus bzw. informiert sich regelmäßig.

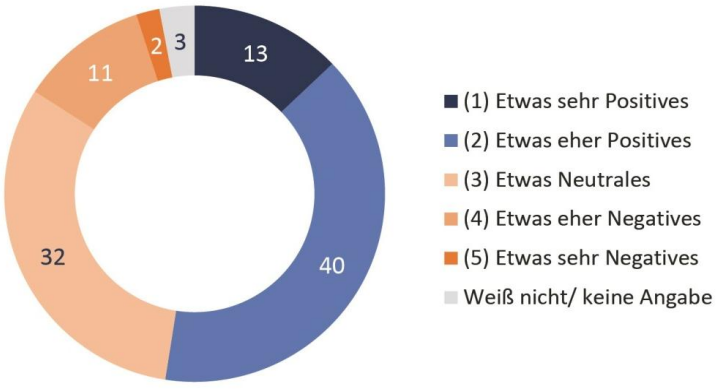
Fünf Nutzergruppen mit unterschiedlichem Wissenstand und Verhaltensweisen
Basierend auf den Befragungsergebnissen konnten fünf Gruppen anhand der Einstellungen und Verhaltensweisen gegenüber und im digitalen Raum segmentiert und analysiert werden:

3.3 Ergebnisse der Online-Befragung

Das folgende Kapitel umfasst die Ergebnisse der repräsentativen Online-Befragung, ergänzt durch vertiefende Einblicke aus der Online-Community. Zitate sind anonymisiert und im Original dargestellt (‚M' steht im Zitat für männlich und ‚W' für weiblich; die Zahl für das Alter).

3.3.1 Verständnis von Digitalisierung und digitaler Gesellschaft

Beim Begriff „Digitalisierung" nannten die Befragten am häufigsten die Schlagworte „Online-Anwendungen", „Internet / DSL" und „Zukunft / Fortschritt / Innovation". Die Befragten stehen der Digitalisierung positiv gegenüber (Abbildung 4): Insgesamt 53 Prozent verbinden mit diesem Begriff etwas (sehr) Positives, nur 13 Prozent etwas (sehr) Negatives. Hinsichtlich der Vor- und Nachteile von Digitalisierung werden die größten Vorteile in der „Schnelligkeit und Effizienz" sowie beim „Zugriff auf Informationen und Wissen" gesehen. Unter den Nachteilen spielt die **Informationssicherheit für die Befragten überwiegend eine große Rolle.** Hier werden die „Preisgabe persönlicher Informationen, Überwachung" und „mangelnder Datenschutz und Datensicherheit" am häufigsten genannt.



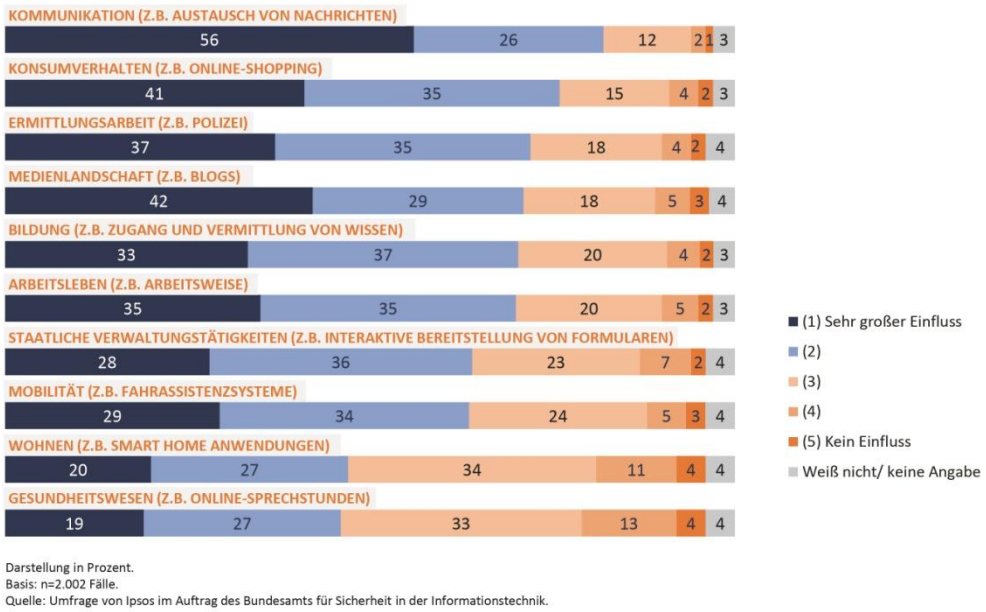
Darstellung in Prozent.
Basis: n=2.002 Fälle.
Quelle: Umfrage von Ipsos im Auftrag des Bundesamts für Sicherheit in der Informationstechnik.

Abbildung 4: Bitte denken Sie an den Begriff "Digitalisierung". Verbinden Sie damit...?

Der Einfluss von Digitalisierung auf verschiedene Bereiche wird von der Bevölkerung als sehr umfangreich bewertet (Abbildung 5, S. 17), am größten in den Bereichen Kommunikation und

Konsumverhalten. Mehr als drei Viertel geben an, dass ein (sehr) großer Einfluss besteht. Auch der Einfluss auf den Bereich Ermittlungsarbeit wird von mehr als 70 Prozent als (sehr) groß angesehen.

In der Rangliste des Einflusses von Digitalisierung auf verschiedene Lebensbereiche befinden sich das Arbeitsleben und die Mobilität im Vergleich zwar auf den hinteren Rängen, doch auch hier schätzen 70 bzw. 63 Prozent der Befragten den Einfluss als (sehr) groß ein. In den Bereichen Wohnen und Gesundheitswesen wird der geringste Einfluss gesehen. Hier geben vier von zehn Befragten an, dass die Digitalisierung große Veränderung in diesen Bereichen bewirkt.



Darstellung in Prozent.
Basis: n=2.002 Fälle.
Quelle: Umfrage von Ipsos im Auftrag des Bundesamts für Sicherheit in der Informationstechnik.

Abbildung 5: Wie groß ist Ihrer Meinung nach der Einfluss der Digitalisierung auf die folgenden Bereiche?

3.3.2 Wahrnehmung von Risiken der Digitalisierung

Als besonders gefährlich wahrgenommen: Soziale Netzwerke und Online-Banking

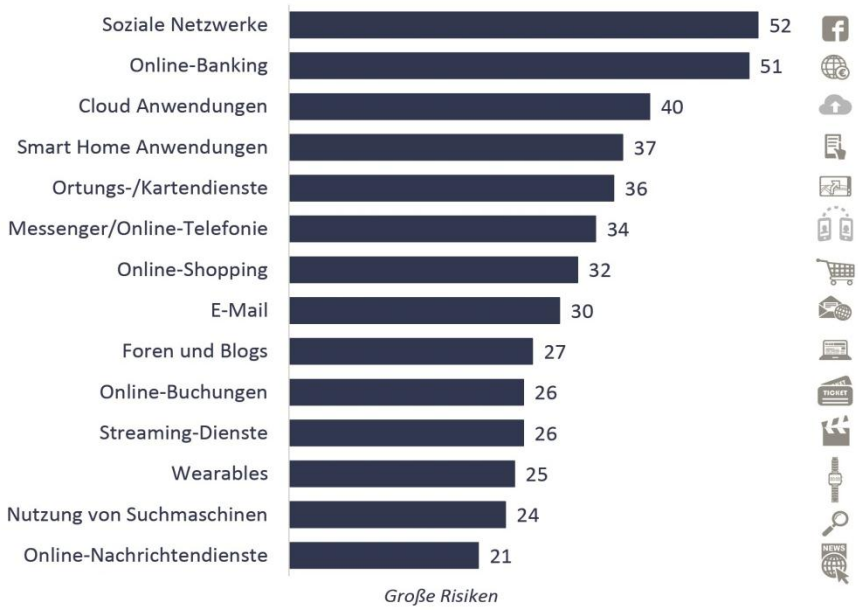
Die größten Gefahrenpotentiale von Online-Aktivitäten werden bei den **sozialen Netzwerken** und beim **Online-Banking** gesehen (Abbildung 6, S. 18). Mehr als die Hälfte der Befragten bewertet sie als risikoreich. Aber auch **Cloud-Anwendungen, Smart-Home** und **Ortungsdienste** werden von mehr als einem Drittel als potentiell gefährlich angesehen. Im Gegensatz zum Online-Banking werden Online-Shopping (32 Prozent) und Online-Buchungen (26 Prozent) als weniger risikoreich bewertet. Auch die E-Mail wird nur von 30 Prozent der Befragten mit einem Risiko verbunden. Dieser relativ niedrige Wert lässt vermuten, dass z.B. die Verbreitung von Viren durch E-Mail-Anhänge nicht in die Risikobewertung mit eingeflossen ist, und sich die Befragten dieser Gefährdung vermutlich nicht bewusst sind. Die geringste Gefahr stellt die Nutzung von Online-Nachrichtendiensten (21 Prozent) dar. Ebenso werden Wearables (25 Prozent) als wenig risikoreich angesehen.

Tatsächliche Negativerfahrungen sind bisher eher selten

Elf Prozent gaben an, negative Erfahrungen mit Internetanwendungen gemacht zu haben. Bei smarten Geräten sind es etwas weniger (sieben Prozent). Negative Erfahrungen bei Internetanwendungen beziehen sich vor allem auf Spam E-Mails (17 Prozent) und Viren (14 Prozent). Viele negative Erfahrungen sind dem Bereich Betrug, Datendiebstahl und Hacking zuzuordnen. Bei den smarten Geräten stehen technische Probleme (24 Prozent) im Vordergrund, es werden aber auch viele negative Erfahrungen mit Datendiebstahl und Betrug verbunden.

Aus den negativen Erfahrungen bei Internetanwendungen folgt ein gesteigertes Misstrauen und höhere Skepsis (17 Prozent) sowie ein vorsichtigerer Umgang mit Daten (12 Prozent). Auch könnte ein Vermeidungsverhalten die Folge sein, so dass zweifelhafte Internetanwendungen zukünftig teilweise gemieden werden, um negative Erfahrungen zu verhindern. Nur etwa jeder Zehnte gibt an,

dass sich negative Erfahrungen nicht auf das eigene Verhalten ausgeübt hätten. Die negativen Erfahrungen bei den smarten Geräten wirken sich vor allem durch eine eingeschränkte Nutzung von smarten Geräten (14 Prozent) aus. Weitere 14 Prozent gaben ein gesteigertes Gefahrenbewusstsein an. Auch hier ist die Anzahl der Befragten relativ hoch, bei denen die negativen Erfahrungen keine Auswirkungen auf das eigene Verhalten ausüben (17 Prozent).



Darstellung: Top-2-Boxes (große Risiken) in Prozent.
Basis: n=2.002 Fälle.
Quelle: Umfrage von Ipsos im Auftrag des Bundesamts für Sicherheit in der Informationstechnik.

Abbildung 6: Inwieweit sehen Sie Risiken bei den folgenden Online-Aktivitäten? Bitte verwenden Sie für Ihre Antwort eine Skala von 1 bis 5, wobei die 1 für "große Risiken" und die 5 für "kleine Risiken" steht.

Angst vor Kontrollverlust bei gleichzeitiger fachlicher Überforderung

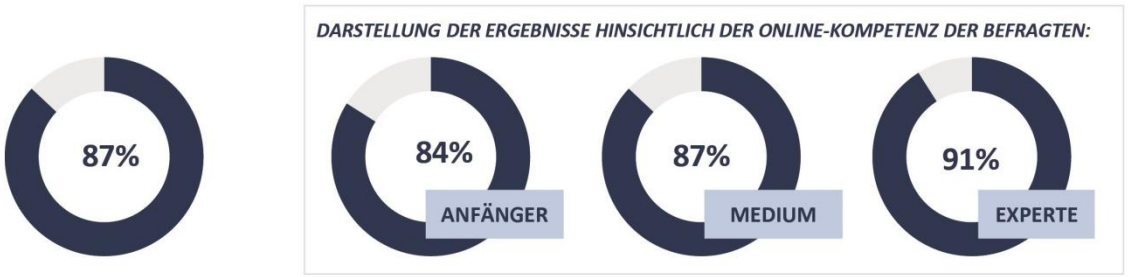
In der **qualitativen Online-Community** zeigt sich, dass die Befragten Angst vor einem potentiellen Kontrollverlust und Datenmissbrauch haben. Das Gefühl der Unsicherheit entsteht und verstärkt sich besonders bei negativen Erfahrungen. Auch bei Seiten, die beispielsweise Tracking-Technologien (z.B. Facebook) nutzen oder Pop-Ups und Plug-Ins enthalten, verstärkt sich dieses unsichere Gefühl. Es wird deutlich, dass Befragte nicht aktiv zwischen Datensicherheit und Datenschutz unterscheiden. Beides wird in der Befragung und der Online-Community nahezu synonym verwendet und in den Kontext der Risiken der digitalen Welt gesetzt. Das in der quantitativen Befragung angesprochene Vermeidungsverhalten bestätigt sich hier. Neben aktiven Gegenmaßnahmen (z.B. Anti-Viren-Software), werden unseriös erscheinende Webseiten zum Teil gänzlich vermieden, um Datensicherheit zu erhöhen. Maßnahmen, die in der Auswertung der Befragung dem Datenschutz zuzuordnen wären, werden kaum angesprochen. Die nicht vorhandene Differenzierung könnte ein Grund für eine unzureichende Sensibilisierung in beiden Bereichen sein und würde daher für eine Intensivierung entsprechender Maßnahmen zur Sensibilisierung sprechen.

3.4 Digitalisierung und Sicherheitsmaßnahmen

3.4.1 Was Nutzerinnen und Nutzer selbst für ihre Sicherheit im digitalen Raum tun

Sicherheit im digitalen Raum ist Nutzerinnen und Nutzern wichtig

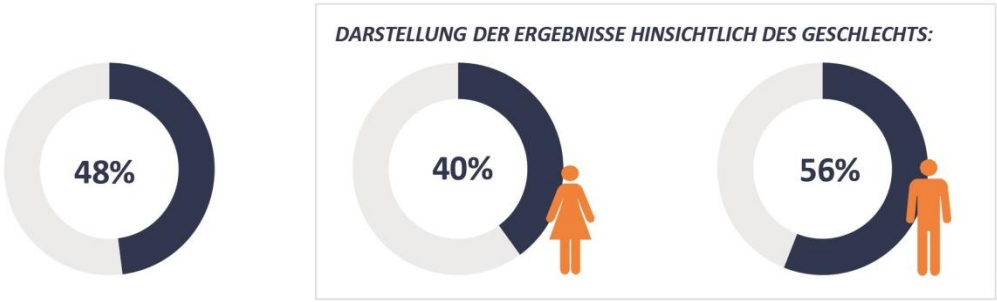
Neun von zehn Befragten werten Sicherheit im digitalen Raum als sehr wichtig (Abbildung 7). Diese Wichtigkeit unterscheidet sich noch einmal gemäß ihrer Online-Kompetenz (Skala: 1 = Anfänger und 5 = Experte). Mit höherer Kompetenz wird auch das Thema Sicherheit wichtiger. Während 84 Prozent der Anfänger (Online-Kompetenz = 1 oder 2) Sicherheit im digitalen Raum als wichtig erachten, sind es bei den Expertinnen und Experten (Online-Kompetenz = 4 oder 5) 91 Prozent.



Darstellung: Top-2-Boxes (stimme voll und ganz/eher zu) in Prozent.
Basis: n=2.002 Fälle.
Quelle: Umfrage von Ipsos im Auftrag des Bundesamts für Sicherheit in der Informationstechnik.

Abbildung 7: Sicherheit im digitalen Raum ist mir persönlich sehr wichtig.

Obwohl Sicherheit im digitalen Raum eine große Rolle spielt, geben weniger als die Hälfte der Befragten an, sich persönlich sehr gut mit diesem Thema auszukennen (Abbildung 8). Diese Kenntnisse unterscheiden sich deutlich hinsichtlich des Geschlechts. Nur 40 Prozent der Frauen geben an, sich sehr gut mit dem Thema Sicherheit im Internet auszukennen. Bei den Männern sind es hingegen 56 Prozent. Hierbei ist darauf hinzuweisen, dass es sich bei den Werten um eine Selbsteinschätzung der jeweiligen Befragten handelt.



Darstellung: Top-2-Boxes (stimme voll und ganz/eher zu) in Prozent.
Basis: n=2.002 Fälle.
Quelle: Umfrage von Ipsos im Auftrag des Bundesamts für Sicherheit in der Informationstechnik.

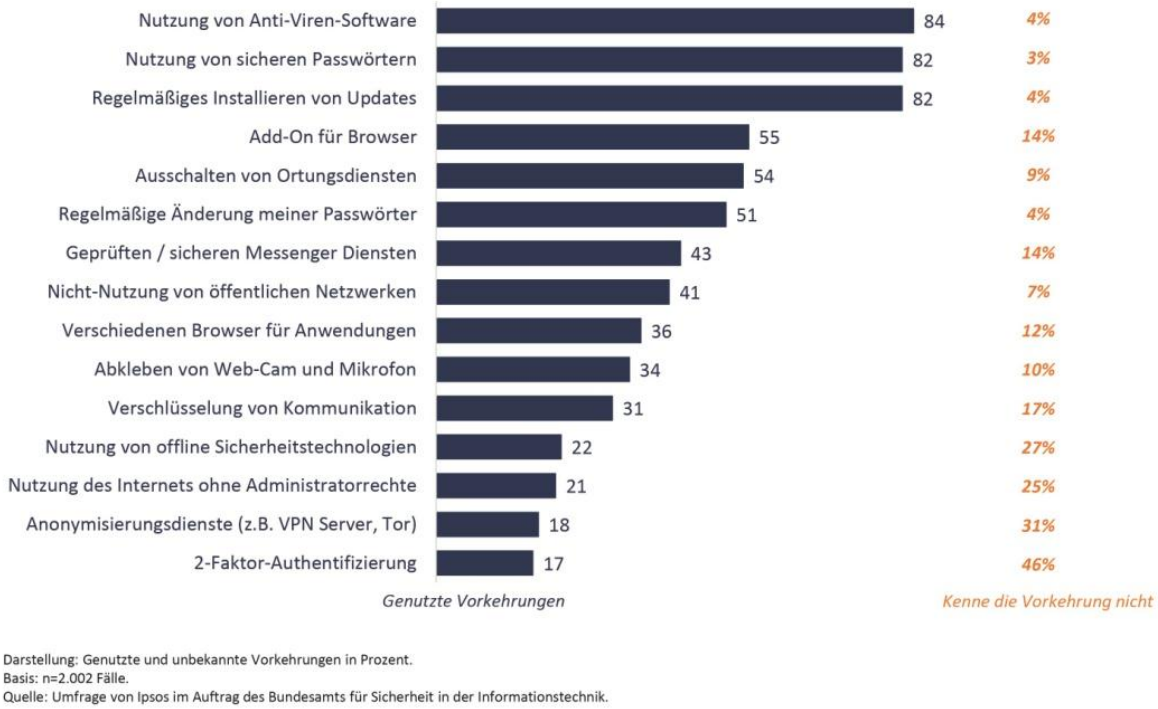
Abbildung 8: Ich kenne mich persönlich sehr gut mit dem Thema Sicherheit im Internet aus.

Vorkehrungen, um sich im Internet zu schützen

Da der Sicherheit im digitalen Raum seitens der Befragten eine hohe Bedeutung beigemessen wird, stellt sich die Frage, welche entsprechenden Vorkehrungen genutzt werden, um sich im Internet zu schützen (Abbildung 9). Mit Abstand am häufigsten werden **Anti-Viren-Software, sichere Passwörter** sowie regelmäßiges Installieren von **Updates** als Vorkehrung genutzt (84 Prozent). Sichere Passwörter werden zwar genutzt, aber nur von rund der Hälfte der Befragten regelmäßig geändert. Mehr als die Hälfte der Befragten nutzt als Vorkehrung ein Add-On für Browser oder schaltet Ortungsdienste aus, 14 Prozent geben an, dass sie Add-Ons für Browser nicht kennen. Die geringste Nutzung (weniger als ein Fünftel) wird bei Anonymisierungsdiensten (z.B. VPN, Server, Tor) und 2-Faktor-Authentifizierung verzeichnet. Es kann vermutet werden, dass die Nutzung dieser beiden Vorkehrungen durch eine gesteigerte Bekanntheit erhöht werden könnte (31 Prozent kennen Anonymisierungsdienste nicht, bei der 2-Faktor-Authentifizierung sind es 46 Prozent).

Barrieren für die Nutzung von Schutzmaßnahmen

Das größte Hemmnis wird in den **zu hohen Kosten** (38 Prozent) gesehen. Mehr als ein Drittel gibt eine **schwere Verständlichkeit**, zu wenig vorhandene Informationen sowie eine **schlechte Bedienbarkeit** als Hindernis für die Nutzung von Sicherheitsmaßnahmen an. Ein geringerer Teil gibt hier Zeitmangel (24 Prozent) und persönliches Desinteresse (20 Prozent) an. Hieraus könnten sich konkrete Lösungsmöglichkeiten ergeben, die Lücke zwischen Wissen und Anwendung zu schließen, da die Mehrheit demnach durchaus Interesse daran hat, die Sicherheit zu verbessern.



Darstellung: Genutzte und unbekannte Vorkehrungen in Prozent.
Basis: n=2.002 Fälle.
Quelle: Umfrage von Ipsos im Auftrag des Bundesamts für Sicherheit in der Informationstechnik.

Abbildung 9: Um die eigenen Daten zu schützen, gibt es eine Vielzahl an Möglichkeiten

Informiert sein und bleiben – eine überfordernde Aufgabe für Nutzerinnen und Nutzer

In der **qualitativen Online-Community** zeigt sich, dass das Thema Sicherheit im digitalen Raum zwar wichtig ist, viele Befragte sich jedoch **nicht aktiv darüber informieren**. Oft gibt es einen externen Auslöser in den allgemeinen Medien, der zu einer Auseinandersetzung mit dem Thema führt. Ein solcher Auslöser war beispielsweise die weltweite Cyber-Attacke mit der Schadsoftware “WannaCry“.

Befragte empfinden das Thema Sicherheit im digitalen Raum generell als **nicht leicht verständlich** und sie **schätzen die eigenen Vorkenntnisse zur Thematik als gering ein**. Diese Aspekte unterstützen eine gefühlte Überforderung und damit die Tatsache, dass Nutzerinnen und Nutzer sich nicht regelmäßig und tiefgründig informieren. So hat eine gefühlt zeitaufwändige Recherche neben Alltagsaufgaben kaum Platz. Die täglich neuen Entwicklungen in dem Bereich geben das Gefühl, dass es **schwer ist, auf dem Laufenden zu bleiben**. Das ständige Informieren über Vorsichtsmaßnahmen **verdirbt den Spaß** an der Internetnutzung. Befragte haben zudem das Gefühl, dass ihr Informationsstand ein Hacken großer Anbieterseiten (z.B. Amazon) nicht verhindern kann. De facto existiert in diesen Fällen eine **Hilflosigkeit des Einzelnen**. Nur der Verzicht z.B. auf Online-Banking und -Shopping würde einen Schutz gewährleisten, was oft aus Gründen der **Bequemlichkeit** abgelehnt wird.

Die Diskussion in der Community zeigt, dass das Gefühl, sich nicht gut genug auszukennen, häufig **verdrängt** wird, wie diese Befragte schildert: *„Ich fühle mich nur sicher, weil ich die Unsicherheit verdränge, besonders bei FB und Google, die meine Daten nutzen.“* (W2, 27). Es besteht bei vielen Personen eine **kognitive Dissonanz**, also ein Spannungszustand zwischen dem gefühlt wichtigen Thema Informationssicherheit auf der einen und der Überforderung und Tatenlosigkeit auf der anderen Seite**.** Dieser als unangenehm empfundene Zustand wird durch das Finden von Ausflüchten kompensiert, um so wieder in einen konsistenten Zustand zu gelangen (Altersgruppen übergreifend).

Informationsquellen zum Thema Sicherheit im digitalen Raum

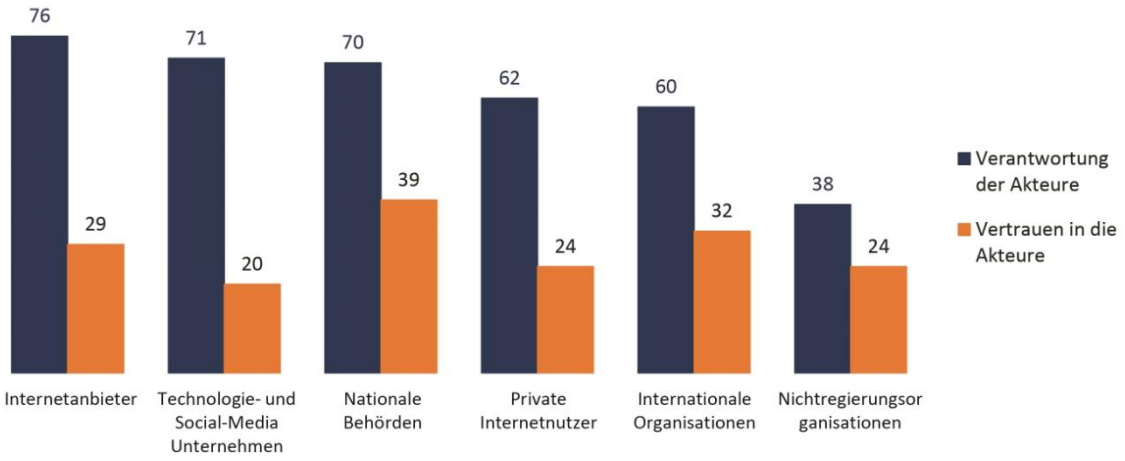
Relevante Informationsquellen sind vor allem **Bekannte und Verwandte**. Ihnen wird vertraut und in der Online-Community bilden sie die wichtigste Quelle. Spezielle **IT-Webseiten für Fachinformationen** (z.B. Chip.de, Heise.de, Golem.de) werden an zweiter Stelle genannt. Von Relevanz sind auch **Nachrichten-Webseiten** mit weniger fachspezifischen Informationen als Kerninhalt (z.B. Spiegel.de, Zeit.de, FAZ.de). Dies stützt die Annahme, dass besonders punktuell Informationen eingeholt

werden. Nämlich dann, wenn in den Medien ein neuer Sicherheitsvorfall diskutiert wird. Informationsangebote des Bundes werden kaum genannt. „Sicher-im-netz.de“ und „BSI-fuer-buerger.de“ wurden nur von zwei Befragten erwähnt.

3.4.2 Maßnahmen zur Erhöhung der Informationssicherheit

Akteure und ihre Verantwortung

Bei der Frage, welche Akteure bei der Herstellung von Sicherheit im digitalen Raum die größte **Verantwortung** tragen sollten, nennen die Befragten die **Internetanbieter, die Technologie- und Social-Media-Unternehmen** sowie die **nationalen Behörden** am häufigsten. Die geringste Relevanz hinsichtlich der Verantwortung wird bei den NGOs (38 Prozent) gesehen.



Darstellung: Top-2-Boxes (große Verantwortung vs. vertraue voll und ganz/vertraue eher) in Prozent.
Basis: n=2.002 Fälle.
Quelle: Umfrage von Ipsos im Auftrag des Bundesamts für Sicherheit in der Informationstechnik.

Abbildung 10: Verantwortung vs. Vertrauen in die Akteure zur Sicherheit im Internet

Das meiste **Vertrauen** (39 Prozent) wird **nationalen Behörden** entgegengebracht. Die größte **Diskrepanz** hinsichtlich Verantwortung und Vertrauen gibt es **bei den Technologie- und Social-Media Unternehmen**: Ihnen wird eine hohe Verantwortung zugeschrieben, sie genießen bei den Befragten allerdings das geringste Vertrauen. Ähnlich ist es bei Internetanbietern. Nur 29 Prozent vertrauen ihnen, obwohl ihnen mehr als drei Viertel eine hohe Verantwortung zuschreiben (Abbildung 10).

Interessant ist dabei, in welcher Verantwortung sich **Nutzerinnen und Nutzer selbst** bei dem Thema sehen. In der Community wurde diese Frage diskutiert. Es sind sich fast alle einig, dass ein **jeder für seine individuelle digitale Sicherheit selbst verantwortlich** ist. Dazu gehört das bereits beschriebene Abwägen, welche Seiten man aufruft, welche Daten man herunterlädt oder teilt und das Installieren und Updaten eines Antivirusprogramms.

> *„In den eigenen vier Wänden **sorgt man auch selbst für seine Sicherheit**, dementsprechend auch im WWW. In der Verantwortung sehe ich allerdings genauso Medien (digital, als auch analog), um uns stets auf den aktuellsten Stand der Technik zu halten / bringen.“ (M2, 29 Jahre)*

> *„In erster Linie **hat man Eigenverantwortung**, in dem man vernünftig mit dem Internet umgeht und vor allen Dingen ein Virenschutzprogramm auf allen internetfähigen Geräten hat. Aber auch alle Firmen und Anbieter stehen in der Pflicht, die Daten der Kunden zu sichern und zu schützen.“ (M3, 47 Jahre)*

Die Online-Community verdeutlicht, wie der hohe Verantwortungs-Wert der Internetanbieter, Technologie- und Social-Media-Unternehmen zu verstehen ist: Die Nutzerinnen und Nutzer fürchten um ihren Datenschutz und fordern, dass die Unternehmen für Sicherheit auf ihren Seiten sorgen und persönliche Daten schützen. Die Befragten sehen keine Einflussmöglichkeiten, weswegen sie sich auf die Betreiber verlassen müssen. Die Politik wird von den Befragten der Community als wichtig empfunden, um einen rechtlichen Rahmen zu geben, der für Sicherheit im Internet sorgt. Hierzu wird auch eine schärfere Strafverfolgung gezählt. Die Schwierigkeit bestehe darin, zeitnah Einfluss zu nehmen. Befragte kritisieren, dass politische Maßnahmen oft sehr langsam vorangehen und daher in einer sich schnell ändernden, dynamischen Umgebung wenig Nutzen haben. Dies gibt erklärende Hinweise auf die große Differenz von 31 Prozentpunkten zwischen gesehener Verantwortung und Vertrauen in die nationalen Behörden in der quantitativen Erhebung.

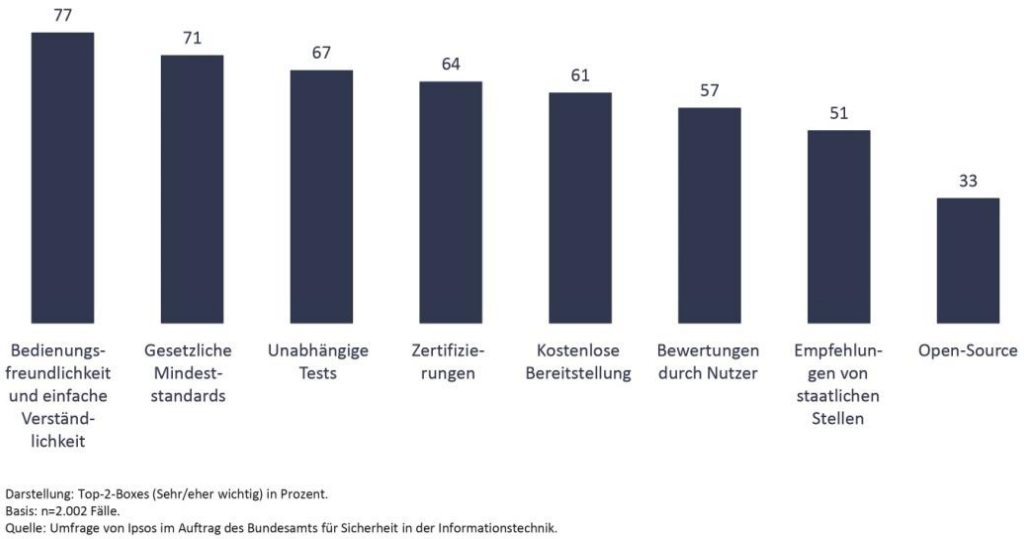


Abbildung 11: Wie wichtig sind Ihnen dabei die folgenden Aspekte, um Ihr Vertrauen in die Sicherheit dieser Produkte und Services zu stärken?

Wie kann Vertrauen in die Sicherheit von Produkten und Services geschaffen werden?

Die Frage zur Stärkung von Vertrauen wird von 77 Prozent der Befragten mit Bedienungsfreundlichkeit und einfacher Verständlichkeit von Sicherheitsmaßnahmen beantwortet (Abbildung 11). Auch tragen gesetzliche Mindeststandards (71 Prozent) und unabhängige Tests (67 Prozent) zur Stärkung des Vertrauens in die Sicherheit bei. Interessanterweise werden **Bewertungen durch Nutzer** (57 Prozent) **vertrauensfördernder bewertet als Empfehlungen von staatlichen Stellen** (51 Prozent). Hier liegt die Vermutung nahe, dass bei Bewertungen durch Nutzer eine größere Vielfalt (z.B. bezüglich Anzahl oder Themenvielfalt) gesehen wird. Ein breites Spektrum an Erfahrungsberichten seitens der Nutzerinnen und Nutzer ermöglicht eine individuelle Suche nach Informationen zu Produkten und Services, die vertrauensbildend wirken können. Bei den Empfehlungen seitens staatlicher Behörden wird das Vertrauen durch zwei Aspekte gemindert. Zum einen wird eine mangelnde Aktualität kritisiert, zum anderen sind Empfehlungen weniger individuell als z.B. Nutzerbewertungen.

Sicherheitstest, Sicherheitsrichtlinien und **klare Haftungsregelungen** würden laut zwei Dritteln der Befragten mehr Sicherheit im digitalen Raum schaffen (Abbildung 12). Die Sicherheitsrichtlinien sowie die klaren Haftungsregelungen verdeutlichen erneut die Verantwortung des Staates, mehr Sicherheit im digitalen Raum zu gewährleisten. Nur vier von zehn Befragten sehen in der Schaffung von weiteren Anreizen (z.B. Entlohnung für das Aufdecken von Sicherheitslücken) eine Voraussetzung für mehr Sicherheit im digitalen Raum, um bestehende Sicherheitslücken zu schließen.

Abbildung 12: Welche Voraussetzungen müssen für Sicherheit im digitalen Raum erfüllt sein?

Konkrete Maßnahmen, um Sicherheit im digitalen Raum zu fördern, sind unter anderem auch **Zertifizierungen und Siegel**. Diese können für IT-Produkte und ihre Sicherheitseigenschaften vergeben werden. In der Online-Community haben Befragte diskutiert, inwiefern es sinnvoll ist, solche Systeme auch für ganze Webseiten zu implementieren. Die Kennzeichnung von sicheren Webseiten wird besonders für solche als wichtig erachtet, auf denen personenbezogenen Daten erhoben und Geschäfte getätigt werden. **Um Vertrauen in eine solche Kennzeichnung zu schaffen, ist jedoch die Beteiligung eines unabhängigen Gremiums zentral**. Dies könne von staatlichen Institutionen, namhaften Zertifizierungsgesellschaften (z.B. TÜV) oder Expertinnen und Experten gestellt werden. Eine zentrale Webseite, die alle als sicher gekennzeichneten Internetseiten verzeichnet, könnte – so die Befragten der Online-Community – Missbrauch vorbeugen. Auf diese Weise kann eine eigene Validierung vorgenommen werden.

Stärkere Bestrafung bei Regelverstößen

Eine angemessene Bestrafung von Internetkriminalität wurde in der Online-Community von einer Vielzahl Teilnehmender diskutiert. Härtere Strafen werden als nötig betrachtet, um ein Gefühl der Sicherheit zu schaffen. Vor allem soll die Bundesrepublik „Internetkriminelle“, wie Hacker, strafrechtlich verfolgen. Ermöglicht werden sollte dies idealerweise durch den Einsatz von Spezialisten, die speziell in dem Bereich Internetkriminalität geschult sind.

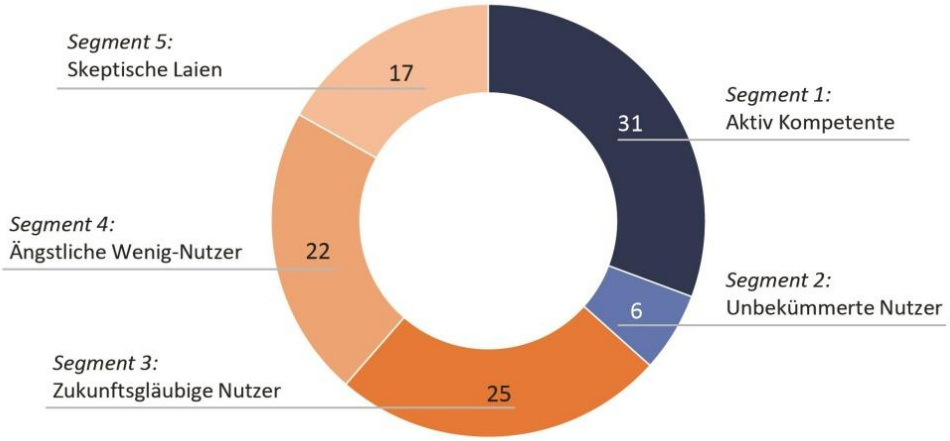
> *„Dubiose Seiten müssten prompt gesperrt werden, **Hackerangriffe vereitelt und härter bestraft werden**, Fakeaccounts gelöscht werden und Scheinfirmen dürften im Netz nicht auftauchen.“ (W5, 26)*

3.5 Überblick über die Segmente

Die Bevölkerung bildet in ihren Wahrnehmungen, Meinungen und Einstellungen gegenüber dem digitalen Raum keine homogene Gruppe. Eine Segmentierung ist ein multivariates Verfahren, mit dem diese Heterogenität der Bevölkerung dargestellt werden kann. Das Hauptziel ist die Aufdeckung verschiedener gesellschaftlicher Gruppen, die sich voneinander abgrenzen, aber in sich Menschen mit homogenen Werten oder Bedürfnissen vereinen. Somit lassen sich **Typologien sozialer Lagen oder Milieus** erstellen, die nicht nur auf rein objektiven Kriterien wie Einkommen oder Bildungsgrad

basieren, sondern auch subjektive Einstellungen berücksichtigen[2]. Anhand einer solchen Gruppierung lässt sich die **natürliche Heterogenität innerhalb einer Gesellschaft** besser verstehen und einordnen. Ebenso ist es möglich, auf dieser Basis zielgruppenspezifische Kommunikation zu entwickeln.

Das multivariate Verfahren zur Berechnung der Segmente bezog die Einstellung (positiv oder negativ) gegenüber dem Begriff „Digitalisierung“ und negative Erfahrungen der Befragten mit Internetanwendungen ein. Die Analyse ergab eine Einteilung in **fünf Segmente** (vgl. Abbildung 13), die unterschiedliche Einstellungen und Verhaltensweisen der Gesellschaft gegenüber dem und im digitalen Raum widerspiegeln. Diese unterscheiden sich besonders durch die Aspekte Online-Kompetenz, Einstellung gegenüber Risiken im digitalen Raum sowie der Intensität der Internetnutzung. Die Differenzierung der Nutzerinnen und Nutzer legt nahe, die offensichtlich heterogene digitale Gesellschaft mit zielgruppenspezifischen Maßnahmen zu adressieren.



Darstellung in Prozent.
Basis: n=2.002 Fälle.
Quelle: Umfrage von Ipsos im Auftrag des Bundesamts für Sicherheit in der Informationstechnik.

Abbildung 13: Übersicht über die Segmente

Aktiv Komponente: ‚Aaktiv Kompetente‘ verfügen über eine hohe Online-Kompetenz und die Befragten geben an, sich persönlich sehr gut mit dem Thema Sicherheit im Internet auszukennen. Online-Aktivitäten werden von ihnen mit einem überdurchschnittlich hohen Risiko bewertet, weshalb sie sich bestmöglich selbst schützen.

Unbekümmerte Nutzer: ‚Unbekümmerten Nutzern‘ ist die Datensicherheit im Vergleich am unwichtigsten. Damit einhergehend haben sie weniger Ängste und Bedenken bei der Internetnutzung und die Risiken in Bezug auf Online-Aktivitäten werden im Vergleich am niedrigsten eingestuft.

Zukunftsgläubige Nutzer: ‚Zukunftsgläubige Nutzer‘ bewerten Digitalisierung (sehr) positiv. Sie weisen eine gute Online-Kompetenz auf sowie eine häufige Internetnutzung. Online-Aktivitäten bewerten ‚zukunftsgläubige Nutzer‘ im Vergleich mit einem geringen Risiko.

Ängstliche Wenig-Nutzer: ‚Ängstlichen Wenig-Nutzern‘ ist Sicherheit im digitalen Raum sehr wichtig. Sie haben die größten Ängste und Bedenken, wenn sie das Internet nutzen. Ihre Online-Kompetenz liegt unter dem Durchschnitt und sie weisen eine geringe Internetnutzung auf.

Skeptische Laien: ‚Skeptische Laien‘ verfügen im Vergleich über die geringste Online-Kompetenz. Online-Aktivitäten verbinden sie mit großen Risiken. Darüber hinaus weisen Sie eine höhere Wahrscheinlichkeit auf, negative Erfahrungen mit Internetanwendungen gemacht zu haben. ‚Skeptische Laien‘ stehen der Digitalisierung am negativsten gegenüber.

[2] Vergleiche Rössel, Jörg (2005): Plurale Sozialstrukturanalyse. Eine handlungstheoretische Rekonstruktion der Grundbegriffe der Sozialstrukturanalyse. VS Verlag: Wiesbaden.

4 Fazit

Die Studienergebnisse weisen für viele Nutzerinnen und Nutzer große Wissensdefizite beim sicheren Umgang mit digitalen Technologien aus. Insgesamt 39 Prozent der Befragten hegt vor allem aufgrund fehlender Kenntnisse über Funktionsweise und Risiken der Technik erhebliche Vorbehalte gegenüber ihrer Verwendung. Nur wenn diese ausgeräumt werden und Wissen für einen sicheren Umgang mit digitaler Technologie vermittelt wird, kann das notwendige Vertrauen hergestellt werden, um die sozialen und wirtschaftlichen Chancen der Digitalisierung tatsächlich auszuschöpfen.

Bei der Bewertung der Gefahren im Umgang mit digitalen Technologien stehen für viele Befragten die Sorge um Datenschutz und Datensicherheit im Internet im Vordergrund; Risiken von z.B. Wearables werden demgegenüber als gering eingeschätzt. Für den souveränen und verantwortungsvollen Umgang mit digitalen Technologien und ein breites Verständnis für die Tragweite des digitalen Wandels muss „Digitalisierung“ über bloße Schlagworte hinaus mit Leben gefüllt werden.

Vorhandene Angebote sind noch wenig bekannt, gelten als komplex oder schwer verständlich. Die Nutzerinnen und Nutzer führen ihre Informationsdefizite z.T. auf die eigene Bequemlichkeit zurück. Informationen zur Digitalisierung und ihrer Risiken sollten auf mehr Kanälen als bisher vermittelt werden. Dazu bieten sich Kooperationen zwischen den Informanten und Multiplikatoren (wie z.B. zivilgesellschaftlichen Organisationen, welche die Informationen in den Communities verbreiten) an.

Die Interviews weisen neben Infomaterialien auch Veranstaltungen als ein geeignetes Mittel aus, über Risiken, Gefahren und Gegenmaßnahmen im digitalen Raum öffentlichkeitswirksam aufzuklären. Auch durch persönliche Kontakte werde der Eindruck von Kompetenz und Vertrauenswürdigkeit vermittelt. Als wichtige vertrauensbildende Faktoren stellen sich zudem die Fachkompetenz und personelle Expertise, eine weitestgehende Skandalfreiheit, eine Gemeinwohl-orientierte Zielausrichtung sowie transparentes, unabhängiges und eigenbestimmtes Handeln der jeweiligen Akteure dar.

Die Online-Befragung zeigt den Wunsch der Bevölkerung nach staatlicher Regulierung und staatlichen Maßnahmen wie Sicherheitstests, Sicherheitsrichtlinien und klaren Haftungsregeln für die digitale Sphäre auf. Behördliche Informationen werden als sehr verlässlich und vertrauenswürdig bewertet. Die Interviews weisen das BSI, die Datenschutzbeauftragten und zivilgesellschaftliche Organisationen/NGOs als besonders kompetent und vertrauenswürdig aus. Demzufolge dürfte eine staatliche Stelle – unterstützt durch zivilgesellschaftliche Organisationen – die besten Aussichten haben, als vertrauenswürdige Informationsquelle im Bereich der Informationssicherheit angenommen zu werden. Den Expertinnen und Experten folgend sollte nicht eine staatliche Stelle allein die Erarbeitung und Bereitstellung der Informationen verantworten. Eine möglichst große Expertise und zugleich Unabhängigkeit könne durch ein Gremium aus zivilgesellschaftlichen Organisationen erreicht werden, das z.B. beim BSI angesiedelt sein könnte. Als Voraussetzung für die Vertrauenswürdigkeit des Gremiums wurde Transparenz in der Besetzung und der Arbeitsweise genannt.

Ein derartiges Experten-Gremium könnte auch bei der Einführung einer Kennzeichnung von Produkten bezüglich ihrer IT-Sicherheit eine maßgebliche Rolle einnehmen. Die Kennzeichnung von IT-Sicherheit (Zertifizierung/Siegelvergabe) stellt dabei überdies eine vielversprechendste Grundlage für eine Haftungsregelung dar. Aus der Onlinebefragung und den Interviews leitet sich die (freiwillige) Zertifizierung von IT-Produkten als hilfreich ab, etwa nach dem Vorbild der TÜV-Prüfsiegel oder den Produkttests der Stiftung Warentest. Zertifikate bergen allerdings die Gefahr, dass Nutzerinnen und Nutzer ohne kritische Reflexion darauf vertrauen und auf den Wissenserwerb zu Sicherheitsrisiken und deren Bekämpfung verzichten. Zertifizierung kann nur einen Baustein in einer größer angelegten Kampagne bilden, die auf unterschiedlichen Kanälen in unterschiedlicher Detailtiefe über Fragen der Sicherheit digitaler Technologie aufklärt. Flankierend sollte dieser Prozess durch Anreize zur Steigerung der Informationssicherheit begleitet werden. Hier nimmt das Thema Haftung eine wichtige Rolle ein. Auch in diesem Kontext wird der Anspruch der gemeinschaftlichen und transparenten Gestaltung zum Einbringen einer zivilgesellschaftlichen Perspektive und Expertise in der Befragung deutlich.