DENN SICHERHEIT KOMMT VON VERANTWORTUNG

10 JAHRE DSIN

DsiN SicherheitsIndex 2016

Digitale Sicherheitslage der Verbraucher in Deutschland

Schirmherrschaft:

Bundesministerium des Innern

DsiN Deutschland sicher im Netz

www.sicher-im-netz.de

Ulrich Kelber

FÜR EINE DIGITALE AUFKLÄRUNG 2.0

Die Vernetzung des digitalen Alltags eröffnet allen Verbraucherinnen und Verbrauchern ein breites Spektrum an neuen Möglichkeiten: von der sozialen Kommunikation im privaten und beruflichen Umfeld, über Erledigungen wie Einkaufen, Reisebuchungen und Bankgeschäfte, Erleichterungen etwa bei Preisvergleichen und Informationsrecherchen bis hin zu neuen Angeboten im Bereich der Mobilität oder der Gesundheitsdienste.

Die Chancen für sämtliche Generationen sind vielfältig. Gerade für ältere Menschen können digitale Dienste eine Bereicherung darstellen, die sie von der persönlichen Mobilität ein Stück weit unabhängig machen. Voraussetzung für eine Entfaltung der digitalen Chancen im Alltag der Verbraucher ist aber, dass sie sicher genutzt werden können und das Vertrauen in die Dienste nicht enttäuscht wird.

Der DsiN-Sicherheitsindex ist ein anschaulicher Gradmesser zur Sicherheitslage der Verbraucher in Deutschland. Die Darstellung der Sicherheitslage in einer Kennziffer gibt Auskunft über den aktuellen Status, und das nun im dritten Jahr. Erfreulich ist, dass die Kennzahl des Sicherheitsindex erneut leicht angestiegen ist. Dies ist darauf zurückzuführen, dass die Zahl der registrierten Sicherheitsvorfälle bei den Verbrauchern zurückgegangen ist.

Zugleich ist aber die gefühlte Verunsicherung gewachsen. Und das digitale Sicherheitsgefälle in Deutschland ist weiterhin ein Faktum, denn fast zwei Drittel aller Nutzer benötigen zusätzliche Hilfestellungen. Hier zeigt der Index Anknüpfungspunkte, wie Verbraucherinnen und Verbrauchern über Aufklärungsarbeit mehr Schutz und Sicherheit vermittelt werden kann.

Das Verbraucherschutzministerium engagiert sich seit Jahren für eine digitale Aufklärung: Wir unterstützen Projekte, die durch die Vermittlung von digitalen Kompetenzen auch die Sicherheit der Nutzer im Umgang mit digitalen Diensten verbessern. Dazu haben wir im vergangenen Jahr mit DsiN im Verbund mit der Bundesarbeitsgemeinschaft der Senioren-Organisationen (BAGSO) den Digital-Kompass gestartet, der Menschen der älteren Generationen bei der sicheren Nutzung des Internets unterstützen soll.

Ich wünsche Ihnen eine angenehme und aufschlussreiche Lektüre!

Ulrich Kelber
Parlamentarischer Staatssekretär beim Bundesminister
der Justiz und für Verbraucherschutz

Dr. Thomas Kremer

Dr. Michael Littger

Denn Sicherheit kommt von Verantwortung

Bereits im dritten Jahr misst der DsiN-Sicherheitsindex die digitale Sicherheitslage der Verbraucher in einer Kennzahl. Die gute Nachricht ist: Zum zweiten Mal in Folge sind sicherheitsrelevante Vorfälle leicht rückläufig. Das Wissen und die Anwendungsbereitschaft zu Schutzmaßnahmen bei Verbrauchern steigen. Dennoch: Kein Grund zum Ausruhen.

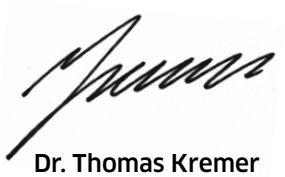
Trotz positiver Trends steigt bei Verbrauchern die Unsicherheit im Umgang mit dem Internet. Auch die Schere zwischen Kenntnis und Nutzung von Schutzmaßnahmen geht weiter auseinander. Dabei fällt auf, dass gerade in neuen digitalen Lebenswelten wie dem vernetzten Fahren Unsicherheiten entstehen; sie werden in diesem Jahr erstmals untersucht.

Es kann auch nicht zufrieden stellen, dass wir ein erhebliches Sicherheitsgefälle zwischen unterschiedlichen Nutzertypen in Deutschland beobachten: Während sich die Gruppe der „Souveränen“ relativ sicher im Netz bewegt, erreichen die Gruppen der „Fatalisten“ mit überwiegend jüngeren Vielnutzern und der „Außenstehenden“ mit vielen älteren Menschen insgesamt nur niedrigere Indexwerte. Das wollen, das müssen wir ändern!

Der DsiN-Sicherheitsindex in Partnerschaft mit TNS Infratest hilft uns besser zu verstehen, wie sich die Sicherheitslage der Verbraucher im Netz darstellt – und welche Anforderungen an eine wirksame Aufklärungsarbeit gestellt werden müssen. Hier zeigt unser aktueller Index einen übergreifenden Trend, Menschen stärker auch zur Umsetzung von Sicherheitswissen zu motivieren. Bei neuen digitalen Lebensfeldern dominiert das Informationsbedürfnis – auch hier werden wir Hilfestellungen anbieten.

Eine erfolgreiche Aufklärungsarbeit muss auf den Dialog mit allen Akteuren der Digitalisierung setzen: Staat, Wirtschaft und Anwender. Wir alle tragen Verantwortung für die Sicherheit und müssen sie auch wahrnehmen.

Wir laden Sie herzlich zum Austausch über die neuen Erkenntnisse ein!



Dr. Thomas Kremer
Vorstandsvorsitzender
Deutschland sicher im Netz e.V.

Dr. Michael Littger
Geschäftsführer
Deutschland sicher im Netz e. V.

Inhalt

Ergebnisse 2016 auf einen Blick

Der DsiN-Sicherheitsindex verbessert sich 2016 zum zweiten Mal in Folge auf inzwischen 65,4 Indexpunkte. Die Gründe dafür sind ein Rückgang der sicherheitsrelevanten Vorfälle aufseiten der Bedrohungslage sowie ein Zuwachs bei der Sicherheitskompetenz und dem Sicherheitsverhalten der Verbraucher[1] aufseiten des Schutzniveaus (dazu Kapitel 1).

Auch in diesem Jahr differenziert der DsiN Sicherheitsindex wieder zwischen vier Verbrauchertypen. Es zeigt sich dabei erneut ein deutliches Sicherheitsgefälle zwischen den Gruppen (dazu Kapitel 2): Die niedrigsten Werte erreichen in diesem Jahr die Fatalisten mit 52,5 Indexpunkten. An der Spitze liegen mit dem höchsten Wert die Souveränen mit 74,7 Indexpunkten. Eine nähere Untersuchung der Verbrauchertypen zeigt Anknüpfungspunkte, um das Sicherheitsniveau durch eine individuelle Ansprache zu erhöhen – und dem Sicherheitsgefälle entgegenzuwirken. Für Aufklärungsarbeit ist dies eine zentrale Erkenntnisgrundlage, um die Sicherheitslage der deutschen Onliner weiter zu verbessern.

Diskrepanz von Schutzkenntnissen und Umsetzung

Ein zentrales Ergebnis der Studie betrifft auch das Verhältnis von Sicherheitskompetenzen der Verbraucher und ihrem Sicherheitsverhalten. Innerhalb aller Verbrauchergruppen hat sich die Diskrepanz zwischen Sicherheitswissen und –verhalten verfestigt: Das Wissen um Schutzmaßnahmen steigt erneut stärker als Motivation und Befähigung ihrer Anwendung. Vor allem bei den Nutzergruppen der Gutgläubigen (62,3 Indexpunkte), der Fatalisten (52,5) und der Außenstehenden (54,7) liegen hier typische Defizite.

Erfreulich ist, dass die Sicherheitslage aller Verbrauchergruppen insgesamt gegenüber dem Vorjahr besser ist, allerdings auf einem noch immer relativ niedrigen Niveau. So zeigen alle Gruppen einen leichten Anstieg bei Sicherheitswissen sowie auch dem Schutzverhalten. Am stärksten verbesserten sich die außenstehenden Nutzer, wenn gleich sie auch weiterhin deutlich unter dem Sicherheitsniveau aller Onliner agieren.

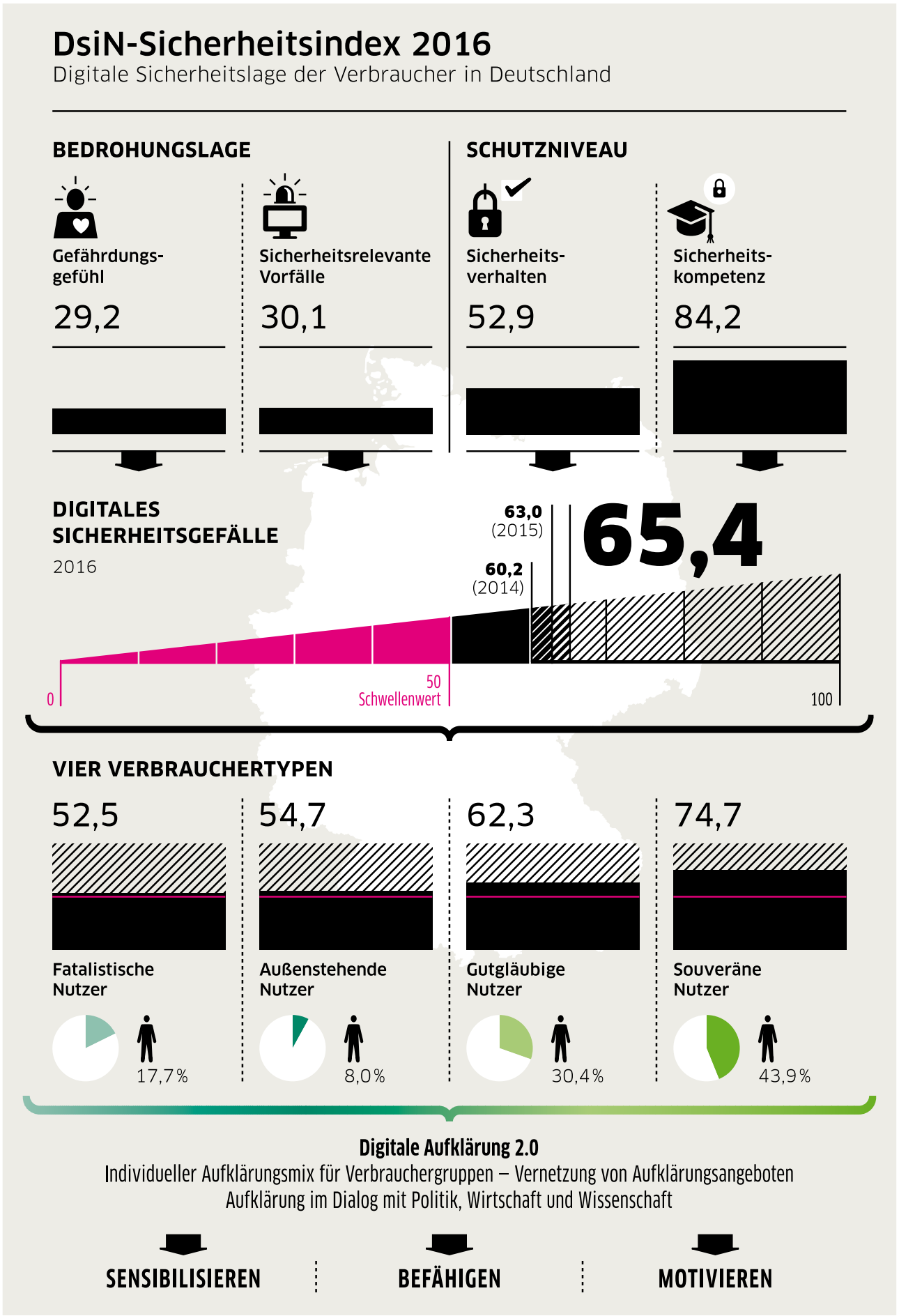
Trotz einer verbesserten Sicherheitslage ist gegenüber dem Vorjahr die Verunsicherung insgesamt merklich gestiegen: Und zwar bei sämtlichen Verbrauchergruppen. Hier ist ein Paradox zwischen objektiver Sicherheitslage und subjektiver Bedrohung erkennbar, dessen Fortschreibung das Risiko einer digitalen Vertrauenskrise birgt.

Verstärkter Aufklärungsbedarf für 60 Prozent der Verbraucher

Weit über die Hälfte der deutschen Onliner – die Gruppe der Fatalisten, Gutgläubigen und der Außenstehenden – bedürfen damit zusätzlicher Unterstützung. Erforderlich sind Maßnahmen der Sensibilisierung und Befähigung sowie vor allem der Motivation (dazu Kapitel 4). Dies gilt in besonderem Maße für die Fatalisten, denen meist jüngere Menschen angehören. Dieses Bedürfnis verstärkt sich mit der Vernetzung neuer Lebensbereiche (dazu Kapitel 3). Der diesjährige DsiN-Sicherheitsindex hat 2016 dazu erstmals die Lage zum vernetzten Verkehrsraum untersucht, bei dem die Verunsicherung von Verbrauchern teilweise auf die Neuartigkeit zurückgeführt werden kann.

* Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben stets auf Angehörige aller Geschlechter.

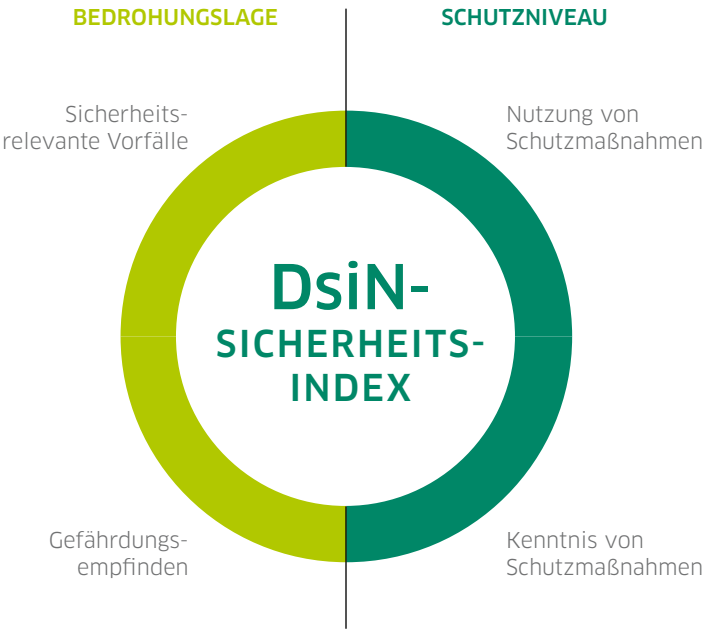
Abb. 1. DsiN-Sicherheitsindex 2016



Ziel und Methode des Sicherheitsindex

Der Sicherheitsindex von Deutschland sicher im Netz e.V. errechnet die digitale Sicherheitslage der deutschen Verbraucher in einer zentralen Kennziffer. Darüber hinaus unterscheidet der Index nach vier verschiedenen Nutzertypen, die eine direkte Vergleichbarkeit der Sicherheitslage bei den Verbrauchergruppen ermöglicht. Sie sind im Wesentlichen auf Unterschiede beim individuellen Risikoverhalten, dem Wissensstand sowie der Handlungsbereitschaft zurückzuführen. Übergreifend untersucht der Index fünf Lebenswelten der Digitalisierung: Erneut werden digitale Gesundheits- und Vitaldienste, Haus- und Heimvernetzung, Einkaufen im Internet sowie Online-Banking betrachtet. Darüber hinaus bindet der Index 2016 erstmals den vernetzten Verkehrsraum mit dem Fokus Automobil ein.

Abb. 2. Berechnung des DsiN-Sicherheitsindex: Kombination aus Bedrohungslage und Schutzniveau



Dynamisches Verhältnis von Bedrohungslage und Schutzniveau

Grundlage des Sicherheitsindex ist eine repräsentative Befragung bei mehr als 2.000 Internetnutzern in Deutschland durch das Markt- und Meinungsforschungsinstitut TNS Infratest. Um die Sicherheitslage abzubilden, untersucht der Index einerseits die Bedrohungslage und andererseits das Schutzniveau der Verbraucher. Für die Ermittlung der Bedrohungslage wurden die konkreten Sicherheitsvorfälle sowie das Gefährdungsgefühl erfragt. Um das Schutzniveau darzustellen, werden die Sicherheitskompetenz, d.h. die Kenntnis von Schutzmaßnahmen, sowie das Sicherheitsverhalten, also die tatsächliche Anwendung dieser Schutzmaßnahmen identifiziert. Jeweils höher gewichtet werden dabei die tatsächlichen sicherheitsrelevanten Vorfälle und das tatsächliche Sicherheitsverhalten.

Grundlage für zielgruppenspezifische digitale Aufklärung 2.0

Wie im Vorjahr wurde außerdem nach Einstellung und Motivation der Nutzer gefragt, die die Sicherheitsfaktoren beeinflussen können. Sie bieten Anknüpfungspunkte, die Aufklärungsarbeit 2.0 (dazu Kapitel 4) konkret an den Bedarfen und Erwartungen der Verbraucher zu orientieren. Auch durch die Aufschlüsselung nach Nutzertypen können konkrete Sicherheitsschwachstellen und zielgruppenspezifische Bedürfnisse erkannt und passgenaue Maßnahmen für die Aufklärungsarbeit abgeleitet werden.

Kapitel 01

DsiN-Sicherheitsindex 2016: 65,4 Punkte

DsiN-Index 2016: Anstieg auf 65,4 Punkte

Der DsiN-Sicherheitsindex 2016 erreicht im dritten Jahr seiner Erhebung 65,4 Punkte. Somit wird im Jahresvergleich deutlich: Die Sicherheitslage der deutschen Onliner hat sich auf den ersten Blick weiter verbessert (2015: 63,0 Punkte; 2014: 60,2 Punkte).

Entwicklung von Bedrohungslage und Schutzniveau

Grundlage der ermittelten Sicherheitslage bildet das Verhältnis zwischen der Bedrohungslage und dem Schutzniveau der Verbraucher: Im Vergleich zu 2015 ist das Schutzniveau der Bürger erneut leicht gestiegen. Vor allem hat die etwas verbesserte Bedrohungslage den leichten Anstieg des Sicherheitsindex um 2,4 Punkte bewirkt.

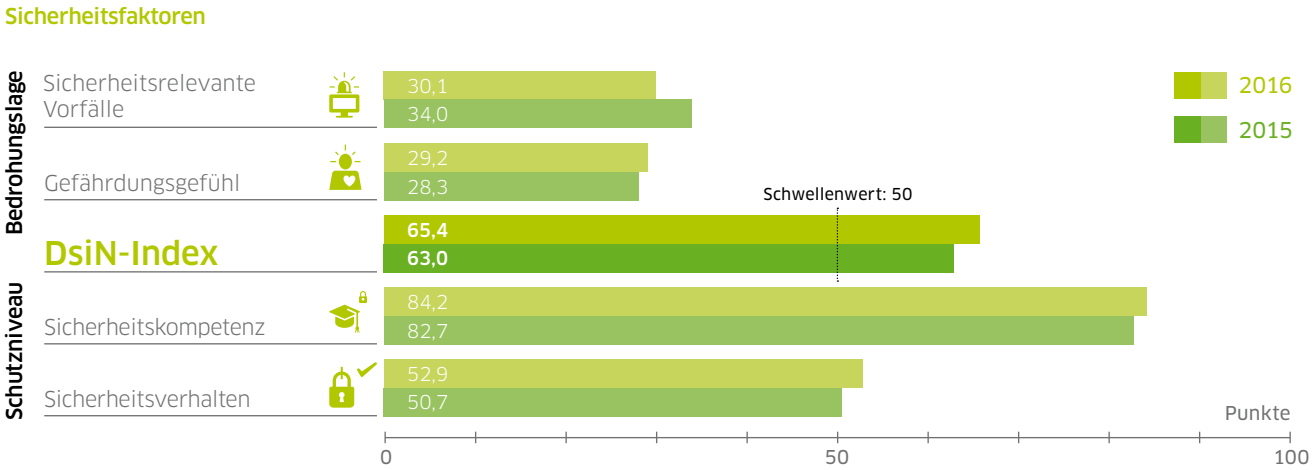
Bedrohungslage

- **Sicherheitsrelevante Vorfälle:** Befragt nach den erlebten Sicherheitsvorfällen gaben die Nutzer weniger Vorfälle an als in den Jahren zuvor. Dadurch ist der Wert für IT-sicherheitsrelevante Vorfälle um 3,9 Punkte auf 30,1 Punkte gesunken. Das ist die größte Verbesserung des Index.
- **Gefährdungsgefühl:** Obwohl die Zahl der selbst registrierten Sicherheitsvorfälle gesunken ist, ist das Gefährdungsgefühl im Vergleich zu den Vorjahren erneut gestiegen. Es liegt 2016 bei 29,2 Punkten (2015: 28,3 Punkte).

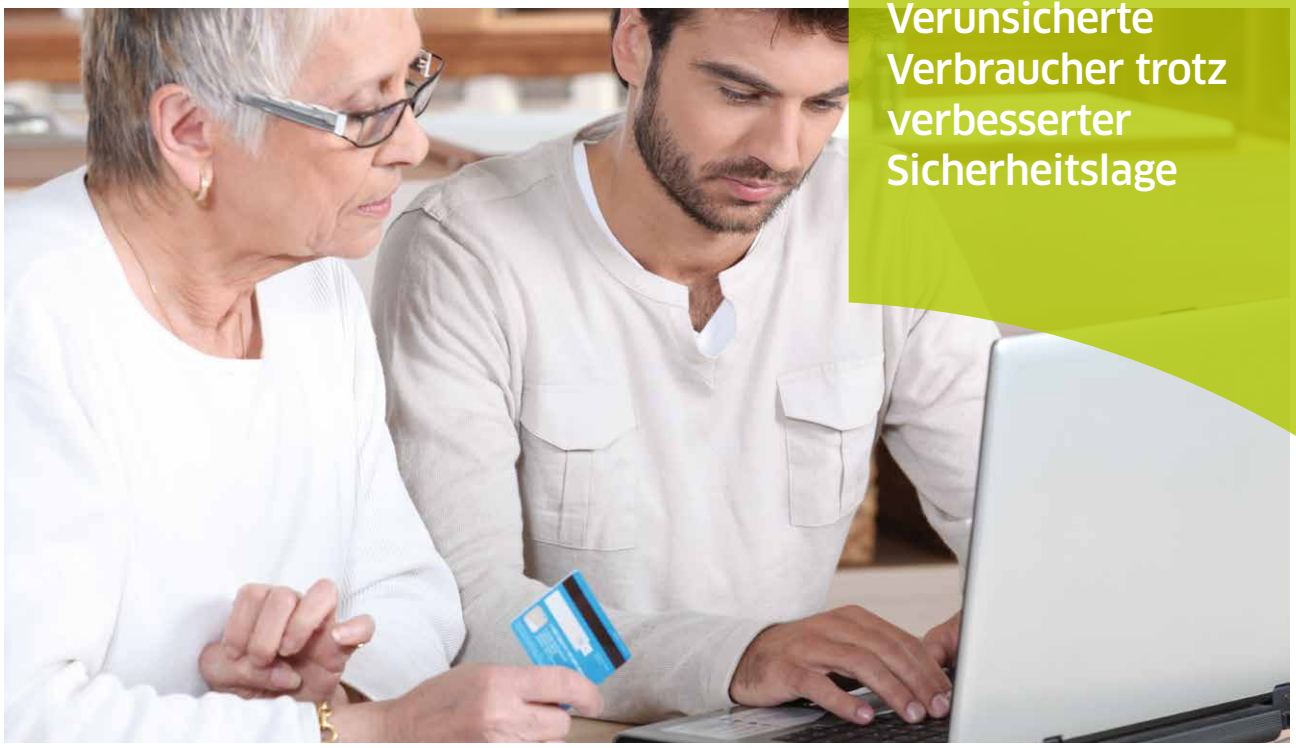
Schutzniveau

- **Sicherheitskompetenz:** Das Sicherheitswissen der Verbraucher ist auch in 2016 erneut gestiegen, und zwar um 1,5 Punkte auf 84,2 Punkte (2015: 82,7 Punkte).
- **Sicherheitsverhalten:** Ebenfalls verbesserte sich die Bereitschaft zur Anwendung von Schutzmaßnahmen und verzeichnet mit 2,2 Punkten einen Anstieg auf 52,9 Punkte (2015: 50,7 Punkte).

Abb. 3. Übersicht Index und Faktoren 2016



Verunsicherte Verbraucher trotz verbesserter Sicherheitslage



Größer werdende Schere zwischen Wissen und Nutzen

Damit liegt der Sicherheitsindex in diesem Jahr 15 Punkte über dem Schwellenwert von 50 Punkten. Würde der Indexwert unter die 50-Punkt-Marke rutschen, würde die Bedrohungslage das Schutzniveau übertreffen und die Sicherheitslage kippen. Aufgrund der weiter bestehenden Nähe zum kritischen Schwellenwert, kann deshalb auch in 2016 nur von einer Verbesserung auf mäßigem Niveau gesprochen werden. Die kaum gestiegenen Werte im Schutzniveau verdeutlichen zudem, wie anfällig Verbraucher für Risiken sind. Des Weiteren bleibt die Diskrepanz zwischen Kenntnis und Anwendung von Sicherheitsmaßnahmen auch 2016 erheblich.

Risiko einer digitalen Vertrauenskrise

Als negativer Faktor wirkt eine zunehmende Verunsicherung der Verbraucher auf die Sicherheitslage: Das Gefährdungsgefühl der Verbraucher ist – trotz verbesserter Sicherheitslage – erkennbar gestiegen und dies schon im zweiten Jahr in Folge. Es führt bei den meisten Nutzern zu einer neuen Unsicherheit und Hemmung im Umgang mit digitalen Diensten im Alltag. Eine Fortschreibung dieser Entwicklung birgt das Risiko einer digitalen Vertrauenskrise mit einer Schwächung von Verbrauchern im souveränen Umgang mit der Digitalisierung insgesamt.

Zusammenfassend lässt sich festhalten, dass ein längerfristiger Trend zu mehr IT-Sicherheit nicht erkennbar ist und dass das aktuelle Schutzniveau nicht ausreichend wäre, um einer verschlechterten Bedrohungslage vorzubeugen.

Die vier Sicherheitsfaktoren

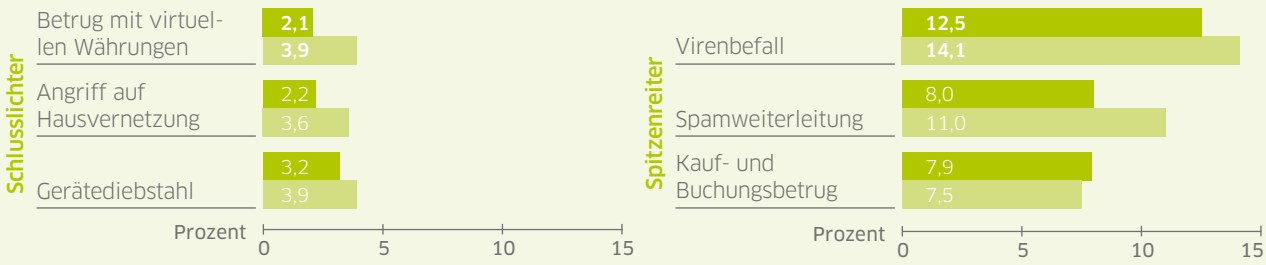
Bedrohungslage

Die Bedrohungslage erfasst selbstregistrierte Vorfälle und das Sicherheitsgefühl bei Verbrauchern anhand von über 40 Szenarien.

1. Sicherheitsrelevante Vorfälle

Trotz eines leichten Rückgangs um 1,6 Prozentpunkte im Vergleich zum Vorjahr führt Schadsoftware auch 2016 die Liste der Sicherheitsvorfälle an. Auf Platz zwei folgt mit 8 Prozentpunkten der unerwünschte E-Mail-Versand im eigenen Namen. Betrugsfälle bei Online-Einkauf oder Online-Buchung liegen auf Platz 3: In den vergangenen 12 Monaten waren 7,9 Prozent der befragten Onliner davon betroffen. Die seltensten Vorfälle – bei zugleich meist höherer Qualität – betreffen Angriffe auf die Hausvernetzung (2,2 Prozent) und den Betrug mit virtueller Währung (2,1 Prozent).

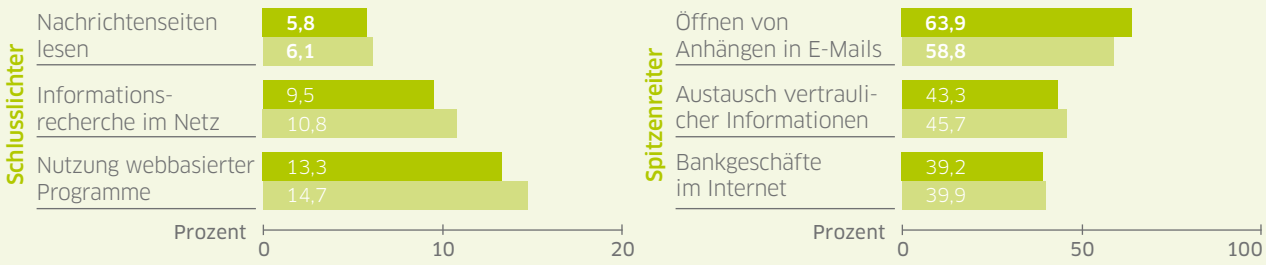
Abb. 4 Spitzenreiter und Schlusslichter Sicherheitsrelevante Vorfälle



2. Gefährdungsgefühl

Die größte Unsicherheit herrscht beim Thema E-Mail: Fast 64 Prozent empfinden das Öffnen von E-Mail-Anhängen als gefährlich oder sehr gefährlich. Den Austausch vertraulicher Daten über das Internet (z.B. mit Behörden) sehen 43,3 Prozent als riskant. Eine deutlich höhere Unsicherheit als im Vorjahr besteht beim Herunterladen von Software oder medialen Inhalten. Vergleichsweise sicher fühlen sich die Befragten beim Lesen von Nachrichtenseiten: Nur 5,6 Prozent sehen sich hier gefährdet. Beim Recherchieren in Suchmaschinen und Nachschlagewerken sind es bereits 9,5 Prozent, die ein Sicherheitsrisiko sehen.

Abb. 5 Spitzenreiter und Schlusslichter Gefährdungsgefühl



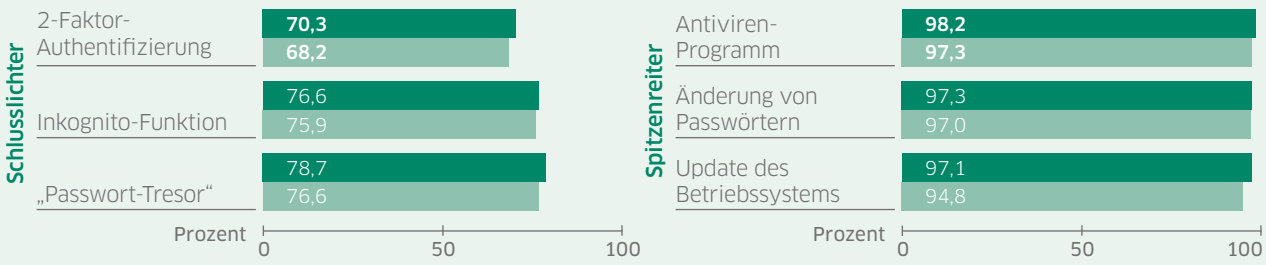
Schutzniveau

Dem individuellen Schutzniveau beim Verbraucher liegt eine Kombination seiner Kompetenzen digitaler Sicherheit und tatsächlicher Sicherheitspraxis zu Grunde.

3. Sicherheitskompetenz

Antivirenprogramme sind fast allen befragten Nutzern bekannt. 98,2 Prozent gaben an, diese elementare Schutzmaßnahme zu kennen. Auch bei dem Thema Passwortsicherheit sind die Bekanntheitswerte sehr gut: 97,3 Prozent geben an, zu wissen, dass Passwörter regelmäßig gewechselt werden sollten und fast 96,8 Prozent der Nutzer wissen, dass es sinnvoll ist, unterschiedliche Passwörter für verschiedene Anwendungen zu nutzen. Am wenigsten bekannt ist die 2-Faktor-Authentifizierung, diese kennen nur 70,3 Prozent der befragten Onliner.

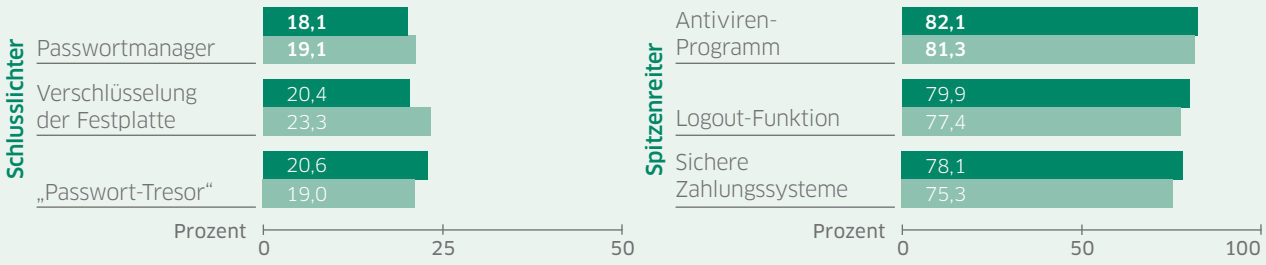
Abb. 6 Spitzenreiter und Schlusslichter Sicherheitskompetenz



4. Sicherheitsverhalten

Hinsichtlich der Schutzmaßnahmen, welche die Befragten aktiv anwenden, ist das Antivirenprogramm am gängigsten: 82,1 Prozent gaben an, eines zu verwenden, das sind 0,8 Prozentpunkte mehr als 2015. Die Logout-Funktion wird von 79,9 Prozent der Befragten genutzt und somit von 2,5 Prozent der Verbraucher mehr als im Vorjahr. Auf Platz drei steht ohne nennenswerte Veränderung mit 78,1 Prozentpunkten die Nutzung von sicheren Zahlungssystemen beim Einkauf im Internet. Am seltensten wird von den Onlinern in Deutschland (18,1 Prozent) ein Passwortmanager genutzt.

Abb. 7 Spitzenreiter und Schlusslichter Sicherheitsverhalten



Drei Viertel der Verbraucher sehen Verantwortung bei sich

Einflussfaktoren aus Verbrauchersicht

Um die Sicherheitslage zu verbessern, müssen die vier Sicherheitsfaktoren beeinflusst werden. Die Studie hat Verbraucher gefragt, welche Maßnahmen sie hierfür als erforderlich und vielversprechend beurteilen.

1. Einfluss auf Sicherheitsvorfälle

76,1 Prozent der Befragten sehen die Verantwortung zum Schutz vor Angriffen zunächst bei sich selbst, wonach sie vorsichtiger mit den eigenen Daten umgehen sollten. Gut die Hälfte glaubt, dass sie häufiger Sicherheitsmaßnahmen einsetzen sollten und erwartet zugleich vom Anbieter, Dienste sicherer zu gestalten.

2. Stärkung der Risikoeinschätzungskompetenz

Um einer Verunsicherung entgegenzuwirken, wünschen sich die Befragten mehr Aufklärung über Risiken digitaler Anwendungen durch Anbieter (54,6 Prozent), mehr Warnhinweise im Internet (52,9 Prozent) sowie eine bessere Aufklärung außerhalb des Netzes (45,3 Prozent).

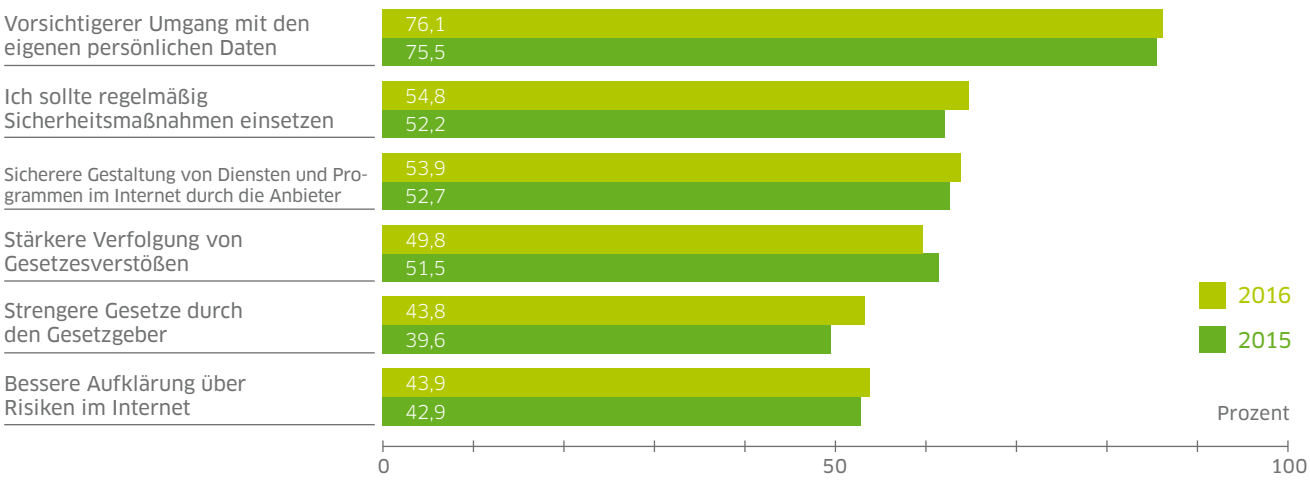
3. Vertiefung von Sicherheitswissen

Um Sicherheitswissen zu stärken, fordern 71 Prozent der Onliner mehr Informationen zum Thema sicheres Surfen. 70,8 Prozent wünschen sich verständlichere Informationen und 70,6 Prozent halten eine zentrale Anlaufstelle im Internet für hilfreich.

4. Motivation zur Anwendung

Drei Viertel der Verbraucher erwarten, dass einfach bedienbare Sicherheitseinstellungen ihre eigene Motivation zu mehr IT-Sicherheit erhöhen. Mit deutlichem Abstand folgt mit 56,5 Prozent der Wunsch nach mehr Anleitungen zum sicheren Verhalten, z. B. durch Bildungseinrichtungen. 54,6 Prozent der Nutzer erhoffen sich durch Unterstützung aus dem privaten Umfeld einen positiven Effekt auf ihre Motivation.

Abb. 8 Selbsteinschätzung der Verbraucher: Wie Sicherheitsvorfälle reduzieren?



Kapitel 02

Digitales Sicherheitsgefälle: Verbrauchertypen

Einfluss von Verbrauchertypen auf Sicherheitslage

Für das Verständnis der IT-Sicherheitslage ist entscheidend, verschiedene Verbrauchertypen zu unterscheiden. Denn diese variiert je nach dem individuellen Wissen und Verhalten. Daraus entsteht ein digitales Sicherheitsgefälle, bei dem die Fatalisten in den vergangen 12 Monaten das neue Schlusslicht bildeten.

Fatalistische Nutzer haben sich zwar 2016 weiter verbessert, weisen dennoch weiterhin einen relativ niedrigen Index von **52,5 Indexpunkten** auf (2014: 44,2 Indexpunkte; 2015: 51,9 Indexpunkte). Sie haben somit die rote Laterne, von der sie sich im Vorjahr befreien konnten, erneut übernommen. Allerdings sind die Fatalisten gar nicht mehr so „fatalistisch": Sie sehen die Bedrohungslage weniger negativ als 2014 und ihr Sicherheitsverhalten hat sich vergleichsweise gebessert. Die Verunsicherung in der meist jungen Nutzergruppe ist dennoch überdurchschnittlich hoch.

Außenstehende Nutzer verbuchen 2016 mit **54,7 Indexpunkten** erneut ein deutlich besseres Ergebnis als im Vorjahr (2014: 45,8 Indexpunkte; 2015: 50,7 Indexpunkte). Damit sind sie im Index an den Fatalisten vorbeigezogen. Auch ist die Gruppe, der vor allem ältere Menschen angehören, im Vergleich zu 2014 deutlich kleiner geworden (9,7 auf 8,0 Prozent). Im 3-Jahresvergleich wird jedoch sichtbar, dass die gefühlte Bedrohungslage trotz gesunkener Zahl an Sicherheitsvorfällen stärker geworden ist.

Gutgläubige Nutzer verbessern sich erneut und erreichen 2016 einen Sicherheitsindex von **62,3 Indexpunkten** (2014: 58,1 Indexpunkte; 2015: 60,5 Indexpunkte). Auffällig sind hier weiterhin die deutliche Wissens-Verhaltenslücke sowie die unzureichende Risikoeinschätzungskompetenz. Gemessen an der Gesamtbevölkerung wird diese Gruppe im 3-Jahresvergleich kleiner: Zählten

Abb. 9 Übersicht über untersuchte Nutzertypen im DsiN-Index

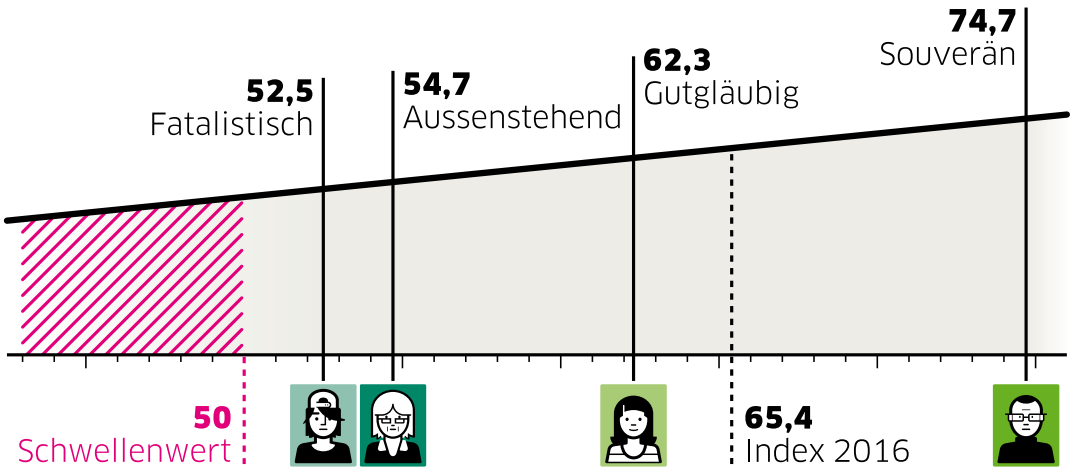
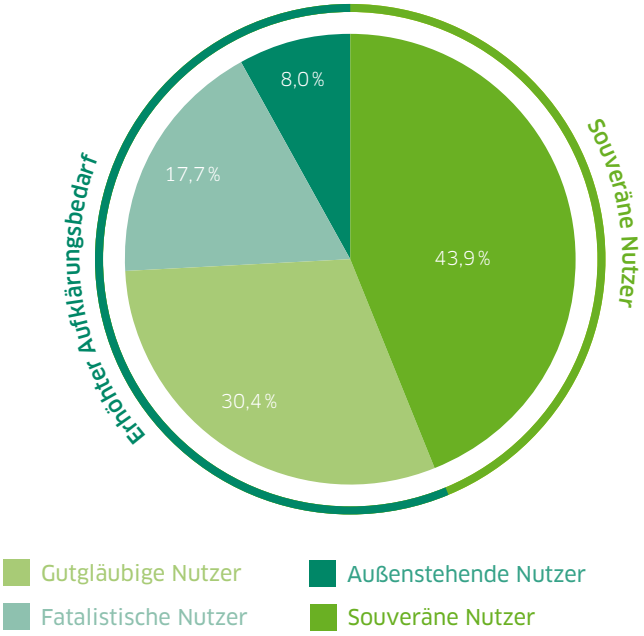


Abb. 10 Anteil der Verbrauchertypen an der Gesamtheit der Onliner



2014 noch 34,7 Prozent der Befragten in diese Gruppe, sind es 2016 noch 30,4 Prozent.

Souveräne Nutzer befinden sich mit dem besten Sicherheitsindex weiterhin an der Spitze und verzeichnen eine Verbesserung um 2,5 Punkte auf **74,7 Indexpunkte** (2014: 72,0 Indexpunkte; 2015: 72,2 Indexpunkte). Der Anteil der souveränen Nutzer steigt erfreulicherweise kontinuierlich (39,8 2014 auf 43,9 Prozent 2016). Bei den souveränen Nutzern gehen die Vorfälle, aber auch die Anwendung von Sicherheitsmaßnahmen leicht zurück.

60 Prozent der Verbraucher haben Unterstützungsbedarf

Etwas mehr als die Hälfte der Onliner – Fatalisten, Gutgläubige und Außenstehende – liegen in der Nähe zum kritischen Schwellenwert von 50-Indexpunkten. Sie zeigen damit verstärkten Aufklärungsbedarf. Eine große Aufgabe bleibt hier insbesondere die Schließung der Schere zwischen Sicherheitskompetenz und -verhalten. Sie erweist sich bei den Gutgläubigen als besonders deutlich. Auch bei den Fatalisten bleibt die Anwendung von Sicherheitsmaßnahmen unterdurchschnittlich; die außenstehenden Nutzer bleiben beim Sicherheitsverhalten Schlusslicht. Aufklärung und Motivation sind also dringend nötig – und zwar solche die sich an individuellen Bedarfen orientieren und nicht nach dem Gießkannenprinzip funktionieren.

Zielgruppenorientiert aufklären und befähigen

Verbraucher ist nicht gleich Verbraucher: Es zeigen sich markante Unterschiede zwischen den verschiedenen Nutzergruppen im Umgang mit digitalen Diensten. Die drei empfohlenen Handlungsschritte sensibilisieren – befähigen – motivieren (ausführlich Kap. 4) müssen daher individuell gestaltet sein:

- Fatalisten sollten vor allem zur Anwendung ihres vorhandenen Wissens motiviert werden, um (Selbst)Vertrauen auf- und Unsicherheiten abzubauen.
- Außenstehende benötigen niedrigschwellige Informationen und konkrete Handlungsempfehlungen.
- Gutgläubige weisen ein unterentwickeltes Risikobewusstsein auf, sodass die Risikoeinschätzungskompetenz gefördert werden muss.
- Die Souveränen müssen darin unterstützt werden, andere im sicheren Umgang mit dem Internet zu begleiten und ihre Verantwortung als Vorbild zu stärken.

Über die Hälfte der Verbraucher weist einen kritischen Sicherheitswert auf

Fatalisten fehlt nicht Information, sondern Motivation

Fatalistische Nutzer (52,5 Punkte)

Der fatalistische Nutzer

Rote Laterne: Die Fatalisten haben erneut die rote Laterne von den außenstehenden Nutzern übernommen – bei einem Sicherheitsindex von nur **52,5 Punkten.**

Typische Merkmale

Fatalistische Nutzer unterlassen Sicherheitsmaßnahmen, obwohl sie Schutzmaßnahmen kennen und sich besonders bedroht fühlen. Sie sind typischerweise unter 30 Jahren; insbesondere die 16- bis 19-Jährigen sind in dieser Gruppe vertreten. Die meisten Nutzer dieser Gruppe (70 Prozent) sind bis zu 20 Stunden in der Woche online. Knapp 18 Prozent aller Internetnutzer gehören in diese Gruppe.

Bedrohungslage

Zwar sind sicherheitsrelevante Vorfälle im Vorjahresvergleich weniger geworden, dennoch fällt der Index mit 44,5 Punkten in dieser Kategorie deutlich höher als bei den anderen Nutzertypen aus. Auch das Gefährdungsgefühl hat sich in dieser Gruppe 2016 im Vergleich zu den Vorjahren verringert, liegt mit 70,1 Punkten aber immer noch sehr weit über dem Durchschnitt. Als besonders gefährlich werden E-Mails mit Anhängen (90,6 Prozent), das Teilen vertraulicher Inhalte (87,6 Prozent) und Bankgeschäfte im Internet (83,2 Prozent) empfunden.

Schutzniveau

Die Sicherheitskompetenz (78,1 Punkte) der fatalistischen Nutzer hat sich seit 2014 in jedem Erhebungsjahr um mindestens 10 Punkte verbessert. Ebenso wie das Sicherheitsverhalten (48,4 Punkte), welches jedoch immer noch unter der kritischen Grenze von 50 Punkten bleibt. Während Anti-Viren-Programme gut bekannt sind und genutzt werden, ist vor allem beim Thema Verschlüsselung die Wissens-Verhaltenslücke am größten. So wissen zwar 86,7 Prozent der Fatalisten, dass sie ihre Festplatte verschlüsseln können, doch nur 18,9 Prozent tun dies auch tatsächlich.

Abb. 11 DsiN-Indexwert für fatalistische Nutzer

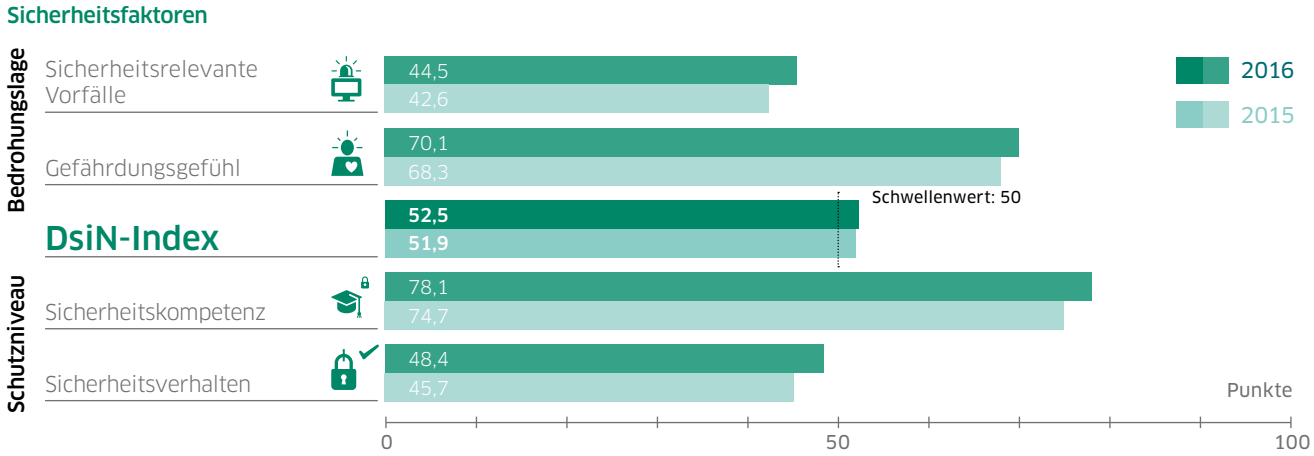
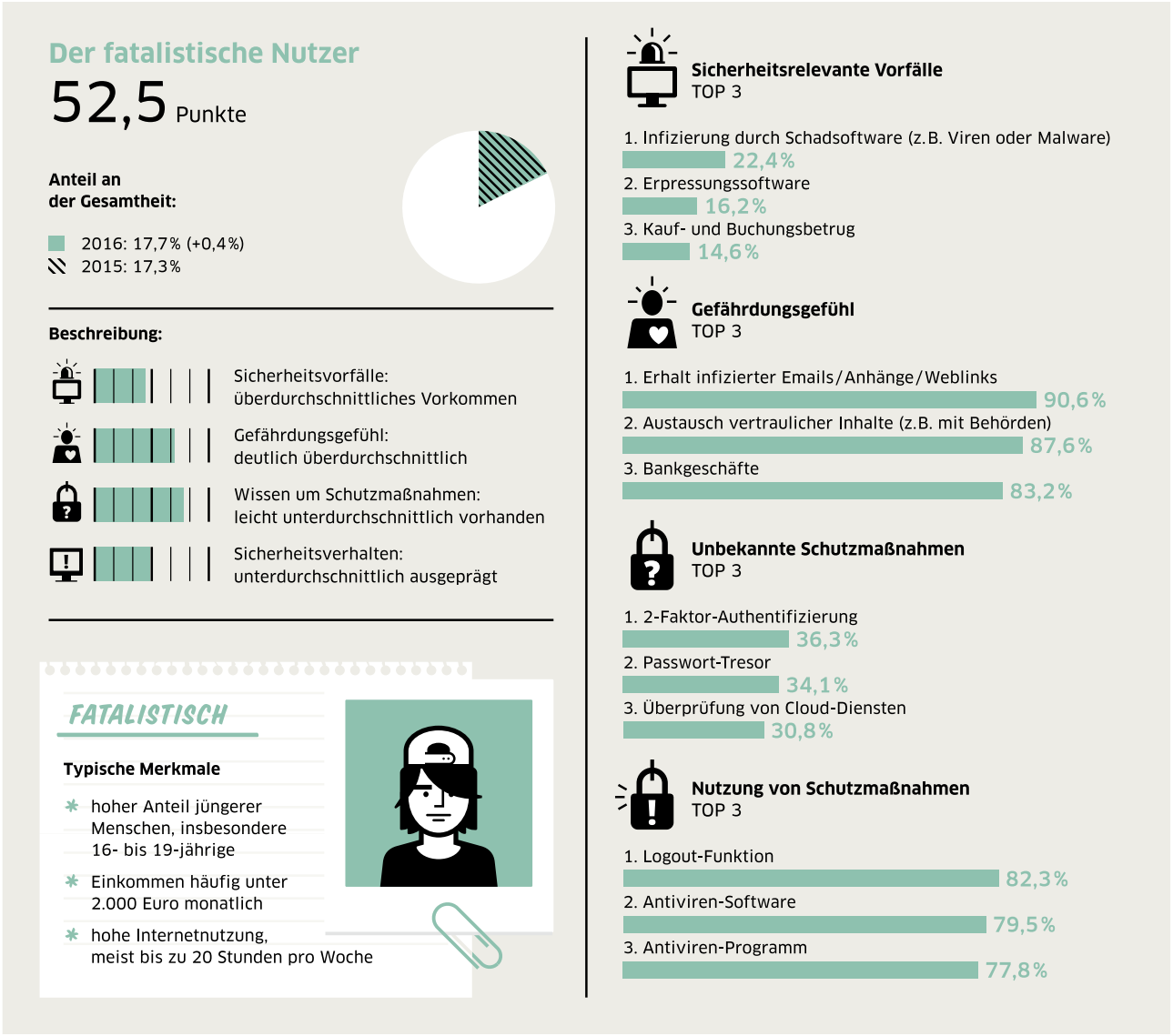


Abb. 12 Steckbrief Fatalistischer Nutzer



Unsicherheit abbauen und zum Handeln motivieren

Fatalisten wissen gut über Sicherheitsmaßnahmen Bescheid, wenden diese aber kaum an, da sie an der Wirksamkeit zweifeln. Um das Vertrauen in Schutzmaßnahmen zu fördern, müssen deren Nützlichkeit sowie die Folgen nachlässigen Handelns veranschaulicht werden. Gute Basis ist die wahrgenommene Eigenverantwortung: 82 Prozent der Fatalisten gaben an, dass sie Sicherheitsvorfälle durch einen vorsichtigeren Umgang mit den eigenen persönlichen Daten reduzieren könnten.

Der DsiN-Index zeigt: Dieser Nutzergruppe fehlt nicht die Information, sondern die Motivation. Um diese zu steigern, wünschen sich die Fatalisten einfachere Sicherheitseinstellungen bei Programmen und Geräten, mehr Anleitungen zum sicheren Verhalten z. B. durch Bildungseinrichtungen und konkrete Ansprachen durch ihr privates Umfeld. Um das erhöhte Gefährdungsgefühl zu senken, sollte das Vertrauen in die eigene Selbstwirksamkeit gefördert werden. Fatalisten müssen bewusst erfahren, dass sich sicherheitsbewusstes Verhalten lohnt.

DsiN-Angebote für fatalistische Nutzer:

- **myDigitalWorld:** Jugendwettbewerb
- **Medien in die Schule:** Materialien für den Unterricht
- **Bottom-Up:** Berufsschüler für IT-Sicherheit
- **IT – Fitness Test:** Online-Wissenscheck

Außenstehende Nutzer (54,7 Punkte)

Der außenstehende Nutzer

Unaufgeklärt: Die Außenstehenden verbuchen dieses Jahr mit **54,7 Punkten** ein um vier Punkte besseres Ergebnis als im Vorjahr. Dennoch bewegen sie sich nach wie vor nur wenig entfernt vom kritischen Niveau.

Typische Merkmale

Die Außenstehenden, überwiegend älter als 50 Jahre und zu über 65 Prozent Frauen, zeigen im Vergleich zu den anderen Nutzergruppen Defizite bei der Kenntnis und der Nutzung von Schutzmaßnahmen. Sie nutzen bevorzugt stationäre PCs und Laptops und sind meist nicht mehr als 20 Stunden wöchentlich online. In der Gesamtgruppe der Onlinenutzer in Deutschland macht die Gruppe der Außenstehenden ca. 8 Prozent aus.

Bedrohungslage

Im 3-Jahresvergleich wird deutlich, dass das Gefährdungsgefühl (26,0 Punkte) dieser Nutzergruppe stärker geworden ist, obwohl die Zahl der Sicherheitsvorfälle gesunken ist. Tatsächlich weisen die Außenstehenden mit einem Indexwert von 20,1 Punkten bei den sicherheitsrelevanten Vorfällen den besten Wert aller Nutzergruppen auf, was sicher auf die geringe Risikoexposition zurückzuführen ist. Besonders skeptisch sind die außenstehenden Nutzer beim Empfang von E-Mails mit Anhängen sowie beim Teilen von vertraulichen Informationen über das Internet.

Schutzniveau

Bei den außenstehenden Nutzern hat sich im Vergleich zu 2014 das Sicherheitswissen leicht verschlechtert, während sich das Verhalten deutlich verbessert hat. Diese Nutzergruppe bleibt aber in beiden Kategorien Schlusslicht. Grundlegende Schutzmaßnahmen wie Anti-Virenprogramme oder die Nutzung unterschiedlicher Passwörter sind auch unter den außenstehenden Nutzern relativ verbreitet. Die größte Diskrepanz zwischen Kennen und Nutzen besteht bei den Themen Datensicherung, Verschlüsselung sowie sichere Entsorgung.

Abb. 13 DsiN-Indexwert für außenstehende Nutzer

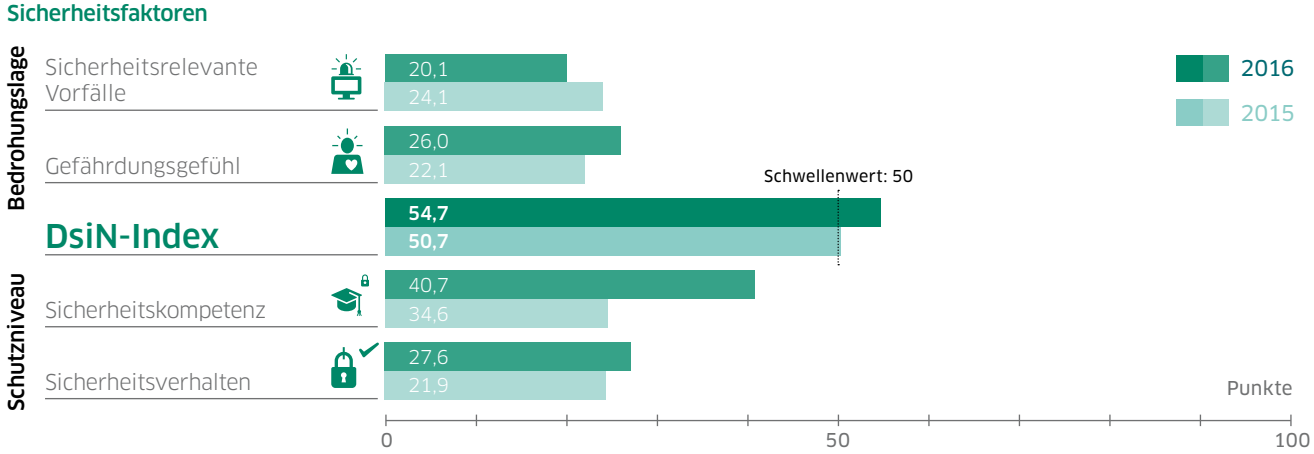
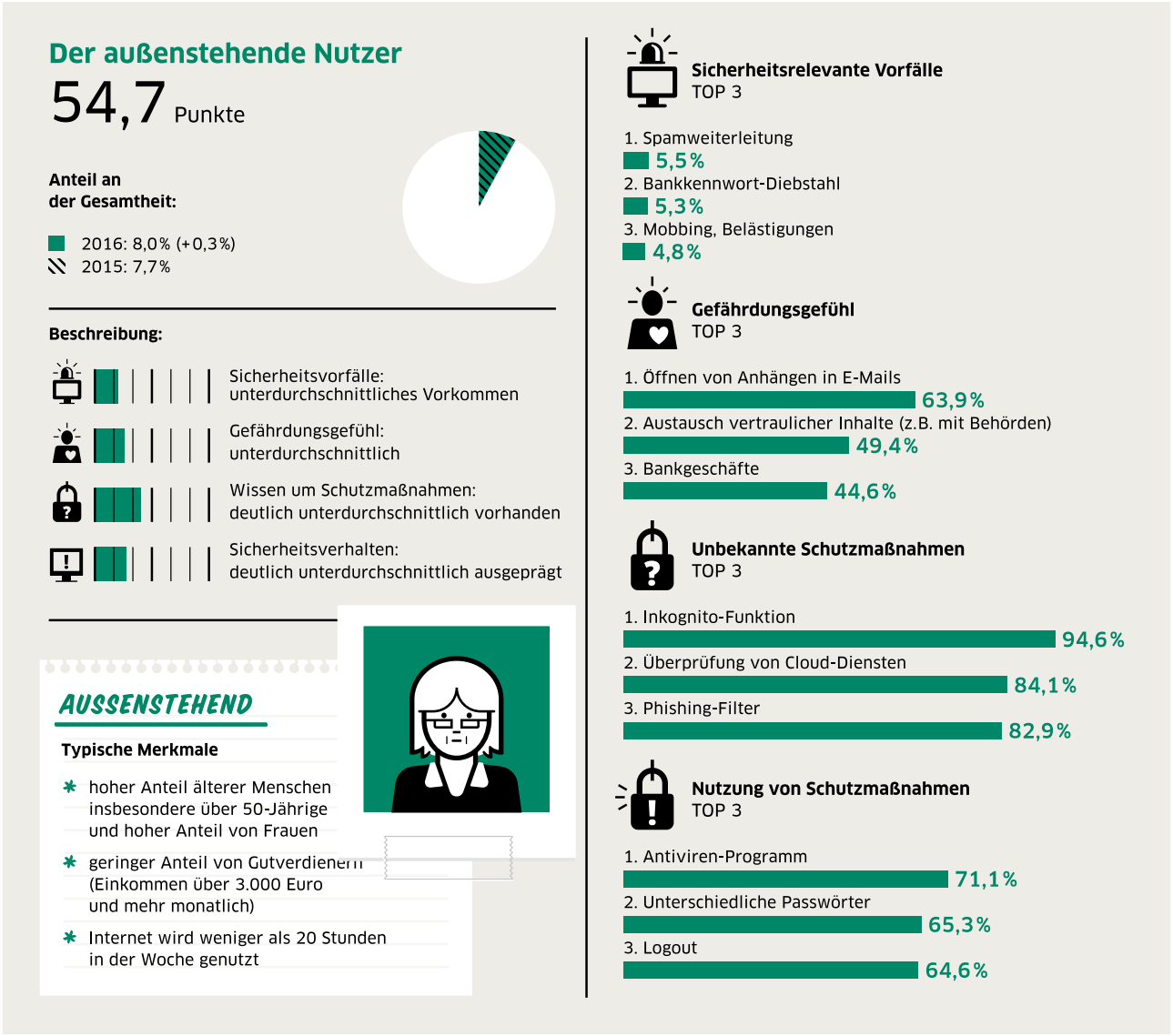


Abb. 14 Steckbrief Außenstehender Nutzer



Wissen und Umsetzungskompetenz stärken

In dieser Gruppe gibt es sowohl beim Sicherheitswissen als auch beim Sicherheitsverhalten große Defizite. Außenstehende Nutzer benötigen daher niedrigschwellige, nach eigener Angabe vor allem verständlichere Informationen sowie konkrete Anleitungen zur Umsetzung. Auch wünschen sich Außenstehende mehr Warnhinweise im Internet zur Stärkung ihres Risikobewusstseins. Einfachere Sicherheitseinstellungen bei Anwendungen sowie Unterstützung durch das private Umfeld werden von der Nutzergruppe als hilfreich für die eigenen Sensibilisierung und Motivation wahrgenommen. Es bedarf daher vertrauenswürdiger Personen als Multiplikatoren, welche die Außenstehenden bei einem sicherheitsbewussten Umgang mit digitalen Diensten begleiten. Gleichzeitig muss die Risikoeinschätzungskompetenz gestärkt werden, um eine gesunde Balance zwischen Vertrauen und Skepsis zu gewährleisten.

DsiN-Angebote für außenstehende Nutzer:

- **Digital-Kompass** für Senioren
- **Goldener Internetpreis** für Senioren
- **IT – Fitness Test:** Online-Wissenscheck
- **DsiN-Sicherheitsbarometer** (auch als App)

Gutgläubige Nutzer (62,3 Punkte)

Der gutgläubige Nutzer

Unbedacht: Die gutgläubigen Nutzer erreichen einen Sicherheitsindex von **62,3 Punkten** und verbessern sich erneut. Defizite liegen in der Einschätzung von digitalen Risiken sowie der adäquaten Anwendung von Schutzmaßnahmen.

Typische Merkmale

Der gutgläubige Nutzer, überwiegend zwischen 30 und 59 Jahren alt, ist insbesondere mit seinem Laptop oder Desktop-PC aber auch häufig mit dem Smartphone online. Meist ist er wöchentlich nicht mehr als 20 Stunden im Internet unterwegs. Gut 30 Prozent aller Onliner gehören zu den gutgläubigen Nutzern.

Bedrohungslage

Das Gefährdungsgefühl bleibt im 3-Jahresvergleich mit 15,4 Punkten relativ konstant und ist deutlich unterdurchschnittlich. Dazu trägt sicher auch bei, dass die tatsächlichen Sicherheitsvorfälle mit 25,3 Punkten in dieser Gruppe zurückgegangen sind. Weniger als die Hälfte (47,3 Prozent) der Gutgläubigen schätzen den Erhalt von E-Mail-Anhängen als potenzielles Risiko ein, nur knapp ein Drittel (27,4 Prozent) sieht das Teilen von vertraulichen Inhalten über das Internet als gefährlich oder sehr gefährlich an.

Schutzniveau

Die gutgläubigen Nutzer haben ihr Sicherheitswissen (84,7 Punkte) sowie ihr Sicherheitsverhalten (35,0 Punkte) im Vergleich zum Vorjahr kaum verbessert und bei der Anwendung von Schutzmaßnahmen sind die Gutgläubigen nachlässiger als 2014. Etwa ein Drittel der gutgläubigen Nutzer nutzt kein Anti-Viren-Programm (32,5 Prozent) und auch keine sicheren Zahlungssysteme im Netz (34,1 Prozent). Die Wissens-Verhaltens-Lücke ist besonders ausgeprägt: Fast alle (98,9 Prozent) wissen, dass sie ihre Passwörter regelmäßig ändern müssen, tatsächlich tun dies aber nur 24,2 Prozent.

Abb. 15 DsiN-Indexwert für gutgläubige Nutzer

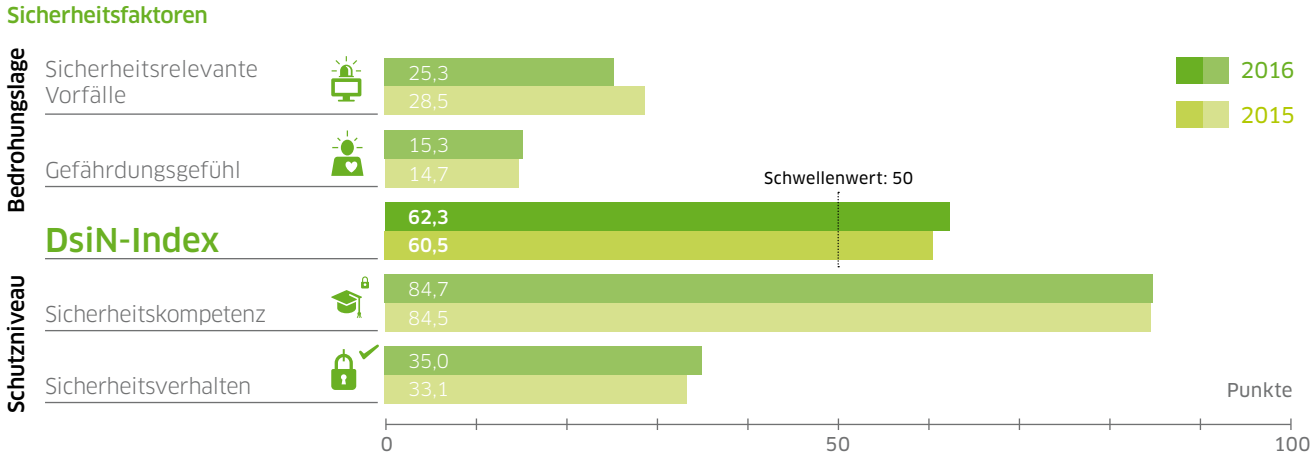
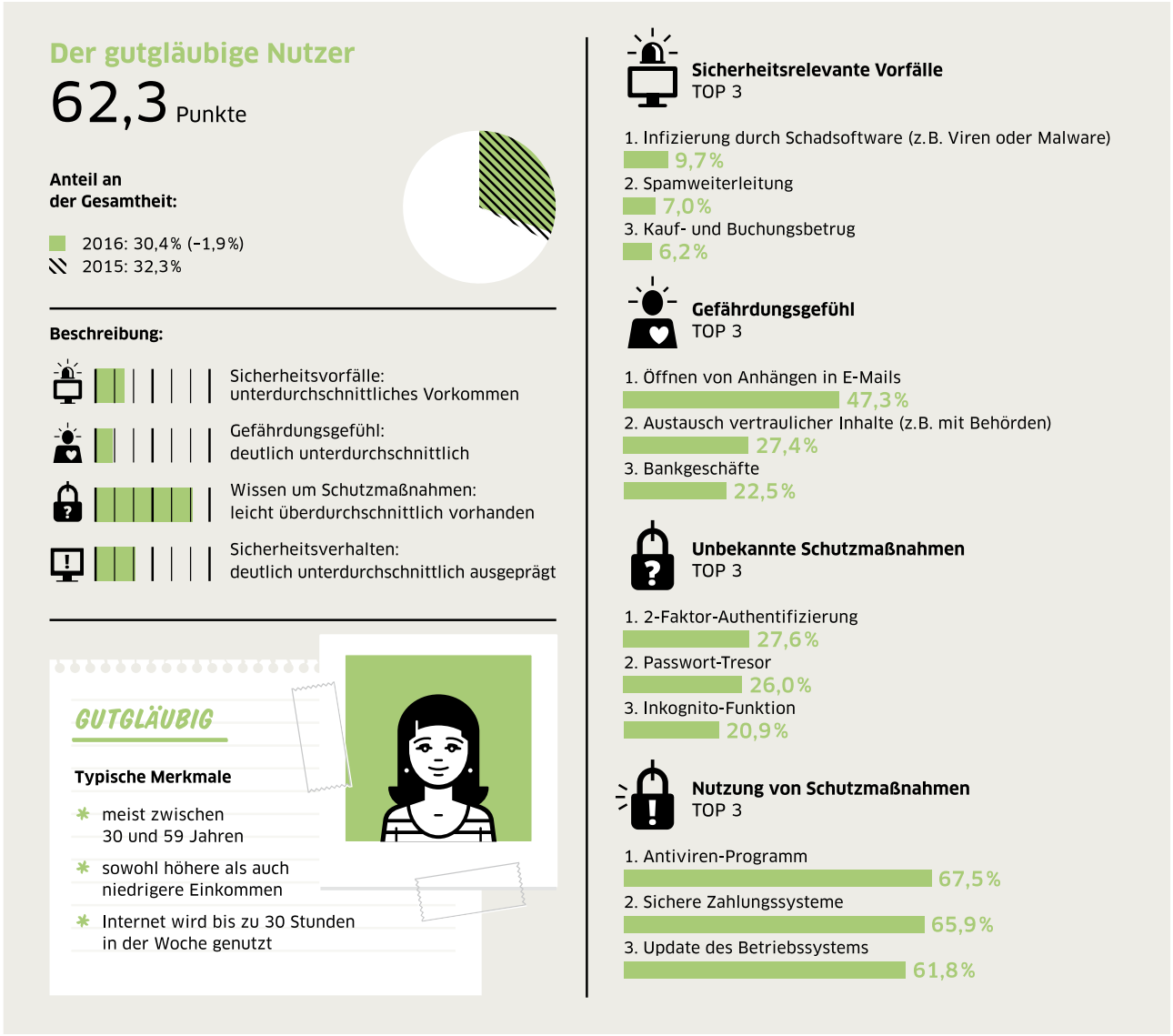


Abb. 16 Steckbrief Gutgläubiger Nutzer



Risikoeinschätzungskompetenz und Motivation fördern

Um die Risikoeinschätzungskompetenz zu fördern, muss dieser Nutzergruppe vermittelt werden, wo Gefahren bei der Nutzung digitaler Dienste lauern, wie diese zu bewältigen sind und welche Auswirkungen nachlässiges Handeln haben kann. Hierfür wünschen sich zwei Drittel der Gutgläubigen mehr Warnhinweise im Internet. Die Hälfte dieser Nutzergruppe fordert Dienstanbieter dazu auf, mehr über Risiken aufzuklären. Einfachere Sicherheitseinstellungen bei Programmen und Geräten sowie eine konkrete Ansprache durch das Umfeld finden die Gutgläubigen motivierend. Dass sie als Nutzer auch eine Eigenverantwortung für ihre Sicherheit tragen, nehmen die Gutgläubigen bereits wahr: Zwei Drittel geben an, dass ein vorsichtigerer Umgang mit den eigenen persönlichen Daten zu weniger IT-Sicherheitsvorfällen führen kann. Die Hälfte bestätigt, dass sie regelmäßiger Sicherheitsmaßnahmen einsetzen sollten. Besonderen Nachholbedarf gibt es im Bereich Verschlüsselung: Hier besteht in dieser Nutzergruppe die größte Wissens-Verhaltens-Lücke.

DsiN Angebote für Gutgläubige Nutzer:

- **DsiN-Sicherheitsbarometer** (auch als App)
- **IT – Fitness Test:** Online-Wissenscheck
- **Videoclips und Tutorials:** Datenverschlüsselung
- **DsiN-Passwort-Wechsel-App**

Souveräne Nutzer (74,7 Punkte)

Der souveräne Nutzer

Konstant überlegen: Unangefochten sind die souveränen Nutzer an der Spitze des Sicherheitsindex mit einem um 2,5 Punkte verbesserten Index von 74,7 Punkten.

Typische Merkmale

Die souveränen Nutzer, oftmals zwischen 40 und 49 Jahren alt, sind meist mit ihren Smartphones oder Laptops im Netz unterwegs und größtenteils mehr als 10 Stunden, 40 Prozent sogar bis zu 20 Stunden wöchentlich online. Dieser Nutzergruppe gehören aktuell knapp 44 Prozent aller Onliner an. Zum Vergleich: 2014 waren es 39,8 Prozent.

Bedrohungslage

Die sicherheitsrelevanten Vorfälle sind bei den souveränen Nutzern mit 29,6 Punkten weiter zurückgegangen. Allerdings steigt in diesem Jahr das Gefährdungsempfinden leicht auf 22,9 Punkte. Auch die souveränen Nutzer empfinden den Erhalt von E-Mail-Anhängen mehrheitlich als gefährlich (64,4 Prozent), danach folgen der Austausch vertraulicher Informationen über das Internet (35,4 Prozent) und der Download von Software (33,5 Prozent). Die Souveränen vertrauen zu 65,6 Prozent mehr als alle anderen Nutzergruppen dem Internet als glaubwürdige Informationsquelle über Sicherheitsmaßnahmen und -risiken.

Schutzniveau

Durch eine Sicherheitskompetenz von 94,4 Punkten und einem Sicherheitsverhalten von 71,7 Punkten ist diese Nutzergruppe weiterhin deutlich besser geschützt als alle anderen. Die Bekanntheit der Sicherheitsmaßnahmen liegt bei den souveränen Nutzern durchgehend bei mindestens 80 Prozent. Bei den meisten Schutzmaßnahmen geben sogar über 90 Prozent an, diese zu kennen. Auch bei der Anwendung stechen die souveränen Nutzer hervor: Bei den meisten der abgefragten Schutzmaßnahmen geben mindestens 60 Prozent der Befragten an, diese auch zu nutzen. Lediglich beim Thema Verschlüsselung haben auch die Souveränen noch Nachholbedarf.

Abb. 17 DsiN-Indexwert für souveräne Nutzer

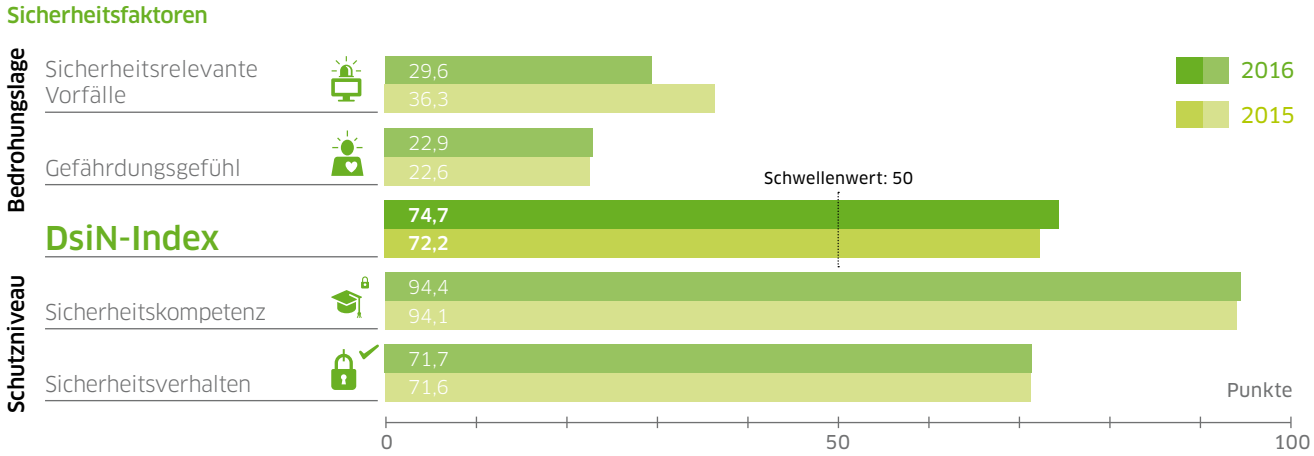
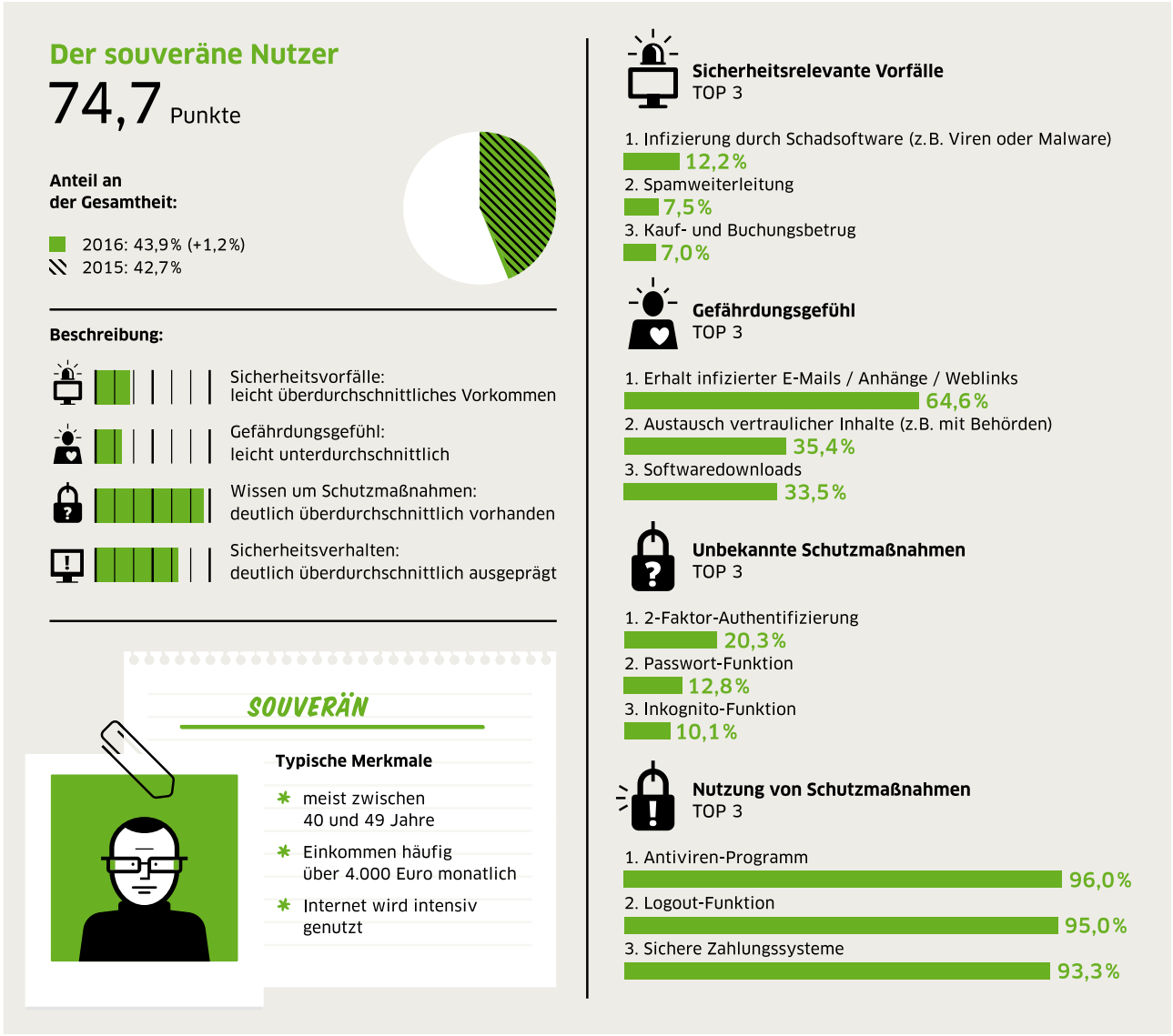


Abb. 18 Steckbrief Souveräner Nutzer



Anteil erhöhen und Verantwortung stärken

Die Gruppe der souveränen Nutzer weist das höchste Schutzniveau auf. Dieses gilt es über aktuelle Informationen und Handlungsempfehlungen auszubauen. Das Sicherheitsverhalten geht bei den Souveränen 2016 leicht zurück. Hier ist etwas mehr Motivation nötig. Als motivierend betrachten 82 Prozent dieser Gruppe einfachere Sicherheitseinstellungen bei Programmen und Geräten. Für je zwei Drittel würden mehr Anleitungen zum sicheren Verhalten sowie eine konkrete Ansprache durch das private Umfeld, das zudem stärker auf IT-Sicherheit achtet, die Motivation steigern.

Eine dringende Handlungsempfehlung bezogen auf die Souveränen ist es, ihnen ihre Verantwortung gegenüber den anderen Nutzergruppen deutlich zu machen. Sie sollten dazu befähigt werden, als Mentor und Vorbild andere aufzuklären und im sicheren Umgang mit dem Internet zu begleiten.

DsiN Angebote für souveräne Nutzer:

- **Digitale Nachbarschaft:** Multiplikatoren im Ehrenamt
- **DsiN-Sicherheitsbarometer** (auch als App)
- **IT – Fitness Test:** Online-Wissenscheck
- **IT-Sicherheitscheck:** Verantwortungsbewusstsein im Beruf

Exkurs: Sicherheitsgefälle der Bundesländer

Mecklenburg-Vorpommern: Spitzenreiter

Bestplatziert bei 70,7 Punkten ist Mecklenburg-Vorpommern. Dieses Bundesland glänzt mit einem ausgeprägten Wissen über Schutzmaßnahmen und einer vergleichsweise hohen Anwendungsrate. Auch liegt hier der Indexwert für sicherheitsrelevante Vorfälle mit 19,5 Punkten am niedrigsten.

Rheinland-Pfalz, Sachsen-Anhalt und Hamburg: Gute Werte für Sicherheitsfaktoren

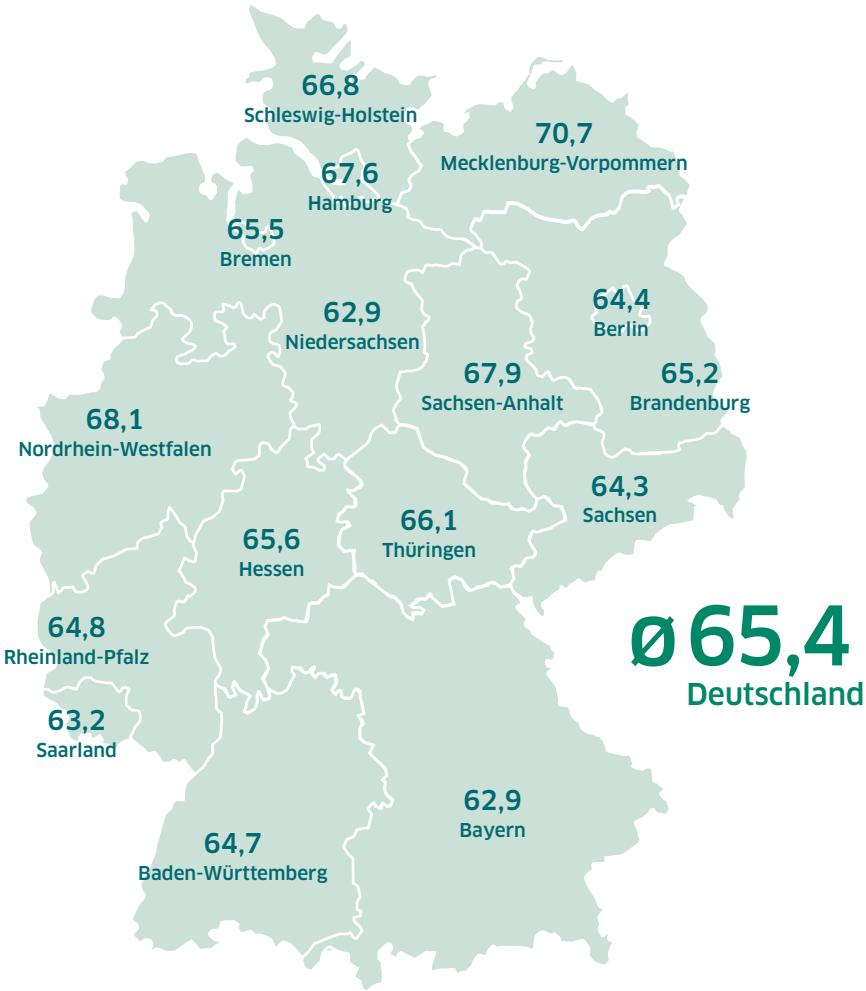
Das Wissen über Schutzmaßnahmen ist 2016 mit 88,5 Punkten am höchsten in Rheinland-Pfalz. Den höchsten Wert beim Sicherheitsverhalten erreicht Sachsen-Anhalt mit 57,6 Punkten. Am sichersten fühlen sich die Verbraucher in Hamburg: Das Gefährdungsgefühl ist mit 22,4 Punkten am niedrigsten.

Bayern, Saarland und Schleswig-Holstein: Rote Laternen bei IT-Sicherheit

Den niedrigsten Index mit 62,87 weist Bayern auf. Das Gefährdungsgefühl ist hier mit 33,0 Punkten am stärksten. Das höchste Vorkommen sicherheitsrelevanter Vorfälle lässt sich im Saarland mit 38,4 Punkten nachweisen. Das Sicherheitswissen ist in Schleswig-Holstein (81,3 Punkte), das Sicherheitsverhalten in Bremen (49,3 Punkten) unzureichend.

Abb. 19 Index nach Bundesländern

70,7 Mecklenburg-Vorpommern
68,1 Nordrhein-Westfalen
67,9 Sachsen-Anhalt
67,6 Hamburg
66,8 Schleswig-Holstein
66,1 Thüringen
65,6 Hessen
65,5 Bremen
65,2 Brandenburg
64,8 Rheinland-Pfalz
64,7 Baden-Württemberg
64,4 Berlin
64,3 Sachsen
63,2 Saarland
62,9 Bayern
62,9 Niedersachsen



Kapitel 03

Im Fokus: Digitale Lebenswelten

Vernetzter Verkehrsraum: das Automobil

Im vernetzten Verkehrsraum ist das digitale Automobil ein wesentlicher Faktor: Schon heute wird der Fahrer von Kameras, Sensoren und vernetzter Fahrzeugelektronik unterstützt. Immer mehr Autos erhalten einen Internetanschluss für die interne und externe Kommunikation. Mit der ab 2018 für alle Neufahrzeuge verpflichtenden Notruffunktion wird voraussichtlich jedes neue Fahrzeug vernetzt sein.

Bereits für 27,4 Prozent der befragten Nutzer sind bestehende IT-Systeme in einem neuen Auto wichtig. Jeweils mehr als die Hälfte der Befragten finden, dass Assistenzsysteme das Autofahren sicherer (55,2 Prozent) und Infotainment-Systeme das Fahren komfortabler machen (51,4 Prozent). Allerdings glauben nur 31,8 Prozent, dass die Vorteile von vernetzten Fahrzeugen die Sicherheitsrisiken überwiegen, wobei hier vor allem die weiblichen Befragten skeptisch sind.

Ängste vor Gefahren überwiegen noch

Bei Datensicherheit antworteten 53,7 Prozent der Verbraucher, dass sie den Download und die Nutzung von Apps für die Systeme im Auto als Risiko wahrnehmen. Dicht dahinter folgen als Risikoträger vernetzte Unter-

Abb. 20 Vorteile Vernetztes Fahren

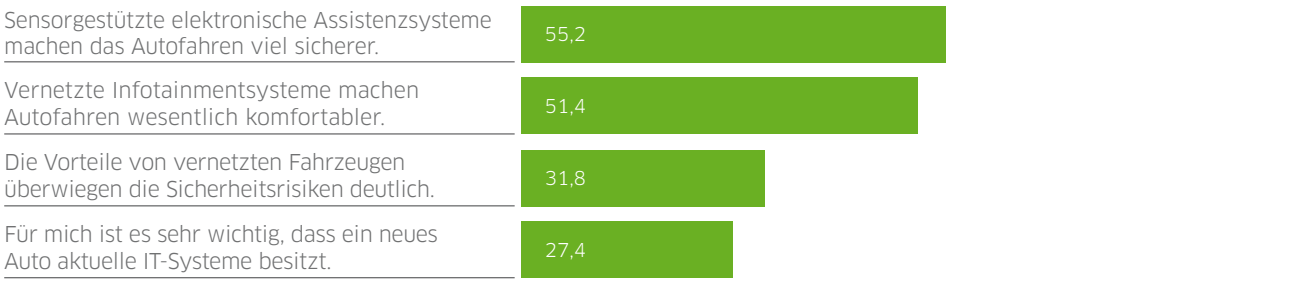


Abb. 21 Sicherheitsrisiken des vernetzten Fahrens bzgl. der Datensicherheit

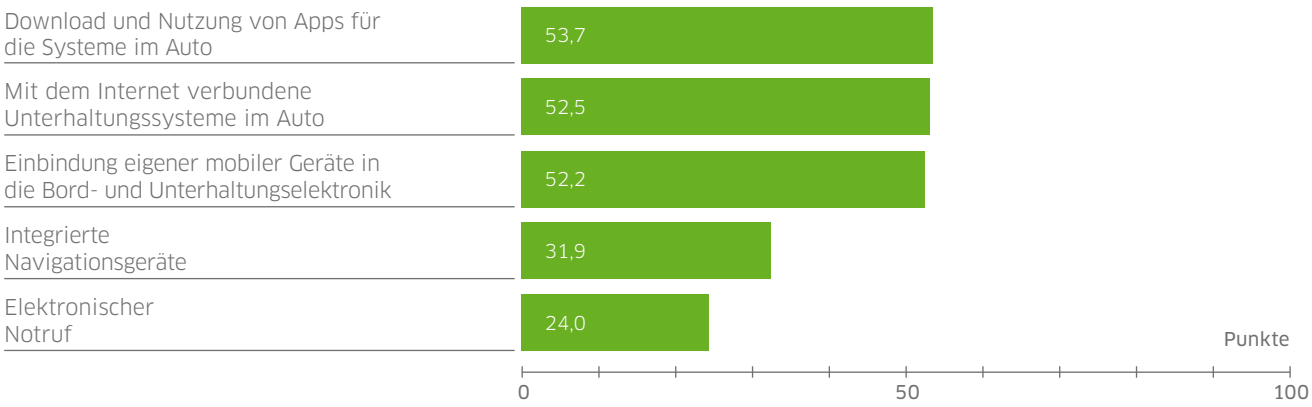
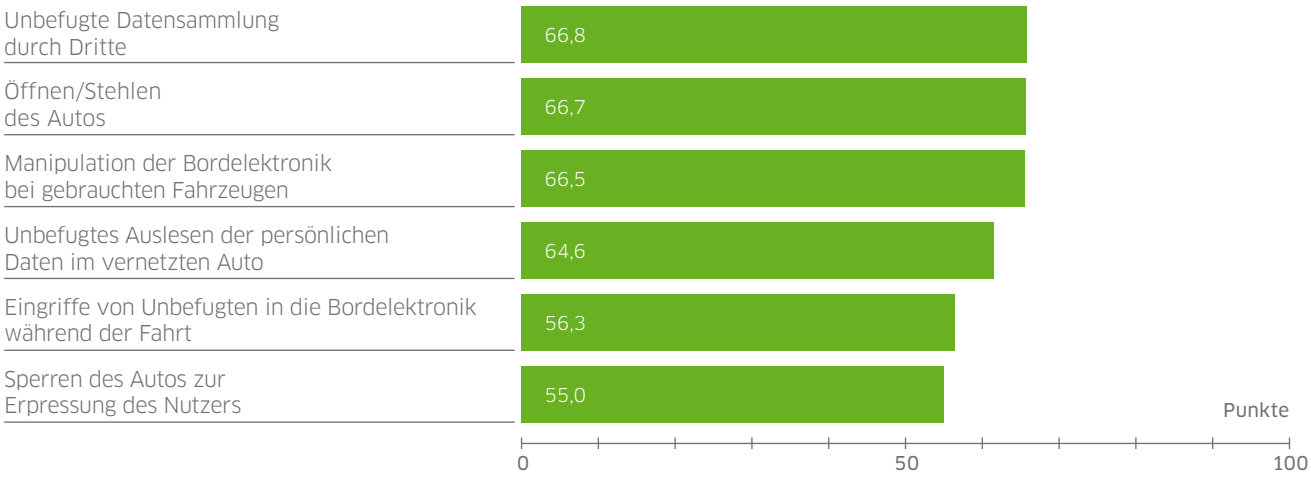


Abb. 22 Vernetztes Fahren Künftige Gefahren



haltungssysteme (52,5 Prozent) sowie die Einbindung eigener Mobilgeräte in die Bord- und Unterhaltungselektronik (52,2 Prozent). Hinsichtlich der Fahrzeugsicherheit sehen 64,9 Prozent der Onliner die Fernsteuerung von Fahrzeugfunktionen per Smartphone als größtes Risiko.

Künftige Gefahren des vernetzten Fahrens vermuten jeweils zwei Drittel der Verbraucher in der unbefugten Datensammlung durch Dritte (66,8 Prozent), dem Öffnen oder Stehlen des Autos durch das Ausnutzen von IT-Systemen (66,7 Prozent) sowie der Manipulation der Bordelektronik bei gebrauchten Fahrzeugen (66,5 Prozent).

Signifikant hoch fällt jedoch die Zahl der Befragten aus, die sich zum jetzigen Zeitpunkt überhaupt noch nicht zum Thema „Vernetztes Fahren“ positionieren wollen oder können. Mit 30,1 Prozent der Frauen und 18,2 Prozent der Männer ist der Frauenanteil in dieser Gruppe zudem sehr hoch. Es ist zu vermuten, dass ein Großteil der Unentschlossenheit auf Unwissen rekurriert.

Sicherheit des vernetzten Fahrens: Eine Frage der Verantwortung

Zuständig für die Sicherheit sind laut Meinung der Befragten vor allem die Fahrzeughersteller (79,2 Prozent) und die Halter selbst (56,7 Prozent). Etwa ein Drittel der Befragten sieht die Zuständigkeit zudem aufseiten der Politik (32,9 Prozent).

Verantwortung der Hersteller:

- Transparenz bei Erhebung und Nutzung der Daten
- Vertraulicher Umgang mit erhobenen Daten und Schutz vor Missbrauch
- Gewährleistung der Nutzer-Souveränität in Bezug auf eigene Daten

DsiN-Angebote

- **AconnectedLife.info: Leben in einer vernetzten Welt.** Tipps, um eigene Daten besser kontrollieren und schützen zu können
- **IT – Fitness Test:** Online-Wissenscheck für souveräne Mediennutzung
- **Kompetenzstelle Verbraucherfragen** im vernetzten Straßenverkehr ab 2016

Gesundheits- und Vitaldienste

Im zweiten Jahr untersucht der DsiN-Sicherheitsindex die digitale Lebenswelt der Gesundheits- und Vitaldienste. Gesundheitsapps und Fitnessarmbänder sind seit dem weiter auf dem Vormarsch. Sie erfassen Bewegungen, Lebensweise und den Biorhythmus, um sie zum Vorteil des Nutzers auszuwerten. Die Menge an erhobenen Daten stellen neue Fragen des Datenschutzes und der IT-Sicherheit.

Die Nutzungsrate von Vital- und Gesundheitsdiensten ist im Vergleich zum Vorjahr um einen Prozentpunkt gestiegen und liegt jetzt bei 8,9 Prozent der befragten Onliner. Es ist davon auszugehen, dass sich dieser Trend zum Selbstmonitoring stärker verbreitet.

Geringes Sicherheitsbewusstsein bei Fitnessapps

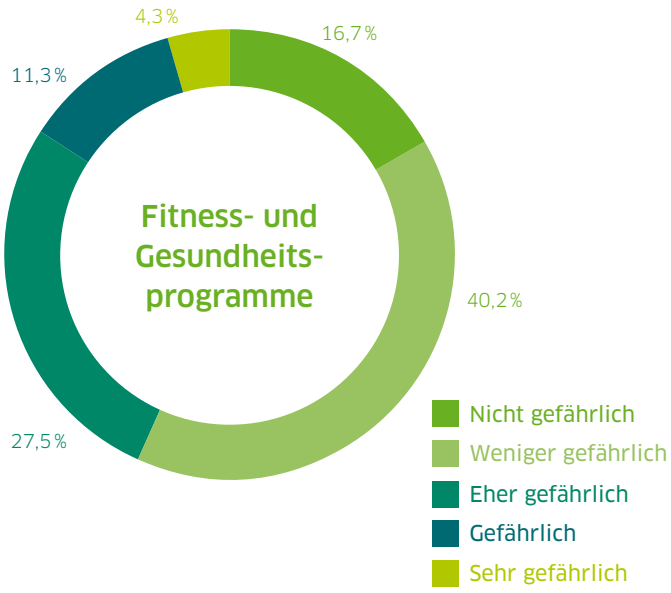
Verbraucher stehen diesen Diensten auch in diesem Jahr eher unkritisch gegenüber. 56,9 Prozent der Internetnutzer halten diese Anwendungen für nicht oder weniger gefährlich (+3,8 Prozentpunkte im Vergleich zu 2015). Lediglich 15,6 Prozent glauben, dass diese gefährlich oder sogar sehr gefährlich sind (+1,6 Prozentpunkte).

Nur 32,6 Prozent der Nutzer halten den Upload von Daten z.B. von Fitnesstrackern in die Cloud für gefährlich. Dementsprechend sind sich zwar knapp 80 Prozent der befragten Verbraucher bewusst, dass Cloud-Dienste vor ihrer Nutzung auf Vertrauenswürdigkeit geprüft werden sollten, aber nur 35 Prozent tun dies auch tatsächlich.

DsiN-Angebote

- **Initiative gut zu wissen**: Infos zu aktuellen Sicherheits- und Datenschutzfragen im Internet
- **AconnectedLife.info: Leben in einer vernetzten Welt.** Tipps, um eigene Daten besser kontrollieren und schützen zu können

Abb. 23 Gefährdungsgefühl bei Gesundheits- und Vitaldiensten



Geringes Sicherheitsbewusstsein bei Gesundheits- und Vitaldiensten

29,2 Prozent der Verbraucher nutzen Online-Dienste über einen vernetzten Fernseher

Haus- und Heimvernetzung

Für den Privatanwender zeigt sich das „Internet der Dinge“ bislang vor allem bei Hausgeräten. Von der smarten Unterhaltungselektronik über die vernetzte Haustechnik bis hin zur Energieverwaltung: Häuser und Wohnungen werden zunehmend „intelligenter“. Das schafft Erleichterungen, aber eben auch neue Angriffsfläche für Datenmissbrauch und IT-Angriffe.

Nutzung aktuell noch überschaubar

Sowohl der Gebrauch vernetzter Haustechnik als auch die Nutzung vernetzter heimischer Unterhaltungselektronik sind nach wie vor noch nicht weit verbreitet. Nur 3,6 Prozent der befragten Internetnutzer geben an, dass ihre Haustechnik vernetzt ist. Bei der Vernetzung von Unterhaltungselektronik sind es immerhin schon 9,3 Prozent. Insgesamt ist das ein kleiner Zuwachs in beiden Kategorien (+1,3 bzw. +1,6) im Vergleich zum Vorjahr.

Smart Home: Geringe Risiken aus Sicht der Verbraucher

Das smarte Zuhause wird von den meisten befragten Onlinern nicht als Sicherheitsrisiko gesehen. Nur 23,4 Prozent der Verbraucher halten die Steuerung und Vernetzung von Haustechnik für gefährlich oder sehr gefährlich (-0,9 Prozentpunkte), bei der Unterhaltungselektronik sind es sogar nur 18,3 Prozent (-2,0 Prozentpunkte).

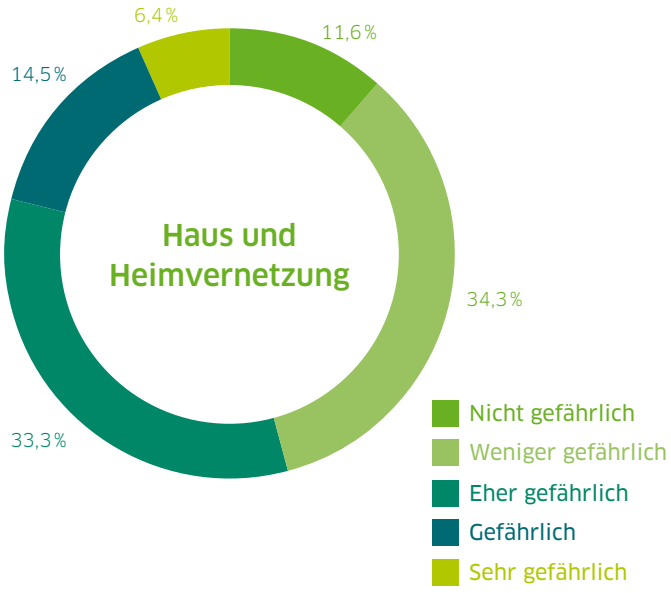
Zahl der Angriffe auf Heimvernetzung noch sehr gering

Nur 2,2 Prozent der befragten Nutzer gaben an, dass ihre Hausvernetzung angegriffen wurde, das sind 1,4 Prozentpunkte weniger als im Vorjahr. Das liegt sicher auch an der noch relativ geringen Verbreitung.

DsiN-Angebote

- **IT – Fitness Test**: Online-Wissenscheck für souveräne Mediennutzung
- **Initiative gut zu wissen:** Infos zu aktuellen Sicherheits- und Datenschutzfragen im Internet
- **AconnectedLife.info: Leben in einer vernetzten Welt.** Tipps, um eigene Daten besser kontrollieren und schützen zu können

Abb. 24 Gefährdungsgefühl bei Haus- und Heimvernetzung



Einkaufen im Internet

Deutsche Onliner bestellen und bezahlen Waren nach wie vor gerne direkt im Internet.

Das Vertrauen in Online-Shopping ist im Vergleich zum Vorjahr relativ stabil geblieben: Nur 20,9 Prozent halten das Einkaufen im Netz für gefährlich oder sogar für sehr gefährlich.

Wenig aber nicht weniger Vorfälle

Betrachtet man die sicherheitsrelevanten Vorfälle beim Online-Shopping, waren 3,8 Prozent der deutschen Onliner in den letzten 12 Monaten von Kreditkartenbetrug betroffen und 5,3 Prozent der Befragten gaben an, dass sie beim Bezahlen im Internet Opfer eines Betrugs geworden sind. Das Ausspähen von Zugangsdaten zu einem Online-Shop kam bei 5,7 Prozent vor und der Betrug bei einem Online-Einkauf oder einer Online-Buchung nannten 7,9 Prozent der Nutzer.

Zu wenige achten auf Gütesiegel

Ganze 93,2 Prozent der befragten Internetnutzer kennen digitale Zahlungssysteme. Auch genutzt werden diese immerhin von 78,1 Prozent. Eine signifikante Diskrepanz zwischen Wissen und Verhalten ist beim Thema Gütesiegel für Online-Shops zu verzeichnen: Während 89,4 Prozent der Verbraucher diese kennen, achten nur 59,2 Prozent auch darauf, ob ein Online-Shop auch tatsächlich zertifiziert ist.

DsiN-Angebote

- **DsiN Bereich für Verbraucher: Einkaufen und Bezahlen**. Tipps, um Online sicher zu bezahlen
- **Kampagne „Online Kaufen –mit Verstand!“:** Regeln, Wissenscheck und Informationsblätter

Abb. 25 Gefährdungsgefühl beim Online-Einkauf

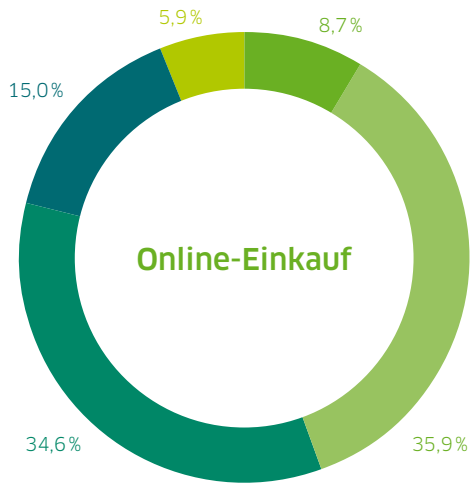
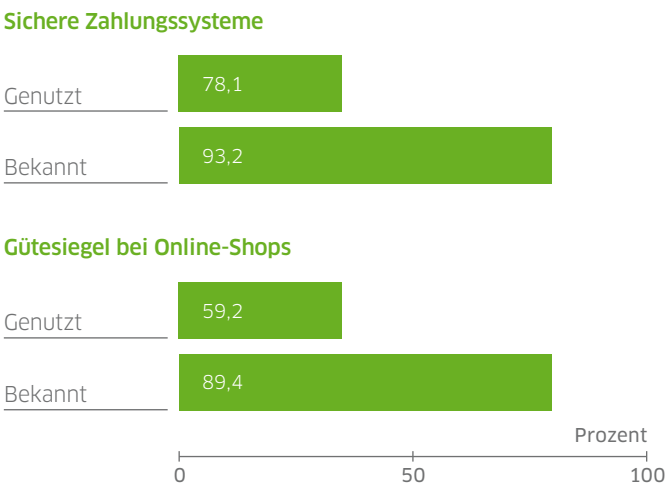


Abb. 26 Diskrepanz Wissen und Verhalten Online-Einkauf



Trotz Verbesserungen im Sicherheitsverhalten und Rückgang der Vorfälle: Verunsicherung beim Online-Banking

Bankgeschäfte im Internet

Weit verbreitet ist das sogenannte Online-Banking: die internetbasierte Abwicklung von Bankgeschäften mit Hilfe von Computer, Smartphone oder anderen Endgeräten.

Mehrheitliche Unsicherheit

Online-Banking wird von nur 27,8 Prozent der Befragten als nicht oder weniger gefährlich eingestuft (-0,4 Prozentpunkte), während 39,1 Prozent Bankgeschäfte über das Internet hingegen für gefährlich oder sehr gefährlich halten (-0,8 Prozentpunkte). Somit wird dieser digitale Dienst im Vergleich zu den anderen Lebenswelten als am unsichersten empfunden.

Ausspähen von Zugangsdaten leicht zurückgegangen

Im Vergleich zum Vorjahr ist die Anzahl der Nutzer, deren Zugangsdaten zum Online-Banking ausgespäht wurden um 0,9 Prozentpunkte auf 4,9 Prozent zurückgegangen.

Leichte Verbesserungen im Sicherheitsverhalten

Knapp 89 Prozent der Verbraucher wissen, dass es verschlüsselte Verbindungen für Online-Banking-Anwendungen gibt. 68,4 Prozent der Onliner wenden diese auch an, das sind 3,5 Prozentpunkte mehr als im Vorjahr. Auch bei der Nutzung von SMS-TANs sind leichte Verbesserungen festzustellen: Die Bekanntheit stieg um 1,1 Prozentpunkte auf 86,2 Prozent und die Nutzung sogar um 2,1 Prozentpunkte auf 56,8 Prozent.

DsiN-Angebote

- **Sicherheitsbarometer: SiBa App.** Tipps bei aktuellen Warnmeldungen
- **Für Verbraucher: Mobile Banking.** 7 Regeln für sicheres mobiles Banking
- **DsiN Sicherheitsbrief: Ihre Bankgeschäfte** Nützliche Informationen und Hinweise

Abb. 27 Gefährdungsgefühl beim Online-Banking

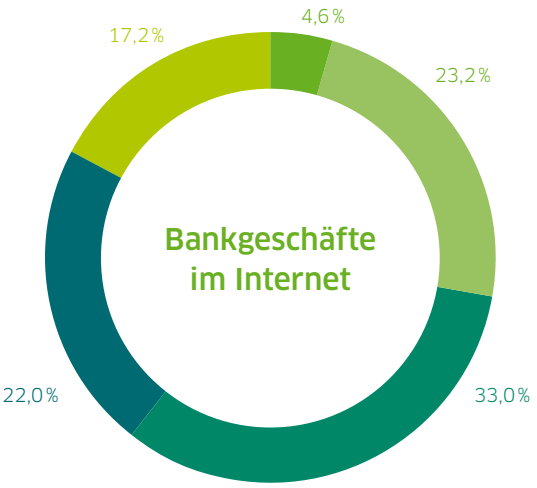
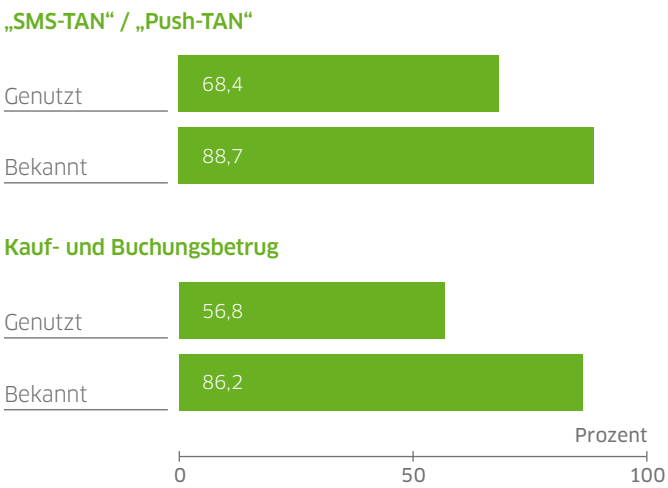


Abb. 28 Diskrepanz Wissen und Verhalten Online-Banking




Datendiebstahl
Datenmissbrauch
Soziale Netzwerke
Unaufmerksamkeit
Ausspionieren
Shoppen mit Kreditkarte
aus Versehen auf unseriöse Seiten gelangen
Trojaner
illegale Datenverknüpfung
Knacken von Zugangscodes
Geheimdienste
gehackte Werbebanner mit Schadcode
Sorglosigkeit in Bezug auf Passwörter
Weitergabe von Email-Adressen
Phishing
Shoppen mit Kreditkarte
Malware
Verbraucherstimmen:
„Die größten Risiken im Netz!“
meine fehlenden PC-Kenntnisse
Spam
Webcam wird gehackt
Viren
Virusscanner nicht installiert
Hacker
schlechte Virensoftware
Rechtsunsicherheit
Bilder ins Netz stellen
Identitätsdiebstahl
Sorglosigkeit in Bezug auf Passwörter
Mails mit Anhang
Beim Onlinebanking ausspioniert zu werden
illegale Datenverknüpfung
gehackte Werbebanner mit Schadcode
Verkauf von personenbezogenen Daten
ungenügende gesetzliche Regelungen
aus Versehen auf unseriöse Seiten gelangen
Der Faktor Mensch

Kapitel 04

Digitale Aufklärung: Sensibilisieren – Befähigen – Motivieren

Handlungsfeld Sensibilisieren

IT-Sicherheit beginnt im Kopf. Der erste Schritt muss sein, Verbraucher direkt anzusprechen und Aufmerksamkeit für IT-Sicherheit sowie ein Bewusstsein für mögliche Risiken zu schaffen. Erst dann verankert sich Wissen um Schutzmaßnahmen nachhaltig bei Nutzern. Hierzu gehört auch, Verbraucher aktiv dazu aufzufordern, das eigene Verhalten mit digitalen Diensten zu beobachten, damit sie eigene Defizite bewusst erkennen.

Sicherheitswissen ausbauen

Zwar haben sich deutsche Onliner – vor allem im Bereich des Basisschutzes – inzwischen umfangreiches Wissen angeeignet, allerdings ist dies hinsichtlich komplexerer Sicherheitsmaßnahmen meist nicht ausreichend. Dies gilt vor allem für die Außenstehenden. Um auf digitale Bedrohungen reagieren zu können, müssen alle Verbraucher unterstützt werden, auch komplexe Schutzvorkehrungen zu kennen und zu verstehen. Dazu gehören Sicherheitsmaßnahmen wie die Daten- und Festplattenverschlüsselung, die Überprüfung von Datenträgern, Passwortmanager, E-Mail Verschlüsselung, Phishing-Filter und die Überprüfung von Cloud-Diensten sowie Passworttresoren.

Der DsiN-Sicherheitsindex 2016 zeigt, dass zwei Drittel der Verbraucher Aufklärung in Form von mehr und zudem verständlicheren Informationen, unter anderem auf einer zentralen Internetseite fordern. Da die Souveränen und Fatalisten schon einen guten Wissensstand aufweisen, benötigen sie Informationen zu komplexeren Schutzmaßnahmen. Die Außenstehenden haben schon beim Grundlagenwissen Nachholbedarf.

Abb. 29 Schlusslichter Kenntnisstand – Gerätesicherheit

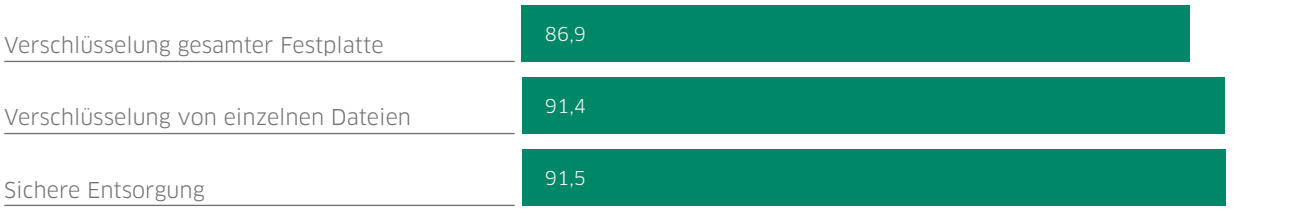


Abb. 30 Schlusslichter Kenntnisstand – Authentifizierung

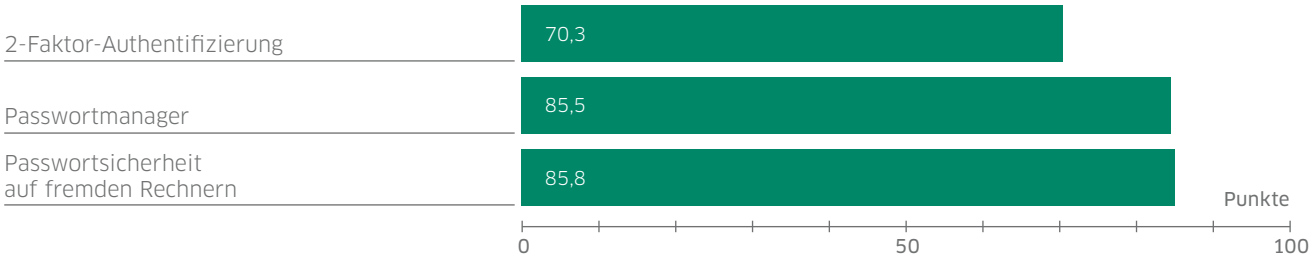


Abb. 31 Schlusslichter Kenntnisstand – E-Mail

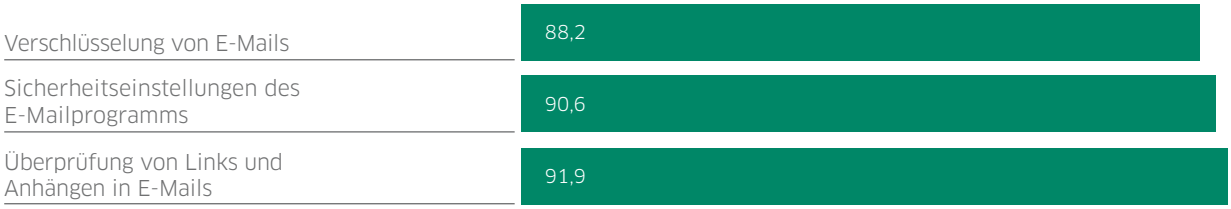


Abb. 32 Schlusslichter Kenntnisstand – Browsing

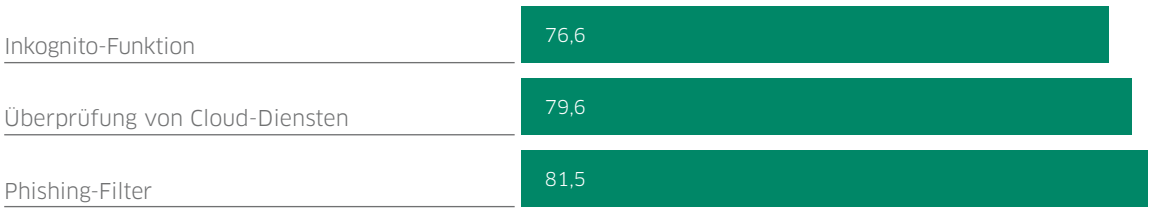
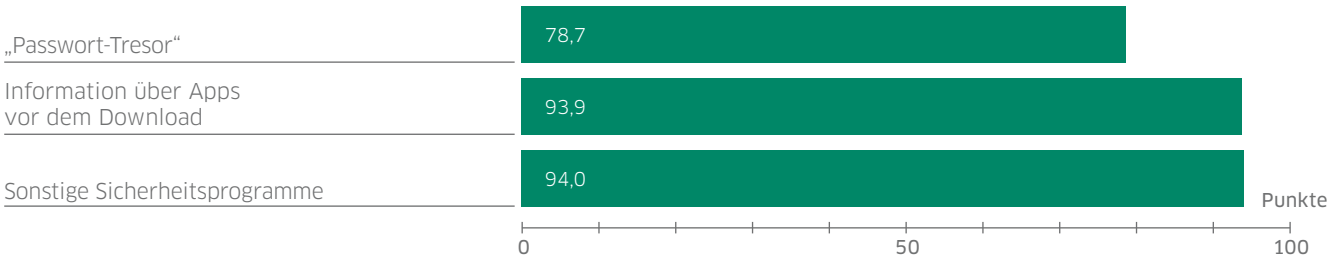


Abb. 33 Schlusslichter Kenntnisstand – mobiles Internet



Handlungsempfehlungen

- **Bewusstsein schaffen**: Außenstehenden aktiv Hinweise und Informationen geben
- **Sicherheitsrisiken verstehen:** Darstellung relevanter Risiken für alle Verbrauchergruppen
- **Basiswissen vermitteln:** Alle Nutzergruppen mit Grundlagenwissen ausstatten
- **Kenntnisse vertiefen:** Komplexere Anforderungen – je nach Bedarf – vermitteln

DsiN-Angebote zur Sensibilisierung:

- **DsiN-Sicherheitsbarometer** (auch als App)
- **Digital-Kompass:** Aufklärungsinitiative
- **Internet- Sicherheitsbriefe:** Wissensvermittlung
- **Initiative gut zu wissen:** Sicherheits- und Datenschutzinfos

Bewusstsein schaffen – über Risiken aufklären – Wissen vermitteln

Handlungsfeld Befähigen

Für eine Befähigung zu mehr IT-Sicherheit ist ein aktiver Ansatz notwendig: Wir müssen auf Verbraucher zugehen und sie dazu anleiten, potentielle Risiken zu erkennen und Maßnahmen tatsächlich umzusetzen. Insbesondere eine Schärfung der Risikoeinschätzungskompetenz ist erforderlich, um souveräner bewerten zu können, welche Maßnahmen für den IT-Schutz sinnvoll sind.

Zielgruppenorientiert über Risiken und Chancen aufklären

Bei der Befähigung zum Selbstschutz ist eine zielgruppenspezifische Aufklärungsarbeit notwendig. So offenbart der Sicherheitsindex ein Gefälle im Gefährdungsgefühl zwischen den einzelnen Nutzergruppen, was auf abweichende Risikoeinschätzungskompetenzen zurückgeführt werden kann. Während die Fatalisten ein sehr ausgeprägtes Bedrohungsgefühl aufweisen, ist ein solches bei den Gutgläubigen kaum vorhanden. Die Kompetenz zum Erkennen echter Risiken in Abgrenzung zur undifferenzierten Verunsicherung muss angeglichen werden. Danach befragt, was für eine Stärkung des Risikobewusstseins hilfreich wäre, wünschen sich 54,6 Prozent der Verbraucher eine bessere Aufklärung über Risiken von den Programm- und Dienstanbietern, gefolgt von dem Wunsch nach mehr Warnhinweisen im Internet (52,9 Prozent), einer besseren Aufklärung außerhalb des Netzes (45,3 Prozent) und mehr Informationen zu Risiken im Netz (42,7 Prozent). Wichtig ist, auch die Chancen der Digitalisierung zu betonen, um Übervorsichtigkeit und Hemmungen abzubauen und Vertrauen zu schaffen.

Komplexer IT-Schutz bleibt für viele Anwender große Hürde

Um das Schutzniveau nachhaltig zu verbessern, müssen Verbraucher Sicherheitsmaßnahmen nicht nur gut kennen, sondern auch anwenden. Vor allem die Gutgläubigen,

Abb. 34 Stärkung des Risikobewusstseins

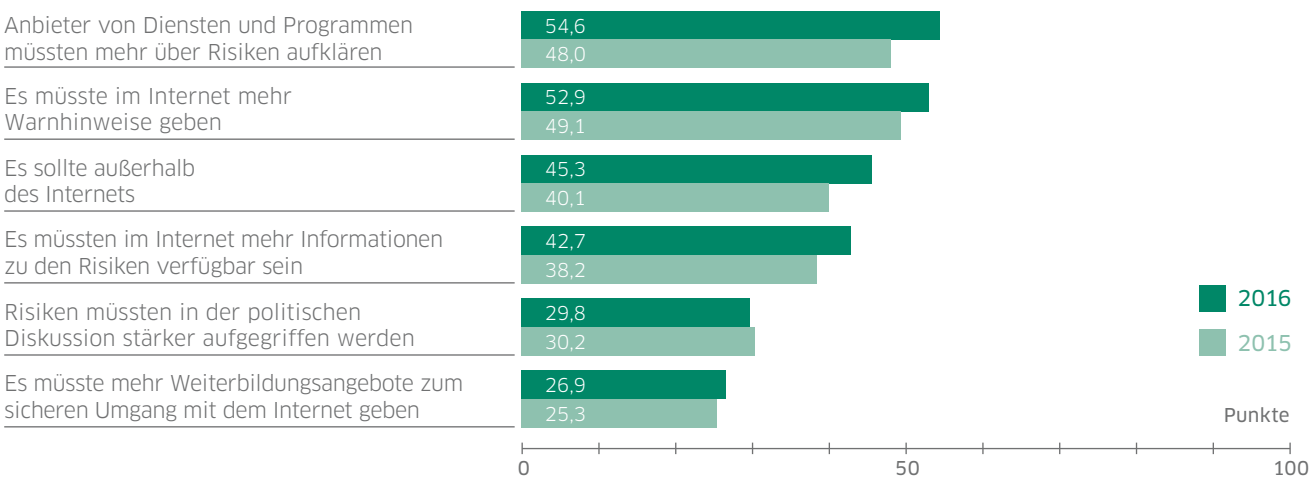
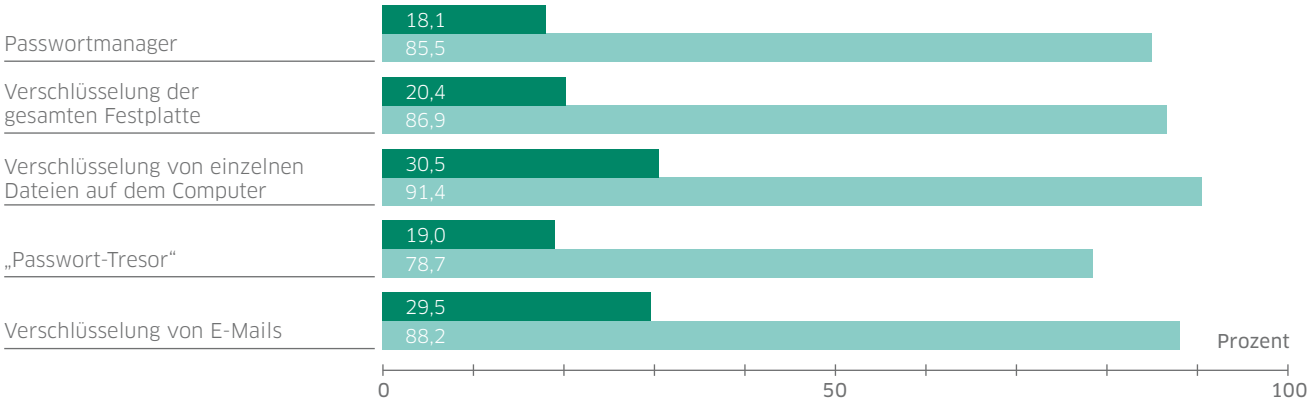


Abb. 35 Kenntnis versus Nutzung – Schlusslichter



Fatalisten und Außenstehenden benötigen diesbezügliche Unterstützung. Besonders auffällig: Je komplexer oder je unbekannter eine Sicherheitsmaßnahme ist, desto seltener erfolgt ihre Anwendung. Vor allem im Bereich Verschlüsselung ist die Wissens-Verhaltens-Lücke sehr groß. Und auch der Passwortmanager bleibt, was die tatsächliche Nutzung betrifft, ein Schlusslicht: Nur 19 Prozent nutzen ihn – und das, obwohl 78,7 Prozent Passwortmanager kennen.

Umsetzungskompetenzen trainieren

Um das Sicherheitsverhalten und die Lücke zwischen Kennen und Nutzen zu schließen, müssen Nützlichkeit und Effektivität von Schutzmaßnahmen sowie die Folgen nachlässigen Verhaltens veranschaulicht werden. Das Selbstvertrauen sowie die Selbstwirksamkeit von Verbrauchern muss gestärkt werden, damit sie in die Fähigkeit vertrauen, notwendige Handlungsweisen souverän und kompetent zu wählen. So können sie das Gefühl der Unsicherheit und Hilflosigkeit und somit auch ihre Hemmungen im Umgang mit digitalen Diensten abbauen. Verbraucher profitieren außerdem von konkreten Anleitungen, wie sie nützliche Vorkehrungen umsetzen und komplizierte Mechanismen im Gebrauch vereinfachen können – beispielsweise die regelmäßige Passwortänderung durch Passwort-Manager.

Handlungsempfehlungen

- **Einschätzungskompetenz fördern:** Unterstützung zur individuellen Risikoeinschätzung
- **Umsetzungskompetenz ausbauen:** Sicherheitswissen auf konkrete Anwendungen beziehen
- **Sicherheitsangebote vereinfachen:** Durch praktische Handhabbarkeit auch komplexere Maßnahmen vermitteln
- **Selbstvertrauen stärken:** Vertrauen in die eigenen Fähigkeiten fördern

DsiN-Angebote zur Befähigung:

- **Bottom-Up:** Berufsschüler für IT-Sicherheit
- **DsiN-Sicherheitsbarometer** (auch als App)
- **DsiN-Aufklärungsfilme**
- **Medien in die Schule:** Material für den Unterricht
- **Digitale Nachbarschaft:** Multiplikatoren im Ehrenamt

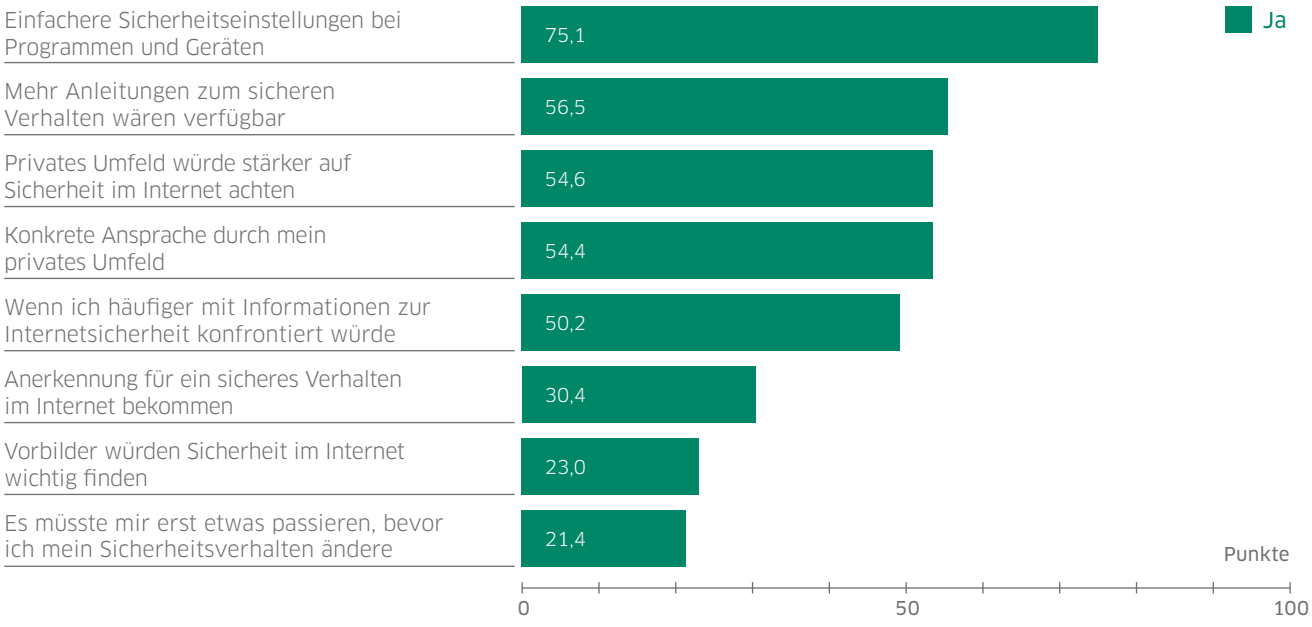
Sicherheitspraxis: Motivieren

Selbst wenn die Kenntnisse um Schutzmaßnahmen und deren Anwendung vorhanden sind, stehen meist Bequemlichkeit oder mangelnde Überzeugung von der Notwendigkeit im Wege. Dabei weiß die Mehrheit der Verbraucher bereits, dass sie für ihre IT-Sicherheit mitverantwortlich ist. Mehr als zwei Drittel geben an, selbst durch einen vorsichtigeren Umgang einen Beitrag zum Abbau sicherheitsrelevanter Vorfälle leisten zu können und die Hälfte der Befragten sieht ein, dass sie regelmäßiger Sicherheitsmaßnahmen einsetzen sollten. Zentraler Ansatzpunkt ist und bleibt deshalb die wirksame Motivation, damit Verbraucher dieser Verantwortung nachkommen.

Motivation durch Anerkennung

Motivation können wir aktiv durch Anreize materieller Art oder – nachhaltiger – durch Anerkennung fördern. Verbraucher, die erfolgreich für ihre IT-Sicherheit Sorge tragen, müssen gesellschaftliches Ansehen genießen und wir müssen ihr Verhalten honorieren – beispielsweise auch im beruflichen Kontext – sodass es ebenfalls für andere erstrebenswert wird, dieser Verantwortung nachzukommen. Unsere Aufgabe hierbei ist zudem, Sicherheitswissen für alle Verbraucher schnell und einfach zugänglich und erlernbar zu machen, damit die Umsetzung unkompliziert realisiert werden kann. Wettbewerbe und die Ausstellung von Zertifikaten bei nach-

Abb. 36 Selbsteinschätzung der Verbraucher: Was motiviert zu IT-Sicherheit?



weisbaren Kompetenzen kann die Motivation, sich für seine IT-Sicherheit einzusetzen, aufseiten der Verbraucher erhöhen. Drei Viertel der Befragten geben außerdem an, dass einfachere Sicherheitseinstellungen der Programme und Geräte ihre Motivation zur Anwendung von Sicherheitsmaßnahmen steigern würden. Etwas mehr als die Hälfte wünscht sich mehr Anleitungen zum sicheren Verhalten, z. B. durch Schulen oder andere Einrichtungen sowie Unterstützung aus dem privaten Umfeld.

Drei Schritten zu mehr Motivation

1. **Erkennen:** Verbraucher sollten selbst das Bedürfnis entwickeln, etwas für ihren Schutz tun zu wollen. Relevant ist also die Vermittlung einer Haltung, die zum sicheren Umgang im Netz „auffordert". Sie verstehen, dass sie selbst Verantwortung für ihr Handeln und ihre Sicherheit tragen und dieser Verantwortung gerecht werden.
2. **Handeln:** Damit Verbraucher die erlernten Schutzmaßnahmen einsetzen, sollten Anleitungen für Sicherheitseinstellungen vereinfacht werden. Auch das Einbinden von Bildungseinrichtungen und des privaten Umfelds ist lohnenswert. Routinetraining fördert, Maßnahmen zu verinnerlichen. Der Bezug aktueller Informationen sollte dafür vereinfacht werden.
3. **Bewältigen:** Damit die Nutzer erfahren, dass ihr Verhalten mehr Sicherheit bewirkt, sollte entsprechende Anerkennung erfolgen: Beispielsweise innerhalb der eigenen Peergroup. Konfrontation mit möglichen Risiken kann den Effekt unterstützen sowie auch regelmäßige und aktive Ansprachen. Vorbilder spielen dafür eine wichtige Rolle.

Handlungsempfehlungen

- **Einsicht durch Anerkennung fördern**: Erfolgsaussichten verdeutlichen und Würdigung verstärken
- **Konkrete Anleitungen verbreiten:** Einfach verständliche Anleitungen für den Alltag verbreiten
- **Vorbilder gewinnen:** Personen mit Vorbildfunktion bei Sicherheitsthemen einbinden
- **Umsetzung vereinfachen:** Sicherheitsoptionen leichter vermitteln

DsiN-Angebote zur Motivation:

- **myDigitalWorld:** Jugendwettbewerb
- **Goldener Internetpreis für Senioren**
- **Digitale Nachbarschaft:** Multiplikatoren im Ehrenamt
- **Internetbeschwerdestelle**
- **DsiN MesseCampus**

Einsicht, einfache Umsetzung und Anerkennung fördern

Fazit: Sicherheit durch Verantwortung stärken

Mit Digitaler Aufklärung 2.0 die Sicherheit für Verbraucher verbessern

Aufklärung ist das Gebot der Stunde! Die Studie zeigt, dass mangelnde Kenntnisse, Motivation und Sorglosigkeit die Sicherheitslage bei fast 60 Prozent der Onliner beeinträchtigen, nur wenige Punkte vom kritischen Schwellenwert entfernt. Im dritten Jahr der Erhebung zeigt die Studie aber auch, dass Verbesserungen möglich sind – so haben sich fast alle Werte seit 2014 verbessert. Die Verunsicherung der Verbraucher hat in dieser Zeit gleichwohl zugenommen und birgt das Risiko einer digitalen Vertrauenskrise. Die Chancen der Digitalisierung werden aber nur zur Entfaltung kommen, wenn Sicherheit und Vertrauen hergestellt und aufrechterhalten werden. Die Studie bietet dafür Anknüpfungspunkte, diesem Ziel im Rahmen einer Digitalen Aufklärung 2.0 näher zu kommen – mit folgenden drei Faktoren

1. Individuelle Aufklärung betreiben – aktiv.
Defizite bei den vier sicherheitsrelevanten Faktoren sind in jeder Verbrauchergruppe anders ausgeprägt und müssen daher individuell adressiert werden. Hinzu kommt das Erfordernis einer aktiven Ansprache: Statt passiver Kommunikation wird es künftig verstärkt um aktive Einbindung von Verbrauchern gehen, um Verhaltensveränderungen zu bewirken. Eine Aufklärung mit der Gießkanne ginge dagegen mit großen Streuverlusten einher.

2. Aufklärungsinitiativen vernetzen – jetzt.
Es gibt zahlreiche Aufklärungsinitiativen mit nützlichen Hilfestellungen im digitalen Alltag für Verbraucher. Hochwertige Angebote sollten besser miteinander vernetzt werden, damit sie einfacher und besser zugänglich werden. Die Transparenz dient darüber hinaus den Anbietern für einen besseren Überblick zum Status Quo und Defiziten von Aufklärungsangeboten.

3. Dialog der Beteiligten verstärken – transparent.
Erst das Zusammenspiel von technologischer Innovation, Regulierungs- und Aufklärungsmaßnahmen bei Verbrauchern ermöglicht es, digitalen Schutz und IT-Sicherheit herzustellen und aufrechtzuerhalten. Daher ist ein Dialog erforderlich, der alle Beteiligten zusammenführt, Defizite in den jeweiligen Bereichen transparent macht und abgestimmte Lösungen fördert.

Glossar

DsiN-Sicherheitsindex	Sicherheitslage deutscher Onliner in einer Zahl – als gewichteter Mittelwert aus den vier Sicherheitsfaktoren. (Nachfolgende vier)
Sicherheitsrelevante Vorfälle	Für die Sicherheit relevante Vorfälle, die von den Onlinern bemerkt wurden.
Gefährdungsgefühl	Das von den deutschen Onlinern selbst eingeschätzte Risiko bei der Nutzung ausgesuchter Technologien und Anwendungen.
Sicherheitskompetenz	Selbstauskunft über die Kenntnis von IT-Schutzmaßnahmen.
Sicherheitsverhalten	Selbstauskunft über die Anwendung von IT-Schutzmaßnahmen.
Indexpunkte	Der DsiN-Index wird auf einer Skala von 1 bis 100 gemessen.
Schwellenwert 50	Bei Werten unter 50 Indexpunkten ist die Bedrohungslage höher als das Schutzniveau.
DsiN-Nutzertypen	Eine Clusterung der deutschen Onliner. Es gibt 4 Nutzertypen, die sich durch typische Verhaltensweisen auszeichnen

Über Deutschland sicher im Netz e.V.

DsiN leistet konkrete Hilfestellung für Verbraucher sowie für kleine und mittlere Unternehmen im sicheren Umgang mit dem Internet. Dafür entwickelt DsiN praktische Angebote und Anleitungen im Verbund mit Unternehmen, Verbänden und Vereinen. Als produktunabhängige Plattform für Aufklärungsinitiativen ist DsiN für neue Mitglieder offen, die IT-Sicherheit als maßgeblich für den Erfolg der Digitalisierung betrachten.

In der Digitalen Agenda der Bundesregierung wurde ein Ausbau der Zusammenarbeit und Unterstützung von DsiN beschlossen. Schon heute verstärkt DsiN seine Aufklärungsarbeit: Für Verbraucher stehen kostenlose Anleitungen zum souveränen digitalen Umgang im Netz im Mittelpunkt wie die SiBa-App zu aktuellen Warnmeldungen und das DsiN-Webportal.

Gegründet wurde DsiN als gemeinnütziger Verein im Nationalen IT-Gipfelprozess der Bundesregierung und steht seit 2007 unter der Schirmherrschaft des Bundesministeriums des Innern. DsiN möchte seine Aufklärungsarbeit im Dialog mit der Politik, der Wissenschaft und weiteren Akteuren der digitalen Gesellschaft weiter stärken.

Impressum

DsiN-Sicherheitsindex 2016
Studie von Deutschland sicher im Netz e.V. zur digitalen Sicherheitslage der Verbraucher in Deutschland

Verantwortlich: Dr. Michael Littger

Redaktion: Nadine Grau (Leitung); Tobias Weber (TNS)

Studienpartner: TNS Infratest

Gestaltung: Studio GOOD, Berlin

Infografiken: Carsten Raffel (USOTA)

Stand: Juni 2016

Deutschland sicher im Netz e.V.
Albrechtstraße 10 b
10117 Berlin
Telefon +49 30 27576 – 310
Telefax +49 30 2757651 – 310
www.sicher-im-netz.de
info@sicher-im-netz.de

Quellennachweise:
BMJV, DTAG, DsiN
Titel / Seite 7, 9, 13, 24, 33: shutterstock.com