



DsiN

SicherheitsIndex 2017

Digitale Sicherheitslage
der Verbraucher in Deutschland

Schirmherrschaft:



Bundesministerium
des Innern



**Deutschland
sicher im Netz**



www.sicher-im-netz.de



Ulrich Kelber

Vertrauen und Verantwortung stärken

Die Chancen der Vernetzung für Menschen steigen mit den vielfältigen Diensten und Technologien, die uns jeden Tag zur Teilnahme einladen. Dies gilt für ältere Generationen mit Erleichterungen beim Onlineeinkaufen und -bezahlen, bei Reisebuchungen und Bankgeschäften. Auch der Videoanruf der Familie trägt zur Lebensfreude und sozialen Anbindung bei. Für jüngere Menschen ist die Digitalisierung längst prägend im Alltag. Digitale Netzwerke führen zu neuen Kommunikationsverhalten, Informationen werden überall und in Echtzeit wie selbstverständlich abgerufen.

Viele Dienste sind einfach zu bedienen und stehen in vielen Fällen auch unentgeltlich zur Verfügung. Mit dem Erfolg der Digitalisierung steigen aber auch die Anforderungen an eine sichere und vertrauenswürdige digitale Umgebung. Denn je größer die Einbindung digitaler Dienste im Alltag erfolgt, desto schwerer wiegen Ausfälle, Manipulationen oder der Missbrauch von Daten. Wir müssen daher wachsam sein, dass Digitalisierung und Sicherheit Hand in Hand gehen und Klarheit besteht, dass beide Seiten einander bedingen.

Der DsiN-Sicherheitsindex ist ein etablierter Gradmesser für die Sicherheitslage der Verbraucher im Cyberraum in Deutschland. Für diese Arbeit ist die Betrachtung der Sicherheitslage nach Verbrauchertypen im Index eine hilfreiche Unterstützung. Sie gibt Auskunft über Defizite und Handlungserfordernisse aus Sicht der Verbraucher.

Das Bundesministerium der Justiz und für Verbraucherschutz versteht digitale Aufklärungsarbeit als Fundament, um Verbrauchern Sicherheit im Netz zu vermitteln. Das Engagement in die Aufklärungsarbeit ist eine wichtige Investition in die digitale Zukunft. Vorbildlich dafür steht der Digital-Kompass für ältere Generationen von Deutschland sicher im Netz (DsiN) im Verbund mit der Bundesarbeitsgemeinschaft der Senioren-Organisationen (BAG-SO), den wir gern auch in Zukunft weiter unterstützen.

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

Bildung für IT-Sicherheit!

Die gute Nachricht zuerst: Das Sicherheitswissen der Verbraucher ist seit 2014 das dritte Mal in Folge gestiegen. Das ist auch ein Ergebnis einer kontinuierlichen und erfolgreichen Aufklärungsarbeit für IT-Sicherheit. Gleichzeitig stellen wir eine höhere Bedrohungslage fest.

Der DsiN-Sicherheitsindex liegt 2017 bei 61,1 Punkten - vier Punkte weniger als noch 2016. Wir können noch nicht absehen, ob hier ein neuer Trend der IT-Sicherheitslage entsteht. Klar ist aber, dass die digitale Durchdringung des Alltags zusätzliche Anforderungen an die Schutzkompetenzen der Verbraucher stellen wird.

Was bereits jetzt offensichtlich ist: Wir müssen das Übel an der Wurzel packen. Digitale Kompetenz ist Schlüsselkompetenz im 21. Jahrhundert: Nur wenn Menschen schon in jungen Jahren in die Lage versetzt werden, auf wachsende und sich verändernde Risiken im Alltag zu reagieren, sind sie gewappnet. Dies bedeutet aber auch, dass IT-Sicherheit und Schutz von Daten zum integralen Bestandteil des Bildungskanons werden muss. DsiN reagiert an dieser Stelle bereits mit einem neuen Bildungsangebot: Digitale Bildung trifft Schule, kurz DigiBitS.

Auch im vierten Erhebungsjahr besteht ein digitales Sicherheitsgefälle in Deutschland. Die Gruppe der Außenstehenden benötigt zusätzliche Hilfsangebote für grundlegendes Sicherheitswissen, während bei den Fatalisten die Motivation im Zentrum steht. Das zeigt uns, dass unser zielgruppenspezifischer Ansatz richtig ist. Wir müssen Verbraucher in ihren digitalen Sicherheitssituationen und Bedarfen ansprechen. Hierin wurden wir durch die Aufnahme in die neue Cyber-Sicherheitsstrategie der Bundesregierung bestärkt.

Und: Verbraucher stehen innovativen Diensten eher skeptisch gegenüber. Bei digitalen Gesundheitsdiensten zeigt uns der Index, dass Verbraucher zwischen Chancen und Risiken noch nicht souverän unterscheiden. Hier können wir unterstützen, eine realistische Abschätzung zu Nutzen und Risiken zu erlernen.

Zu guter Letzt: Digitale Aufklärung und digitale Sicherheit gibt es nicht umsonst. Aufklärungsarbeit erfordert Ressourcen, um nachhaltig und in der Breite die Menschen zu erreichen. Unserer Ansicht nach sollten deshalb 10 Prozent des Budgets für IT-Sicherheit in die Aufklärungsarbeit von Anwendern, Verbrauchern, Unternehmen und Organisationen fließen.

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

| | |
|--|----|
| Vertrauen und Verantwortung stärken | 3 |
| Grußwort von Ulrich Kelber, Parlamentarischer Staatssekretär beim Bundesministerium der Justiz und für Verbraucherschutz | |
| Bildung für IT-Sicherheit | 4 |
| Vorwort von Dr. Thomas Kremer und Dr. Michael Littger | |
| Inhaltsübersicht | 5 |
| Ergebnisse 2017 auf einen Blick | 6 |
| Ziel und Methode des Sicherheitsindex | 8 |
| KAPITEL 1 DsiN-Sicherheitsindex 2017: 61,1 Punkte | 9 |
| Indexwert 2017: Rückgang auf 61,1 Punkte | 10 |
| Die vier Sicherheitsfaktoren | 12 |
| Einflussfaktoren für IT-Sicherheit | 14 |
| KAPITEL 2 IT-Sicherheitsgefälle: Unterschiede zwischen Verbrauchertypen | 15 |
| IT-Sicherheitslage: Abhängigkeit von Verbrauchertypen | 16 |
| Außenstehende Nutzer (49,4 Punkte) | 18 |
| Fatalistische Nutzer (50,0 Punkte) | 20 |
| Gutgläubige Nutzer (58,4 Punkte) | 22 |
| Souveräne Nutzer (69,4 Punkte) | 24 |
| Verbraucherstimmen: Was wünschen sich Verbraucher für mehr IT-Sicherheit? | 26 |
| KAPITEL 3 Digitale Lebenswelten | 27 |
| Fokusthema: Gesundheit und Fitness digital | 28 |
| Vernetzter Verkehrsraum: Das Automobil | 30 |
| Haus- und Heimvernetzung | 31 |
| Einkaufen im Internet | 32 |
| Bankgeschäfte im Internet | 33 |
| KAPITEL 4 Digitale Aufklärung: Selbstkompetenzen für IT-Sicherheit stärken | 34 |
| Digitale Aufklärung durch digitale Bildung | 35 |
| Grundlagen: Informieren und Sensibilisieren | 36 |
| Anleiten und Befähigen | 38 |
| Eigenverantwortung stärken und Motivieren | 40 |
| Fazit: Selbstkompetenzen für IT-Sicherheit frühzeitig stärken | 42 |
| Glossar | 42 |
| Über Deutschland sicher im Netz e.V. | 43 |
| Impressum | 44 |

Ergebnisse 2017 auf einen Blick

Der DsiN-Sicherheitsindex 2017 liegt bei **61,1 Punkten** und ist somit gegenüber dem Vorjahr um 4,3 Punkte niedriger. Ausschlaggebend dafür ist ein höherer Indexwert der Sicherheitsvorfälle bei Verbrauchern. Dieser Wert liegt nun bei 41,7 Punkten (2016: 30,1 Punkte). Das Sicherheitswissen konnten die deutschen Onliner im Vergleich zum Vorjahr um 2,2 Punkte auf 86,4 Punkte steigern; gleichzeitig ist das Sicherheitsverhalten um 1,5 Punkte auf 51,4 Punkte gesunken. Die Diskrepanz zwischen Kenntnis und Nutzung von Schutzmaßnahmen hat damit weiter zugenommen (siehe dazu Kapitel 1).

Ein Viertel der Verbraucher besonders gefährdet

Der DsiN-Sicherheitsindex differenziert zwischen vier Verbrauchertypen (siehe dazu Kapitel 2) und offenbart dadurch ein digitales Sicherheitsgefälle: Während die Gruppe der Souveränen mit 69,4 Indexpunkten einen relativ guten Wert erreicht, liegen die Außenstehenden mit 49,4 Indexpunkten unter dem kritischen Schwellenwert von 50 Punkten und übernehmen die rote Laterne unter allen Verbrauchergruppen. Die Fatalisten mit 50,0 Indexpunkten liegen auf dem vorletzten Platz. Bei beiden Gruppen erreicht oder übersteigt die Bedrohungslage das Schutzniveau. Aber auch die Gruppe der Gutgläubigen benötigt mit 58,4 Indexpunkten weitere Hilfsangebote. Ein zentraler Nutzen der Studie ergibt sich aus den konkret ableitbaren Zielen für die Aufklärungsarbeit: Während Außenstehende leicht verständliche Informationen und konkrete Handlungsempfehlungen benötigen, müssen Fatalisten eine realistische Risikoeinschätzung trainieren zum Abbau einer diffusen Verun-

sicherung. Gutgläubige weisen die größte Diskrepanz zwischen Sicherheitswissen und -verhalten auf und müssen zur Anwendung ihres vorhandenen Wissens motiviert werden. Souveräne Nutzer sollten in die Aufklärungsarbeit einbezogen werden, um andere im sicheren Umgang mit dem Internet zu unterstützen.

Übergreifende Schlüsselqualifikation: Digitale Kompetenz

Die Förderung digitaler Kompetenz als übergreifende Schlüsselqualifikation entwickelt sich zur Kernaufgabe digitaler Aufklärung 2.0 (siehe dazu Kapitel 4): Sie befähigt Verbraucher, einem wachsenden Spektrum an Bedrohungen entgegenzutreten – für einen souveränen Umgang mit der voranschreitenden Digitalisierung. Dies wirkt dem Szenario entgegen, dass die Bedrohungslage künftig das Schutzniveau der Verbraucher übertreffen könnte. Digitale Aufklärungsarbeit muss Hilfe zur Selbsthilfe leisten, damit Verbraucher Verantwortung übernehmen können für ihre digitale Sicherheit.

Der DsiN-Index untersucht auch die Sicherheitslage in einzelnen digitalen Lebenswelten. 2017 stehen die digitalen Gesundheits- und Fitnessdienste im Fokus. Verbraucher erkennen den Nutzen von Gesundheitsdiensten, wenn es um die Früherkennung von Krankheiten und die Verbesserung der Qualität der medizinischen Grundversorgung geht. Skepsis überwiegt, wenn der Mehrwert für die eigene Gesundheit nicht unmittelbar erkennbar ist. Allerdings ist die Zahl derjenigen Befragten, die sich nicht äußern können oder wollen, signifikant hoch. Hier kann digitale Aufklärung das Wissen für souveräne Entscheidungen stärken.

* 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 2017

DsiN-Sicherheitsindex 2017

Digitale Sicherheitslage der Verbraucher in Deutschland

BEDROHUNGLAGE



Gefährdungsgefühl

27,1



Sicherheitsvorfälle

41,7

SCHUTZNIVEAU



Sicherheitswissen

86,4



Sicherheitsverhalten

51,4

GESAMTINDEX UND ENTWICKLUNG

2017

61,1

63,0
(2015)

60,2
(2014)

65,4
(2016)

0

50
Schwellenwert

100

DIGITALES SICHERHEITSGEFÄLLE: DIE VIER VERBRAUCHERTYPEN

49,4

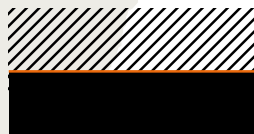


Außenstehende
Nutzer



6,4%

50,0



Fatalistische
Nutzer



17,2%

58,4



Gutgläubige
Nutzer



33,9%

69,4



Souveräne
Nutzer



42,5%

Digitale Aufklärung 2.0

Individueller Aufklärungsmix für Verbrauchergruppen – Vernetzung von Aufklärungsangeboten
Aufklärung im Dialog mit Politik, Wirtschaft und Wissenschaft

SENSIBILISIEREN

BEFÄHIGEN

MOTIVIEREN

Ziel und Methode des Sicherheitsindex

Der DsiN-Sicherheitsindex bildet die digitale Sicherheitslage der Verbraucher in Deutschland in einer Kennziffer auf einer Skala von 0 bis 100 ab. Zudem unterscheidet er nach vier verschiedenen Verbrauchertypen und nimmt fünf digitale Lebenswelten in den Fokus: Digitale Gesundheits- und Vitaldienste als Fokusthema 2017 sowie Haus- und Heimvernetzung, Online-Shopping, Online-Banking und den vernetzten Verkehrsraum. Für die vorliegende Studie hat das Markt- und Meinungsforschungsinstitut KANTAR TNS rund 2.000 Verbraucher befragt – repräsentativ für alle deutschen Internetnutzer über 16 Jahre.

Dynamisches Verhältnis von Bedrohungslage und Schutzniveau

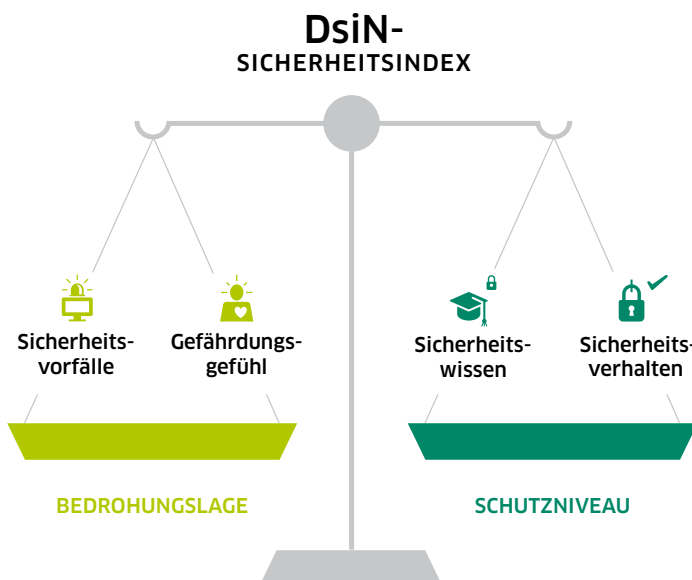
Um die Sicherheitslage zu ermitteln, vergleicht der DsiN-Index die Bedrohungslage mit dem

Schutzniveau der Nutzer. Bei einem Indexwert über 50 überwiegt das Schutzniveau der Verbraucher, bei einem Wert darunter überwiegt hingegen die Bedrohungslage. Zur Darstellung der Bedrohungslage fragt der Index nach erlebten IT-Sicherheitsvorfällen sowie dem persönlichen Gefährdungsgefühl bei verschiedenen digitalen Anwendungen. Für das Schutzniveau werden das Wissen zu Schutzmaßnahmen sowie deren tatsächliche Anwendung ermittelt. Durch die voranschreitende Digitalisierung verändern sich die abgefragten Faktoren stetig: Neue Dienste kommen hinzu, damit verändern sich auch die Bedrohungsszenarien. Um mit der Digitalisierung und der veränderten Umwelt Schritt zu halten, reagierte der DsiN-Sicherheitsindex 2017 erneut mit einer Aktualisierung der abgefragten Items.

Grundlage für bedarfsorientierte digitale Aufklärung 2.0

Damit Aufklärung wirken kann, muss sie Menschen erreichen – doch Nutzer unterscheiden sich voneinander: Der DsiN-Index unterscheidet deshalb vier verschiedene Verbrauchertypen mit individuellen Sicherheitslagen – abhängig vom persönlichen Risikoverhalten, dem Wissenstand sowie der Bereitschaft, Schutzvorkehrungen anzuwenden. Außerdem werden Nutzer nach ihren Einstellungen und Motivationen zur Verbesserung ihrer IT-Sicherheit befragt. Daraus können eine bedarfsgerechte Aufklärungsarbeit 2.0 und eine zielgruppenorientierte Ansprache abgeleitet werden (siehe dazu Kapitel 4).

Abb. 2. Berechnung des DsiN-Sicherheitsindex: Verhältnis zwischen Bedrohungslage und Schutzniveau



A close-up photograph of a person's hands typing on a silver laptop keyboard. The keyboard has Cyrillic characters. A large, semi-transparent green shape is overlaid on the top left and center of the image, containing white text. In the background, a glass of water is visible on a desk.

Kapitel 01

**DsiN-Sicherheitsindex
2017: 61,1 Punkte**

Indexwert 2017: Rückgang auf 61,1 Punkte

Nachdem der DsiN-Sicherheitsindex in den letzten drei Erhebungsjahren kontinuierlich gestiegen ist, sank er in diesem Jahr im Vergleich zu 2016 um 4,3 Punkte auf einen Wert von **61,1 Indexpunkten**. Dabei ist das Schutzniveau der Verbraucher weitgehend stabil geblieben; die Messung der Bedrohungslage ist jedoch erheblich gestiegen.

Entwicklung von Bedrohungslage und Schutzniveau

Der Indexwert setzt sich aus vier Sicherheitsfaktoren zusammen, die in der Bedrohungslage und dem Schutzniveau der Verbraucher abgebildet werden (siehe dazu Ziel und Methode des DsiN-Sicherheitsindex auf Seite 8). Wie auch der Gesamtindex werden die vier Sicherheitsfaktoren jeweils auf einer Skala von 0 bis 100 Punkten gemessen.

Bedrohungslage

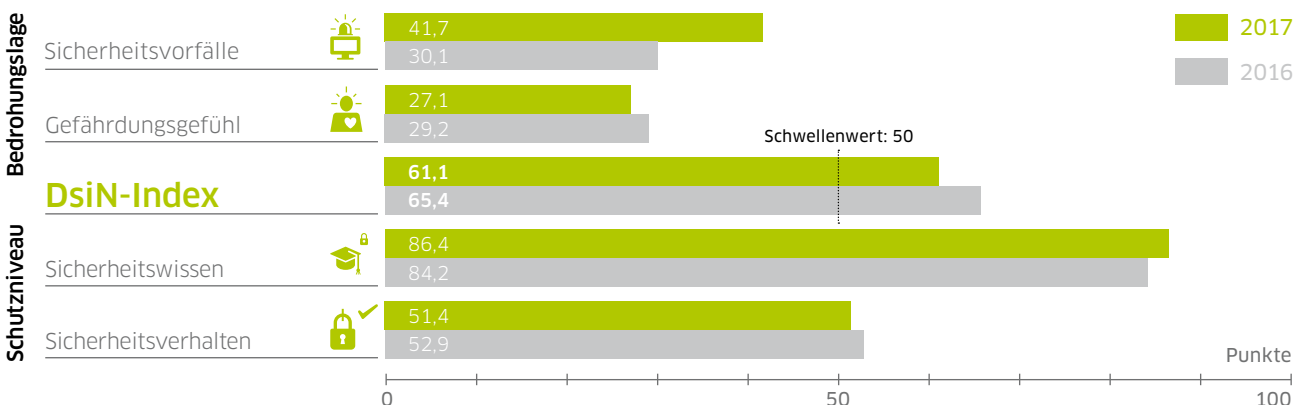
- **Sicherheitsvorfälle:** 2017 hat der DsiN-Index deutlich mehr Sicherheitsvorfälle als in den Jahren zuvor gemessen. Das führt zu einem Anstieg des Wertes um 11,6 auf 41,7 Punkte (2016: 30,1 Punkte).
- **Gefährdungsgefühl:** Im Gegensatz zu den Vorjahren ist das Gefährdungsgefühl – geringfügig – gesunken, und zwar um 2,1 auf einen diesjährigen Wert von 27,1 Punkten (2016: 29,2 Punkte).

Schutzniveau

- **Sicherheitswissen:** In Hinblick auf ihr Sicherheitswissen haben sich die Verbraucher in 2017 erneut verbessert, und zwar um 2,2 auf 86,4 Punkte (2016: 84,2 Punkte).
- **Sicherheitsverhalten:** Bei der Bereitschaft zur Anwendung von Schutzmaßnahmen kommt es 2017 allerdings zu einem Abfall um 1,5 Punkte. Damit liegt der Wert bei 51,4 Punkten (2016: 52,9 Punkte).

Abb. 3. Übersicht Index und Faktoren 2017

Sicherheitsfaktoren





Neue Gefahren
beeinflussen
Bedrohungslage

Bedrohungslage steigt

Kritisch wird die Sicherheitslage, wenn die 50-Punkte-Marke auf der Indexskala unterschritten wird: Die Bedrohungslage würde das Schutzniveau übertreffen und die digitale Sicherheitslage der Verbraucher kippen. Mit 61,1 Punkten liegt der Indexwert 2017 nur 11,1 Punkte über diesem Schwellenwert. Obwohl 2017 das Sicherheitswissen der Verbraucher sogar um 2,2 Punkte steigt – der größte Zuwachs seit Beginn der Erhebung –, ist die Anzahl der benannten Angriffe 2017 deutlich höher als 2016. Bereits in den Vorjahren zeichnete sich ab: Sollte sich die Bedrohungslage merklich verschlechtern, könnte das – zwar kontinuierlich wachsende – Schutzniveau der Verbraucher dem allein nicht standhalten. Nachdem die Messung der Sicherheitsvorfälle in diesem Jahr um über 10 Indexpunkte gestiegen ist, kündigt sich dieses Szenario mehr denn je an.

Steigende Diskrepanz zwischen Wissen und Nutzen

Bereits in den drei vorherigen Erhebungsjahren hat der DsiN-Index eine drastische Wissens-Verhaltens-Schere aufgezeigt: Verbraucher verfügen über deutlich mehr IT-Schutzwissen als sie tatsächlich zur Anwendung bringen. Diese Diskrepanz zwischen Wissen und Verhalten hat sich 2017 noch einmal deutlich verschärft: Das IT-Sicherheitswissen der Verbraucher hat um 2,2 Punkte zugenommen. Gleichzeitig ist das Sicherheitsverhalten um 1,5 Punkte zurückgegangen. Immerhin: Die Wahrnehmung, dass gegen Sicherheitsvorfälle etwas getan werden muss und kann, ist aufseiten der Verbraucher signifikant hoch.

Die vier Sicherheitsfaktoren

Bedrohungslage

Die Bedrohungslage erfasst selbstregistrierte Vorfälle sowie das persönliche Gefährdungsgefühl im Umgang mit digitalen Diensten bei Verbrauchern anhand von etwa 50 Szenarien.

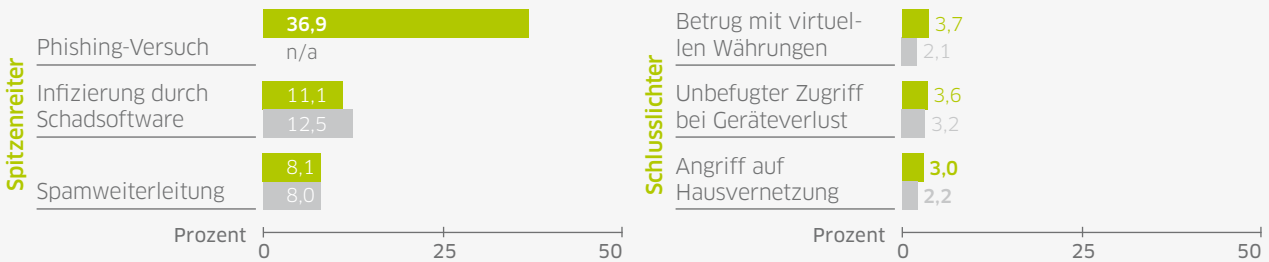


1. Sicherheitsvorfälle

Auf dem ersten Platz der registrierten Sicherheitsvorfälle liegt in diesem Jahr mit 37 Prozent der Phishing-Angriff. Mit deutlichem Abstand folgt auf dem zweiten Platz mit 11 Prozent die Infizierung mit Schadsoftware - mit stetigem Rückgang im Vierjahresvergleich (2014: 19,6 Prozent). Wie bereits 2016 verzeichneten 8 Prozent der befragten Verbraucher Betrugsfälle beim Online-Einkauf oder der Online-Buchung. Die seltensten Vorfälle betreffen Angriffe auf die Hausvernetzung (3 Prozent), den unbefugte Zugriff auf mobile Geräte sowie den Betrug mit virtueller Währung (jeweils 4 Prozent). Alle drei Angriffsarten sind im Vorjahresvergleich leicht gestiegen.

Abb. 4 Spitzenreiter und Schlusslichter Sicherheitsvorfälle

■ 2017 ■ 2016

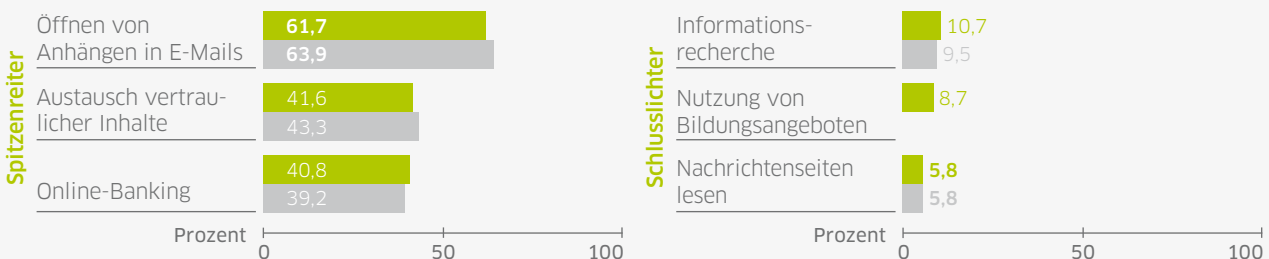


2. Gefährdungsgefühl

Nach wie vor herrscht die größte Unsicherheit beim Thema E-Mails: 62 Prozent der befragten Onlinenutzer halten das Öffnen von E-Mail-Anhängen für riskant. Auf Platz zwei liegt weiterhin der Online-Austausch vertraulicher Daten (z.B. mit Behörden), den 42 Prozent als gefährlich oder sehr gefährlich sehen. Bei Bankgeschäften im Internet fühlen sich 41 Prozent der Befragten unsicher. Wie im Vorjahr sehen Verbraucher das geringste Risiko beim Lesen von Nachrichtenseiten (5,8 Prozent) sowie bei der Nutzung von Online-Bildungsangeboten (8,7 Prozent) und dem Recherchieren im Internet (10,7 Prozent).

Abb. 5 Spitzenreiter und Schlusslichter Gefährdungsgefühl

■ 2017 ■ 2016



Schutzniveau

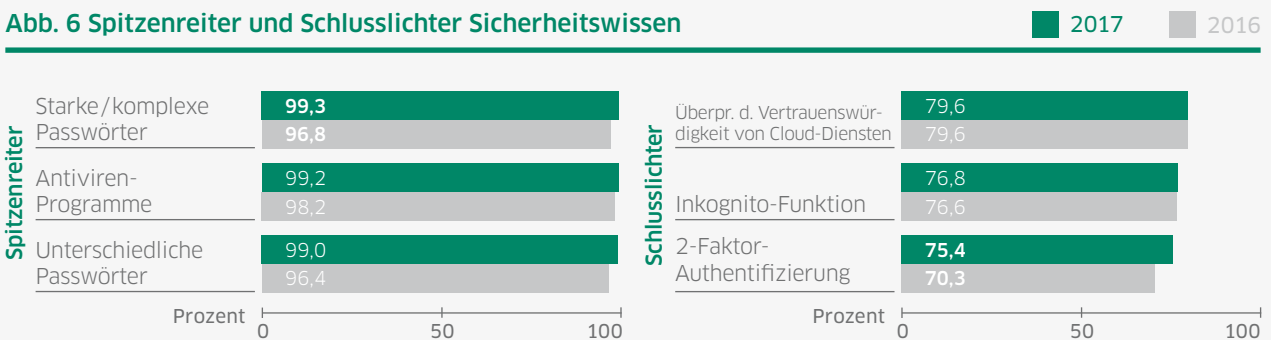
Das individuelle Schutzniveau beim Verbraucher kombiniert das vorhandene Sicherheitswissen mit dem Sicherheitsverhalten.

3. Sicherheitswissen

Nahezu alle befragten Nutzer, mit 99 Prozent nochmal um 3 Prozentpunkte mehr als im Vorjahr, wissen um die Schutzfunktion starker Passwörter. Genauso viele Onliner kennen den elementaren Schutz durch Antivirenprogramme (+1 Prozent) und wissen, dass die Nutzung unterschiedlicher Passwörter zu mehr IT-Sicherheit beiträgt (+2,6 Prozent). Am wenigsten bekannt ist die 2-Faktor-Authentifizierung, diese kennen 24,6 Prozent der befragten Onliner nicht – jedoch immerhin 5 Prozent mehr als im Vorjahr.



Abb. 6 Spitzenreiter und Schlusslichter Sicherheitswissen

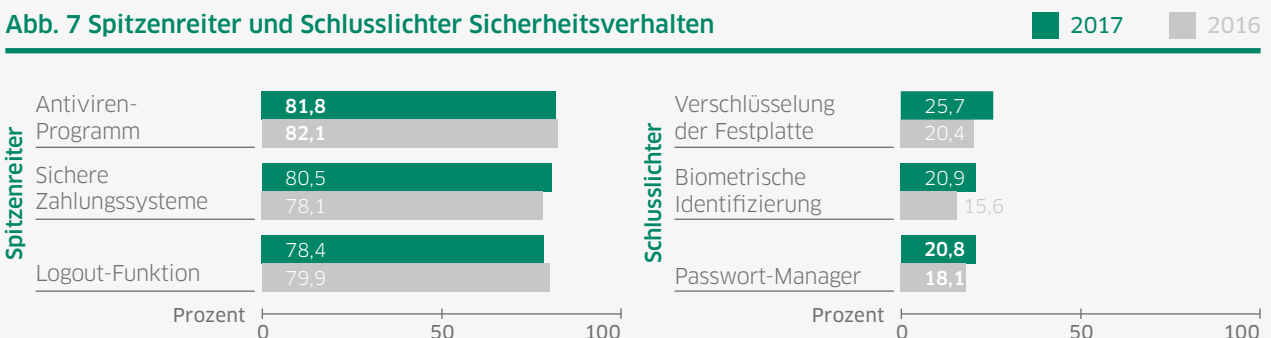


4. Sicherheitsverhalten

Am häufigsten setzen Verbraucher Antivirenprogramme als Schutzmaßnahme ein: 81,8 Prozent gaben an, ein solches zu nutzen. Die Zahl ist im Vergleich zum Vorjahr stabil geblieben. Als zweithäufigste Sicherheitsvorkehrung nutzen Verbraucher sichere Zahlungssysteme mit inzwischen 80,5 Prozent, das ist ein Zuwachs von 2,4 Prozentpunkten im Vergleich zum Vorjahr. Auf dem dritten landet mit 78,4 Prozent die Logout-Funktion, die 2017 aber knapp 2 Prozent weniger nutzen als im Vorjahr. Schlusslicht bei den genutzten Sicherheitsvorkehrungen bildet die Nutzung eines Passwortmanagers: Nur 20,8 Prozent der Befragten greifen auf ihn zurück, aber immerhin 2,7 Prozent mehr als im Vorjahr.



Abb. 7 Spitzenreiter und Schlusslichter Sicherheitsverhalten



Einflussfaktoren für IT-Sicherheit

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

1. Einfluss auf Sicherheitsvorfälle

2017 nehmen Verbraucher die Notwendigkeit von Maßnahmen, um sicherheitsrelevante Vorfälle zu vermeiden, sehr deutlich wahr – und zwar bei allen Aussagen. 84,4 Prozent geben an, dass sie vorsichtiger mit den eigenen Daten umgehen sollten. Drei Viertel glauben, dass sie häufiger Sicherheitsmaßnahmen einsetzen sollten. 71,9 Prozent der Nutzer fordern strengere Gesetze.

2. Stärkung der Risikoeinschätzungskompetenz

70,5 Prozent der Verbraucher fordern Anbieter von Diensten und Programmen dazu auf, mehr über Risiken aufzuklären. Eine verstärkte Aufklärung außerhalb des

Internets wünschen sich 63,4 Prozent und 63,2 Prozent fordern mehr Informationen im Internet.

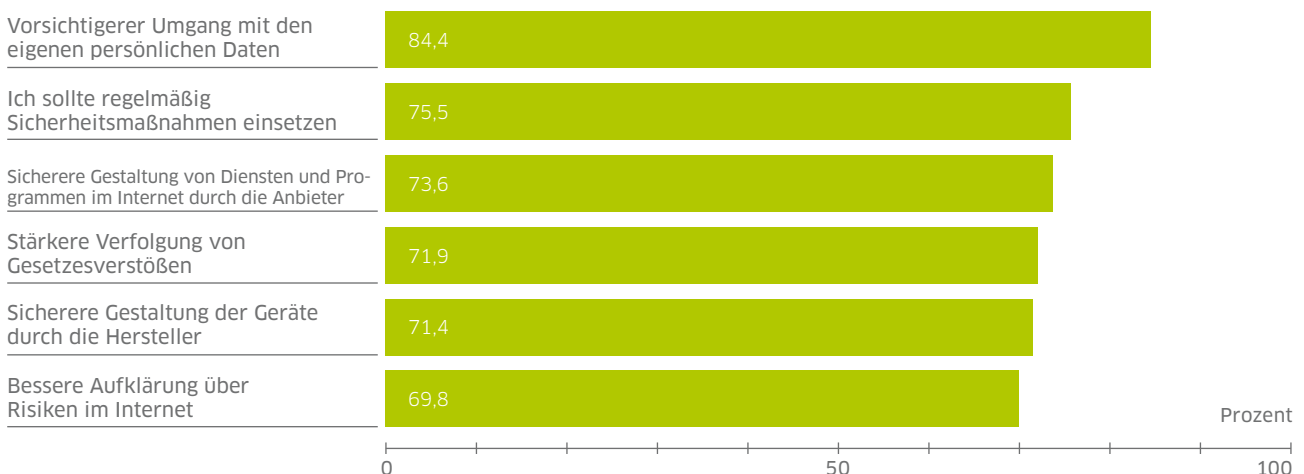
3. Vertiefung von Sicherheitswissen

Um Sicherheitswissen zu stärken, wünschen sich 74,8 Prozent der Onliner verständlichere Informationen und 75,3 Prozent erachten eine stärkere Bündelung von Informationen, wie man sich im Internet besser schützen kann, als sinnvoll. 72,9 Prozent halten Aufklärungsangebote in der schulischen oder beruflichen Bildung für hilfreich.

4. Motivation zur Anwendung

Wie im letzten Jahr motivieren einfachere Sicherheitseinstellungen bei Programmen und Geräten die Nutzer bei einem Wert von 77,1 Prozent am meisten. Aber auch eine konkrete Ansprache im Beruf (57,6 Prozent) und durch das private Umfeld (56,2 Prozent) motiviert Verbraucher zur Anwendung von Schutzmaßnahmen.

Abb. 8 Selbsteinschätzung der Verbraucher: Wie Sicherheitsvorfälle reduzieren?



Kapitel 02

IT-Sicherheitsgefälle: Unterschiede zwischen Verbrauchertypen



IT-Sicherheitslage: Abhängigkeit von Verbrauchertypen

Die persönliche IT-Sicherheit hängt sowohl vom individuellen Wissen als auch dem Verhalten ab. Der DsiN-Index unterscheidet deshalb nach vier Verbrauchertypen mit unterschiedlichen Werten. Im Vierjahresvergleich wird ein starkes digitales Sicherheitsgefälle zwischen den Verbrauchertypen sichtbar: Neues Schlusslicht bilden 2017 die Außenstehenden – dicht gefolgt von den Fatalisten.

Außenstehende Nutzer landen mit einem um 5,3 Punkte gesunkenen Index von **49,4 Punkten** unter dem Schwellenwert 50 (2016: 54,7 Indexpunkte). Sie tragen mit diesem niedrigsten Wert aller vier Gruppen die rote Laterne. Zwar konnten sie ihr Sicherheitswissen um 4,1 Punkte steigern, die Sicherheitsvorfälle sind in dieser Gruppe aber um 14,4 Punkte stark gestiegen. Diese Nutzer, der vor allem ältere Menschen angehören, entwickeln sich im Vierjahresvergleich und mit einem diesjährigen Häufigkeitsanteil von 6 Prozent

jedoch zu einer schwindenden Gruppe (2016: 8,0 Prozent).

Fatalistische Nutzer unterscheiden sich mit einem Indexwert von **50 Punkten** im Gesamtergebnis kaum von den außenstehenden Nutzern. Sie sind zwar nicht mehr Träger der roten Laterne, haben sich aber ebenfalls verschlechtert, und zwar um 2,5 Punkte (2016: 52,5 Indexpunkte). Mit 50 Punkten sind sie auch auf dem Scheidepunkt: ihre Sicherheitslage droht zu kippen. Ausschlaggebend hierfür ist, dass fatalistische Nutzer die meisten Angriffe sowie die höchste Verunsicherung verzeichnen. Auch wenden sie nach wie vor vorhandenes Sicherheitswissen nicht ausreichend an.

Gutgläubige Nutzer verzeichnen ebenfalls einen gesunkenen Indexwert, und zwar um 3,9 auf **58,4 Punkte** (2016: 62,3 Indexpunkte). Auch in dieser Gruppe ist ein deutlicher Anstieg der Sicherheitsvorfälle – hier sind es 9,4 Punkte – der Hauptgrund. Das Gefährdungsempfinden bleibt unverändert auf

Abb. 9 Übersicht über untersuchte Nutzertypen im DsiN-Index

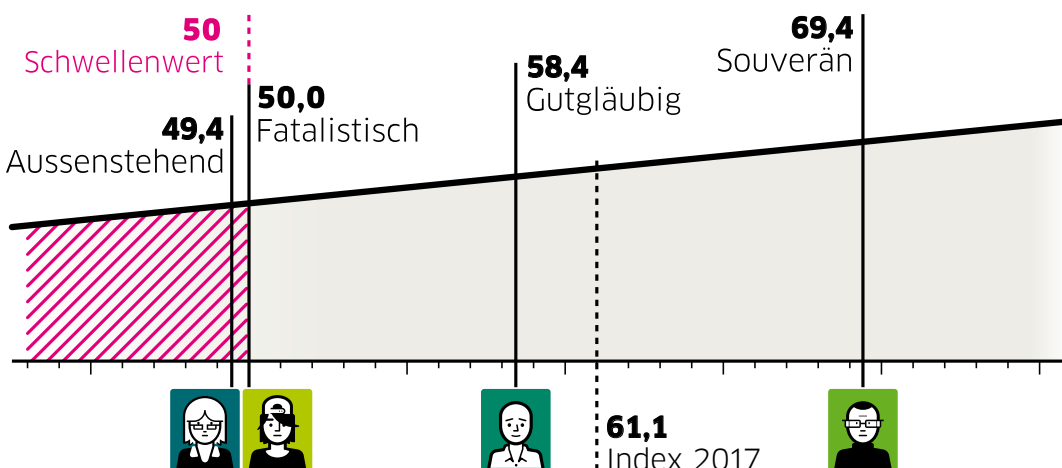
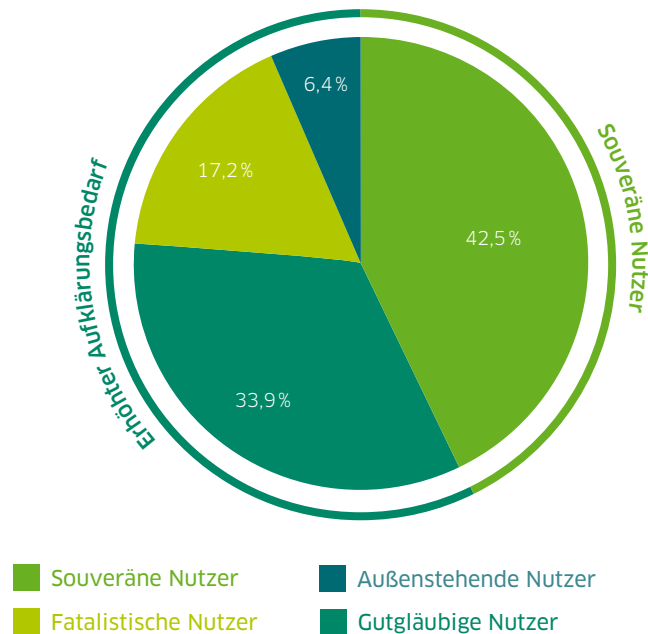


Abb. 10 Anteil der Verbrauchertypen an der Gesamtheit der Onliner



demselben unterdurchschnittlichen Niveau und die Diskrepanz zwischen Wissen und Verhalten ist bei dieser Gruppe auch weiterhin am größten.

Souveräne Nutzer befinden sich mit dem höchsten Sicherheitsindex von **69,4 Punkten** weiterhin an der Spitze – verzeichnen jedoch ebenfalls eine Verschlechterung, in ihrem Fall um 5,3 Punkte (2016: 74,7 Indexpunkte). Das liegt vor allem an dem Anstieg der Sicherheitsvorfälle um ganze 15,1 Indexpunkte. Ihr Sicherheitswissen wie auch ihr Sicherheitsverhalten konnten die souveränen Nutzer auch dieses Jahr verbessern – wenn auch nur minimal.

Sicherheitslage bei fast einem Viertel gekippt

Erstmals seit 2014 liegen gleich zwei Verbrauchertypen, die Fatalisten und die Außenstehenden, nicht mehr über der kritischen 50-Punkte-Marke. Aber auch die Gutgläubigen sind unzureichend geschützt. Es zeigt sich ein digitales Sicherheitsgefälle: Alle drei Verbrauchertypen und somit über die Hälfte aller Verbraucher zeigen verstärkten Unterstützungsbedarf. Bei fast einem Viertel der Verbraucher ist die digitale Sicherheitslage sogar gekippt. Um die Situation zu verbessern, müssen Verbraucher ihre Handlungskompetenz ausbauen und ihr vorhandenes Sicherheitswissen auch tatsächlich anwenden. Neben dem Informieren und Sensibilisieren bleiben deshalb vor allem die Befähigung und Motivation wichtige Aufgabe digitaler Aufklärungsarbeit – und zwar orientiert an individuellen Bedarfen (siehe dazu ausführlich Kapitel 4).

Aufklärung: zielgruppengerecht und bedarfsorientiert

Im Umgang mit digitalen Diensten zeigen sich markante, verbrauchertypabhängige Unterschiede – diese müssen bei einer bedarfsge-rechten Aufklärung berücksichtigt werden:

- Außenstehende benötigen leicht verständliche Informationen und konkrete Handlungsempfehlungen, um sich endlich aufgeklärter und sicherer zu verhalten.
- Fatalisten sollten in einer realistischen Risikoeinschätzung gefördert werden, um (Selbst)Vertrauen auf- und Unsicherheiten abzubauen.
- Gutgläubige weisen die größte Diskrepanz zwischen Sicherheitswissen und -verhalten auf. Sie müssen vor allem zur Anwendung ihres vorhandenen Wissens motiviert werden.
- Souveräne Nutzer können andere im sicheren Umgang mit dem Internet begleiten und als Vorbild wirken – und sollten somit in die Aufklärungsarbeit einbezogen werden.

Außenstehende Nutzer (49,4 Punkte)



Der außenstehende Nutzer

Rote Laterne: Die außenstehenden Nutzer bilden in diesem Jahr das Schlusslicht. Mit **49,4 Indexpunkten** unterschreiten sie die kritische Grenze von 50. Gleichzeitig sinkt der Anteil der Außenstehenden und beträgt dieses Jahr nur 6 Prozent von der Gesamtheit aller Verbrauchertypen.

Typische Merkmale

Zur Gruppe der außenstehenden Nutzer gehören überwiegend ältere Menschen ab 50 Jahren. Sie nutzen das Internet meist weniger als 20 Stunden pro Woche, bevorzugt auf Laptops oder stationären PCs. Im Vergleich zu den anderen Verbrauchertypen weisen sie starke Defizite bei der Kenntnis und Nutzung von Schutzmaßnahmen auf.

Bedrohungslage

Der außenstehende Nutzer zeigt mit 22,5 Punkten ein sehr unterdurchschnittliches Gefährdungsgefühl, das im Vergleich zum letzten Jahr (2016: 26,0 Punkte) weiter gesunken ist und sich damit dem Wert aus 2015 mit 22,1 Punkten angenähert hat. Einzig

der Erhalt von E-Mail Anhängen wird von dieser Gruppe mehrheitlich als bedrohlich empfunden. Gleichzeitig ist die Zahl der Sicherheitsvorfälle stark gestiegen: Waren die außenstehenden Nutzer bisher vergleichsweise selten von Sicherheitsvorfällen betroffen, steigt dieser Wert 2017 auf 34,5 Punkte.

Schutzniveau

Deutlich zugelegt haben die Außenstehenden bei ihrem Sicherheitswissen: Mit 44,8 Punkten ist das im Vierjahresvergleich der höchste für diesen Verbrauchertyp gemessene Wert. Ihr Sicherheitsverhalten ist hingegen leicht gesunken, liegt aber mit 26,4 Punkten höher als 2015 und 2014. Dennoch bilden die Außenstehenden in diesen beiden Kategorien weiterhin das Schlusslicht. Grundlegende Schutzmaßnahmen wie die sichere Nutzung von Passwörtern und Antivirenprogrammen sind am bekanntesten. Die größte Diskrepanz zwischen dem Wissen und der Anwendung besteht bei der Überprüfung der Vertrauenswürdigkeit externer Datenträger.

Abb. 11 DsiN-Indexwert für außenstehende Nutzer

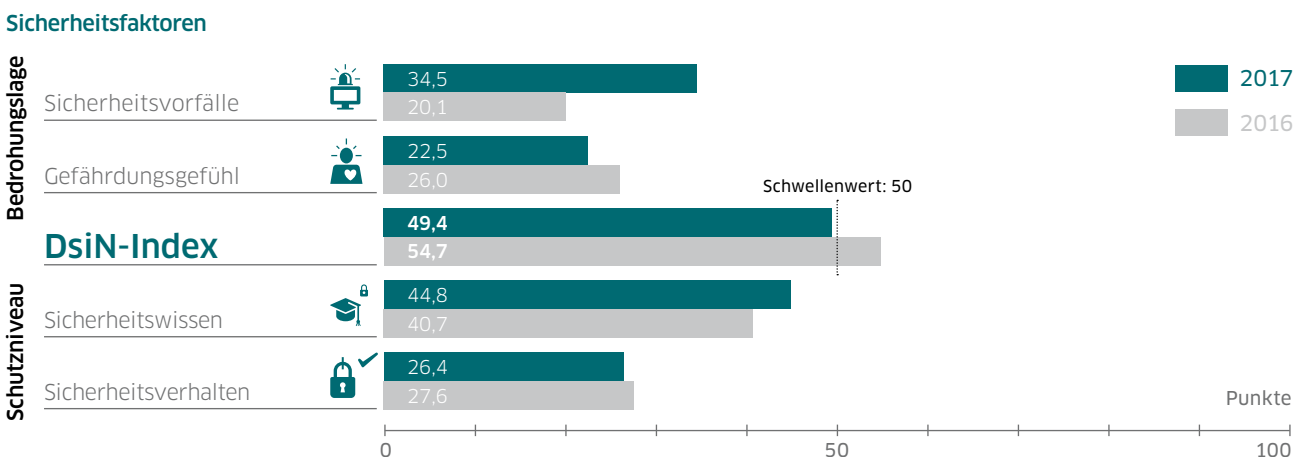
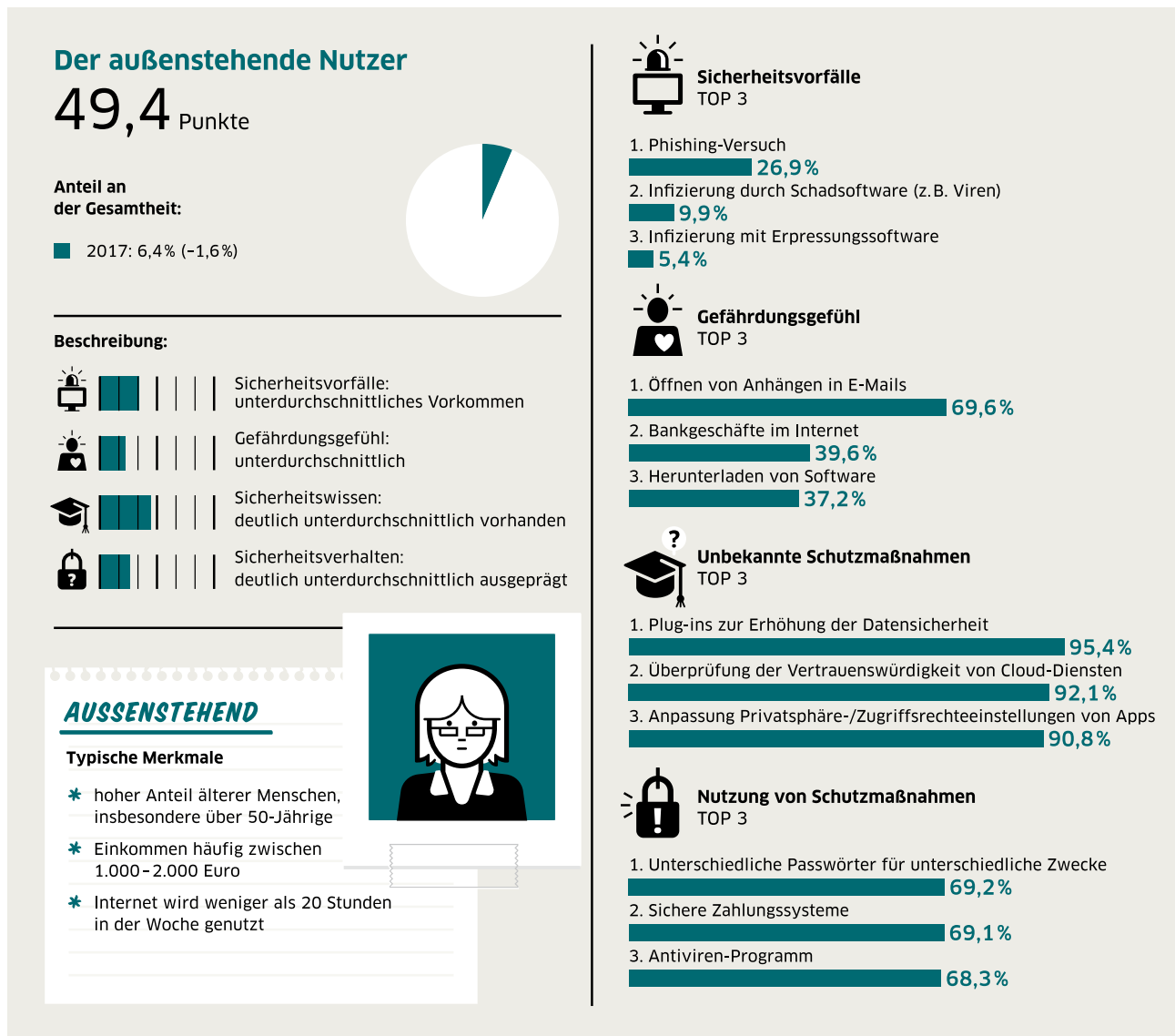


Abb. 12 Steckbrief Außenstehender Nutzer



Sicherheitswissen und Risikoeinschätzungskompetenz fördern

Die außenstehenden Nutzer weisen die größten Defizite beim Sicherheitswissen und Sicherheitsverhalten auf und müssen daher besonders sensibilisiert werden: Digitale Aufklärung muss ihr Bewusstsein für potentielle und akute IT-Risiken fördern – durch Verdeutlichung der Relevanz sowie der persönlichen Betroffenheit. Dafür wünschen sie sich verständlichere Informationen, die durch die Anbieter von Diensten wie auch über Weiterbildungen vermittelt werden sollen. Am meisten motiviert fühlen sie sich durch einfachere Sicherheitseinstellungen bei Programmen und Geräten

sowie durch konkrete Ansprache und Unterstützung im privaten Umfeld. Doch auch die Kompetenz zur realistischen Risikoeinschätzung sowie die Eigenverantwortung muss in dieser Gruppe verbessert werden. Viele außenstehende Nutzer sehen hier allein den Gesetzgeber in der Pflicht, Sicherheitsrisiken zu vermeiden.



DsiN-Angebote für außenstehende Nutzer:

- **Digital-Kompass** mit digitalen Stammtischen für Senioren
- **Goldener Internetpreis** für ältere Generationen
- **Digitale Nachbarschaft** für ehrenamtlich aktive Bürger
- **IT-Fitness-Test:** Wissenscheck für Einsteiger
- **DsiN-Sicherheitsbarometer (SiBa-App):** Die News- und Ratgeber-App zu unterschiedlichen Lebensfeldern

Fatalistische Nutzer (50,0 Punkte)



Der fatalistische Nutzer

Verunsichert: Die fatalistischen Nutzer landen knapp vor den außenstehenden Nutzern auf dem vorletzten Platz. Der Indexwert ist im Vergleich zum Vorjahr um 2,5 Punkte auf **50 Punkte** gesunken (2016: 52,5 Punkte). Damit bewegt sich diese Gruppe genau auf dem Schwellwert. Ihre Sicherheitslage droht zu kippen.

Typische Merkmale

Der Anteil der unter 30-Jährigen ist bei den Fatalisten im Vergleich zu den anderen Gruppen am höchsten. Die meisten fatalistischen Nutzer sind zwischen 10 bis 30 Stunden in der Woche online. Hierfür nutzen sie stationäre PCs, Laptops und Smartphones gleichermaßen. 17,2 Prozent aller deutschen Onliner gehören dieser Gruppe an.

Bedrohungslage

Bei den IT-Sicherheitsvorfällen kommt es in dieser Gruppe – wie auch bereits in den Jahren zuvor – zu einer Zunahme. 2017 liegt dieser Wert bei 50,6 Punkten (2016: 44,5 Punkte),

damit verzeichnen die Fatalisten die meisten Angriffe. Im Vergleich zu den anderen Verbrauchergruppen fällt der Anstieg allerdings gering aus. Das Gefährdungsempfinden bleibt mit 70,2 Punkten im Vergleich zum letzten Jahr überdurchschnittlich hoch. Als besonders gefährlich empfinden die Fatalisten das Öffnen von E-Mail Anhängen, aber auch die Nutzung sozialer Netzwerke und das Auslagern eigener Dateien.

Schutzniveau

Auch 2017 konnten die Fatalisten – wie in den Jahren zuvor – ihr Sicherheitswissen leicht ausbauen und liegen nun bei 79,6 Punkten. Im Gegensatz zu den Vorjahren ist der Wert für das Sicherheitsverhalten in diesem Jahr allerdings auf 47,6 Punkte geringfügig gefallen. Antivirenprogramme und die sichere Verwendung von Passwörtern sind bei den fatalistischen Nutzern sehr bekannt und kommen auch häufig zum Einsatz. Zu hohen Diskrepanzen zwischen Wissen und Verhalten kommt es dagegen bei der Verschlüsselung

Abb. 13 DsiN-Indexwert für fatalistische Nutzer

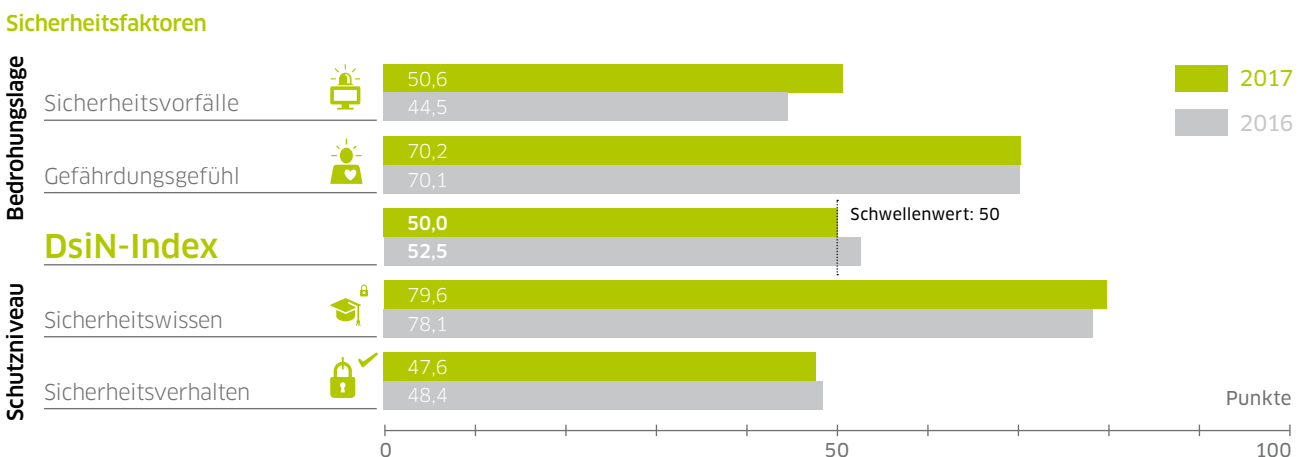
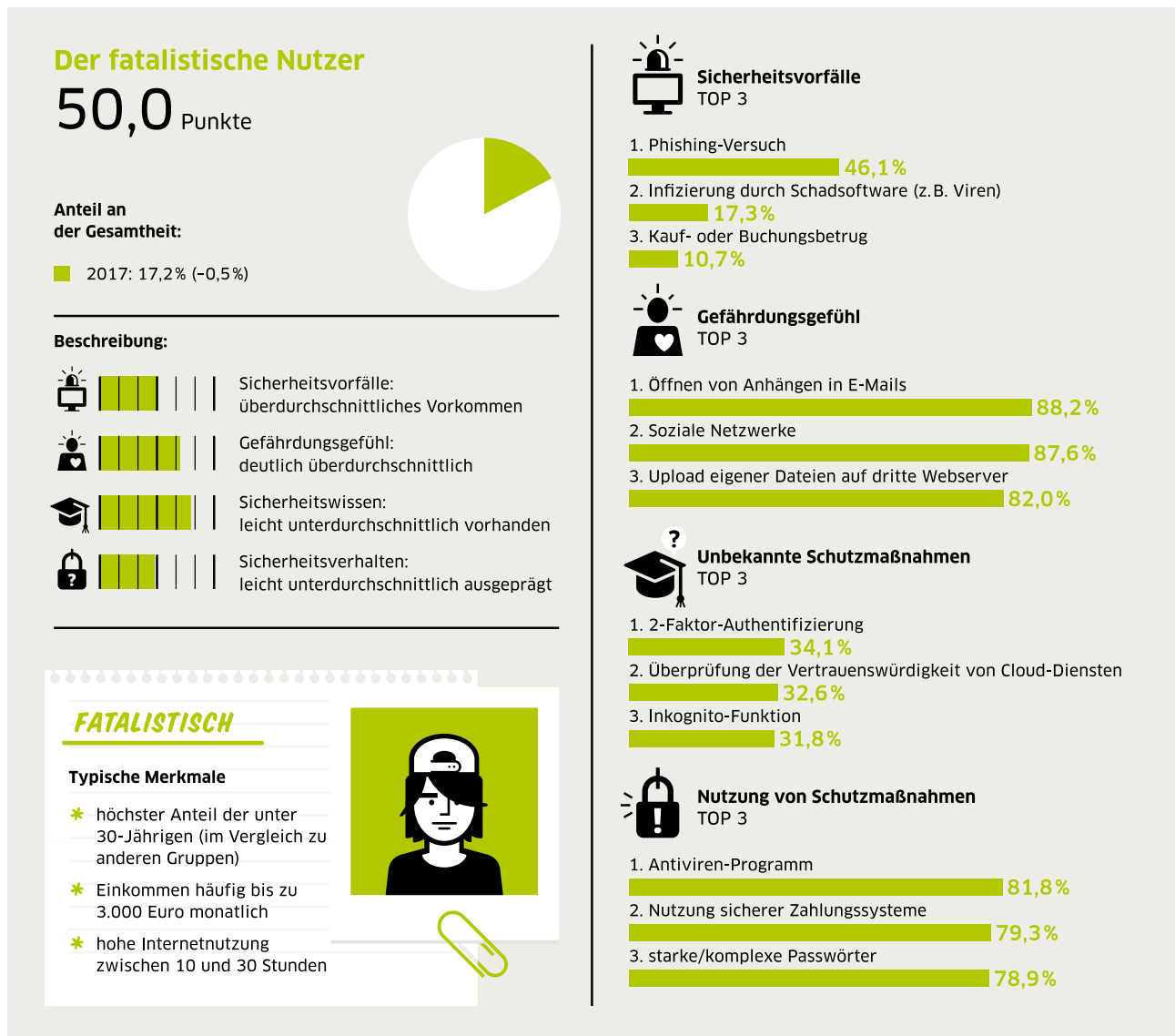


Abb. 14 Steckbrief Fatalistischer Nutzer



der eigenen Festplatte und der Anpassung von Zugriffsrechten und Privatsphäre-Einstellungen in Apps.

Zur Anwendung des Wissens motivieren

Trotz ihres überdurchschnittlichen Gefährdungsempfindens besitzt diese Gruppe eine fatalistische Grundhaltung: Auch wenn Schutzvorkehrungen in großer Ausprägung bekannt sind, setzen Fatalisten diese nur in einem geringen Maß tatsächlich um. Zur Reduzierung ihrer hohen Verunsicherung trägt die Förderung einer realistischen Risikoeinschätzungs-kompetenz bei. Um Fatalisten zu motivieren, muss digitale Aufklärung den konkreten Nutzen von Schutzmaßnahmen sowie die Folgen von

nachlässigem Handeln veranschaulichen. Außerdem sollte entsprechende Anerkennung erfolgen, zum Beispiel innerhalb der Peer-group. Fatalisten müssen verstehen, dass sich der eigene Beitrag zu ihrer IT-Sicherheit lohnt. Daneben empfinden sie eine konkrete Ansprache in Beruf und Schule sowie auch einfachere Sicherheitseinstellungen als motivierend.



DsiN-Angebote für fatalistische Nutzer:

- **myDigitalWorld:** Jugendwettbewerb
- **DigiBitS – Digitale Bildung trifft Schule:** Materialsammlung für Lehrkräfte
- **Bottom-Up:** Berufsschüler für IT-Sicherheit
- **DsiN-Sicherheitsbarometer (SiBa-App):** Die News- und Ratgeber-App

Gutgläubige Nutzer (58,4 Punkte)



Der gutgläubige Nutzer

Sorglos: Mit einem Indexwert von **58,4 Punkten** landen die gutgläubigen Nutzer wie auch im letzten Jahr auf dem zweiten Platz. Eines ihrer größten Defizite liegt weiterhin in der Einschätzung von digitalen Risiken. Doch auch die Wissens-Verhaltens-Schere geht in dieser Gruppe immer weiter auseinander.

Nutzer mit einem unveränderten Wert von 15,3 Punkten weiterhin deutlich unterdurchschnittlich. Weniger als die Hälfte der gutgläubigen Nutzer schätzen das Öffnen von E-Mail Anhängen als potentielles Risiko ein. Auch der Austausch von vertraulichen Daten wird nur von 30,2 Prozent als gefährlich oder sehr gefährlich empfunden.

Typische Merkmale

Die Mehrheit der gutgläubigen Nutzer ist zwischen 20 und 29 bzw. 40 und 49 Jahre alt. Meist sind sie wöchentlich zwischen 10 und 20 Stunden im Internet unterwegs, vor allem mit Laptops und Smartphones. Der Anteil der gutgläubigen Nutzer unter den Verbrauchern ist auf 34 Prozent gestiegen. Sie bilden damit die zweitgrößte Gruppe.

Schutzniveau

Im Vergleich zu 2016 (84,7 Punkte) konnten die gutgläubigen Nutzer ihr Sicherheitswissen auf 87 Punkte verbessern. Im Gegensatz dazu sind sie in ihrem Sicherheitsverhalten nachlässiger geworden und fallen mit 33,6 Punkten fast auf den schlechtesten Wert von 2015 (33,1 Punkte) zurück. Besonders selten nutzen sie Verschlüsselungstechniken. Aber auch bei grundlegenden Schutzmaßnahmen wie der Anwendung von Antivirenprogrammen und der Verwendung von starken und unterschiedlichen Passwörtern ist die Lücke zwischen Wissen und Verhalten stark ausgeprägt.

Bedrohungslage

Auch bei den gutgläubigen Nutzern sind die sicherheitsrelevanten Vorfälle (34,7 Punkte) stark angestiegen. Dennoch bleibt das Gefährdungsgefühl der gutgläubigen

Abb. 15 DsiN-Indexwert für gutgläubige Nutzer

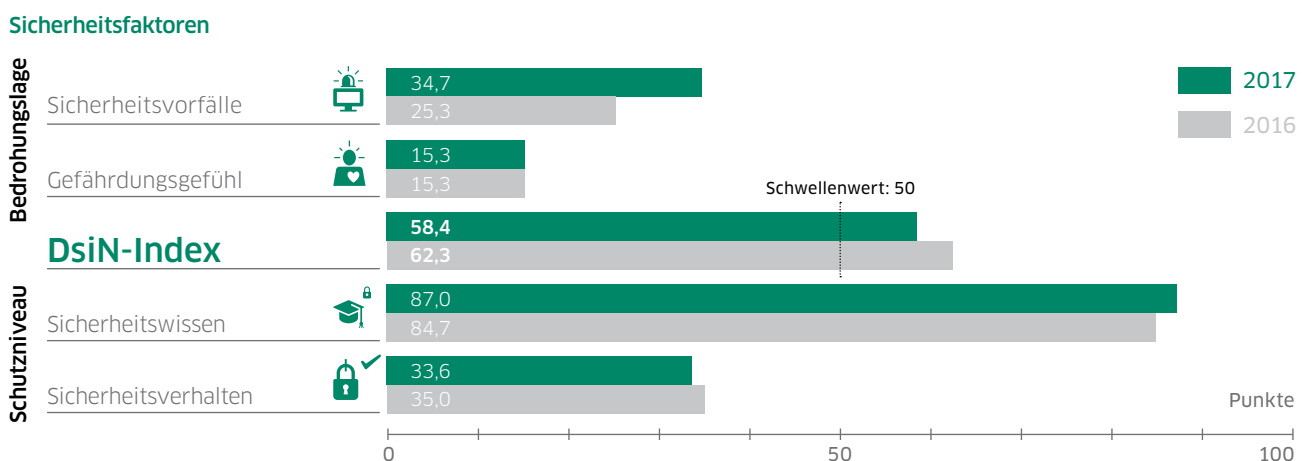
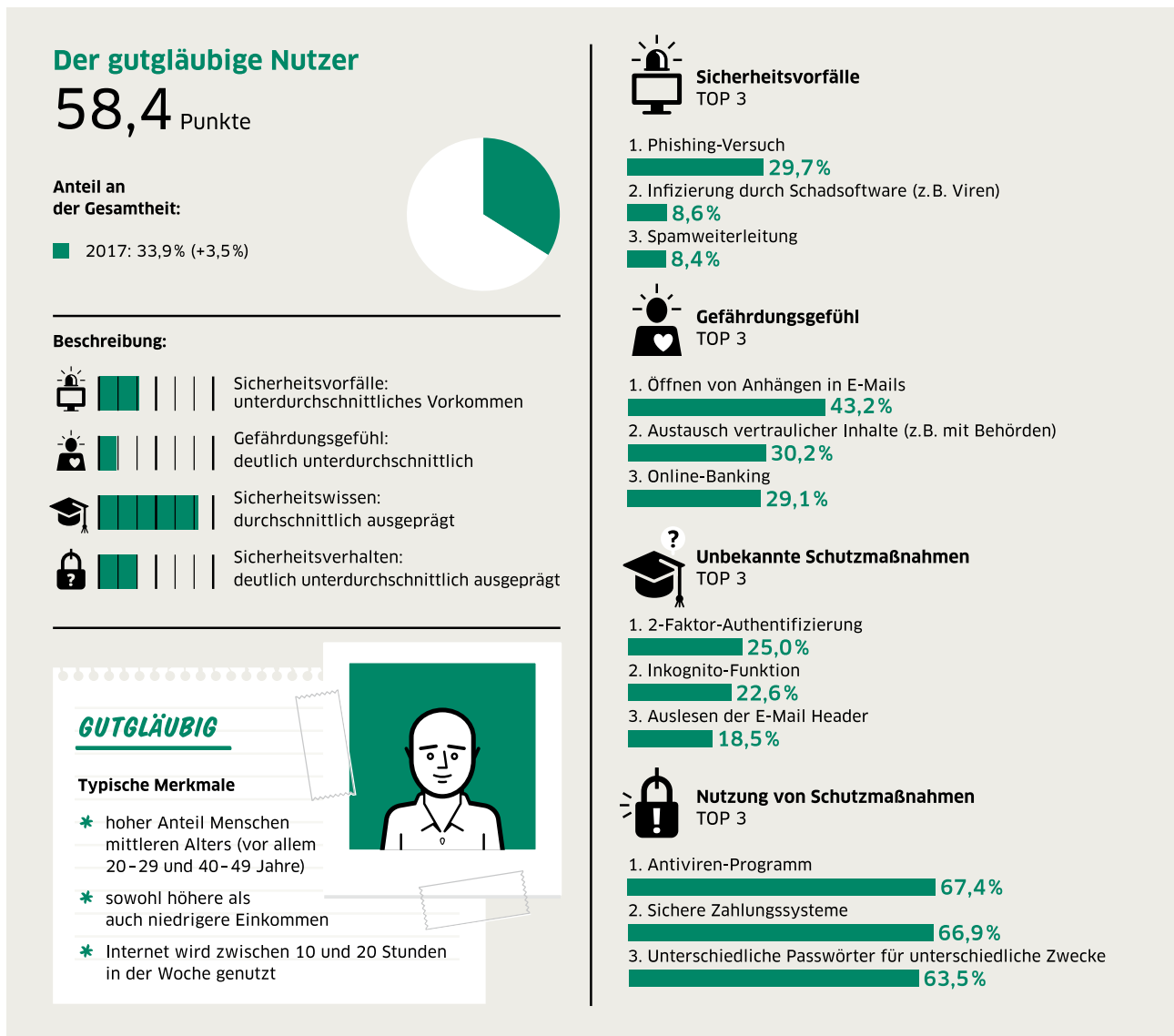


Abb. 16 Steckbrief Gutgläubiger Nutzer



Risikoeinschätzung trainieren und zur Wissensanwendung motivieren

Gutgläubige Nutzer zeichnen sich insbesondere durch ein unterdurchschnittliches Gefährdungsempfinden und eine geringe Anwendungsbereitschaft von Sicherheitswissen aus. Obwohl sie vor allem die Anbieter von Diensten und Programmen in der Pflicht sehen, ihre Produkte mit einfacheren Sicherheitseinstellungen auszustatten, sind sich rund drei Viertel der gutgläubigen Nutzer dennoch bewusst, dass ein vorsichtigerer Umgang mit den eigenen Daten zu weniger IT-Sicherheitsvorfällen führen kann. 60 Prozent geben außerdem an, dass sie regelmäßig Sicherheitsmaßnahmen einsetzen sollten. Der

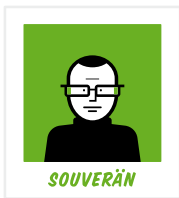
Fokus der digitalen Aufklärung sollte bei dieser Gruppe darauf gerichtet sein, die Gefahren bei der Nutzung digitaler Dienste stärker bewusst zu machen und die Auswirkungen von nachlässigem Sicherheitsverhalten aufzuzeigen, um Gutgläubige zur Anwendung zu motivieren. Dafür wünschen sich gutgläubige Nutzer zudem mehr Warnhinweise im Internet.



DsiN-Angebote für gutgläubige Nutzer:

- **DsiN-Sicherheitsbarometer (SiBa-App):** Die News- und Ratgeber-App
- **IT-Fitness-Test:** Wissenscheck für Einsteiger
- **Videoclips und Tutorials:** Datenverschlüsselung
- **Digitale Nachbarschaft:** Für ehrenamtlich aktive Bürger

Souveräne Nutzer (69,4 Punkte)



Der souveräne Nutzer

Die souveränen Nutzer bleiben den restlichen Verbrauchertypen auch weiterhin konsequent voraus. Zwar treten auch in dieser Gruppe vermehrt IT-Sicherheitsvorfälle auf, doch verzeichnen sie mit **69,4 Punkten** den höchsten Indexwert.

Typische Merkmale

Die meisten souveränen Nutzer sind zwischen 30 und 49 Jahren alt. Die Gruppe nutzt alle Zugangswege zum Internet in einem größeren Maß als die anderen Verbrauchertypen, bevorzugt aber mobile Geräte. Souveräne Nutzer sind meist zwischen 10 und 30 Stunden wöchentlich online. 42,5 Prozent der Verbraucher und somit 1,4 Prozent weniger als im Vorjahr gehören dieser Gruppe an.

Bedrohungslage

Die souveränen Nutzer verzeichnen den stärksten Anstieg bei den sicherheitsrelevanten Vorfällen: Der Indexwert steigt von 29,6 Punkten in 2016 auf 44,7 Punkte in diesem Jahr. Souveräne reagieren mit einem leicht erhöhten

Gefährdungsempfinden: Der Wert steigt von 22,9 Punkte im Vorjahr auf aktuell 24 Punkte. Vor allem empfinden diese Nutzer das Öffnen von E-Mail Anhängen mehrheitlich als gefährlich. Auch für die Gefahren beim Austausch von vertraulichen Daten über das Internet sowie Online-Bankgeschäften sind sie misstrauischer.

Schutzniveau

Mit einem auf 95,6 Punkte gestiegenen Sicherheitswissen ist diese Gruppe auch weiterhin deutlich am besten informiert. Die souveränen Nutzer konnten zudem im Gegensatz zu den anderen Verbrauchertypen ihr Sicherheitsverhalten (73,1 Punkte) auch in diesem Jahr weiter verbessern. Mehr als 80 Prozent der abgefragten Sicherheitsmaßnahmen sind den souveränen Nutzern zu über 95 Prozent bekannt. Auch in ihrem Schutzverhalten heben sie sich stark ab und zeigen sich vorbildlich bei der Anwendung von Schutzmaßnahmen. Wie auch im letzten Jahr haben die Souveränen lediglich bei dem Thema Verschlüsselung Nachholbedarf.

Abb. 17 DsiN-Indexwert für souveräne Nutzer

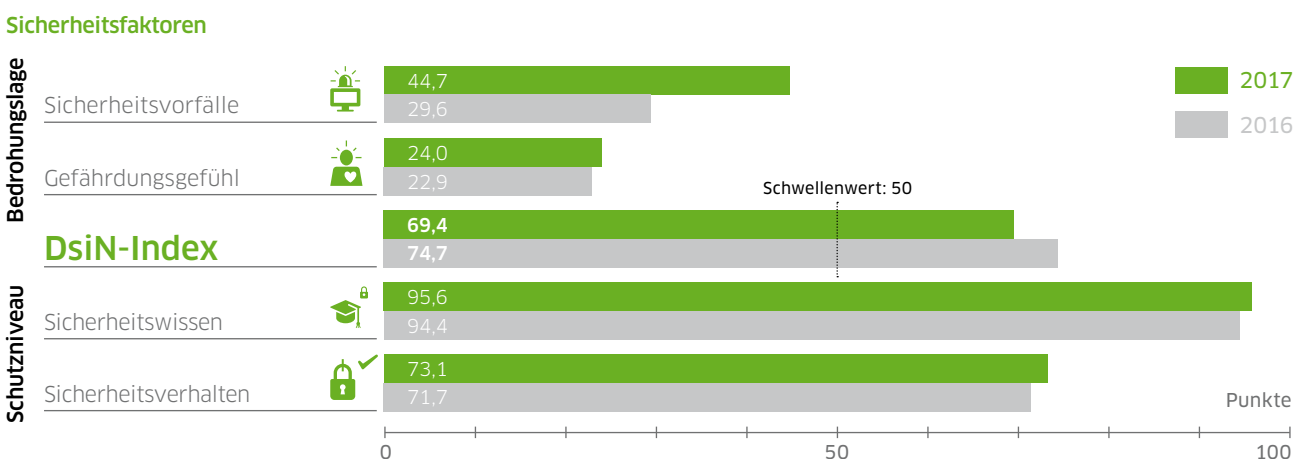
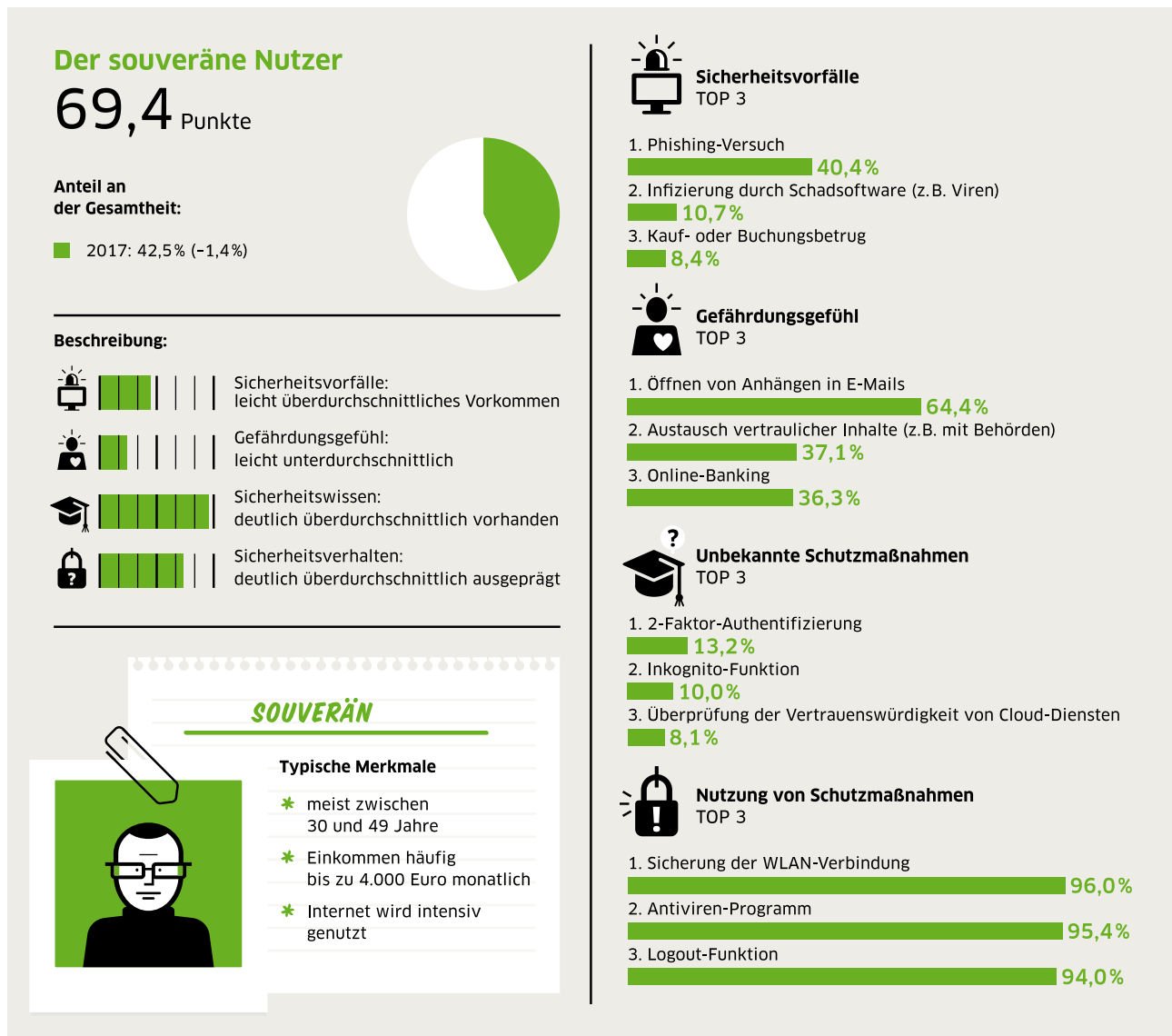


Abb. 18 Steckbrief Souveräner Nutzer



Niveau ausbauen und als Vorbild wirken

Die Gruppe der souveränen Nutzer hat auch dieses Jahr ihr Schutzniveau weiter ausgebaut und als einzige Gruppe ihr Sicherheitsverhalten verbessert. Zudem ist 90 Prozent der Souveränen ihre Verantwortung zum vorsichtigeren Umgang mit den eigenen persönlichen Daten bewusst. Leider ist ihr Gesamtanteil leicht zurückgegangen. Um die Anzahl der souveränen Nutzer wieder zu steigern, sollte stets über aktuellste Risiken und Angebote informiert und zu neuen Sicherheitsmaßnahmen motiviert werden. Zudem wünschen sich die Souveränen eine sicherere Gestaltung der Dienste und Programme. Weiterhin sollte ihnen ihre Ver-

antwortung gegenüber anderen Verbrauchertypen bewusst gemacht werden: Im Rahmen einer digitalen Aufklärung können sie motiviert werden, als Vorbild und Multiplikator über den sicheren Umgang mit dem Internet aufzuklären.



DsiN-Angebote für souveräne Nutzer:

- **Digitale Nachbarschaft:** Multiplikatoren im Ehrenamt
- **DsiN-Sicherheitsbarometer (SiBa-App):** Die News- und Ratgeber-App
- **DigiBitS – Digitale Bildung trifft Schule:** Materialsammlung für Lehrkräfte
- **DsiN-MesseCampus:** Einstiegsmöglichkeiten für Studierende in IT-Sicherheitsbranche

REDUZIERUNG DER SICHERHEITSVORFÄLLE

STÄRKUNG DES RISIKOBEWUSSTSEINS

Internetführerschein

Achtsamkeit der Anbieter

Aufklärung in Schulen **Selbstinformation** Mehr Nachrichten

Bessere Rückverfolgung und härtere Strafen bei Verstößen

Schulung

Aufklärung in der Schule beginnen

Offenheit der betroffenen Unternehmen Expertenrat

Erfahrungsberichte von Geschädigten **kurze Begriffserklärung**

Warnhinweise beim Erwerb der Software

Verschärfende Gesetze

Weiterbildungsprogramme

Verbraucherstimmen:

Was wünschen sich Verbraucher für mehr IT-Sicherheit?

Informationen in Foren

private Hilfe

Mehr Presseberichte

Broschüren TV Werbung

Weiterbildungen

Schulfach werden

Vor allem in der jungen Generation aufklären **Hilfeseiten**

Vorträge in Bildungseinrichtungen

Aufklärung über Folgen

Seniorenseminare

Bessere Aufklärung von Politik

Kostenlose und einfach verständliche Software

Internetkurs

Alle Möglichkeiten zusammengefasst in einem Buch

Leichte Einstellmöglichkeiten

Erinnerungsapp

VERBESSERUNG VON SICHERHEITSWISSEN

MOTIVATION ZU EINEM SICHEREREN VERHALTEN IM INTERNET

Kapitel 03

Digitale Lebenswelten



Fokusthema: Gesundheit und Fitness digital

Erstmals wurde in diesem Jahr die digitale Sicherheitslage von Verbrauchern bei Gesundheits- und Fitnessdiensten vertiefend untersucht: Digitale Gesundheitsprogramme und -dienste betreffen vorrangig medizinische Angebote, Fitnessprogramme hingegen die eigene Kontrolle von Vitalfaktoren wie Ernährungs- oder Bewegungsverhalten.

Auffällig ist ein relativ hoher Anteil von Verbrauchern, die derzeit noch keine Aussagen zu Vorteilen, Nutzen oder Sicherheitsbedenken angeben; durchschnittlich ein Fünftel antwortete mit „weiß nicht“. Auch bewegen sich die gegebenen Antworten

stark im Mittelfeld, sodass positive und negative Stimmen dicht beieinanderliegen.

Insgesamt fühlen sich Verbraucher bei der Nutzung von Fitness- und Gesundheitsprogrammen vergleichsweise sicher: Nur 20,2 Prozent der Nutzer empfinden ein erhöhtes Gefährdungsgefühl. Anders beim elektronischen Austausch zwischen Patienten und Ärzten von gesundheitsbezogenen Daten: Hier sehen 58,2 Prozent der Verbraucher ein hohes oder zumindest mittleres Risiko. 25 Prozent der Verbraucher erwarten hier ein geringes bzw. kein Risiko (siehe Abb. 21). Weniger Skepsis haben Verbraucher bei

Abb. 19 Zustimmung Nutzen von Gesundheits- und Fitnessdiensten

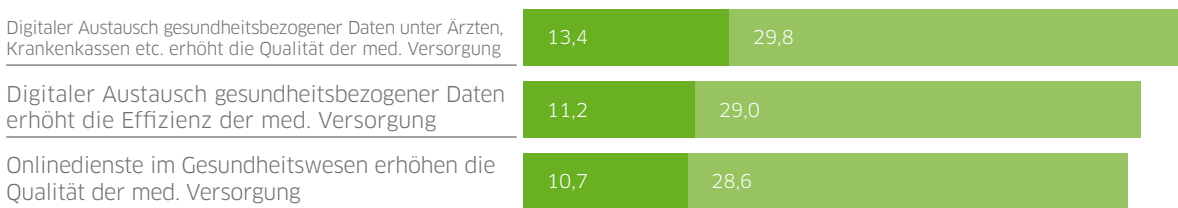


Abb. 20 Zustimmung Verwendung von Gesundheits- und Fitnessdiensten

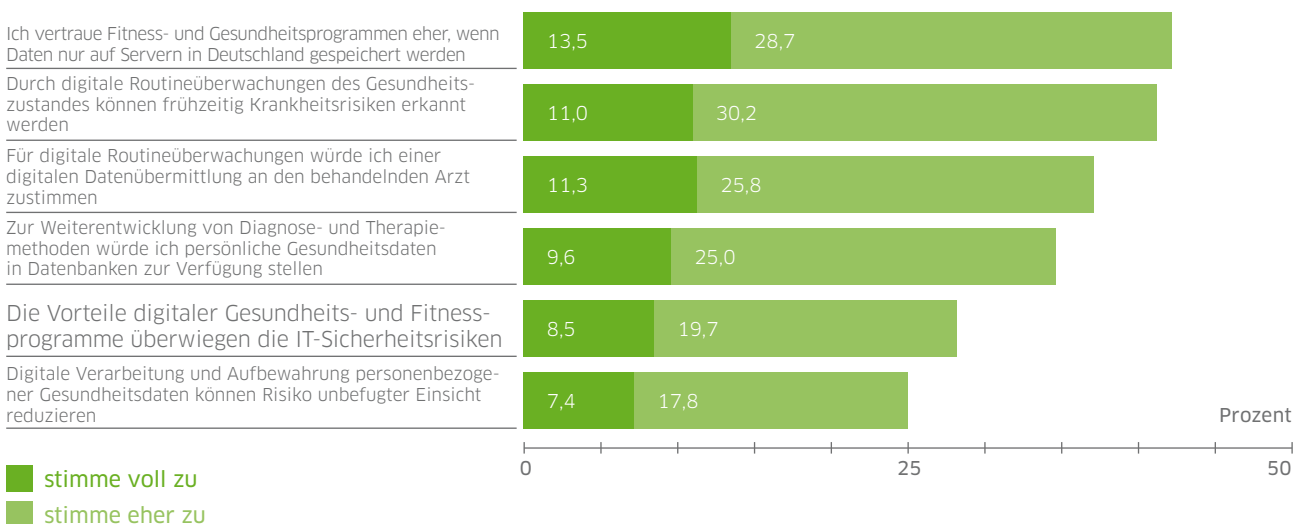
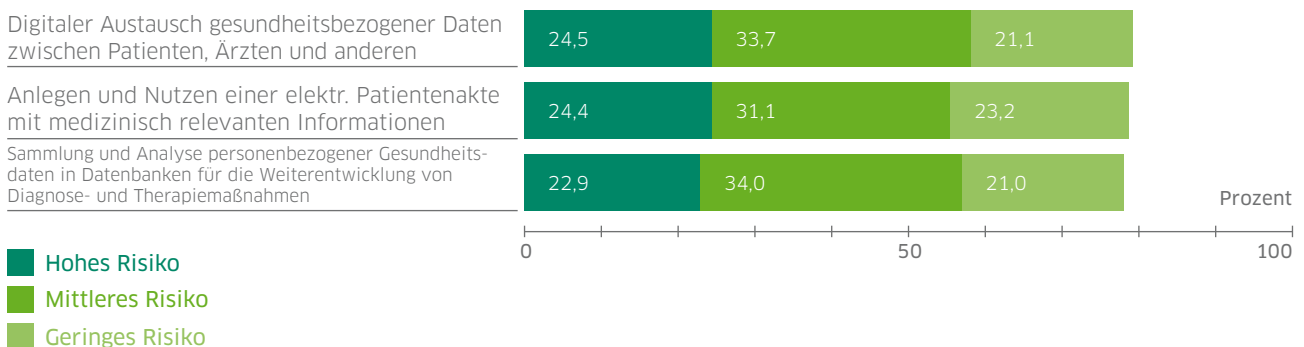


Abb. 21 Top 3 der Risikowahrnehmung Gesundheits- und Fitnessdienste

Gesundheitsdiensten zu rein administrativen Vorgängen: Eine Online-Terminvereinbarung halten die Befragten mehrheitlich (57,7 Prozent) für nicht oder kaum riskant.

Teilweise Potentiale erkannt

Ein positives Stimmungsbild herrscht, wenn Dienste die Versorgungsqualität verbessern sollen: 43,2 Prozent der Befragten stimmen zu, dass der digitale Austausch gesundheitsbezogener Daten die Qualität der medizinischen Versorgung erhöht (siehe Abb. 19). 41,2 Prozent der Verbraucher befürworten digitale Gesundheitsdienste für die frühzeitige Erkennung von Krankheitsrisiken durch digitale Routineüberwachungen (siehe Abb. 20).

Direkt nach den Vorteilen und IT-Risiken durch Gesundheits- und Fitnessprogrammen befragt, erklären 51,4 Prozent, dass aus ihrer Sicht die IT-Risiken überwiegen, während für 28,2 Prozent die Vorteile dominieren. 42,2 Prozent der Verbraucher vertrauen Fitness- und Gesundheitsprogrammen zudem eher, wenn ihre Daten ausschließlich auf Servern in Deutschland gespeichert werden.

Wissen und damit Vertrauen schaffen

Anknüpfungspunkte für Aufklärungsmaßnahmen können die fehlende Einschätzungskompetenz (18 Prozent der Befragten antworteten mit „weiß nicht“) sowie die weit verbreitete Unentschlossenheit im Umgang mit Gesund-

heitsdiensten sein, die vermutlich auf Unwissenheit beruhen. Hier trägt die Vermittlung von Grundlagenwissen und Verhaltensvorschlägen dazu bei, dass Verbraucher eine bewusste Entscheidung treffen können. Dies erfordert verständliches sowie bedarfsgerechtes und zielgruppenorientiertes Basiswissen. Komplexe Maßnahmen können durch praktische Handhabbarkeit und konkrete Anleitungen ermöglicht werden. Mit dem Verständnis steigen die eigenen Einschätzungskompetenzen zu Chancen und tatsächlichen Risiken.

Sicherheit auch durch Anbieter

Im Rahmen der Aufklärungsarbeit muss die geäußerte Skepsis in die weitere Entwicklungsarbeit eingebunden werden. Dazu kann die Transparenz der Anbieter bei der Erhebung und im Umgang mit Daten helfen, um Verbrauchern souveräne Entscheidungen zu ermöglichen. Digitale Aufklärungsarbeit kann und sollte zu diesen Themen zwischen Politik, Wirtschaft und Gesellschaft vermitteln.



DsiN-Angebote:

- **Digital-Kompass:** Materialien zum Thema Gesundheit, E-Health, Telemedizin; Handreichung Nr. 8: Digitale Zukunft – Neue Anwendungen und Möglichkeiten
- **DsiN-Sicherheitsbarometer (SiBa-App):** Die News- und Ratgeber-App, auch zum Themenfeld „Gesundheit- und Vitaldienste“
- **IT-Fitness-Test:** Online-Wissenscheck für souveräne Mediennutzung

DsiN-Angebote:

- **Meine Verkehrswelt: digital | vernetzt | sicher:** Informationsportal (im Aufbau)
- **DsiN-Sicherheitsbarometer (SiBa-App):** Die News- und Ratgeber-App



Vernetzter Verkehrsraum: Das Automobil

Auch die Mobilität wird immer digitaler: Eine vernetzte Fahrzeugelektronik unterstützt Fahrer zunehmend und ermöglicht eine internetbasierte Kommunikation innerhalb des Fahrzeugs sowie mit anderen Verkehrsteilnehmern und der Umgebung.

Chancen werden stärker wahrgenommen

Im Vergleich zum Vorjahr stehen Verbraucher der vernetzten Mobilität wesentlich positiver gegenüber: Alle abgefragten Aspekte verzeichnen ein deutliches Plus (siehe Abb. 22). Die höchste Zustimmung erfährt – wie schon 2016 – die Aussage, dass elektronische Assistenzsysteme das Autofahren sicherer machen: 71,9 Prozent der Befragten stimmen dem zu (+16,7 Prozent zum Vorjahr). Auch sind inzwischen 40,3 Prozent der Meinung, dass die Vorteile von vernetzten Fahrzeugen die Sicherheitsrisiken deutlich überwiegen (+8,9 Prozent).

Angst vor Risiken bei Datensicherheit und Datenschutz

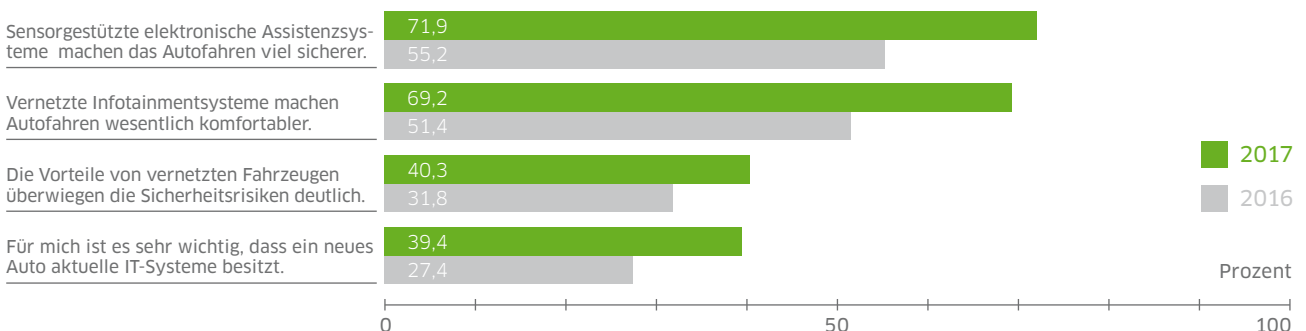
Die größten Sicherheitsrisiken für ihre Daten

sehen Verbraucher mit 59,1 Prozent nach wie vor beim Download und der Nutzung von Apps für Fahrzeugsysteme (+5,4 Prozent); gefolgt von vernetzten Unterhaltungssystemen mit 56,5 Prozent (+4 Prozent) sowie der Einbindung von Mobilgeräten in die Fahrzeugelektronik mit 54,4 Prozent (+2,2 Prozent). Als wahrscheinlichste Gefahren sehen Verbraucher die unbefugte Datensammlung durch Dritte wie z.B. die Überwachung des Fahrverhaltens (75,1 Prozent; +8,3 Prozent) sowie das unbefugte Auslesen sensibler Daten (74,2 Prozent; +9,6 Prozent). Zuständig für die Sicherheit sind für 83,5 Prozent der Befragten die Fahrzeughersteller (+4,3 Prozent).

Mehr Verbraucher als 2016 können sich äußern

Verbraucher beziehen inzwischen stärker Stellung zum Thema: Während im letzten Jahr der Durchschnittswert für die Angabe „Weiß nicht“ bei 19,7 Prozent lag, liegt der Wert diesjährig bei 9,7 Prozent. Dies lässt vermuten, dass sich das Thema immer mehr etabliert und sich Verbraucher mehr Wissen angeeignet haben.

Abb. 22 Vorteile des Vernetzten Fahrens



Haus- und Heimvernetzung

Für Verbraucher wird das Internet der Dinge beim „Smart Home“ greifbar. Hierzu gehört neben Unterhaltungselektronik – wie dem vernetzten Fernseher – auch die Haustechnik. Mit den neuen Möglichkeiten entstehen aber auch neue Angriffsflächen für Datenmissbrauch und Cybercrime.

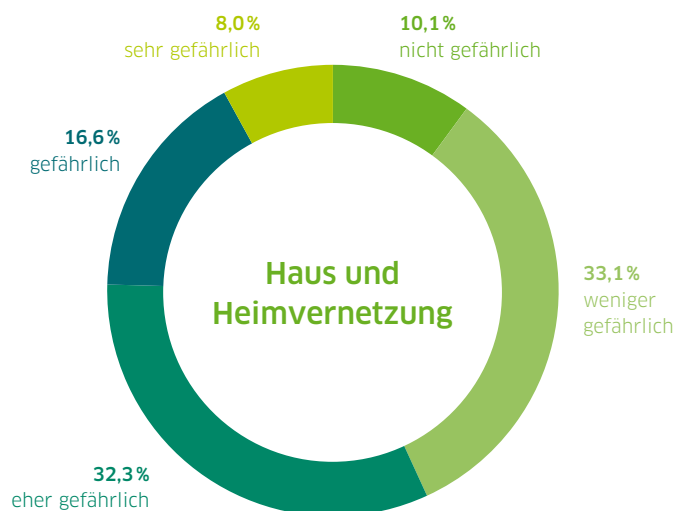
Das vernetzte Zuhause gehört (noch) nicht zum Alltag

Die kontinuierliche Entwicklung der Nutzungszahlen hat sich fortgesetzt. So gibt es einen leichten Anstieg bei der Vernetzung von Unterhaltungselektronik mit einem Zuwachs von 2 Prozent (wie auch im Vorjahr) auf 11,3 Prozent. Die Vernetzung von Haustechnik hat dieses Jahr bei kaum veränderten 3,7 Prozent (+0,1 Prozent zu 2016 sowie +1,4 zu 2015).

Durchschnittlich 1/4 der Verbraucher sieht Risiken

Nur gut jeder vierte Verbraucher (28 Prozent) empfindet die Steuerung und Vernetzung von Haustechnik für gefährlich oder sehr gefährlich. Gleichwohl ist damit die Risikoeinschätzung im Vergleich zum Vorjahr um 4,6 Prozent angestiegen. Im Vierjahresvergleich stellt dies erstmals einen erkennbaren Anstieg dar. Die Nutzung von Unterhaltungselektronik stufen in diesem Jahr 21 Prozent als gefährlich oder sehr gefährlich ein (+2,7 Prozent zum Vorjahr). Beide Werte zusammen ergeben das Gefährdungsgefühl in Bezug auf die Haus- und Heimvernetzung gesamt (Abb. 23).

Abb. 23 Gefährdungsgefühl bei Haus und Heimvernetzung gesamt



Zahl der Angriffe auf Heimvernetzung steigt etwas

3 Prozent der Befragten gaben an, dass ihre Hausvernetzung angegriffen wurde. Das sind 0,8 Prozent mehr im Vergleich zum Vorjahr. Die niedrigen Werte hängen sicherlich auch mit der relativ geringen Verbreitung zusammen.



DsiN-Angebote:

- **Digital-Kompass:** Handreichung Nr.8: Digitale Zukunft – Neue Anwendungen und Möglichkeiten
- **DsiN-Sicherheitsbarometer (SiBa-App):** Die News- und Ratgeber-App, auch zum Themenfeld „Haus- und Heimvernetzung“
- **IT-Fitness-Test:** Online-Wissenscheck für souveräne Mediennutzung

Einkaufen im Internet

DsiN-Angebote:

- **Digitale Nachbarschaft:** Sicher im Netz einkaufen und bezahlen für Einsteiger und Fortgeschrittene
- **Digitalkompass:** Handreichung Nr. 5: Online-Einkaufen und Online-Banking
- **DsiN-Rubrik für Verbraucher:** Online sicher bezahlen & Shopping mit Verstand inkl. Video-Clip „Sicherer Online-Kauf“ www.sicher-im-netz.de



Drei von vier Onlinern kaufen im Internet ein (77,6 Prozent). Damit ist Online-Shopping nach der E-Mail-Kommunikation die zweitstärkste Online-Aktivität. Das Vertrauen in Online-Shopping bleibt stabil auf relativ hohem Niveau: 20,2 Prozent der Verbraucher halten das Einkaufen im Netz für gefährlich.

Leichter Anstieg an Vorfällen

Die Anzahl an Sicherheitsvorfällen beim Online-Shopping hat sich leicht erhöht: So waren 4,7 Prozent der Befragten in den letzten 12 Monaten von Kreditkartenbetrug betroffen (+0,9 Prozent zum Vorjahr). Weitere 5,7 Prozent gaben an, beim Zahlungsvorgang im Internet Opfer eines Betrugs geworden zu sein (+0,4 Prozent). Das Ausspähen von Zugangsdaten zu einem Online-Shop hat sich von 5,7 Prozent auf 6,0 Prozent erhöht. Den Betrug bei einem Online-Einkauf oder einer Online-Buchung durch nicht erbrachte Leistung nannten 7,6 Prozent (-0,3 Prozent).

Gütesiegel: Wissen ungleich Verhalten

Sichere digitale Zahlungssysteme sind 93,9 Prozent der Befragten bekannt und werden mit 80,5 Prozent auch fast genauso häufig genutzt (+2,4 Prozent). Die Diskrepanz zwischen Wissen und Verhalten wird somit im Vierjahresvergleich kleiner. 2014 lag die Differenz noch bei 17 Prozent, in diesem Jahr nur noch bei 13,4 Prozent. Beim Thema Gütesiegel herrscht weiterhin eine signifikante Diskrepanz zwischen Wissen und Verhalten. Während 89,4 Prozent Gütesiegel kennen, achten nur 57,5 Prozent der Verbraucher darauf: Das sind 1,7 Prozent weniger als 2016. Im Vierjahresvergleich wird die Lücke zwischen Wissen und Verhalten somit erstmals wieder größer.

Abb. 24 Gefährdungsgefühl beim Online-Einkauf

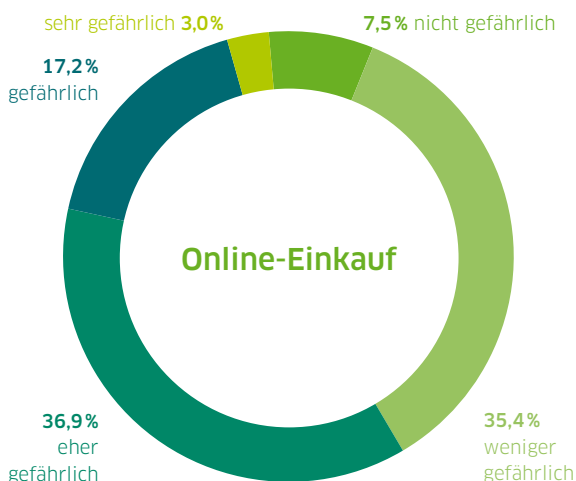
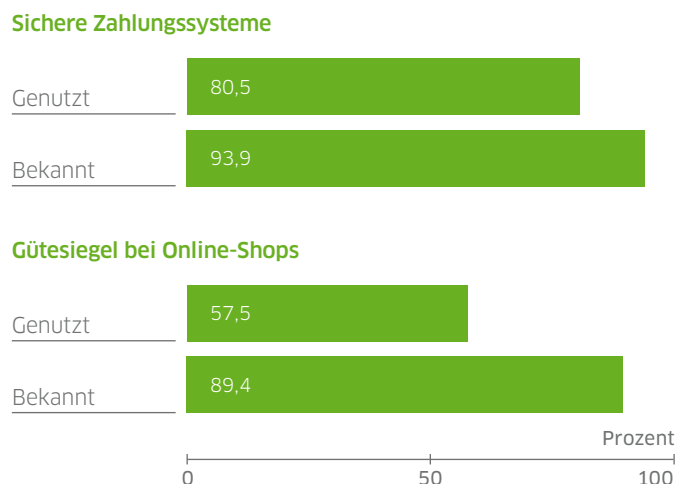
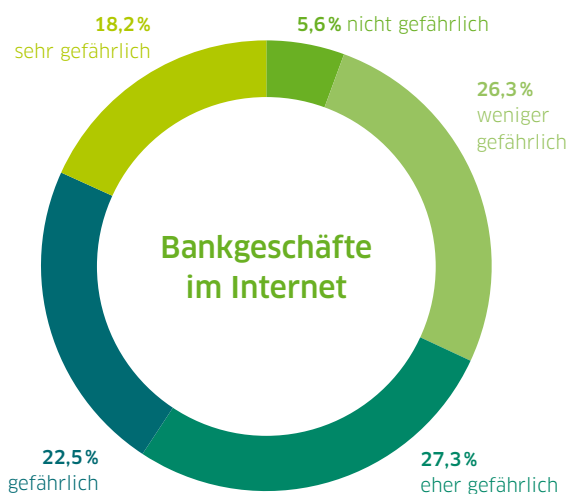


Abb. 25 Diskrepanz Wissen und Verhalten beim Online-Einkauf



Bankgeschäfte im Internet

Abb. 26 Gefährdungsgefühl beim Online-Banking



Online-Banking ist bei Verbrauchern weit verbreitet. Mit 61,5 Prozent landet es auf dem vierten Platz der genutzten digitalen Dienste.

Mehrheitliche Unsicherheit

Online-Banking wird im Vergleich zu anderen Diensten weiterhin als am gefährlichsten empfunden: 40,8 Prozent der Verbraucher halten Bankgeschäfte über das Internet für gefährlich oder sehr gefährlich, (+1,6 Prozent zum Vorjahr).

Ausspähen von Zugangsdaten: Wert erneut leicht zurückgegangen

Im Vorjahresvergleich ist die Anzahl der Nutzer, deren Zugangsdaten beim Online-Banking ausgespäht wurden, um 0,5 Prozentpunkte auf 4,4 Prozent zurückgegangen.

Kennen vs. Nutzen: Verbesserungen im Vierjahresvergleich

90,8 Prozent der Verbraucher wissen, dass

Abb. 27 Diskrepanz Wissen und Verhalten beim Online-Banking

„SMS-TAN“ / „Push-TAN“



Kauf- und Buchungsbetrug



Prozent

0 50 100

es verschlüsselte Verbindungen für digitale Bankgeschäfte gibt; eine Steigerung von knapp einem Prozent im Vergleich zum Vorjahr. Dennoch nutzen Verbraucher diese Verbindungen mit nur 66,8 Prozent seltener als noch 2016 (-1,6 Prozent). SMS-Tans verzeichnen hingegen in Hinblick auf die Bekanntheit mit 90,4 Prozent (+4,2 Prozent) und die tatsächliche Nutzung mit inzwischen 64,4 Prozent (+7,6 Prozent) eine Steigerung bei den Nutzern. Im Vierjahresvergleich wird die Diskrepanz zwischen Wissen und Verhalten in beiden Bereichen zunehmend kleiner.



DsiN-Angebote:

- **Digitale Nachbarschaft:** Sicher im Netz einkaufen und bezahlen für Einsteiger und Fortgeschrittene
- **Digitalkompass:** Handreichung Nr. 5: Online-Einkaufen und Online-Banking
- **Mobile Banking:** Themenfeld auf auf www.sicher-im-netz.de



Kapitel 04

**Digitale Auf-
klärung: Selbst-
kompetenzen
für IT-Sicherheit
stärken**

Digitale Aufklärung durch digitale Bildung

Die komplexe Sicherheitslage, die im vorliegenden Index erkennbar wird, erfordert als Reaktion die Fähigkeit, auf steigende, wechselnde und unbekannte Anforderungen und Risiken souverän zu reagieren. Hierzu zählt unter anderem die Kompetenz, sich selbst weiterbilden zu können. Diese Fähigkeit ist bei souveränen Nutzern bereits besser ausgeprägt als bei anderen Verbrauchertypen. Eine grundlegende digitale Kompetenz wirkt dem Szenario entgegen, dass die Bedrohungslage und das Schutzniveau der Verbraucher in den nächsten Jahren (weiter) auseinanderdriften.

Der Erwerb digitaler Grundkompetenzen von Verbrauchern erhält damit einen zentralen Stellenwert als Schlüsselqualifikation für den sicheren Umgang mit der Digitalisierung. Dieser Anspruch fand in der Cyber-Sicherheitsstrategie der Bundesregierung Ausdruck im Ziel „digitale Kompetenz bei allen Anwendern“ zu fördern und digitale Bildung zum „festen Bestandteil des Bildungskanons“ zu entwickeln.

Aufklärung sollte hierbei dem Ansatz folgen, Verbraucher durch Hilfe zur Selbsthilfe auf diese Herausforderung vorzubereiten. Die Studie zeigt, dass es eine geteilte Verantwortung für die Aufklärungsarbeit gibt: Neben der Familie und dem sozialen Umfeld, die mit 48,6 Prozent die wichtigste Informationsquelle der Befragten sind, ist es die Aufgabe von Bildungseinrichtungen

und -initiativen, Verbraucher im sicheren Umgang mit Medien zu befähigen. 72,9 Prozent erwarten mehr Aufklärungsangebote in ihrer beruflichen oder schulischen Aus- und Weiterbildung, 57,6 Prozent fühlen sich durch eine persönliche Ansprache im schulischen oder beruflichen Umfeld zur Wissensumsetzung motiviert.

Im Bildungsbereich greift auch künftig der DsiN-Ansatz einer digitalen Aufklärung 2.0: Die Schule ist der optimale Ort zur sicheren Erprobung und Anwendung (neuer) digitaler Medien, und zwar so früh wie möglich. Darüber hinaus werden Lehrkräfte zielgruppenspezifisch befähigt und mit guten Initiativen vernetzt. Sie sind damit, neben den Schülern, Multiplikatoren für gelebte IT-Sicherheit, die über die Sensibilisierung hinausreicht und zur Anwendung des erlernten Wissens motiviert.

Übergreifende Schlüsselkompetenzen für Verbraucher, die sie auf neue Dienste übertragen können

Grundlagen: Informieren und Sensibilisieren

Damit Verbraucher selbstbestimmt entscheiden können, welche Dienste sie nutzen möchten und wie sie sich schützen können, ist der Erwerb von Wissen zu Funktionsweisen sowie Risiken und Schutzmaßnahmen grundlegend. Hierfür müssen Verbraucher zunächst für die Relevanz des Themas sensibilisiert werden: Daher ist der erste Schritt, aktiv auf Verbraucher zuzugehen und Aufmerksamkeit sowie persönliche Anknüpfungspunkte für das Thema IT-Sicherheit zu erzeugen.

Betroffenheit erkennen – Relevanz wahrnehmen

Hilfreich für eine wirksame Sensibilisierung ist die Darstellung konkreter Relevanz und Betroffenheit im Alltag: Dies erfordert eine

Berücksichtigung der verschiedenen Zielgruppen mit unterschiedlichen Nutzungsgewohnheiten, Defiziten und Risikoexpositionen (siehe dazu Kapitel 2). Um eine bedarfsgerechte Ansprache zu gestalten, muss Aufklärung jüngere Menschen eher zu Themen wie Smartphones oder Spielekonsolen, dem Herunterladen von Apps, Filmen und Musik oder der Nutzung von Messenger-Diensten und sozialen Netzwerken ansprechen – denn diese Angebote nutzen sie häufiger als andere Altersgruppen, wie der Index 2017 aufzeigt. Ältere Generationen brauchen dagegen entsprechend ihrer Nutzungsgewohnheiten vor allem Informationen zu Sicherheitsvorkehrungen am Laptop und Desktop-PC und für Dienste wie dem Online-Banking.

Abb. 28 Genutzte Informationsquellen der Verbraucher

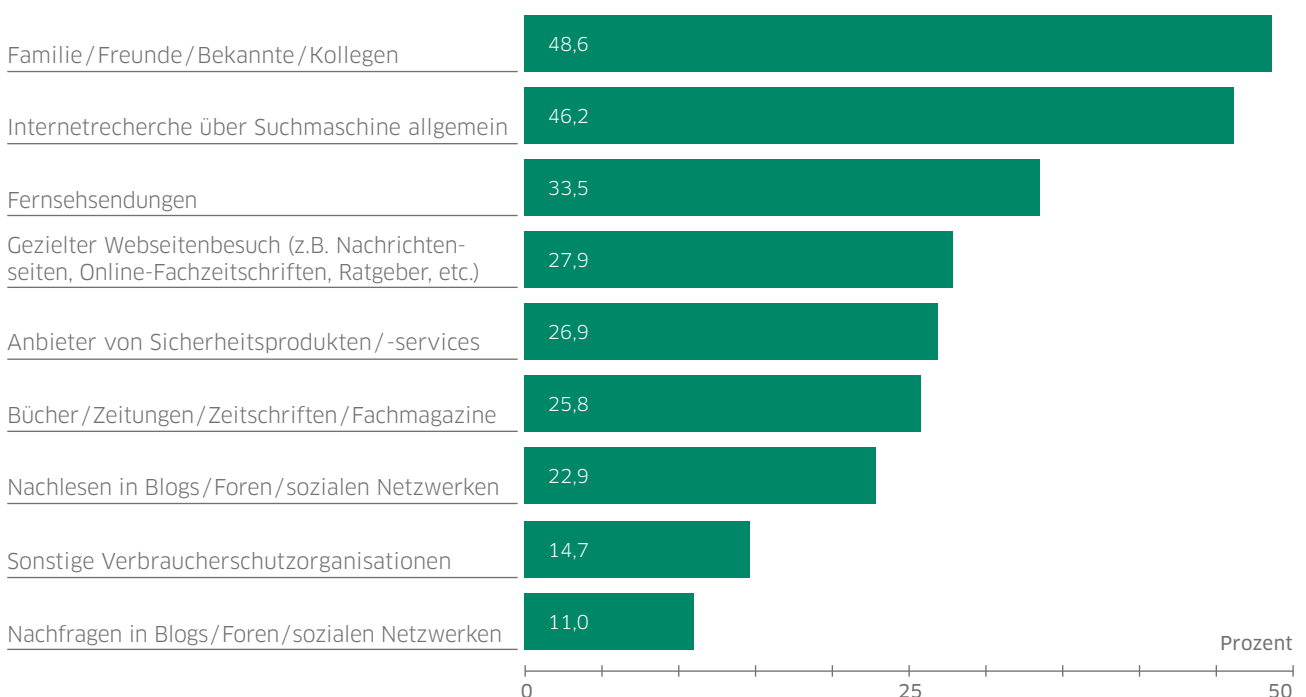
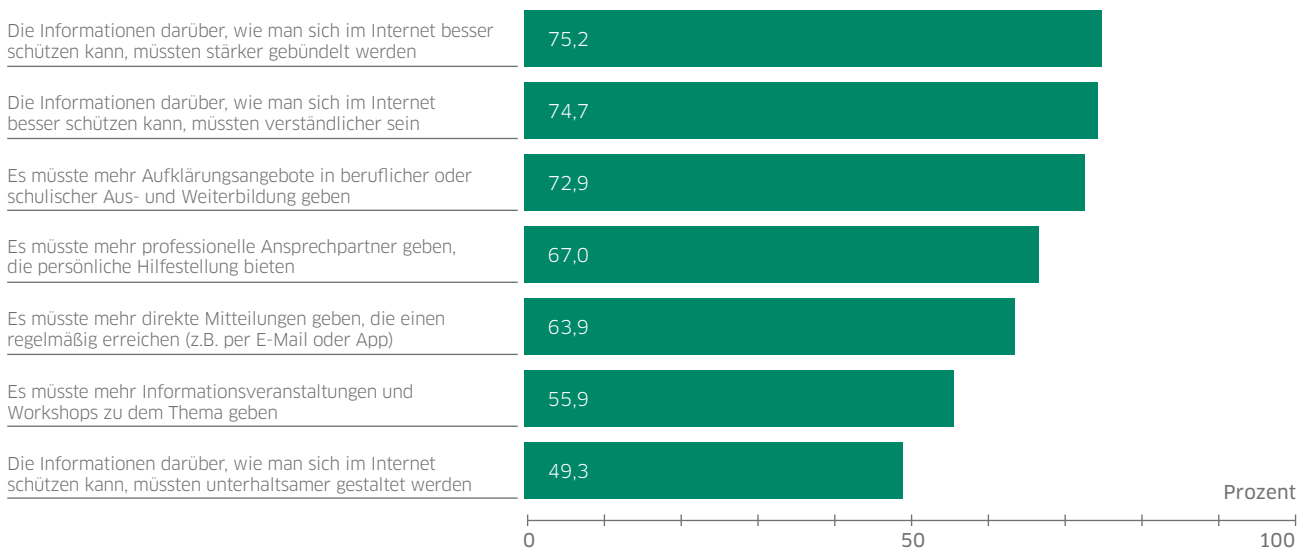


Abb. 29 Verbrauchersicht: Wie Sicherheitswissen verbessern?

Basis- und Fachkenntnis – je nach Bedarf

Auch Defizite sind unterschiedlich ausgeprägt: Verbraucher haben sich – vor allem beim Basisschutz, wie der sicheren Nutzung von Passwörtern – inzwischen umfangreiches Wissen angeeignet. Dies gilt vor allem für Fatalisten, Gutgläubige und Souveräne. Sie brauchen daher tiefergehende Informationen zu komplexeren Sicherheitsmaßnahmen. Dazu gehören die Überprüfung der Vertrauenswürdigkeit von

Cloud-Diensten, die Inkognito-Funktion sowie die 2-Faktor-Authentifizierung (siehe dazu auch Abb. 6 Seite 11, Sicherheitswissen). Außenstehende Nutzer benötigen Unterstützung beim Basiswissen: Sie hinken insbesondere im Bereich Smartphone und Apps hinterher aber auch beim sicheren (drahtlosen) Surfen.



Handlungsempfehlungen:

- **Bewusstsein für Relevanz schaffen**
Eigene Betroffenheit verdeutlichen
- **Potentielle Sicherheitsrisiken aufzeigen**
Praxisnah und zielgruppengerecht
- **Basiswissen vermitteln**
Außenstehenden aktiv Informationen geben
- **Kenntnisse vertiefen**
Komplexere Kenntnisse – je nach Bedarf

DsiN-Angebote zur Sensibilisierung:

- **IT-Fitness-Test:** Wissenscheck für Einsteiger
- **DsiN Sicherheitsbarometer (SiBa-App):** Die News- und Ratgeber-App
- **Aktionsbund Digitale Sicherheit:** Materialsammlung zu Aufklärungsangeboten
- **Verbraucher-Rubrik** auf www.sicher-im-netz.de

Anleiten und Befähigen

Nutzer müssen ihre Kenntnisse auch anwenden: Der großen Diskrepanz zwischen Wissen und Verhalten kann durch ein konkretes Anleiten entgegengewirkt werden, das zur Umsetzung von Grundwissen beiträgt. Dieser Bedarf wird besonders erkennbar bei den außenstehenden, fatalistischen und gutgläubigen Nutzern.

Unterstützung bei komplexen Schutzmaßnahmen

Je anspruchsvoller oder unbekannter eine Sicherheitsmaßnahme ist, desto weniger wird sie von Verbrauchern genutzt. Neben dem Passwortmanager, der biometrischen Identifizierung und der sicheren Aufbewahrung betrifft dies auch das Thema Verschlüsselung (siehe Abb. 30). Hier nützen Anleitungen zu konkreten Diensten und kleinschrittige Veranschaulichungen: beispielsweise in Video-clips und interaktiven Angeboten, um Sicherheitsmaßnahmen selbst zu erproben und somit zu verinnerlichen.

Aufklärung persönlich und vor Ort

Direkte Ansprechpartner vor Ort ermutigen zur individuellen Nachfrage. Digitale Aufklärung schafft hier Räume zum Austausch, um es Nutzern zu ermöglichen, voneinander zu lernen. Souveräne Nutzer können dabei als Multiplikatoren und Vorbilder für IT-Sicherheit sehr gut eingebunden werden. Auch sollte diese Aufklärung bereits in der Schule und im Elternhaus starten.

Selbstsicherheit durch Routine

Durch eine regelmäßige Auseinandersetzung mit dem Thema können Verbraucher ihre Umsetzungskompetenz trainieren und IT-Sicherheitsverhalten zur Routine machen. So gewinnen sie Selbstsicherheit und können passende Sicherheitsmaßnahmen anwenden. Gleichzeitig bauen sie ihr Gefährdungsgefühl im Umgang mit digitalen Diensten ab – zugunsten souveräner Risikoeinschätzung. Letzteres ist insbesondere für die Fatalisten ein notwendiges Ziel der Aufklärungsarbeit.

Abb. 30 Kenntnis versus Nutzung – Top 6 der größten Diskrepanzen

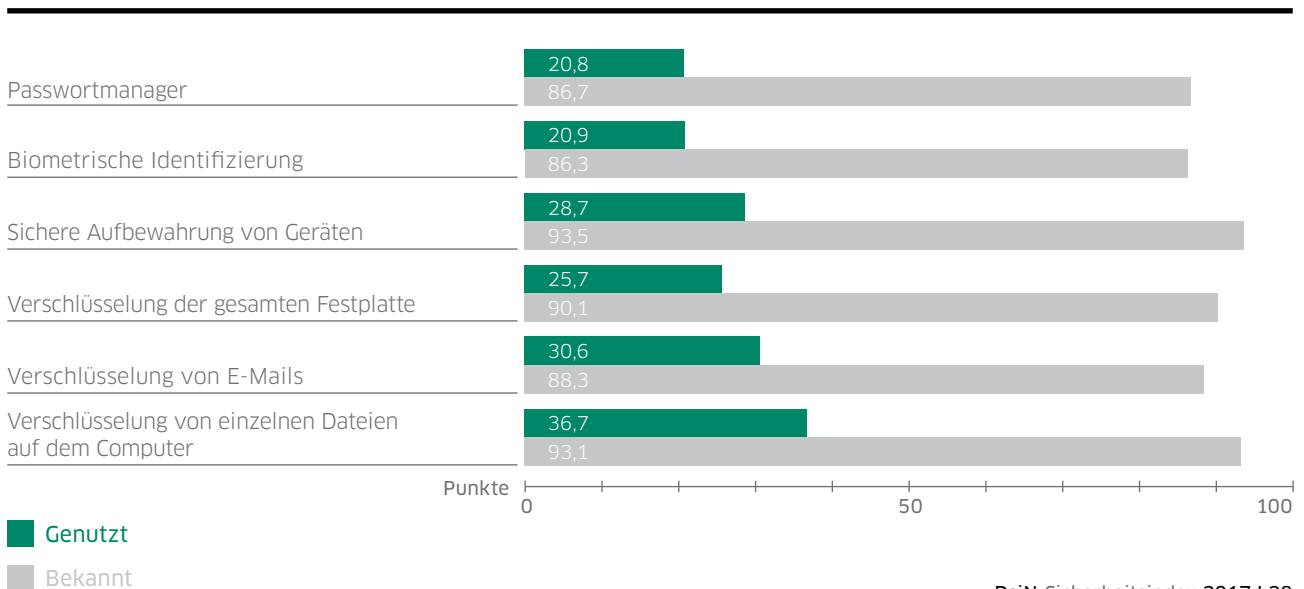
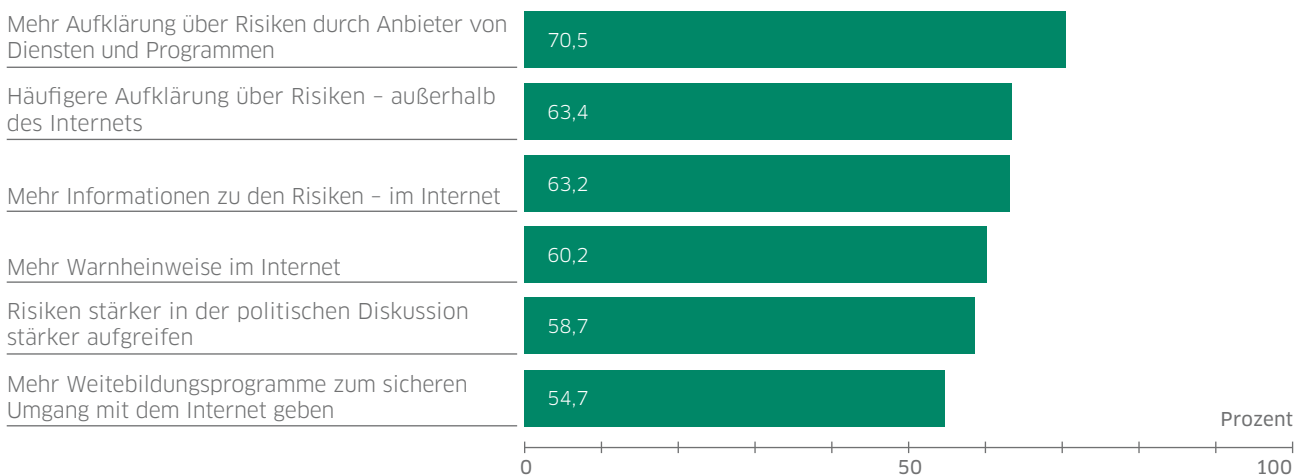


Abb. 31 Verbrauchersicht: Wie Risikobewusstsein stärken?

Balance zwischen Unbedarftheit und Verunsicherung

Eine souveräne Risikoeinschätzung ist die Grundlage für ein sicheres Verhalten im Netz. So zeigen Fatalisten ein meist übertriebenes Gefährdungsgefühl, während Gutgläubige hier kaum sensibilisiert sind: Ihre Fähigkeit zum Einschätzen realistischer Risiken muss verstärkt werden. Danach befragt, was für eine Stärkung des Risikobewusstseins hilfreich wäre, wünschen sich 70,5 Prozent der Verbraucher insbesondere eine bessere Auf-

klärung über Risiken von den Programm- und Diensteanbietern. Auch mehr Informationen über Risiken außerhalb des Internets (63,4 Prozent) sowie innerhalb des Netzes (63,2 Prozent) zählen zu Maßnahmen mit der höchsten Zustimmung (siehe Abb. 31). Wichtig ist, auch die Chancen der Digitalisierung zu betonen, um Übervorsichtigkeit und Hemmungen abzubauen und Vertrauen zu schaffen.



Handlungsempfehlungen:

- **Individuelle Unterstützung**
direkt und vor Ort
- **Risikoeinschätzungskompetenz**
in Abgrenzung zu Unbedarftheit und Verunsicherung fördern
- **Umsetzungskompetenz**
durch Alltagsroutine trainieren
- **Sicherheitsangebote**
durch praktische Handhabbarkeit auch komplexere Maßnahmen ermöglichen

DsiN-Angebote zur Befähigung:

- **Digital-Kompass** mit Digitalen Stammtischen für Senioren
- **Digitale Nachbarschaft** für ehrenamtlich aktive Bürger
- **Bottom-Up:** Berufsschüler für IT-Sicherheit
- **DigiBits - Digitale Bildung trifft Schule:** Materialsammlung für Lehrkräfte
- **DsiN-Aufklärungsfilme** z.B. zum Thema Verschlüsselung

Eigenverantwortung stärken und Motivieren

Mit der Motivation der Verbraucher zur Anwendung ihres Wissens, kann ebenfalls die Diskrepanz zwischen Kenntnis und Nutzung von Schutzmaßnahmen abgebaut werden. Digitale Aufklärung kann hier ansetzen und Verbraucher zu sicherem Handeln motivieren. Vor allem fatalistische sowie gutgläubige Verbraucher sind hier anzusprechen (siehe dazu auch Kapitel 2).

Eigenverantwortung stärken

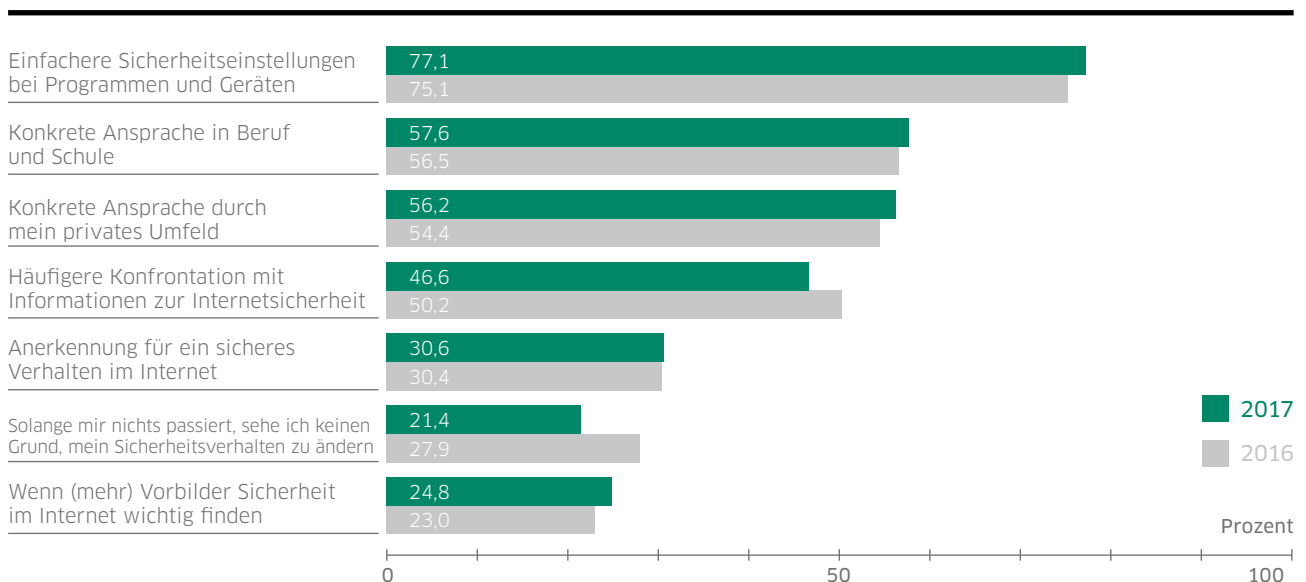
Motivation kann durch Einsicht zur Eigenverantwortung gestärkt werden: Vielversprechend erscheint hier, dass schon 84,4 Prozent der Verbraucher der Meinung sind, dass sie vorsichtiger mit den eigenen Daten umgehen sollten und drei Viertel glauben, dass sie häufiger Sicherheitsmaßnahmen einsetzen sollten (siehe dazu Seite 12: Einflussfaktoren aus Verbrauchersicht). Diese Wahrnehmung muss durch

eine digitale Aufklärung 2.0 weiter ausgebaut werden: Verbraucher müssen selbst das Bedürfnis entwickeln, etwas für ihre Sicherheit tun zu wollen. Und sie müssen einsehen, dass sie hierfür mitverantwortlich sind. Hierbei sollten die gutgläubigen Nutzer besonders bestärkt und aktiviert werden, sie hinken in der Wahrnehmung der Eigenverantwortung hinterher.

Anreize durch Anerkennung

Ein Beitrag zur Motivation liegt auch in Anreizen, die persönliche Vorteile ermöglichen. Schulungen mit Zertifizierungen schaffen berufliche Vorteile, Wettbewerbe versprechen soziale Anerkennung und Gewinne - und fördern zugleich die Auseinandersetzung mit sicherheitsrelevanten Themen. So kann das Engagement aufseiten der Verbraucher, sich aktiv für ihre IT-Sicherheit einzusetzen, erhöht werden.

Abb. 32 Was Verbraucher zu IT-Sicherheit motiviert



Persönliche Ansprache durch Vorbilder

Ein Viertel der Verbraucher (24,8 Prozent) fühlt sich durch Vorbilder, zum Beispiel innerhalb der eigenen Peergroup, zur Anwendung von Sicherheitsmaßnahmen animiert. Auch eine Ansprache in Beruf und Schule oder durch das private Umfeld empfinden Verbraucher als sehr motivierend (siehe Abb. 33). Eine digitale Aufklärung muss Verbraucher also vor allem an Orten erreichen, an denen sie bereits viel Zeit verbringen: Im näherem sozialen, familiären, schulischem und beruflichen Umfeld.

von Updates als Nutzungszweck des Internets nennen, nutzen bereits 67,4 Prozent der Befragten automatische Updates als Sicherheitsvorkehrung. Eine Rückmeldung an die Anbieter zu Hürden bei der Anwendung von Sicherheitseinstellungen kann daher die Sicherheitslage verbessern und den Austausch zwischen technischer Expertise und praktischen Nutzererfahrungen verstärken.

Schutzvorkehrungen vereinfachen

Wie im Vorjahr fühlen sich deutsche Onliner durch einfach bedienbare Sicherheitseinstellungen motiviert: 77,1 Prozent und somit 2 Prozent mehr als 2016 sehen hier motivationssteigerndes Potential. Das dies tatsächlich besonders motiviert, wird in puncto Updates sichtbar: Während nur 51,7 Prozent das (manuelle) Herunterladen



Handlungsempfehlungen:

- **Einsicht durch Anerkennung fördern**
Erfolgsaussichten verdeutlichen und Würdigung verstärken
- **Eigenverantwortung stärken**
um Gutgläubigkeit entgegenzuwirken
- **Vorbilder gewinnen**
Souveräne Nutzer als Multiplikatoren einbinden
- **Umsetzung vereinfachen**
Sicherheitsmaßnahmen leichter gestalten

DsiN-Angebote zur Motivation:

- **myDigitalWorld:** Jugendwettbewerb
- **Goldener Internetpreis** für Senioren
- **Digitale Nachbarschaft:** Multiplikatoren im Ehrenamt
- **Bottom-Up:** Berufsschüler für IT-Sicherheit

Selbstkompetenzen für IT-Sicherheit frühzeitig stärken

Die gute Botschaft: Das Schutzniveau der Verbraucher hat sich das dritte Jahr in Folge verbessert. Diesen positiven Trend gilt es durch Aufklärungsarbeit zu verstärken. Aber: Auch die Wissens-Verhaltens-Schere öffnet sich weiter. Die Motivation zur Anwendung steht im Fokus digitaler Aufklärung!

Hilfe zur Selbsthilfe gegen steigende Bedrohungslage

Das Schutzniveau der Verbraucher steigt – jedoch langsam. Zugleich nehmen die Angriffsflächen mit der voranschreitenden Digitalisierung zu. Um dieser Entwicklung zu begegnen, muss Aufklärung verstärkt auf Selbstkompetenzen setzen: Die Fähigkeit, IT-Sicherheitswissen und Handeln selbstständig neuen Gegebenheiten anzupassen, wird zur Grundlage eines sicheren und souveränen Verhaltens im Netz.

Digitale Bildung – so früh wie möglich

Die frühzeitige Vermittlung von Schlüsselkompetenzen zur sicheren Nutzung der digitalen Chancen muss zum Grundkanon der Bildungsarbeit gehören. Die zielgruppenspezifische Ansprache ist dafür der notwendige Ansatz, um schon junge Menschen auf eine selbstbestimmte und sichere Nutzung vorzubereiten – ohne die heute älteren Generationen zu vernachlässigen. Niemand darf abgehängt werden!

Digitale Aufklärung braucht den Dialog

Aufklärungsarbeit muss als gleichgewichteter Baustein in der IT-Sicherheitsdebatte von Politik, Wirtschaft und Gesellschaft anerkannt und entsprechend ausgestattet werden. Erst im gemeinsamen Engagement und Erfahrungsaustausch kann Aufklärungsarbeit erfolgreich wirken und IT-Sicherheit gelingen. Dies fördert auch die Akzeptanz digitaler Innovation als Grundlage einer sicheren und breiten Teilhabe der Gesellschaft an den digitalen Chancen.

Glossar

| | |
|--------------------------------------|---|
| DsiN-Sicherheitsindex | Sicherheitslage deutscher Onlineur in einer Zahl – als gewichteter Mittelwert aus den vier Sicherheitsfaktoren (s.u.). |
| Indexpunkte | Der DsiN-Index sowie die vier Faktoren werden auf einer Skala von 1 bis 100 gemessen. |
| Schwellenwert 50 | Bei Werten unter 50 Indexpunkten ist die Bedrohungslage höher als das Schutzniveau. |
| Verbrauchertypen | Eine Clusterung der deutschen Onlineur. Es gibt 4 Verbrauchertypen, die sich durch typische Verhaltensweisen auszeichnen. |
| Die vier Sicherheitsfaktoren: | |
| Sicherheitsvorfälle | IT-sicherheitsrelevante Vorfälle, die von den Onlineur registriert wurden. |
| Gefährdungsgefühl | Das persönliche Gefühl der Gefährdung bei der Nutzung ausgesuchter Technologien und Anwendungen. |
| Sicherheitskompetenz | Selbstauskunft über die Kenntnis von IT-Schutzmaßnahmen. |
| Sicherheitsverhalten | Selbstauskunft über die Anwendung von IT-Schutzmaßnahmen. |

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 2017

Studie von Deutschland sicher im Netz e.V. zur digitalen
Sicherheitslage der Verbraucher in Deutschland

Verantwortlich: Dr. Michael Littger

Redaktion: Nadine Berneis (Leitung); Hanna Lückmann;
Anita Möllering; Karola Ettner (Kantar TNS); Tobias Weber (Kantar TNS)

Studienpartner: Kantar TNS Infratest

Gestaltung: Studio GOOD, Berlin

Infografiken: Carsten Raffel (USOTA)

Fotoquelle: shutterstock.com

Stand: Mai 2017

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 9, 11, 15, 27, 34: shutterstock.com