



DsiN

SicherheitsIndex 2015

Digitale Sicherheitslage
der Verbraucher in Deutschland

Schirmherrschaft:



Bundesministerium
des Innern



**Deutschland
sicher im Netz**



Ulrich Kelber

Geleitwort

Für die meisten Verbraucherinnen und Verbraucher ist die Digitalisierung im Alltag eine großartige Bereicherung: Soziale Netzwerke erleichtern den Kontakt zu Freunden, das Einkaufen, Bankgeschäfte und Urlaubsbuchungen lassen sich jederzeit und an jedem Ort erledigen. Unterhaltungsangebote sind einfacher wahrzunehmen. Wir sind auf dem Weg zum vernetzten Fahren, intelligente Haus- und Heimdienste werden angeboten – mit neuen Möglichkeiten für den Alltag.

Die wachsende Vernetzung aller Lebensbereiche eröffnet neue Chancen für die Gesellschaft insgesamt, gerade auch älteren Generationen, denen das Internet ein selbständiges, aktives Leben bis ins hohe Alter ermöglichen kann. Voraussetzung für eine echte Entfaltung der digitalen Chancen ist aber, dass die angebotenen Dienste und Technologien auch sicher und leicht zu handhaben sind. Damit Anwender in die digitale Welt mit ihren neuen Angeboten wirklich vertrauen können – und nicht enttäuscht werden, müssen Schutz und Sicherheit der Verbraucher an erster Stelle stehen.

Der DsiN-Sicherheitsindex liefert einen zuverlässigen Gradmesser, um die digitale Sicherheitslage in Deutschland anschaulich darzustellen. 2014 haben wir die erste Untersuchung vorgestellt. Der Vergleich mit den Ergebnissen des Vorjahres zeigt, dass die digitale Sicherheitslage zwischen den Verbrauchergruppen weiterhin unterschiedlich ausfällt. Ein Zustand, mit dem wir nicht zufrieden sein können.

Die Defizite bei den verschiedenen Verbrauchertypen fordern spezifische Maßnahmen zur Abhilfe. Neben der Vermittlung von konkretem Sicherheitswissen gehört dazu auch, die Nutzer zur Anwendung der Maßnahmen zu motivieren – als zentraler Baustein für digitalen Schutz und Vertrauen.

Mit zahlreichen Initiativen der Verbraucheraufklärung setzt sich das Bundesministerium der Justiz und für Verbraucherschutz für eine Digitale Aufklärung ein. Wir unterstützen Projekte, die der Steigerung der Medienkompetenz der Verbraucherinnen und Verbraucher dienen. Hier setzen wir auch auf die Zusammenarbeit mit DsiN.

Ich wünsche Ihnen eine angenehme und aufschlussreiche Lektüre!

Ulrich Kelber
Parlamentarischer Staatssekretär beim
Bundesminister der Justiz und für Verbraucherschutz



Hartmut Thomsen



Dr. Michael Littger

IT-Sicherheit ist eine Gemeinschaftsaufgabe

Der leichte Anstieg des Index im zweiten Jahr seiner Erhebung ist für uns eine erfreuliche Bestätigung, dass wir uns – bei aller berechtigten Sorge um digitale Sicherheit – keineswegs im „freien Fall“ befinden: Die relevanten Sicherheitsvorfälle bei Verbrauchern waren in den vergangenen Monaten rückläufig, das Wissensniveau der Nutzer hat sich etwas verbessert. Gleichwohl gibt es keinen Grund, die Hände in den Schoß zu legen. Auch, weil immer neue Lebensfelder wie die Gesundheits- und Vitaldienste sowie Hausvernetzung in den digitalen Alltag Einzug halten.

Zur Debatte um Schutz, Sicherheit und Vertrauen schafft der Index einen Orientierungspunkt, der den Status Quo und Entwicklungen der Sicherheitslage sichtbar und vergleichbar macht – über tagesaktuelle Ereignisse und Meldungen hinaus. Die Bestandsaufnahme des Index zur digitalen Sicherheit dient aber auch als Grundlage für die Arbeit von Deutschland sicher im Netz, um Handlungsbedürfnisse der Verbraucher besser zu verstehen und daraus gezielte Maßnahmen für eine wirksame Aufklärungsarbeit abzuleiten.

Die Aufteilung des Index nach Verbrauchergruppen macht ein erhebliches Sicherheitsgefälle in Deutschland sichtbar: Während die souveränen Nutzer gute Indexwerte erreichen, droht jeder vierte Verbraucher in der digitalen Sicherheit abgehängt zu werden. Dies gilt für die Gruppe der Fatalisten mit vielen jüngeren Menschen sowie auch für die Gruppe der Außenstehenden mit vorrangig älteren Menschen. Nur wenn wir es schaffen, alle Menschen im digitalen Wandel mitzunehmen, können sich die Chancen der Digitalisierung wirklich entfalten.

Die Ergebnisse zeigen, dass eine Unterstützung der Menschen im sicheren Umgang mit dem Internet nach individuellen Bedürfnissen erfolgen muss – statt einer Aufklärung mit der Gießkanne. Wir wollen auch eine stärkere Vernetzung guter Initiativen, um Transparenz und Zugang von Aufklärungsarbeiten für Verbraucher zu verbessern. Und eine wirksame Aufklärungsarbeit braucht den Dialog mit Politik, Wirtschaft und Wissenschaft, denn Schutz und Vertrauen ist eine Gemeinschaftsaufgabe aller Beteiligten im Digitalen Wandel.

Wir wünschen eine angenehme Lektüre!

Hartmut Thomsen
Vorsitzender (amt.)
Deutschland sicher im Netz e. V.

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

Inhalt

- Schutz und Vertrauen durch digitale Aufklärung**
Geleitwort von Ulrich Kelber, BMJV 3
- IT-Sicherheit ist eine Gemeinschaftsaufgabe**
Vorwort von Hartmut Thomsen und Michael Littger 4
- Inhaltsverzeichnis 5
- Zentrale Ergebnisse 6
- Studiendesign 8
- KAPITEL 1 | Sicherheitsindex 2015: 63,0 Punkte** 9
 - Positiver Trend auf mäßigem Niveau 10
 - Schutzniveau versus Bedrohungslage 11
 - DsiN-Sicherheitsfaktoren 12
 - Relevante Einflussfaktoren 14
- KAPITEL 2 | Digitales Sicherheitsgefälle** 15
 - Vier Verbrauchertypen – vier Sicherheitslagen 16
 - Außenstehende Nutzer (50,7 Punkte) 18
 - Fatalistische Nutzer (52,0 Punkte) 20
 - Gutgläubige Nutzer (60,5 Punkte) 22
 - Souveräne Nutzer (72,2 Punkte) 24
 - Verbraucherstimmen: „Die größten Risiken im Netz!“ 26
- KAPITEL 3 | Fokus: Digitale Lebenswelten** 27
 - Gesundheits- und Vitaldienste digital 28
 - Haus- und Heimvernetzung 29
 - Einkaufen im Internet 30
 - Online-Banking 31
- Exkurs – Index nach Bundesländern 32
- KAPITEL 4 | Digitale Aufklärung: Handlungsfelder!** 34
 - Risikoeinschätzungskompetenz stärken 35
 - Sicherheitswissen ausbauen und vertiefen 36
 - Umsetzungskompetenzen trainieren 38
 - Sicherheitspraxis: Motivieren 39
- Infografik: DsiN-Sicherheitsindex 2015** 41
- Glossar 42
- Über Deutschland sicher im Netz e.V. 43
- Impressum** 44

Der Sicherheitsindex steigt – das Gefälle bleibt

Die gute Nachricht ist der leichte Anstieg des DsiN-Sicherheitsindex 2015 auf 63,0 Punkte. Damit hat sich der Abstand zum kritischen Schwellenwert von 50 Punkten gegenüber dem Vorjahr um 2,8 Punkte verbessert. Unterhalb des Schwellenwerts würde die Bedrohungslage das Schutzniveau überflügeln und die Sicherheitslage zu kippen drohen. Gleichwohl gibt die aktuelle Sicherheitslage mit 13 Punkten oberhalb des Schwellenwerts keinen Grund zur Zufriedenheit; es müssen Anstrengungen unternommen werden, um das Niveau zu halten und nach Möglichkeit auszubauen.

Eine große Herausforderung sind die unterschiedlichen Sicherheitslagen der Verbrauchertypen. Die niedrigsten Werte erreichen nur 50,7 Punkte und liegen unmittelbar im Schwellenbereich, die höchsten Werte liegen bei 72,2 Punkten – mit steigender Tendenz. Daraus entsteht ein enormes digitales Sicherheitsgefälle bei Verbrauchern in Deutschland. Es zeigt auch, dass die Sicherheitslage maßgeblich vom Verhalten und den Kenntnissen der Anwender im digitalen Alltag abhängt.

Diskrepanz von Wissen und Handeln

Innerhalb der Verbrauchergruppen fällt die Diskrepanz zwischen Sicherheitswissen und -verhalten auf. Gerade in der Gruppe der Außenstehenden – mit 50,7 Punkten der niedrigste Indexwert – hat sich diese Schere weiter geöffnet. Demgegenüber bleibt bei den Fatalisten (52 Punkte) die mangelnde Bereitschaft und Gleichgültigkeit zur Umsetzung des vorhandenen Sicherheitswis-

sens bestehen. Ähnlich ist es auch in der Gruppe der Gutgläubigen (60,5 Punkte), die allerdings wegen einer ausgeprägten Unbedarftheit keine Vorkehrungen treffen.

Die Sicherheitslage dieser drei Verbrauchergruppen hat sich gegenüber dem Vorjahr verbessert. Diese Entwicklung ist allerdings vorrangig auf einen Rückgang der Sicherheitsvorfälle zurückzuführen. Das Schutzniveau blieb eher konstant oder ist rückläufig, sodass bei einer erneuten Zunahme von Vorfällen keine ausreichenden Vorkehrungen bestehen. Auffällig ist auch, dass trotz eines Rückgangs der Sicherheitsvorfälle die Verunsicherung in allen Gruppen spürbar gestiegen ist. Damit laufen im Jahre 2015 Gefährdungsgefühl und tatsächliche Gefährdungslage stärker auseinander.

Verstärkter Aufklärungsbedarf für 60 Prozent der Verbraucher

Knapp 60 Prozent der deutschen Nutzer – die Gruppe der Fatalisten, Gutgläubigen oder Außenstehenden – zeigen ein verstärktes Aufklärungsbedürfnis. Dies gilt in besonderem Maße für die Fatalisten, denen meist jüngere Menschen angehören und für die Außenstehenden (vor allem die älteren Generationen). Zusammengekommen ist dies jeder vierte Verbraucher. Dies gilt umso mehr, als die Digitalisierung in weitere Lebensbereiche greift, die ihrerseits neue Orientierungshilfe und Anleitungen erfordern. Der DsiN-Sicherheitsindex hat 2015 dazu erstmals auch Vital- und Gesundheitsdienste sowie Hausvernetzung in die Befragungen eingebunden.

DIGITALES SICHERHEITSGEFÄLLE 2015

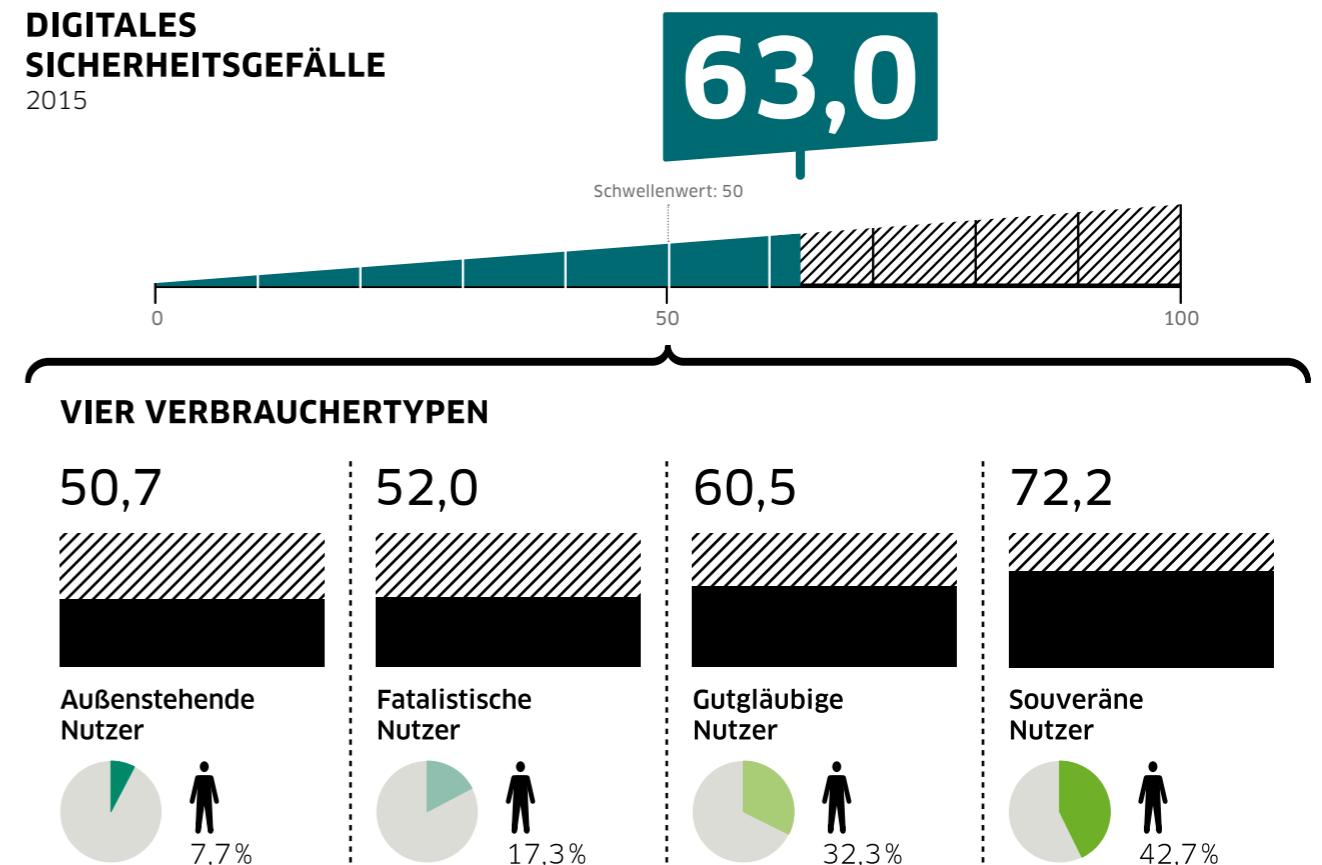


Abb. 1: Digitales Sicherheitsgefälle in Deutschland

Eine Digitale Aufklärung 2.0 kann dem digitalen Sicherheitsgefälle entgegenwirken, indem sie die konkreten Bedürfnisse und Defizite der Verbraucher(gruppen) behandelt, die die Studie offenlegt. So müssen Fatalisten viel stärker zum Handeln motiviert werden, Außenstehende hingegen mit Grundlagenwissen vertraut gemacht werden. Der Index hat dazu erstmals auch nach Motiven und Motivationen gefragt.

Die Relevanz einer Aufklärungsarbeit über einen individuellen Maßnahmenmix anstelle von Aufklärung mit der Gießkanne wird damit eindrucksvoll bestätigt. Konkret ergeben sich daraus vier Handlungsfelder, die im Kapitel 4 behandelt werden:

- **Risikoeinschätzungskompetenz stärken**
Für eine bessere Wahrnehmung und Bewertung relevanter Risiken
- **Sicherheitswissen ausbauen und vertiefen**
Zur Verständnissförderung effektiver Sicherheitslösungen

- **Umsetzungskompetenz trainieren**
Unterstützung zur Anwendung im Alltag erzeugen
- **Sicherheitspraxis: Motivation erzeugen**
Zur Überwindung von Barrieren und Bequemlichkeit beitragen

Sämtliche Handlungsfelder werden von DsiN mit konkreten Handlungsversprechen unterlegt, die im Bericht dargestellt sind. Darüber hinaus werden im Verbund mit unseren Mitgliedern permanent neue Ideen und Projekte entwickelt, die sich auch als Ergebnis aus dem Index ergeben. Die regelmäßige Erhebung des DsiN-Sicherheitsindex wird die Entwicklung der digitalen Sicherheitslage auch künftig begleiten.

Index zur Digitalen Sicherheitslage der Verbraucher

Der DsiN-Sicherheitsindex bildet die digitale Sicherheitslage der Verbraucher in einer Kennzahl ab. Die jährliche Erhebung macht Veränderungen und Entwicklungen im Vergleich zum Vorjahr sichtbar. Er basiert auf der Annahme, dass Sicherheit im Internet ein dynamisches Verhältnis von Bedrohungslage einerseits und Schutzniveau der Verbraucher andererseits ist:

Um die Sicherheitslage abzubilden, kombiniert der Index die Erfassung von Sicherheitsvorfällen und des Gefährdungsgefühls auf der einen Seite mit der Kenntnis und Anwendung von Schutzmaßnahmen auf der anderen Seite (Abb. 2). Jeweils höher gewichtet werden dabei das tatsächliche Verhalten und die konkrete Bedrohungslage.

Der Index differenziert die Sicherheitslage anhand verschiedener Nutzertypen. Dadurch wird eine direkte Vergleichbarkeit der Sicherheitslage zwischen Verbrauchergruppen ermöglicht, deren Unterschiede auf individuellen Verhaltensweisen, Kenntnissen oder Risikoeinschätzung beruhen – entsprechend der vier Sicherheitsfaktoren.



DsiN-Sicherheitsindex im Jahresvergleich

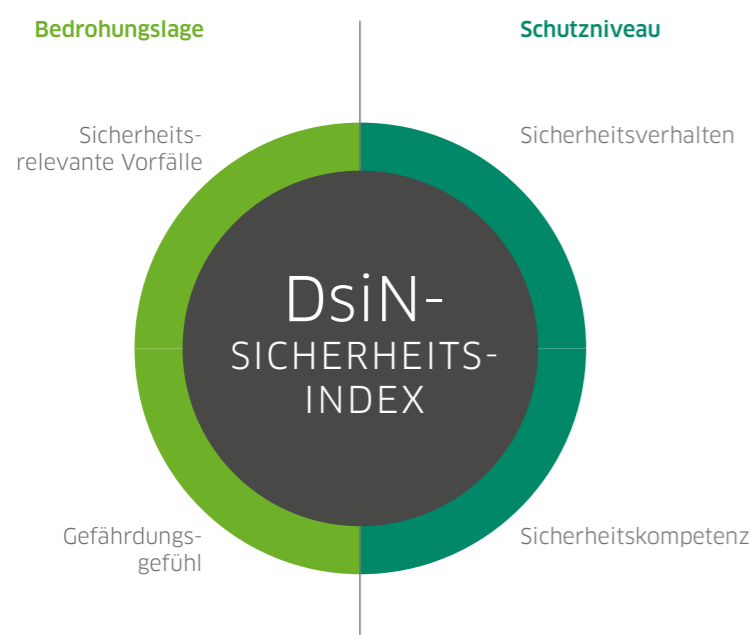
Dem DsiN-Index liegt eine repräsentative Umfrage von TNS Infratest bei 2.010 Internetnutzern in Deutschland zu Grunde. Zur Erfassung wurden über 40 Szenarien erhoben, die nach konkreten Vorfällen, Kenntnissen und Anwendungen von Schutzmaßnahmen fragen.



Basis für Digitale Aufklärung 2.0

Die praktische Verwertung der Ergebnisse für die Aufklärungsarbeit und Unterstützung von Verbrauchern ist ein zentrales Ziel. 2015 wurde dazu erstmals auch nach Einstellung und Motivation der Nutzer gefragt, die die Sicherheitsfaktoren beeinflussen können. Sie bieten Anknüpfungspunkte, die Aufklärungsarbeit 2.0 konkret an den Bedürfnissen und Erwartungen der Verbraucher auszurichten.

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



Kapitel 1

Sicherheitsindex 2015: 63 Punkte

Sicherheitsindex 2015: Anstieg auf 63,0 Punkte

Positiver Trend auf mäßigem Niveau

Die Sicherheitslage der deutschen Onliner hat sich im vergangenen Jahr auf 63,0 Punkte (2014: 60,2 Punkte) leicht verbessert. Damit liegt der Index 13 Punkte über dem Schwellenwert von 50 Punkten, unterhalb dessen die Bedrohungslage das Schutzniveau übertrifft und die Sicherheitslage zu kippen droht (s. Abb. 3). Drei von vier DsiN-Sicherheitsfaktoren haben sich zudem positiv entwickelt:

- weniger verzeichnete Angriffe (**Sicherheitsvorfälle**)
- leichter Ausbau der Kompetenzen der Verbraucher (**Sicherheitskompetenz**) und
- leicht verbesserte Bereitschaft zur Anwendung von Sicherheitsmaßnahmen (**Sicherheitsverhalten**).

Jedoch ist auch das **Gefährdungsgefühl** der Verbraucher erkennbar gestiegen. Es führt bei den meisten Verbrauchern zu einer neuen Unsicherheit und Hemmung im Umgang mit digitalen Diensten im Alltag.

Die Verbesserung des Index erfolgt auf einem mäßigen Ausgangsniveau. Die kaum gestiegenen Werte im Schutzniveau verdeutlichen die Anfälligkeit der Verbraucher für Risiken. Ein längerfristiger Trend zu mehr IT-Sicherheit ist nicht erkennbar.

Die insgesamt verbesserte Sicherheitslage 2015 beruht vorrangig auf dem Rückgang der Sicherheitsvorfälle; demgegenüber wirkt eine neue Verunsicherung der Verbraucher als negativer Faktor auf die Sicherheitslage.

Das aktuelle Schutzniveau wäre nicht ausreichend, um eine künftige Verschlechterung der Bedrohungslage auszugleichen. Die Diskrepanz zwischen Kenntnis und Anwendung von Sicherheitsmaßnahmen bleibt auch 2015 erheblich.

Schutzniveau versus Bedrohungslage

Grundlage der ermittelten Sicherheitslage bilden die Bedrohungslage und das Schutzniveau der Verbraucher: Im Vergleich zu 2014 ist das Schutzniveau der Bürger gegen Cyberrisiken nahezu konstant geblieben. Vorrangig hat die etwas verbesserte Bedrohungslage im Durchschnitt aller Verbrauchertypen den leichten Anstieg des DsiN-Sicherheitsindex um 2,8 Punkte bewirkt.

Bedrohungslage Bei den Nutzern selbst wurden weniger Angriffe verzeichnet. Dadurch nahm die Bedrohungslage 2015 um 6,1 Punkte auf 34,0 Punkte (2014: 40,1 Punkte) ab – die größte Verbesserung gegenüber dem Vorjahr. Die Entwicklung des Gefährdungsgefühls steigerte sich hingegen auf 28,3 Punkte (2014: 27,2 Punkte).

Schutzniveau Die Sicherheitskenntnisse der Verbraucher stiegen 2015 um 2,1 Punkte auf 82,7 (2014: 80,6 Punkte). Die tatsächliche Verwendung von Sicherheitsmaßnahmen blieb mit 50,7 Punkten hingegen nahezu konstant (2014: 49,6 Punkte). Die Diskrepanz von Sicherheitskenntnis einerseits und der Umsetzung von Maßnahmen andererseits erhöhte sich gegenüber dem Vorjahr damit sogar um einen Punkt auf 32 Punkte.

Erstmals wurden Verbraucher im Index 2015 auch nach den Einflüssen auf Sicherheitsfaktoren gefragt. Die Fragen umfassten Motive und Motivation, die zur Verbesserung der eigenen Sicherheitslage führen. Danach empfinden beispielsweise 75 Prozent der Verbraucher das eigene Verhalten als Chance zur Verbesserung der IT-Sicherheitslage. Mit deutlichem Abstand dahinter folgen regulative und technische Maßnahmen (s. dazu S. 14).

75%

der Verbraucher geben an, IT-Schutz sei durch Umsicht zu verbessern

Die Sicherheitslage verbessern: Anknüpfungspunkte

Eine Verbesserung der vier Sicherheitsfaktoren wirkt sich positiv auf die Sicherheitslage aus. Anknüpfungspunkte für Veränderungen werden anhand folgender Handlungsfelder in Kapitel 4 zusammengestellt:

- Risikoeinschätzungskompetenz verbessern
- Sicherheitswissen ausbauen und vertiefen
- Umsetzungskompetenz trainieren
- Sicherheitspraxis: zur Anwendung motivieren

Sicherheitsfaktoren

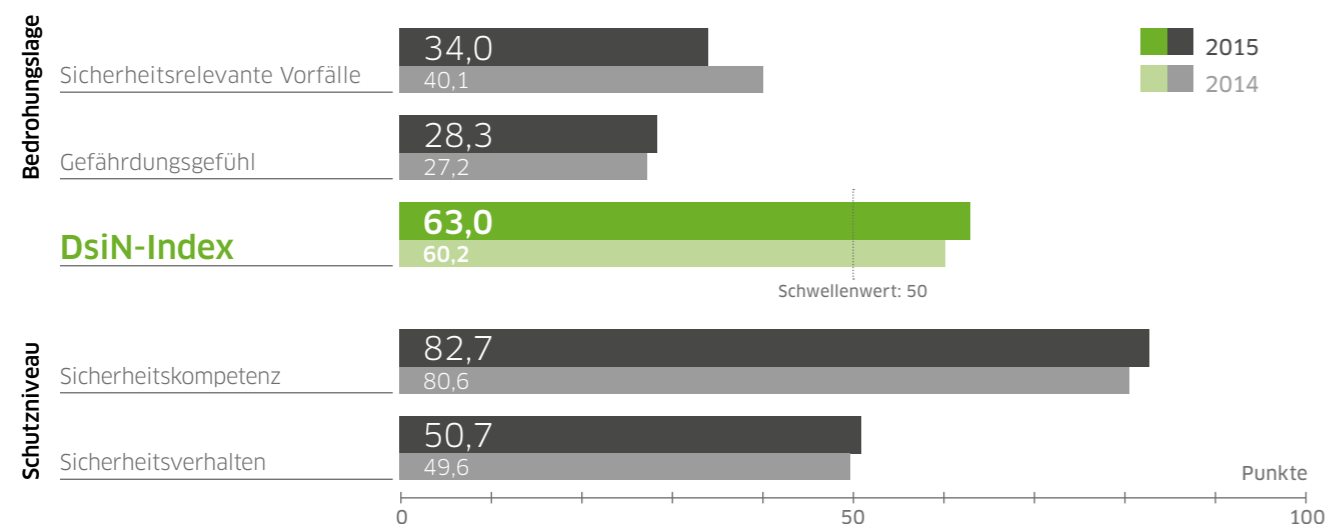


Abb. 3. DsiN-Sicherheitsindex 2015 (Punktwerte)

Erkennbarer Anstieg der Verunsicherung bei Verbrauchern

DsiN-Sicherheitsfaktoren

Der Berechnung der vier Sicherheitsfaktoren, auf denen der Index beruht, liegen jeweils über 40 Szenarien zu Grunde, die nach einer Rangliste bewertet werden.

1. Sicherheitsrelevante Vorfälle

An erster Stelle der selbst registrierten Vorfälle stehen Viren und Malware, gefolgt vom Versenden unerwünschter E-Mails im eigenen Namen. Aber auch konkrete Erfahrungen mit Betrug im Bereich Buchungen oder Shopping liegen vorn. *Ausführlich S. 35.*

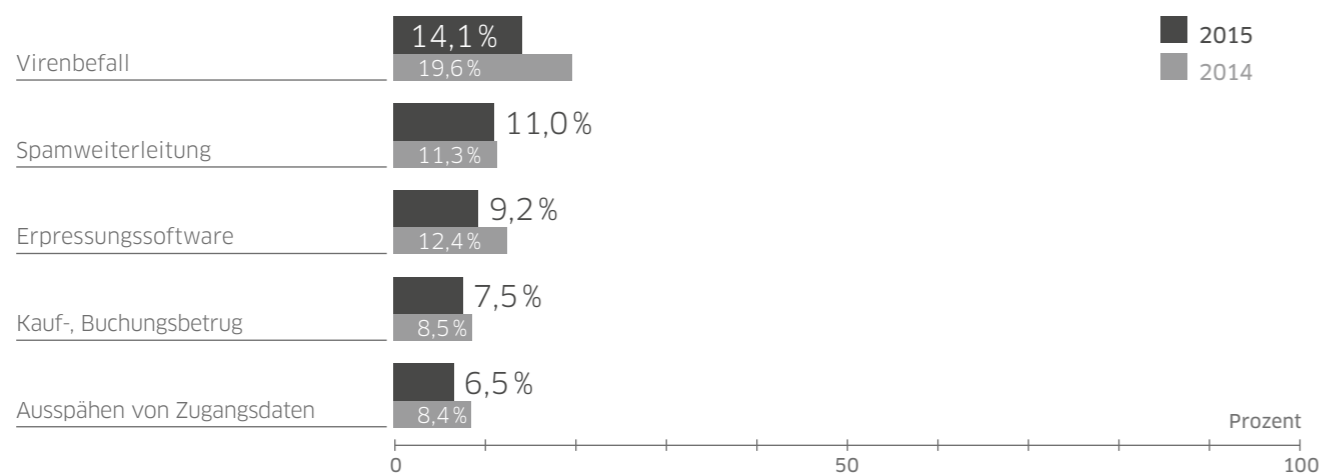


Abb. 4 Registrierte Sicherheitsvorfälle: TOP 5

2. Gefährdungsempfinden

Unsicherheit im Netz empfinden knapp 60 Prozent der Nutzer beim Öffnen von Anhängen in E-Mails. An zweiter Stelle steht das Teilen von vertraulichen Inhalten über das Internet, z.B. mit Behörden, Banken oder Versicherungen. An dritter Stelle folgt das Gefährdungsgefühl im Umgang mit Banking. *Ausführlich S. 35.*

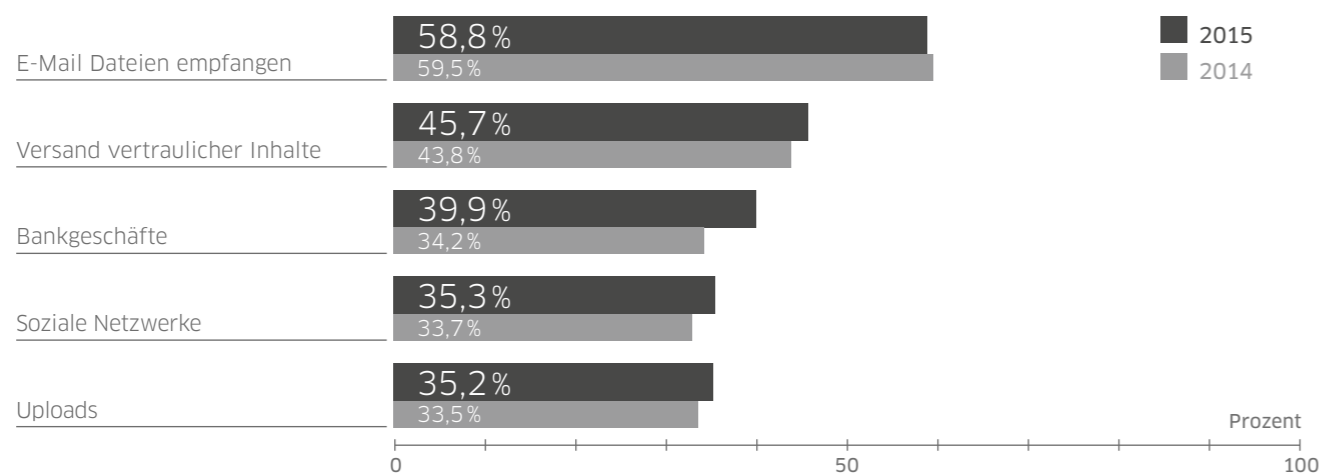


Abb. 5 Gefährdungsgefühl: TOP 5

3. Kenntnis von Schutzmaßnahmen

Bei den Kenntnissen über Schutzmaßnahmen liegen 2015 Antivirenprogramme mit einer Kenntnisverbreitung von 97,4 Prozent an erster Stelle. Unter den TOP 5 liegt weiterhin die Änderung von Passwörtern. Die Notwendigkeit, unterschiedliche Passwörter zu benutzen und diese regelmäßig zu ändern, ist vier Prozent unbekannt, fast drei Prozent weniger als 2014. Hingegen hat sich die Kenntnis über Datensicherung leicht verbessert auf jetzt 95,4 Prozent der Verbraucher. *Ausführlich S. 36*

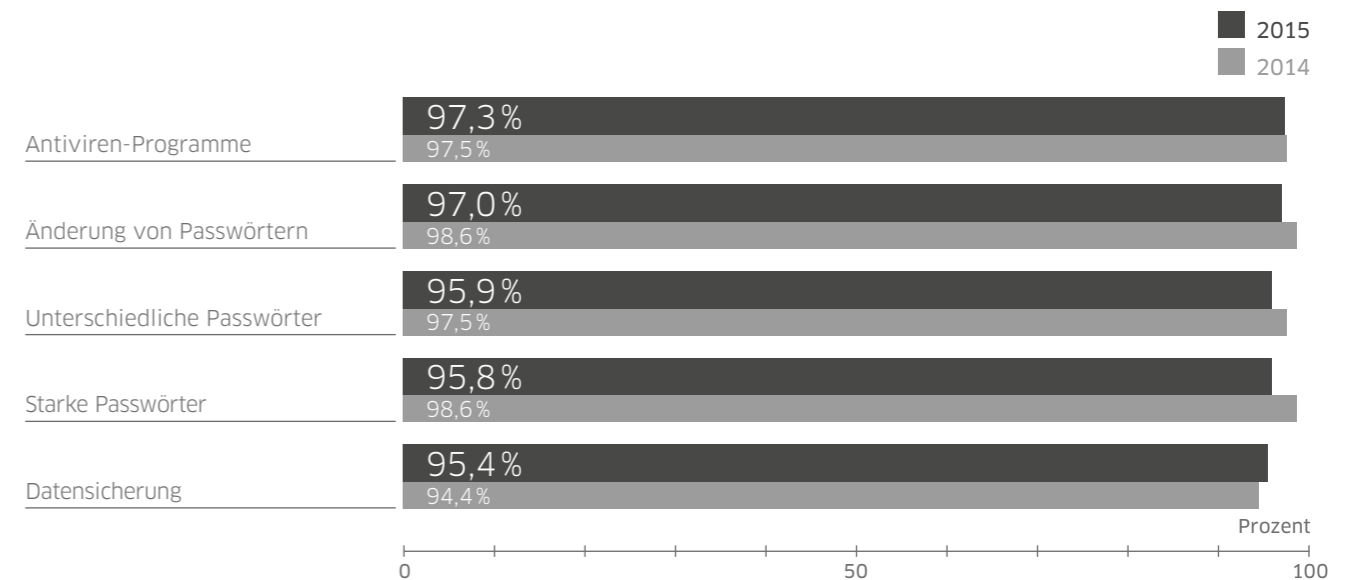


Abb. 6 Kenntnis von Schutzmaßnahmen: TOP 5

4. Anwendung von Schutzmaßnahmen

Die Aktivierung von Antivirenprogrammen ist 2015 Spitzenreiter der verwendeten Schutzmaßnahmen, wenn auch um 5 Prozentpunkte rückläufig. Neu an zweiter Stelle rangiert die Logout-Funktion mit 77,4 Prozent, gefolgt von der Nutzung unterschiedlicher Passwörter auf Platz drei. Damit verwendet immer noch jeder vierte Onliner nur ein Passwort für verschiedene Web-Anwendungen. *Ausführlich S. 38*

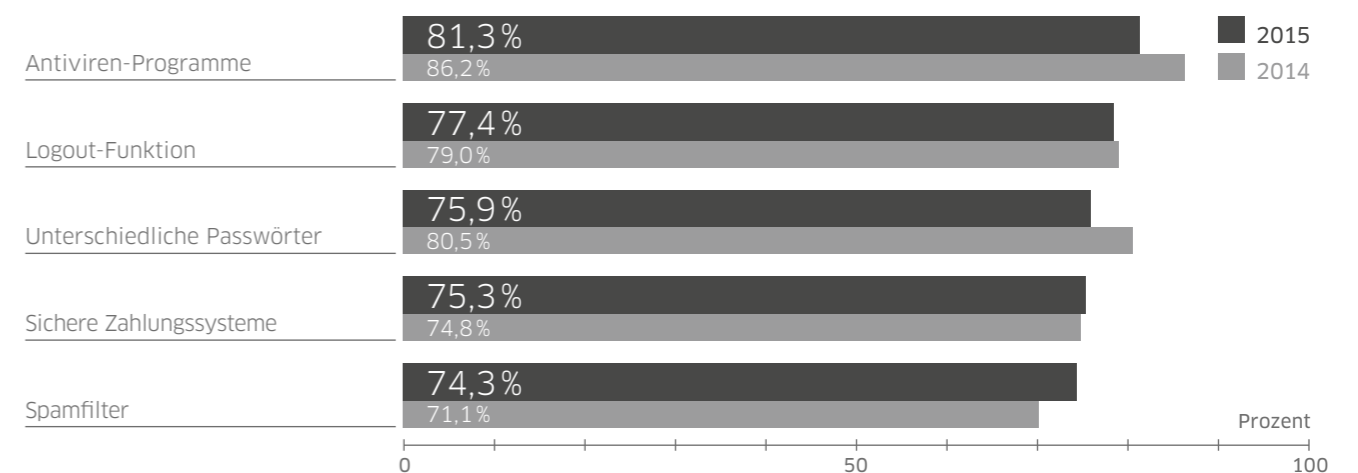


Abb. 7 Anwendung von Schutzmaßnahmen: TOP 5

Relevante Einflussfaktoren

Veränderungen der vier DsiN-Sicherheitsfaktoren wirken auf den Status der Sicherheitslage. 2015 wurde erstmals erhoben, welche Verhaltensmotive aus Sicht der Verbraucher eine Rolle spielen.

52,2%

lassen sich durch ihr privates Umfeld zu mehr Sicherheit motivieren

1. Einfluss auf Sicherheitsvorfälle

75 Prozent der Verbraucher erwarten einen Rückgang der eigenen Sicherheitsvorfälle durch einen „vorsichtigeren Umgang mit den eigenen persönlichen Daten“. Im Abstand von 23 Prozentpunkten folgen eine „sichere Gestaltung von IT-Diensten“ (52,7 Prozent) sowie der „Einsatz von Sicherheitsmaßnahmen“. Eine „bessere Aufklärung über Risiken“ sehen immer noch 42,9 Prozent als ursächlich, hinter einer „stärkeren Strafverfolgung“ von Cyberkriminellen.

2. Stärkung der Risikoeinschätzungskompetenz

Zur Verbesserung der eigenen Risikoeinschätzungskompetenz empfinden die Verbraucher Warnhinweise (49,1 Prozent) und Aufklärungsmaßnahmen über Risiken (48,0 Prozent) als wirksamste Methoden. Es folgen die „Aufklärung außerhalb des Internets“ sowie „bessere Informationen im Internet“ (42,9 Prozent).

3. Vertiefung von Sicherheitswissen

Um Sicherheitswissen zu verbessern, empfehlen die Verbraucher eine leichtere Verständlichkeit der Informationen im Netz (72,3 Prozent), gefolgt vom Wunsch nach zusätzlichen und zentral gebündelten Informationen (70 Prozent).

4. Motivation zur Anwendung

Eine praktische Umsetzung der Sicherheitslösungen halten die Verbraucher durch „einfachere Sicherheitseinstellungen“ (73,9 Prozent) und „mehr Anleitungen zum sicheren Verhalten“ (58,1 Prozent) für möglich. Die Mehrheit empfindet die Haltung zu IT-Sicherheit im privaten Umfeld als entscheidend (52,2 Prozent). Jeder Dritte nennt persönliche Anerkennung (32,4 Prozent) und die Rolle von Vorbildern (25,1 Prozent) als motivierend, gefolgt vom Sicherheitsvorfall (23,6 Prozent) bei jedem vierten Verbraucher.

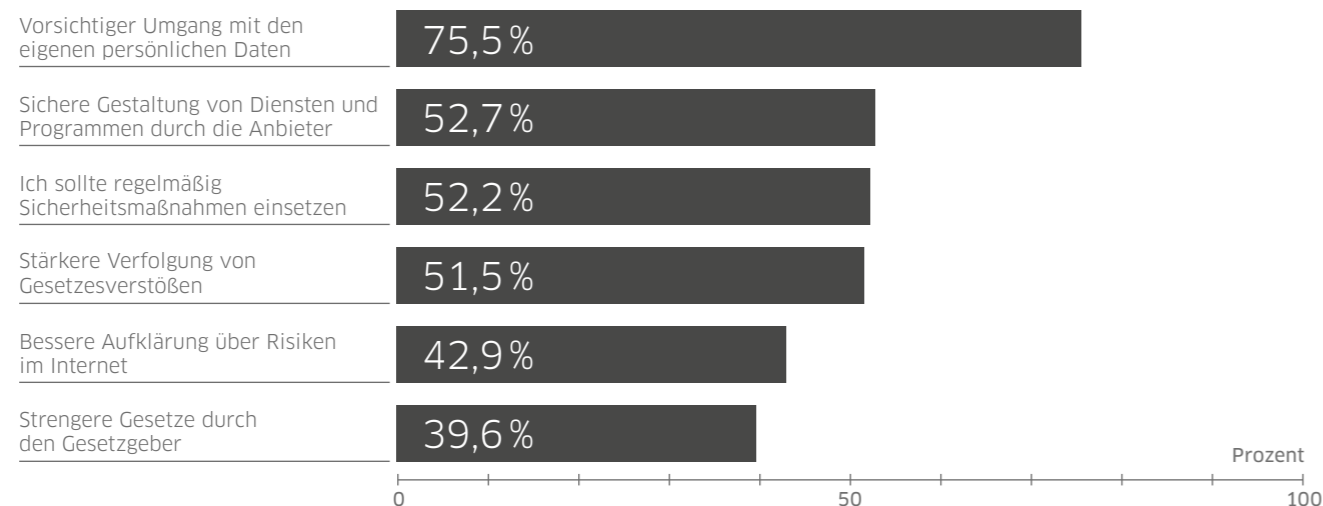


Abb. 8 Selbsteinschätzung der Verbraucher: Wie Sicherheitsvorfälle reduzieren?



Kapitel 2

Digitales Sicherheitsgefälle

Vier Verbrauchertypen – vier Sicherheitslagen

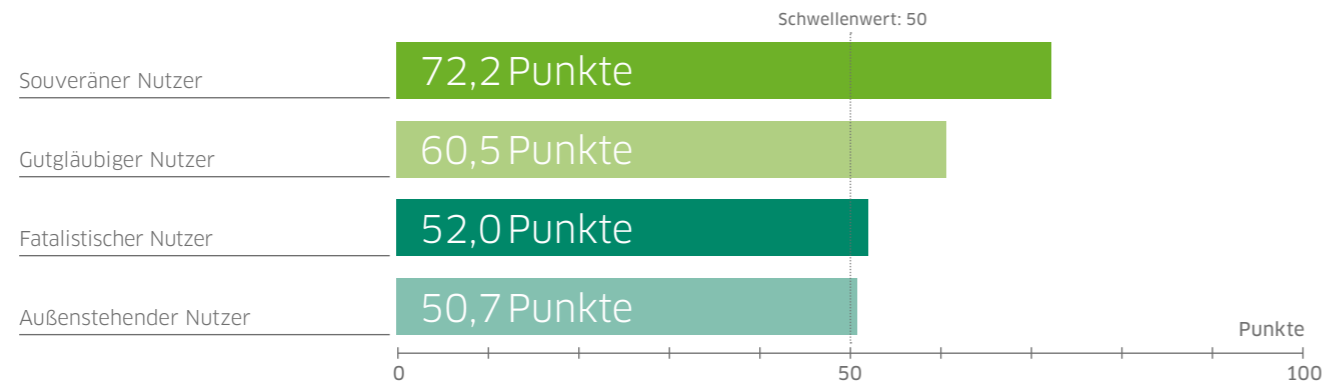


Abb. 9 Verbrauchertypen mit unterschiedlicher Sicherheitslage im Internet (DsiN-Index Punkte)

Die Verteilung der Indexwerte auf vier Nutzergruppen deckt ein digitales Sicherheitsgefälle in Deutschland auf: Unter denselben regulativen und technischen Rahmenbedingungen fällt die individuelle Sicherheitslage sehr unterschiedlich aus – vom guten Indexwert der souveränen Nutzer (72,2 Punkte) zu einem Indexwert von nur 50,7 Punkten bei den außenstehenden Nutzern. Insgesamt verfestigt sich damit das Ungleichgewicht zwischen verschiedenen Verbrauchergruppen gegenüber 2014. Ausschlaggebend für das Sicherheitsgefälle sind Unterschiede bei den DsiN-Sicherheitsfaktoren.

Außenstehende Nutzer haben mit **50,7 Punkten** das niedrigste Sicherheitsniveau der betrachteten Nutzertypen. Sie übernehmen die rote Laterne von den Fatalisten. Auffällig in dieser Gruppe sind die weiter wachsenden Wissensdefizite bei Schutzmaßnahmen von 34,6 Punkten (2014: 42 Punkte) bei leicht verbesserter Umsetzung.

Fatalistische Nutzer weisen die dynamischste Entwicklung auf, mit einem Plus von 7,7 Punkten auf **52,0 Punkte**. Auch sie

überschreiten 2015 die kritische Schwelle von 50 Punkten. Charakteristisch bleibt jedoch die enorme Schere zwischen Wissen und Bereitschaft zur Umsetzung: Die Kenntnisse von Sicherheitsmaßnahmen liegen bei 74,7 Punkten, ihre praktische Anwendung aber bei nur 45,7 Punkten.

Gutgläubige Nutzer verfügen über eine vergleichsweise hohe Sicherheitskompetenz, setzen diese aber wegen eines stark unterentwickelten Gefährdungsgefühls kaum ein. In diesem Jahr ist das Sicherheitswissen der Gutgläubigen nochmals um 3,2 Punkte auf nun **84,5 Punkte** gestiegen, im gleichen Zeitraum das Schutzverhalten allerdings um 3,1 Punkte auf 33,1 Punkte zurückgegangen.

Souveräne Nutzer zeichnet eine – im Vorjahresvergleich – konstant gute Sicherheitslage aus. Diese gründet sich auf einer hohen Sicherheitskompetenz (94,1 Punkte) und relativ guter Umsetzung (71,6 Punkte). Sie nutzen das Internet überdurchschnittlich, sind – gemessen daran – aber seltener von sicherheitsrelevanten Vorfällen betroffen (36,3 Punkte).

Besondere Unterstützung für 60 Prozent der Verbraucher

Positiv ist, dass 2015 alle Nutzergruppen den als kritisch einzuschätzenden Schwellenwert von 50 Punkten immerhin erreicht oder überschritten haben. Damit liegen erstmals auch die Fatalisten und Außenstehenden leicht oberhalb der kritischen Zone, bei der die Sicherheitslage zu kippen droht. Gleichwohl liegen weiterhin 60 Prozent der Onliner nur wenige Punkte über dem kritischen Schwellenwert von 50 Punkten. Dies gilt insbesondere für die bereits benannten Gruppen der Fatalisten und der Außenstehenden – zusammen jeder vierte Internetnutzer in Deutschland – mit Werten zwischen 50 und 52 Punkten. Sie bedürfen der besonderen Unterstützung.



Schere zwischen Wissen und Umsetzungsbereitschaft

Auch für die Souveränen – mit 42,7 Prozent die größte Verbrauchergruppe – hat Aufklärung eine besondere Relevanz. Sie

unterliegen einer größeren Risikoexposition und bedürfen daher zusätzlicher und aktualisierter Schutzkenntnisse. Als Vorbilder in der Gesellschaft können sie zudem motiviert und befähigt werden, andere im sicheren Umgang mit dem Internet zu begleiten und als Vorbild zu wirken.

Aufklärung auf individuelle Bedürfnisse ausrichten

Die typischen Fähigkeiten und Defizite der Verbrauchergruppen begründen individuelle Bedürfnisse der Aufklärungsarbeit. Während Außenstehende vorrangig mit Standards der Sicherheit vertraut gemacht werden müssen, steht bei Fatalisten – bei recht gutem Wissensstand – die Motivation zur Umsetzung im Vordergrund.

Bei Gutgläubigen ist die unzureichende Risikoeinschätzungskompetenz Kernthema, um tatsächliche Risiken zu erkennen und darauf zu reagieren. Souveräne haben die Chance, als Vorbilder und Trainer für IT-Sicherheit in ihrer Umgebung zu wirken und sollten entsprechend geschult werden.

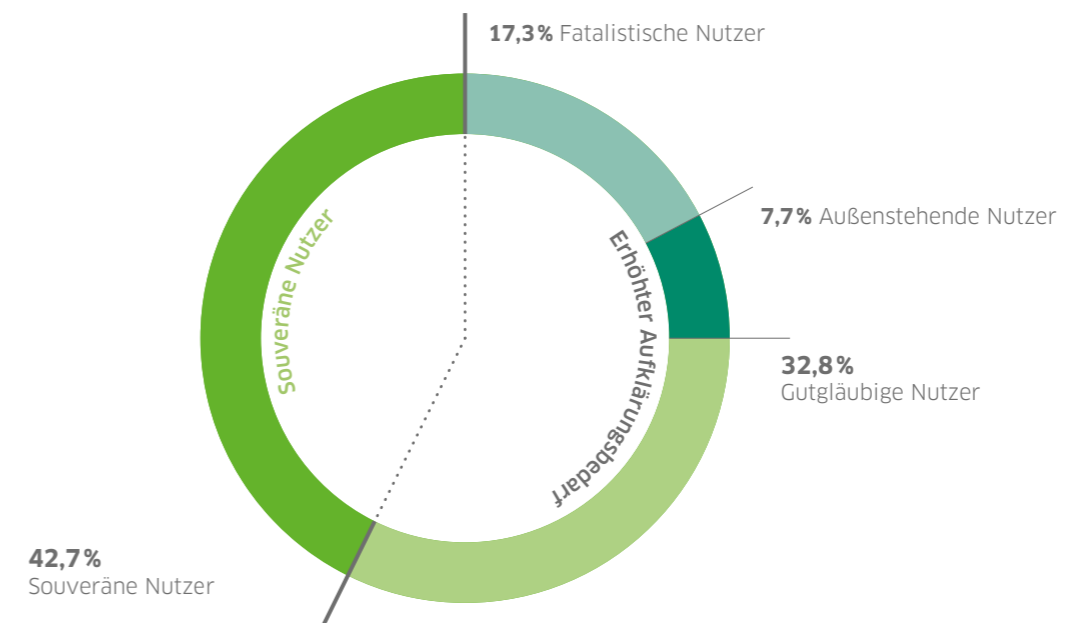
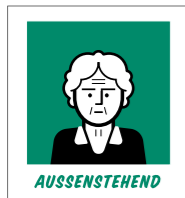


Abb. 10 Anteil der Nutzergruppen an der Gesamtheit der Onliner

Außenstehende Nutzer (50,7 Punkte)



Der außenstehende Nutzer

Rote Laterne

Der Indexwert für Außenstehende liegt mit 50,7 Punkten auf dem letzten Rang aller Verbrauchergruppen.

Die außenstehenden Nutzer, etwa acht Prozent aller Onliner, sind meist ältere Menschen zwischen 60 und 69 Jahren, fast 80 Prozent sind weiblich. Sie surfen über stationäre PCs und Laptops, selten über Smartphones oder Tablets. Die private Internetnutzung liegt meist bei 10 Stunden pro Woche.

Bedrohungslage

Auffällig ist der Rückgang registrierter Vorfälle um ein Drittel auf 24,1 Punkte (2014: 36,6 Punkte). Zwar zeigt diese Gruppe eine nur geringe Risikoexposition auf, da sie das Internet nur unterdurchschnittlich nutzt; der Rückgang ist gleichwohl überraschend deutlich. Das Gefährdungsgefühl ist hingegen nahezu konstant geblieben. Kon-

kret empfinden außenstehende Nutzer das Öffnen von Anhängen in E-Mails mit 53,3 Prozent und den Austausch vertraulicher Inhalte (46,5 Prozent) als gefährdend – nahezu gleichauf mit dem Bundesdurchschnitt (58,8 bzw. 45,7 Prozent).

Schutzniveau

Die Kenntnisse der Außenstehenden haben sich 2015 weiter verschlechtert auf 34,6 Punkte (2014: 42 Punkte), das Sicherheitsverhalten stieg – auf niedrigem Niveau – auf 22 Punkte. Damit verfestigt das Ergebnis die typischen Schwachstellen dieser Gruppe: niedrige Sicherheitskenntnisse gepaart mit unzureichendem Sicherheitsverhalten. Konkret verwenden in dieser Gruppe 37,2 Prozent kein Antiviren-Programm, über die Hälfte (52 Prozent) auch keine sicheren Zahlungssysteme beim Online-Einkauf. Damit droht diese Gruppe den Anschluss zu verlieren.

Sicherheitsfaktoren

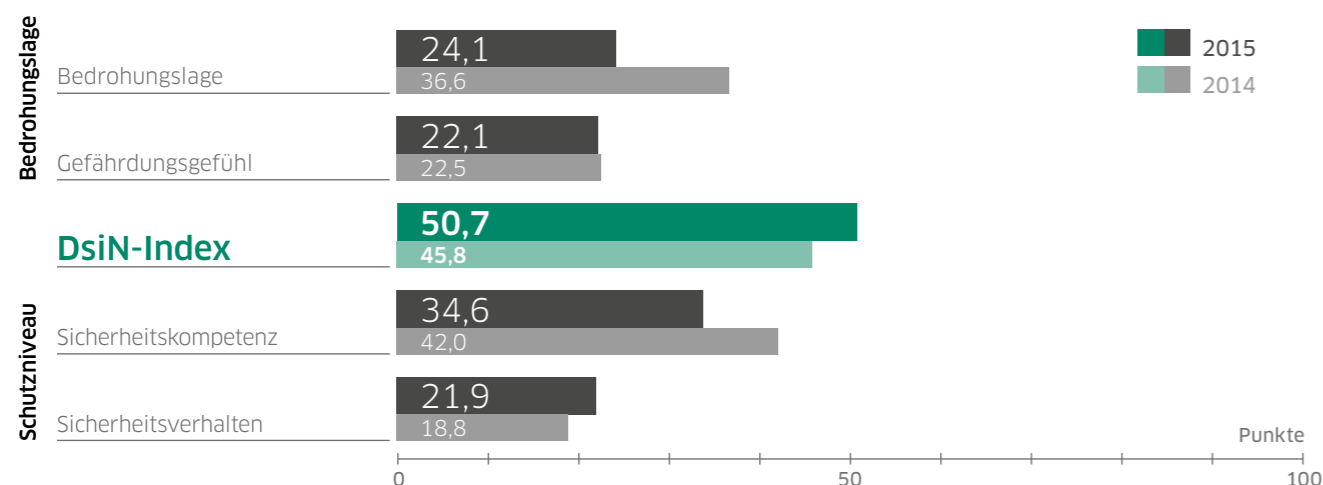


Abb. 11 DsiN-Sicherheitsindex-Punkte für außenstehende Nutzer

Der außenstehende Nutzer

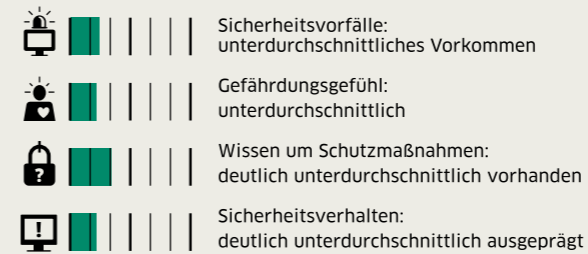
50,7 Punkte

Anteil an der Gesamtheit:

2015: 7,7% (-2,0%)
2014: 9,7%



Beschreibung:



AUßENSTEHEND

Typische Merkmale

- * hoher Anteil älterer Menschen insbesondere 60 - 69-jährige
- * hoher Anteil von Frauen
- * geringer Anteil von Gutverdienern (Einkommen über 3.000 Euro und mehr monatlich)
- * Internet wird meist 10 Stunden in der Woche genutzt



Sicherheitsrelevante Vorfälle TOP 3

1. Erhalt unerwünschter E-Mails („Spam“) **63,3%**
2. Erhalt infizierter E-Mails / Anhänge / Weblinks **29,1%**
3. Infizierung durch Schadsoftware (z.B. Viren oder Malware) **10,7%**



Gefährdungsgefühl TOP 3

1. Öffnen von Anhängen in E-Mails **53,3%**
2. Austausch vertraulicher Inhalte (z.B. mit Behörden) **46,5%**
3. Bankgeschäfte **38,8%**



Unbekannte Schutzmaßnahmen TOP 3

1. Inkognito-Funktion **94,0%**
2. Überprüfung von Cloud-Diensten **91,5%**
3. Phishing-Filter **87,9%**



Nutzung von Schutzmaßnahmen TOP 3

1. Antiviren-Programm **62,8%**
2. Installation von Updates **62,1%**
3. Unterschiedliche Passwörter **57,9%**

Abb. 12 Steckbrief Außenstehender Nutzer: 50,7 Punkte

Basiswissen einfach und niederschwellig vermitteln

Das typische Defizit der Außenstehenden sind unzureichende Sicherheitskenntnisse kombiniert mit einem geringen Umsetzungsgrad. Das Interesse an Sicherheitsfragen ist in dieser Gruppe nicht weit verbreitet. Knapp 22 Prozent – der niedrigste Wert aller Nutzergruppen – möchten sich aktiv mit Sicherheitsfragen befassen. Damit sind niederschwellige Aufklärungsmaßnahmen kombiniert mit Anleitungen zur Umsetzung das „Gebot der Stunde“. Warnhinweise im Internet werden von der Nutzergruppe als besonders wirksam zur Sensibilisierung wahrgenommen. Auch hier können vertrauenswürdige Personen als Multiplikatoren in der Zielgruppe Wirkung entfalten – einschließlich der Unterstützung durch konkrete Trainings.



DsiN Angebote für außenstehende Nutzer:

- **Goldener Internetpreis**
Wettbewerb für aktive Senioren und Trainer
- **Life in a Connected World**
Praxisnahe Plattform Datenkompetenz
- **Digitale Stammtische für Senioren**
Aufklärungsinitiative für ältere Generationen
- **IT-Sicherheitsbrief für ältere Generationen**
Regelmäßige, einfache Basisinformationen

Fatalistische Nutzer (52,0 Punkte)



Der fatalistische Nutzer

Nachlässig

Mit 52,0 Punkten hat sich die Sicherheitslage dieser Verbrauchergruppe verbessert – und hat doch noch erhebliches Potenzial nach oben.

Der fatalistische Nutzer ist typischerweise unter 30 Jahren, hier insbesondere zwischen 16 und 19 Jahren. Er verfügt über ein Einkommen von oftmals unter 1.000 Euro im Monat und ist privat bis zu 20 Stunden in der Woche aktiv im Netz. Die betroffenen Nutzer machen gut 17 Prozent aller Onliner in Deutschland aus.

Bedrohungslage

Bei den fatalistischen Nutzern haben die sicherheitsrelevanten Vorfälle 2015 deutlich abgenommen. Dennoch liegen die Vorfälle mit 42,6 Punkten immer noch weit über dem Durchschnitt. Mit 68,3 Punkten erreichen sie den mit Abstand höchsten Wert bei

dem subjektiven Gefährdungsgefühl. Den Erhalt von E-Mail-Dateien stufen 86,9 Prozent als gefährlich ein (in anderen Gruppen nur 58,8 Prozent). Fast ebenso hoch schätzen sie mit 83,3 Prozent die Gefährdung durch die Nutzung sozialer Netzwerke ein (in anderen Gruppen nur 35,3 Prozent).

Schutzniveau

Das Schutzniveau der fatalistischen Nutzer ist erkennbar gestiegen. Grund ist eine Verbesserung der Sicherheitskenntnisse um 7,7 Punkte. Nachholbedarf besteht aber weiterhin im tatsächlichen Verhalten. Mit 45,7 Punkten liegen Fatalisten hier deutlich unter dem Gesamtdurchschnitt von 50,7 Punkten – trotz guter Kenntnisse und hohem Gefährdungsgefühl. Konkret verzichtet diese Gruppe auf Basisschutzmaßnahmen wie Passwortänderungen (47,1 Prozent) und die Überprüfung der Vertrauenswürdigkeit von Websites (48,4 Prozent).

Sicherheitsfaktoren

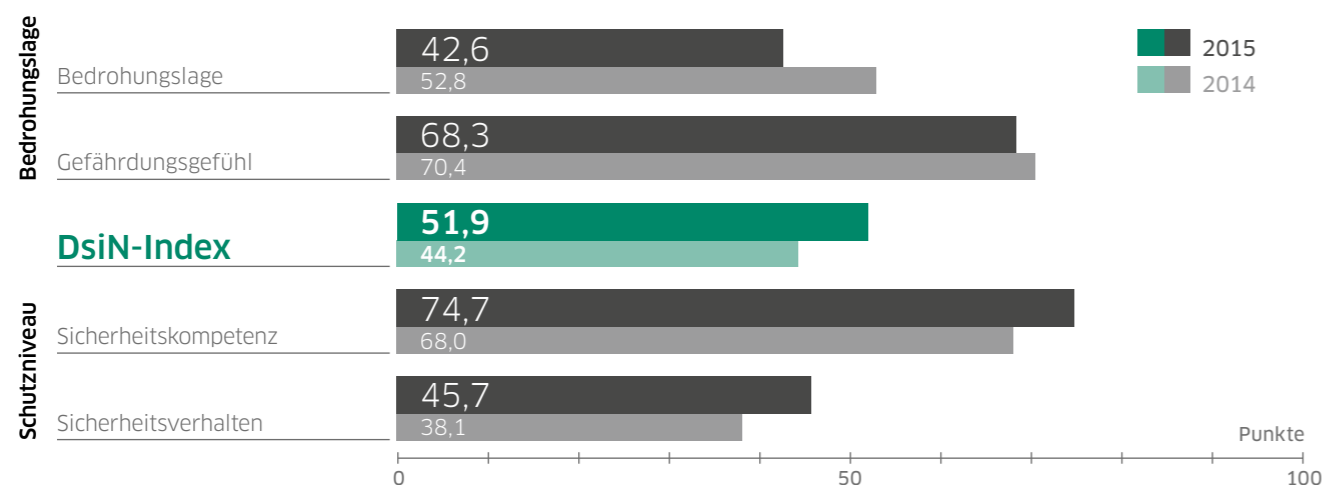


Abb. 13 DsiN-Sicherheitsindex-Punkte für fatalistische Nutzer

Der fatalistische Nutzer

52,0 Punkte

Anteil an der Gesamtheit:

- 2015: 17,3% (+1,5%)
- 2014: 15,8%



Beschreibung:

- Sicherheitsvorfälle: überdurchschnittliches Vorkommen
- Gefährdungsgefühl: deutlich überdurchschnittlich
- Wissen um Schutzmaßnahmen: leicht unterdurchschnittlich vorhanden
- Sicherheitsverhalten: unterdurchschnittlich ausgeprägt

FATALISTISCH

Typische Merkmale

- hoher Anteil jüngerer Menschen, insbesondere 16- bis 19-jährige
- Einkommen häufig unter 1.000 Euro monatlich
- hohe Internetnutzung, meist bis zu 20 Stunden pro Woche



Sicherheitsrelevante Vorfälle TOP 3

- Erhalt unerwünschter E-Mails („Spam“): 67,6%
- Erhalt infizierter E-Mails / Anhänge / Weblinks: 43,2%
- Infizierung durch Schadsoftware (z.B. Viren oder Malware): 18,1%



Gefährdungsgefühl TOP 3

- Erhalt infizierter Emails/Anhänge/Weblinks: 86,9%
- Austausch vertraulicher Inhalte (z.B. mit Behörden): 85,2%
- Soziale Netzwerke: 83,3%



Unbekannte Schutzmaßnahmen TOP 3

- 2-Faktor-Authentifizierung: 54,2%
- Passwort-Tresor: 39,9%
- Elektronische Signaturen: 35,5%



Nutzung von Schutzmaßnahmen TOP 3

- Logout-Funktion: 79,6%
- Antiviren-Programm: 79,0%
- Unterschiedliche Passwörter: 76,3%

Abb. 14 Steckbrief Fatalistischer Nutzer: 42,0 Punkte

Motivation zur Umsetzung von Schutzmaßnahmen

Einem überdurchschnittlichen Gefährdungsgefühl steht in dieser Gruppe eine fatalistische Grundhaltung bei der Anwendung von Maßnahmen gegenüber. Zusätzliches Sicherheitswissen könnte die Sicherheitslage kaum verbessern, solange die Umsetzung ausbleibt.

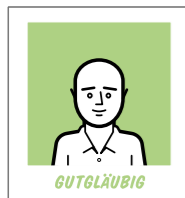
Digitale Aufklärung müsste daher die konkrete Nützlichkeit von Schutzmaßnahmen illustrieren und zur Anwendung des bereits vorhandenen Wissens motivieren: Die Folgen des eigenen Handelns müssen verdeutlicht werden. Konkret lehnen 83,9 Prozent dieser Gruppe ab, digitale Dienste unter Umständen seltener zu nutzen, wenn es der eigenen Sicherheit dient. Vorhandene Informationen über Sicherheit im Internet empfindet diese Gruppe als wenig hilfreich.



DsiN Angebote für fatalistische Nutzer:

- Jugendwettbewerb myDigitalWorld: Ideen und Projekte für mehr IT-Sicherheit
- DsiN-Aufklärungsfilme: Informationen zum sicheren Verhalten im Netz
- Medien in der Schule: Unterrichtsmaterial für Schüler
- Verschlüsselung: Einfach gemacht: Videoclips und Tutorials für Verschlüsselung

Gutgläubige Nutzer (60,5 Punkte)



Der gutgläubige Nutzer

Leicht verbessert

Die gutgläubigen Nutzer weisen mit **60,5 Punkten** einen leicht überdurchschnittlichen Indexwert auf, konnten sich im Vorjahresvergleich um **2,4 Punkte verbessern**.

Gutgläubige Nutzer – meist zwischen 30 und 59 Jahren – verwenden Laptops und klassische Desktop-PCs. Smartphones nutzen nicht einmal die Hälfte von ihnen (43 Prozent), Tablets ein gutes Viertel (27 Prozent). Sie surfen privat bis zu 30 Wochenstunden und machen 32 Prozent aller Onliner aus. Nur 69 Prozent meinen, sie sollten vorsichtiger mit ihren Daten umgehen. Sie liegen damit klar unter dem Gesamtdurchschnitt aller Verbrauchergruppen von 76 Prozent.

Bedrohungslage

Charakteristisch in dieser Gruppe bleibt auch gegenüber 2014 das ausgesprochen schwach ausgeprägte Gefährdungsgefühl,

das mit 14,7 Punkten einen hohen Grad der Unbedarftheit aufweist. Die sicherheitsrelevanten Vorfälle in dieser Nutzergruppe stark – um 8,1 Punkte – auf 28,5 Punkte zurückgegangen. Konkret zählen auch in dieser Gruppe unerwünschte E-Mails zu den häufigsten sicherheitsrelevanten Vorfällen (57 Prozent).

Schutzniveau

Auffällig in dieser Nutzergruppe sind die guten Kenntnisse zu Schutzmaßnahmen mit 84,5 Punkten (2014: 81,3 Punkte) bei vergleichsweise niedriger Umsetzung von 33,1 Punkten. Damit ist die Wissens-Verhaltens-Lücke im Vergleich zum Vorjahr nochmals gewachsen und in dieser Nutzergruppe weiterhin mit Abstand am größten. Konkret wissen 98,2 Prozent, wie starke Passwörter generiert werden, aber nur 58,4 Prozent wenden dieses Wissen auch an. 93,1 Prozent kennen das SMS-TAN-Verfahren beim Online-Banking, aber nur 38,6 Prozent nutzen es.

Sicherheitsfaktoren

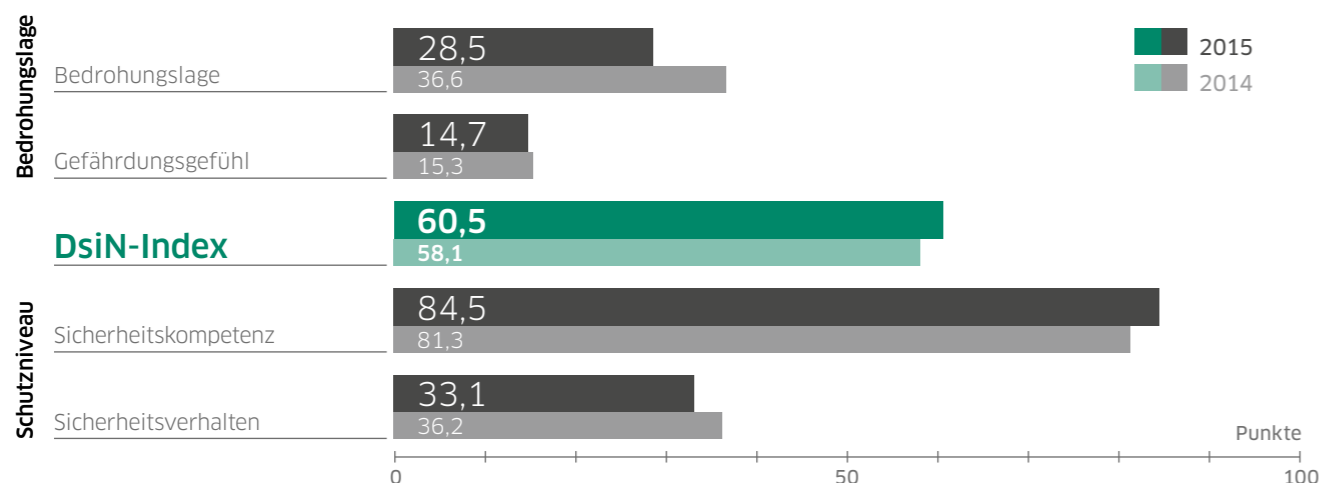


Abb. 15 DsiN-Sicherheitsindex-Punkte für gutgläubige Nutzer

Der gutgläubige Nutzer

60,5 Punkte

Anteil an der Gesamtheit:

- 2015: 32,3% (-2,7%)
- 2014: 35,0%



Beschreibung:

- Sicherheitsvorfälle: unterdurchschnittliches Vorkommen
- Gefährdungsgefühl: deutlich unterdurchschnittlich
- Wissen um Schutzmaßnahmen: leicht überdurchschnittlich vorhanden
- Sicherheitsverhalten: deutlich unterdurchschnittlich ausgeprägt

GUTGLÄUBIG

Typische Merkmale

- meist zwischen 30 und 59 Jahren
- sowohl höhere als auch niedrigere Einkommen
- Internet wird bis zu 30 Stunden in der Woche genutzt



Sicherheitsrelevante Vorfälle TOP 3

- Erhalt unerwünschter E-Mails („Spam“) **57,0%**
- Erhalt infizierter E-Mails / Anhänge / Weblinks **28,9%**
- Infizierung durch Schadsoftware (z.B. Viren oder Malware) **10,8%**



Gefährdungsgefühl TOP 3

- Öffnen von Anhängen in E-Mails **39,5%**
- Austausch vertraulicher Inhalte (z.B. mit Behörden) **29,7%**
- Bankgeschäfte **10,8%**



Unbekannte Schutzmaßnahmen TOP 3

- Passwort-Tresor **26,7%**
- 2-Faktor-Authentifizierung **26,1%**
- Inkognito-Funktion **19%**



Nutzung von Schutzmaßnahmen TOP 3

- Antiviren-Programm **71,1%**
- Sichere Zahlungssysteme **63,4%**
- Logout-Funktion **62%**

Abb. 16 Steckbrief Gutgläubiger Nutzer: 60,5 Punkte

Aufklären und die Risikoeinschätzungs-kompetenz ausbauen

Die geringe Anwendungsbereitschaft von vorhandenem Sicherheitswissen ist die Charakteristik dieser Nutzergruppe. Die Aufklärungsarbeit muss daher in der Vermittlung von Risikoeinschätzungs-kompetenz ansetzen als Voraussetzung, um die Handlungserfordernisse im Netz besser zu verstehen. Dabei muss anschaulich dargestellt werden, wo Gefahren bestehen.

Die gutgläubigen Verbraucher selbst halten Warnhinweise im Internet für ein geeignetes Instrument, um Sicherheitsrisiken besser einschätzen zu können.



DsiN Angebote für gutgläubige Nutzer:

- DsiN-Sicherheitsbarometer**
Regelmäßige Updates zur Sicherheitslage
- IT-Fitnesstest**
Selbsttest zur IT-Sicherheitskompetenz
- Verschlüsselung: Einfach gemacht**
Videoclips und Tutorials für Verschlüsselung
- IT-Fitness-Akademie**
Themenübergreifende Unterstützung

Souveräne Nutzer (72,2 Punkte)



Der souveräne Nutzer

Gleichbleibend gut

Der Indexwert der souveränen Nutzer hat sich im Vorjahresvergleich von einem hohen Niveau um 0,2 Punkte auf 72,2 Indexpunkte leicht verbessert.

Der souveräne Nutzer ist meist zwischen 40 und 49 Jahren alt, selten über 60 und verfügt über eine höhere Bildung und mit 4.000 Euro über ein hohes Haushaltseinkommen. Zwei Drittel in dieser Gruppe surfen mehr als 10 Wochenstunden privat, 43 Prozent über 20 Stunden. Die Mehrheit nutzt Smartphones, gefolgt von Laptops und Desktop-PCs. 82 Prozent der souveränen Nutzer meinen, mit den eigenen Daten vorsichtiger sein zu müssen und sind damit auch hier Spitzenreiter.

Bedrohungslage

Die sicherheitsrelevanten Vorfälle sind bei den souveränen Nutzern leicht auf 36,3 Punkte zurückgegangen. Trotz einer intensi-

ven Internetnutzung in dieser Gruppe liegen hier weniger Angriffe als beim fatalistischen Nutzer vor. Auch empfinden sie das Internet als kaum gefährlich; dieser Wert ist gegenüber 2014 weitgehend konstant. Dies untermauert die Annahme eines „gefestigten Umgangs“ mit dem Internet.

Schutzniveau

Die Sicherheitskompetenz der souveränen Nutzer ist mit 94,1 Punkten ausgesprochen hoch - und konstant gegenüber 2014. Sie wenden Schutzmaßnahmen zudem relativ häufig an bei einem Wert von 71,6 Punkten. Auch dieser Wert verzeichnet lediglich einen Rückgang um 1,8 Punkte und ist damit auf hohem Niveau recht konstant. Konkret verschlüsseln 46,6 Prozent der Souveränen ihre E-Mails, während der Bundesdurchschnitt bei 28,6 Prozent liegt.

Sicherheitsfaktoren

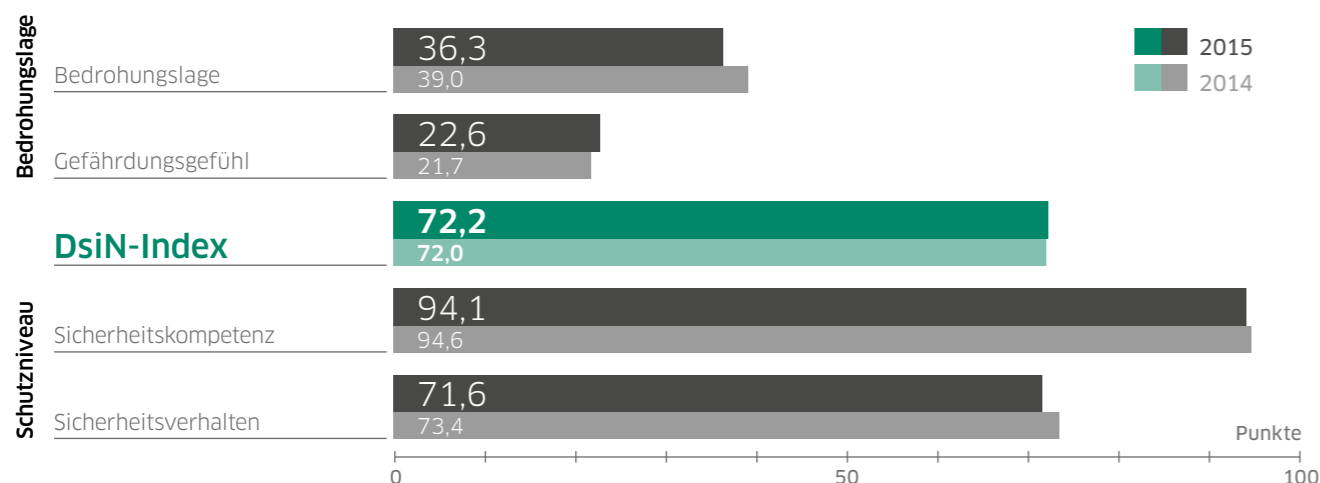


Abb. 17 DsiN-Sicherheitsindex-Punkte für souveränen Nutzer

Der souveräne Nutzer

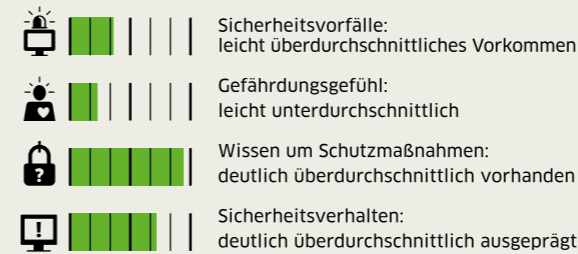
72,2 Punkte

Anteil an der Gesamtheit:

2015: 42,7% (+2,9%)
2014: 39,8%



Beschreibung:



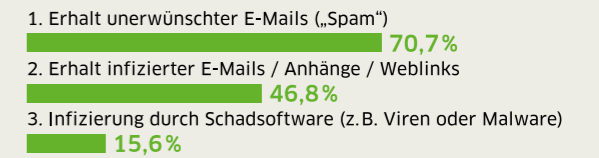
SOVERÄN

Typische Merkmale

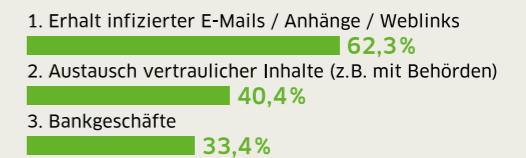
- * meist zwischen 40 und 49 Jahre
- * Einkommen häufig über 4.000 Euro monatlich
- * Internet wird intensiv genutzt



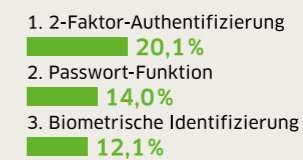
Sicherheitsrelevante Vorfälle TOP 3



Gefährdungsgefühl TOP 3



Unbekannte Schutzmaßnahmen TOP 3



Nutzung von Schutzmaßnahmen TOP 3

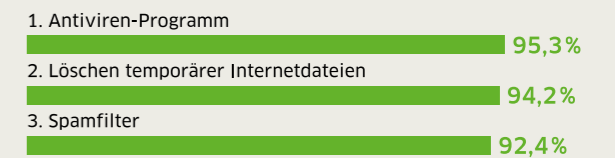


Abb. 18 Steckbrief Souveräner Nutzer: 72,2 Punkte

Niveau halten – als Vorbild wirken

Aufgrund seines guten Grundwissens sollte der souveräne Nutzer stets über aktuellste Angebote und deren Sicherheitsmaßnahmen informiert werden. Zugleich kann diese Gruppe geschult werden, andere Verbraucher im sicheren Umgang mit dem Netz aufzuklären und als Vorbild zu wirken. Damit leistet diese Nutzergruppe einen zusätzlichen Beitrag für Sicherheit im Netz und hält das eigene, gute Sicherheitsniveau.

Die souveränen Nutzer sehen die Verantwortung für die Sicherheit ihrer persönlichen Daten im Netz vor allem bei sich selbst. 58 Prozent sagen, dass sie öfter Sicherheitsmaßnahmen einsetzen sollten, um die Anzahl der Vorfälle zu reduzieren.



DsiN Angebote für souveräne Nutzer:

- **DsiN-Passwort-Wechsel-App**
Tool zur Erinnerung und Erleichterung häufiger Passwortwechsel
- **Internetbeschwerdestelle**
Hinweise auf illegale Inhalte im Netz
- **Digitale Nachbarschaft**
Ehrenamtlich Engagierte leiten Internetnutzer an
- **Security-News-App**
Portal mit Nachrichten zur aktuellen Sicherheitslage

Datendiebstahl **Datenmissbrauch**
Soziale Netzwerke Unaufmerksamkeit
Ausspionieren Shoppen mit Kreditkarte
aus Versehen auf unseriöse Seiten gelangen **Trojaner**
illegale Datenverknüpfung
Knacken **Geheimdienste**
von Zugangscodes gehackte Werbebanner mit Schadcode
Sorglosigkeit in Bezug auf Passwörter
Weitergabe von Email-Adressen
Malware
Spam
Webcam wird gehackt
Hacker
Rechtsunsicherheit
Bilder ins Netz stellen **Identitätsdiebstahl**
Sorglosigkeit in Bezug auf Passwörter
Mails mit Anhang Beim Onlinebanking
illegale Datenverknüpfung **ausspioniert zu werden**
gehackte Werbebanner mit Schadcode
Verkauf von personenbezogenen Daten
ungenügende gesetzliche Regelungen aus Versehen
Der Faktor Mensch auf unseriöse Seiten gelangen

Verbraucherstimmen:
„Die größten Risiken im Netz!“

Phishing

Shoppen mit Kreditkarte
meine fehlenden PC-Kenntnisse

Viren

Virusscanner nicht installiert

schlechte Virensoftware

Kapitel 3

Fokus: Digitale Lebenswelten



Gesundheits- und Vitaldienste digital

Vernetzte Gesundheits- und Vitaldienste ermöglichen, Daten über körpereigene Funktionen zu erheben und zu verarbeiten, um daraus einen zusätzlichen oder persönlichen Nutzen zu ziehen.

Rasanten Wachstum im vergangenen Jahr zu verzeichnen

Das Angebot der sogenannten Gesundheits- und Vitaldienste ist in den vergangenen 12 Monaten sprunghaft gestiegen und wurde daher in die Wertung des Sicherheitsindex aufgenommen. Danach liegt die gegenwärtige Verbreitung bei 7,9 Prozent der deutschen Onliner mit voraussichtlich weiter steigender Tendenz.

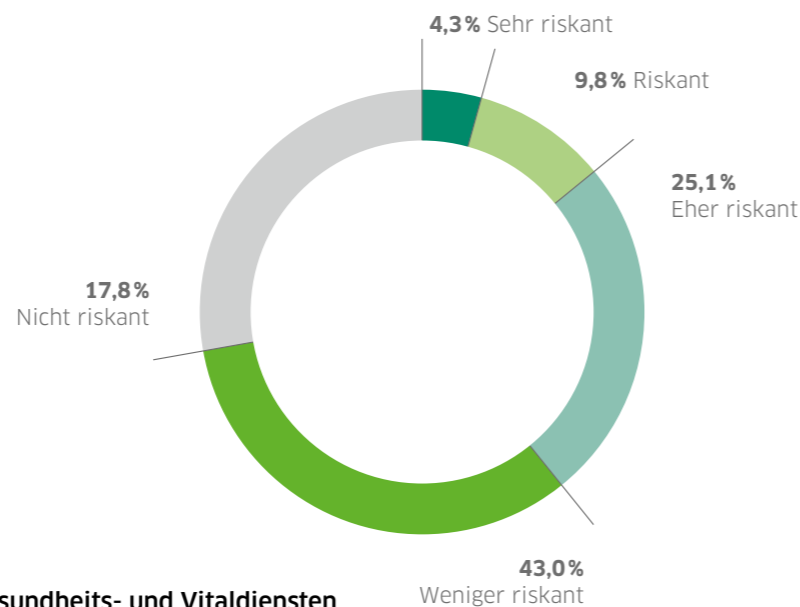
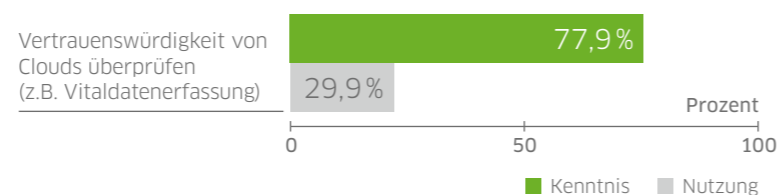


Abb. 19 Gefährdungsgefühl bei vernetzten Gesundheits- und Vitaldiensten

- Vital- und Gesundheitsdienste empfinden 14 Prozent der Verbraucher wenigstens als riskant.
- Dem Hochladen der Daten in die Cloud stehen 35 Prozent der Nutzer kritisch gegenüber.

Verbraucher zeigen Vorbehalte im Hinblick auf das Schutzniveau und die Vertrauenswürdigkeit von gesundheitsbezogenen Diensten; 14 Prozent empfinden ihre Nutzung als ein deutliches Risiko. Dies umfasst auch die typische Einbindung von Clouddiensten, denen 35 Prozent der Nutzer skeptisch gegenüber stehen. In die Unsicherheit vermischt sich Unwissenheit durch mangelnde Sicherheitskompetenz. Zwei Drittel geben an, die tatsächliche Sicherheit der Cloud-Dienste nicht selbst prüfen zu können oder zu wollen.

Abb. 20: Diskrepanz – Wissen und Verhalten



DsiN-Angebote

- **Seniorenwettbewerb**
Goldener Internetpreis
- **Gut zu wissen**
Kompetenzvermittlung für mobile Anwendungen
- **Datenkompetenz**
AconnectedLife.info

Haus- und Heimvernetzung

Von Heimelektronik in der Unterhaltung bis zu Vernetzung der Haustechnik und Energiesysteme – das „intelligente Haus“ hält zunehmend Einzug in den digitalisierten Alltag der Verbraucher.

Unterhaltung ist Vorreiter der Vernetzung.

Durchdringung vernetzter Dienste im Haus liegt bei 7,7 Prozent durch digitale Unterhaltungselektronik. Bei 2,3 Prozent liegt die Durchdringung in der Vernetzung von Haustechnik. Mit einer weiteren Verbreitung der Heimelektronik sowie der Haustechnik und auch Energie-Steuerungssysteme ist zu rechnen.

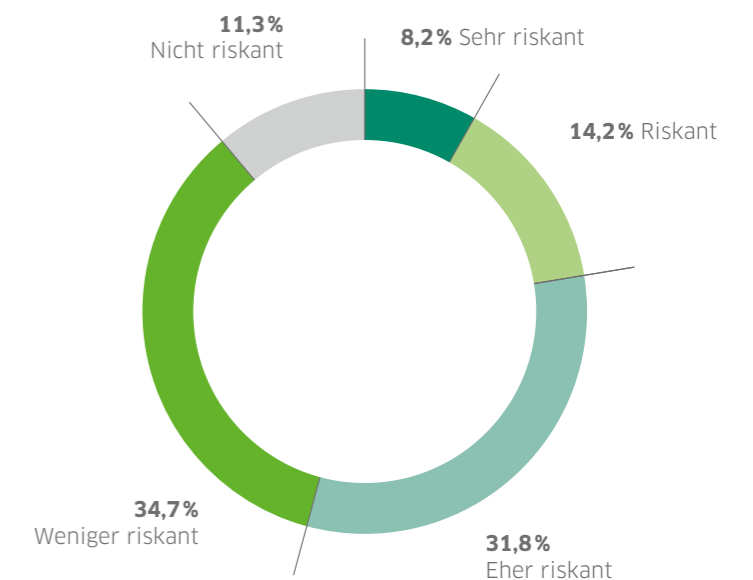


Abb. 21 Gefährdungsgefühl bei Haus- und Heimvernetzung

- Gut 22 Prozent der Nutzer halten Haus- und Heimvernetzung für riskant.

Gemessen an der noch geringen Verbreitung der Haus- und Heimvernetzung ist die Anzahl der registrierten Angriffe auf Systeme der Heimvernetzung frappierend hoch: 3,6 Prozent der befragten Nutzer gaben an, dass ihre Hausvernetzung bereits angegriffen wurde.

Zahlreiche Sicherheitsvorfälle bei Haus- und Heimvernetzung



DsiN-Angebote

- **DsiN-Sicherheitstipps**
Tipps im Überblick, z.B. zur sicheren WLAN-Nutzung
- **DsiN-Sicherheitsbarometer**
Aktuelle Gefahrenlage im Überblick

Einkaufen im Internet

Einkaufen im Netz gehört zu den beliebtesten Aktivitäten der deutschen Internetnutzer. Trotz steigender Verbreitung ist das Vertrauen in Online-Shopping 2015 zurückgegangen.

- Rund 4 Prozent der befragten Nutzer waren schon Opfer von Kreditkartenbetrug.
- 19 Prozent empfinden Online-Shopping als (sehr) riskant.
- Zugangsdaten wurden bei sechs Prozent ausgespäht.
- Betrugsopfer beim Zahlungsvorgang wurden bereits sechs Prozent.

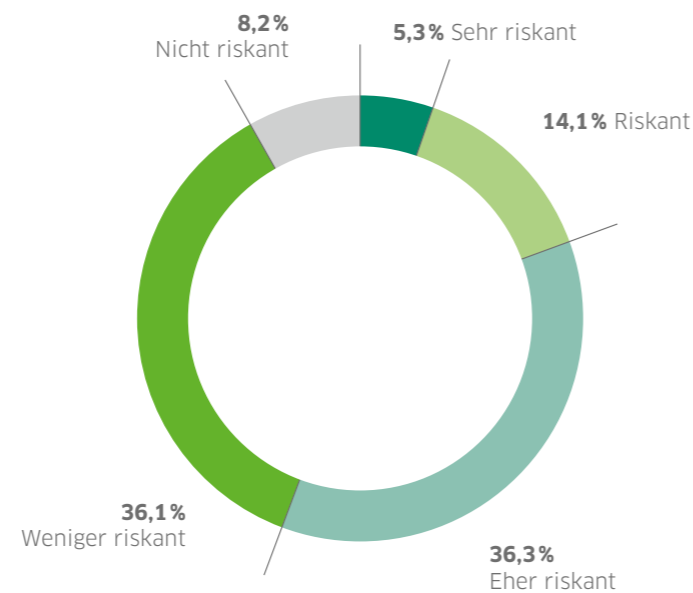
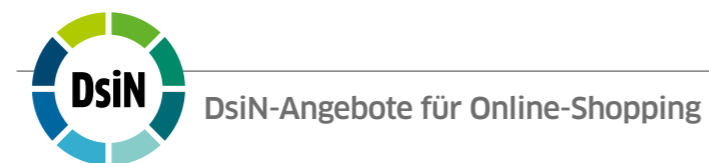
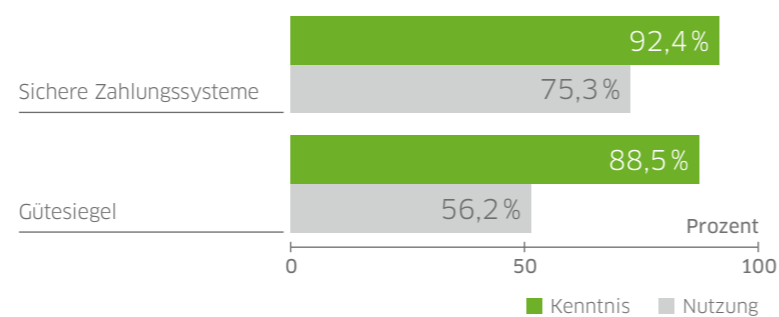


Abb. 22 Gefährdungsgefühl beim Shopping

Das Vertrauen in Online-Shopping hat 2015 um 13 Prozentpunkte abgenommen. Die Zahl der erfolgreichen Ausspähattacken ist gegenüber 2014 konstant bei 6 Prozent geblieben – auf demselben Niveau blieb auch die Quote der Betrugsopfer.

Auffällig ist die Diskrepanz zwischen Wissen und Verhalten: Obwohl 92 Prozent der Internetnutzer sichere Zahlungssysteme kennen, werden diese nur von 75 Prozent auch tatsächlich genutzt. Dies entspricht auch dem Defizit bei Gütesiegeln für Online-Shops: Bei einem Bekanntheitsgrad von fast 89 Prozent achten darauf beim Einkauf nur 56 Prozent der Verbraucher.

Abb. 23 Diskrepanz – Wissen und Verhalten beim Online-Einkauf



- **Einkaufen mit Verstand:** Sicher Online Einkaufen
- **DsiN-Passwort-Wechsel-App:** Passwörteränderung leicht gemacht

Online-Banking

Das Tätigen von Bankgeschäften im Internet ist heute weit verbreitet. Heraus sticht in der aktuellen Studie ein erhöhtes Gefährdungsgefühl der Nutzer beim Online-Banking.

- Rund 40 Prozent der Verbraucher empfinden Bankgeschäfte im Internet als mindestens riskant.
- Sicheren Internetverbindungen schenken 35 Prozent keine Beachtung.

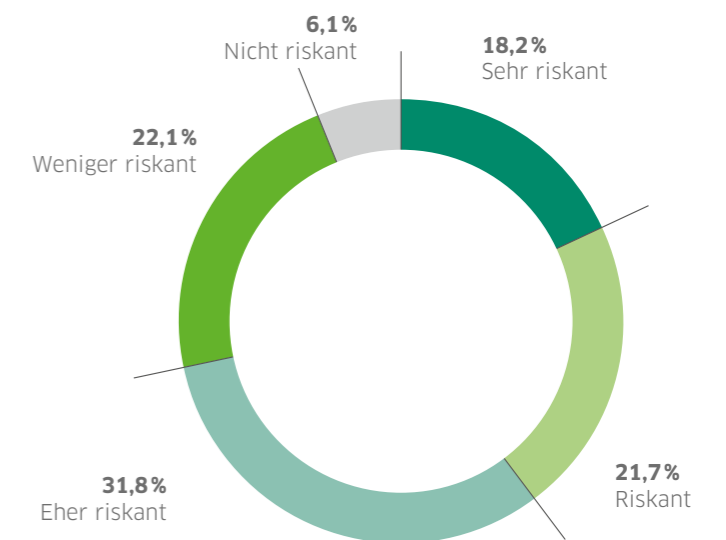
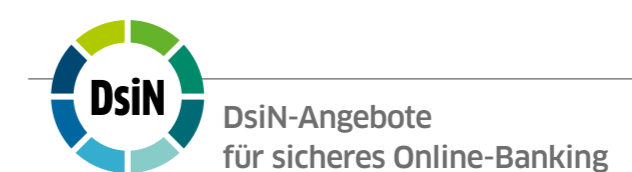
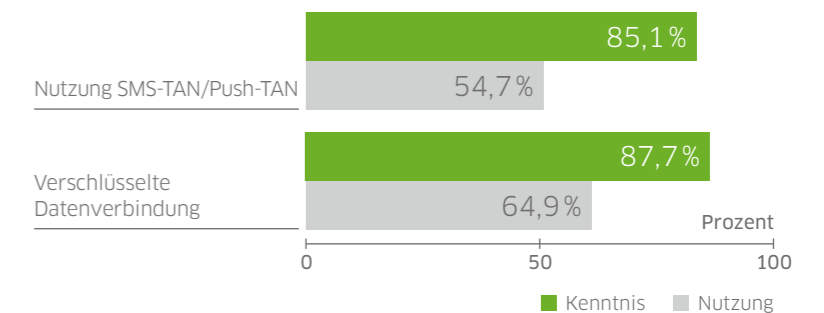


Abb. 24 Gefährdungsgefühl beim Online-Banking

Das Gefährdungsgefühl beim Online-Banking ist 2015 deutlich gestiegen: Zusätzliche 5,6 Prozent der Verbraucher sehen dieses als sehr riskant an, insgesamt 18,2 Prozent. Zwar sind verschlüsselte Datenverbindungen gut 88 Prozent der Nutzer bekannt, 35 Prozent schenken ihnen trotz Kenntnis aber keine Beachtung. 55 Prozent verwenden SMS-TANs – bei einem Bekanntheitsgrad von 85 Prozent.

Abb. 25 Diskrepanz – Wissen und Verhalten beim Online-Banking



- DsiN Sicherheitsbrief zum Online-Banking
- IT-Fitness Test für IT-Sicherheit
- Digitale Nachbarschaft für ehrenamtlich Engagierte

Deutlicher Anstieg des Gefährdungsgefühls beim Online-Banking in 2015

Exkurs – Index nach Bundesländern

Die ostdeutschen Länder holen kräftig auf und belegen 2015 die Spitzenränge. Aber auch alle anderen Bundesländer liegen oberhalb des kritischen Schwellenwerts von 50 Punkten.

Bestplatziert bei 65 Punkten

Die Sicherheitsvorfälle (34,2 Punkte) werden beim Spitzenreiter Thüringen durch ein sehr gut ausgeprägtes Sicherheitsverhalten überkompensiert (58,1 Punkte). Auffällig hier ist allerdings eine hohe Verunsicherung (32 Punkte) der Verbraucher im Netz. Die weiteren Erstplatzierten – Sachsen und Brandenburg – weisen ebenfalls vergleichsweise hohe Sicherheitskompetenzen auf (86,1 bzw. 84,5 Punkte).

Rote Laterne

Für das Saarland (39,4 Punkte) und Hamburg (36 Punkte) waren die sicherheitsrelevanten Vorfälle ausschlaggebend für die Positionierung. Hamburg liegt bei der Anwendung

von Sicherheitsmaßnahmen auf dem hinteren Platz (48,3 Punkte). Im Saarland fällt ein relativ geringes Gefährdungsempfinden bei der Internetnutzung auf. Bayern, Berlin und Hessen weisen recht häufige sicherheitsrelevante Vorfälle auf; darüber hinaus schneidet Berlin beim Schutzverhalten unterdurchschnittlich ab (49,4 Punkte).

Weitere Besonderheiten

Niedersachsen und Bremen zeichnen sich durch eine geringe Bedrohungslage aus – bei nur mäßigem Schutzverhalten. Das geringste Gefährdungsgefühl besteht in Bremen, das in den Charakter einer Unbedarftheit umschlägt (21,5 Punkte). Ein gutes Wissensniveau zeigt sich in Sachsen-Anhalt. Bei unterdurchschnittlichen Sicherheitsvorfällen ist jedoch die Verunsicherung höher als im Bundesvergleich. Entsprechendes gilt für Baden-Württemberg. Nordrhein-Westfalen liegt bei sämtlichen Sicherheitsfaktoren im unteren Mittelfeld.

Verunsicherte Verbraucher trotz Bestplatzierung

65,7	Thüringen
65,7	Sachsen
65,7	Brandenburg
65,4	Schleswig-Holstein
65,0	Mecklenburg-Vorpommern
64,7	Niedersachsen
64,7	Bremen
64,5	Rheinland-Pfalz
64,2	Sachsen-Anhalt
63,7	Baden-Württemberg
62,2	Nordrhein-Westfalen
62,1	Hessen
61,0	Bayern
61,0	Berlin
60,7	Hamburg
60,7	Saarland

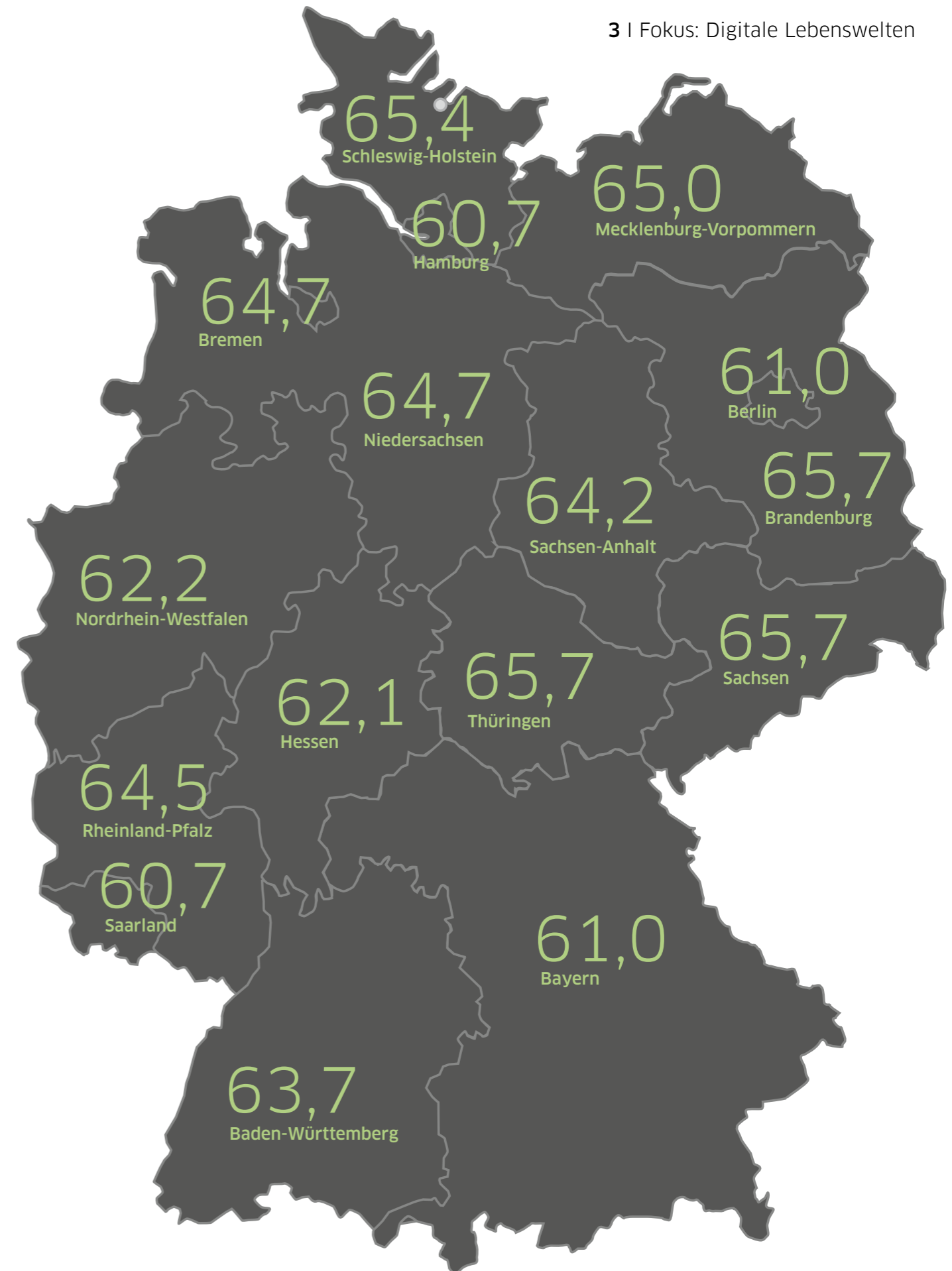


Abb. 26 Index nach Bundesländern

Risikoeinschätzungs- kompetenz stärken

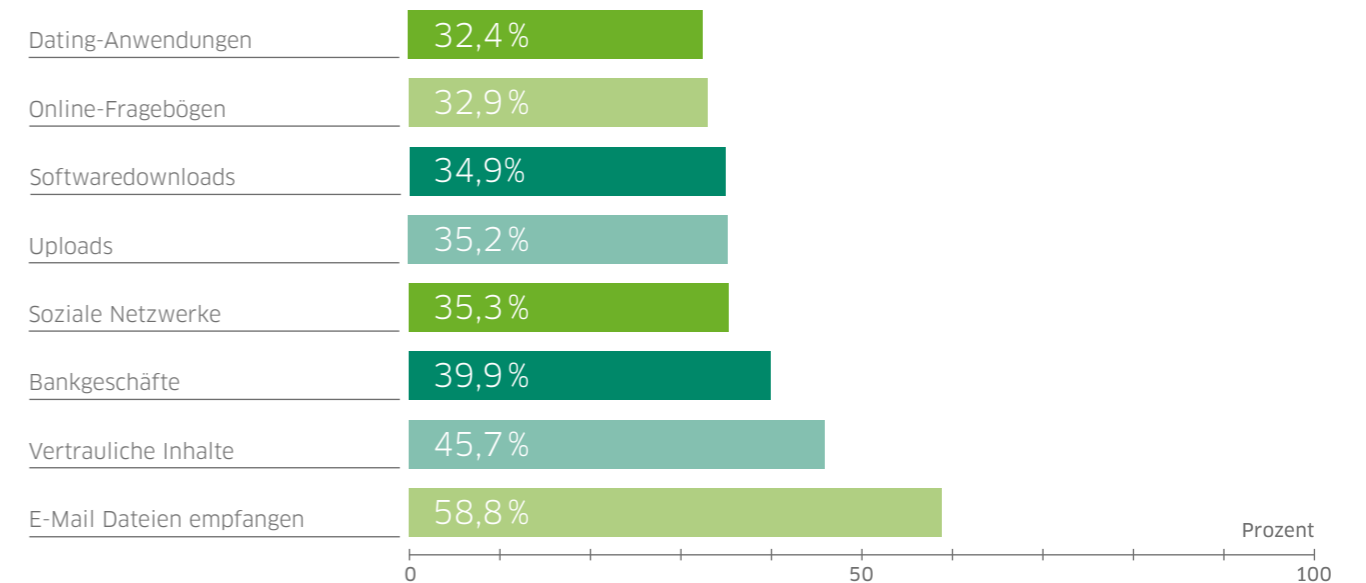


Abb. 27 Gefährdungsempfinden nach Anwendungen

Einschätzungskompetenz schärfen

Das Bewusstsein für Risiken im Netz gilt als „Eintrittskarte“ für eine souveräne Online-Aktivität. Erst das Wissen um Risiken kann den Schritt zur Anwendung von Sicherheitswissen auslösen. Es ist die Grundlage, um zu bewerten, ob und welche Maßnahmen zum Schutz zu treffen sind. Ein umfassendes Bewusstsein für die eigenen Risiken sollte daher der Ausgangspunkt der Aufklärungsarbeit sein.

Balance zwischen Unbedarftheit und Verunsicherung

Wichtiger Indikator für die Einschätzungskompetenz ist das Sicherheitsgefühl; der Sicherheitsindex zeigt hier eine deutliche Schere. So steht ein „Überrisikogefühl“ der Außenstehenden einer regelrechten „Unbedarftheit“ der Fatalisten und Gutgläubigen gegenüber. Die Kompetenz zum Erkennen echter Risiken in Abgrenzung zur undifferenzierten Verunsicherung muss angeglichen werden.

Bewusstsein für relevante Risiken schaffen

Aufgabe der Aufklärung muss sein, ausreichende Aufmerksamkeit für die angemessene Einschätzung von Risiken zu schaffen. Damit wird vorhandene Unbedarftheit abgebaut und eine ungerechtfertigte „Verunsicherung“ vermieden. Anstelle einer Aufklärung „mit der Gießkanne“ tun Maßnahmen not, die das jeweilige Sicherheitsempfinden erhöhen.



Handlungsempfehlungen Digitale Aufklärung 2.0

- **Bewusstsein schaffen**
Informationen aktiv vermitteln
- **Sicherheitsrisiken**
Relevante Sicherheitsrisiken aufzeigen
- **Einschätzungskompetenz**
Individuelle Risikoeinschätzung trainieren
- **DsiN-Tools (Auszug)**
Jugendwettbewerb myDigitalWorld; Einfach verschlüsseln; Plattform Datenkompetenz

Kapitel 4

Digitale Aufklärung: Handlungsfelder!

Sicherheitswissen ausbauen und vertiefen

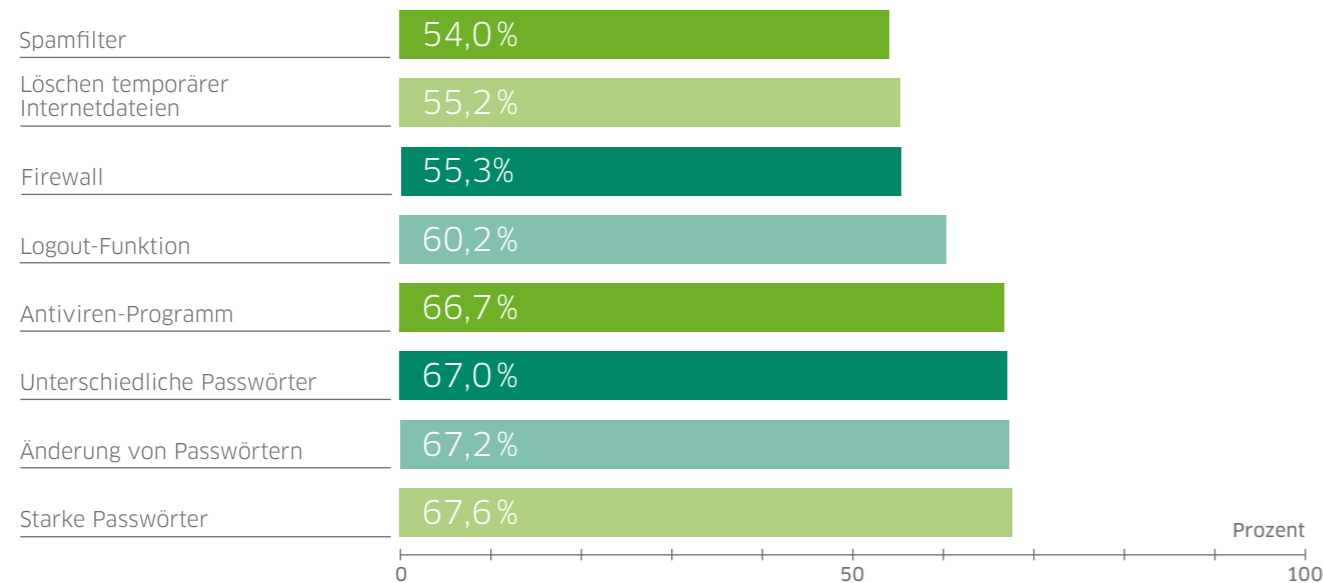


Abb. 28 „Gute“ Sicherheitskenntnisse: Spitzenreiter

Sicherheitswissen erweitern

Um auf Risiken und Bedrohungen im Netz reagieren zu können, müssen die relevanten Sicherheitsmaßnahmen besser bekannt sein. Zwar ist ein Grundwissen rudimentärer Sicherheitsmaßnahmen schon gut verbreitet. Die qualifizierten Kenntnisse hingegen sind oftmals nicht ausreichend. So sind selbst starke Passwörter nur bei 67,6 Prozent der Nutzer „gut bekannt“ (s. Abb. 28).

Ein ähnliches Bild ergibt sich bei Maßnahmen wie der Verwendung unterschiedlicher Passwörter für verschiedene Zwecke (67 Prozent) sowie der Aktivierung eines Antiviren-Programms (33,3 Prozent).

Vertiefung bei komplexeren Sicherheitsmaßnahmen

Sicherheit ist nicht immer einfach – auch wenn dies wünschenswert ist. Entsprechend landen komplexere Sicherheitsmaßnahmen abgeschlagen auf den hinteren Plätzen bei den guten Sicherheitskenntnissen (s. Abb. 29). Relevante Felder wie sichere Cloudnutzung (24 Prozent) oder die Inkognito-Funktion beherrschen nur 28 Prozent. Zur biometrischen Identifizierung und zu elektronischen Signaturen haben nicht einmal zwei von drei Verbrauchern ausreichende Kenntnisse.

Ziel sollte sein, das Niveau bei relevanten einfachen und auch komplexeren Sicherheitsmaßnahmen auf ein gutes Niveau anzuheben.

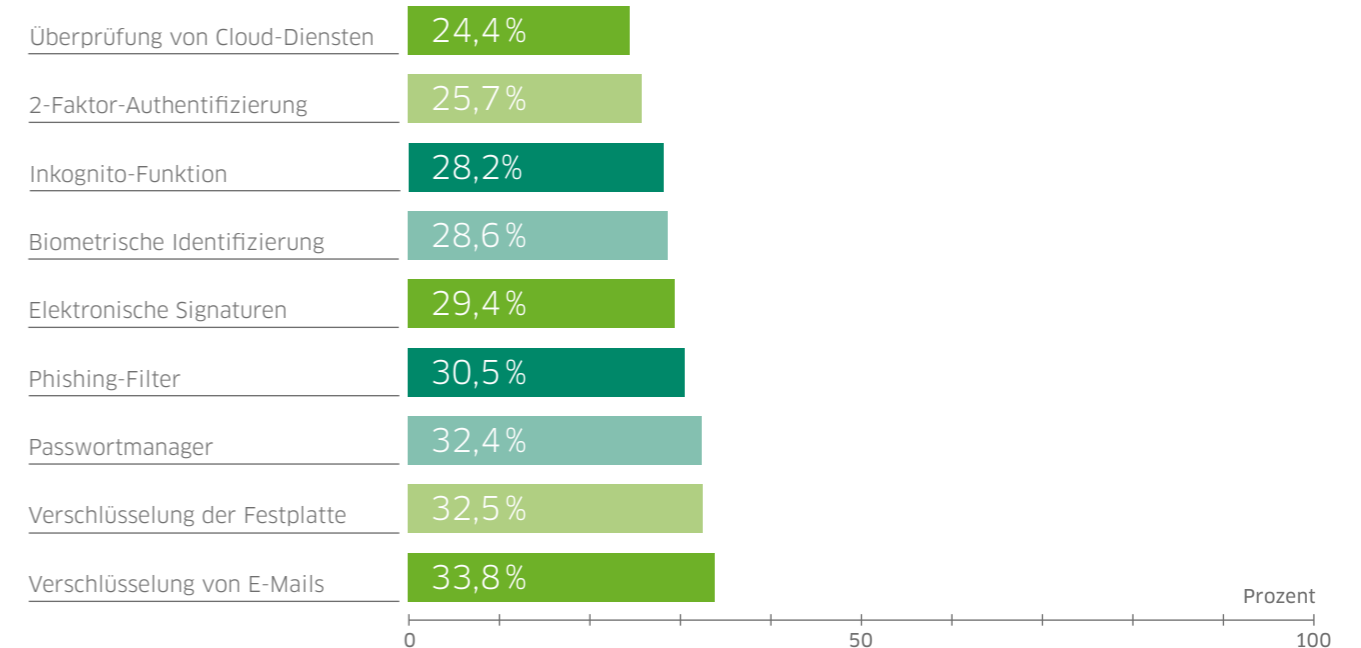
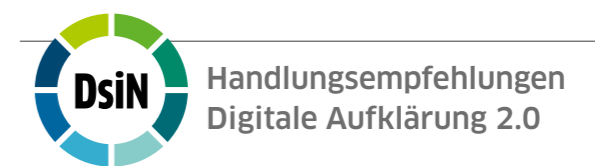


Abb. 29 „Gute“ Sicherheitskenntnisse: Schlusslichter

Mix an Sicherheitskompetenzen

Die Anhebung des Sicherheitswissens – gerade auch von unbekannteren Tools – ist ebenso erforderlich wie die Schließung spezifischer Defizite innerhalb der Nutzergruppen. Dies gilt im besonderen Maße für die Außenstehenden, die schon bei einfachen Sicherheitsmaßnahmen „scheitern“. Die anderen Gruppen sollten darüber hinaus über kompliziertere Sicherheitsmaßnahmen informiert und zu ihrer Nutzung befähigt werden.

Dieser Ansatz wird durch die Selbsteinschätzung der Verbraucher bestätigt, die sich einen erhöhten Aufklärungs- und Unterstützungsbedarf für einen souveränen Umgang mit dem Internet wünschen. Auffällig ist auch hier, dass die souveränen Nutzer das größte Interesse an der Weiterbildung zu Sicherheitsfragen aufweisen. Im Umkehrschluss müssen die anderen Gruppen – Fatalisten und Gutgläubige – auf eigenen Wegen für das Thema begeistert werden.



- **Basiswissen vermitteln**
Alle Nutzergruppen mit Grundlagenwissen ausstatten
- **Kenntnisse vertiefen**
Komplexere Anforderungen je nach Bedürfnis vermitteln
- **DsiN-Tools (Auszug)**
IT-Fitness Test und Academy, Sicherheitsbarometer, Medien in die Schule, Kaufen mit Verstand

Umsetzungskompetenzen trainieren

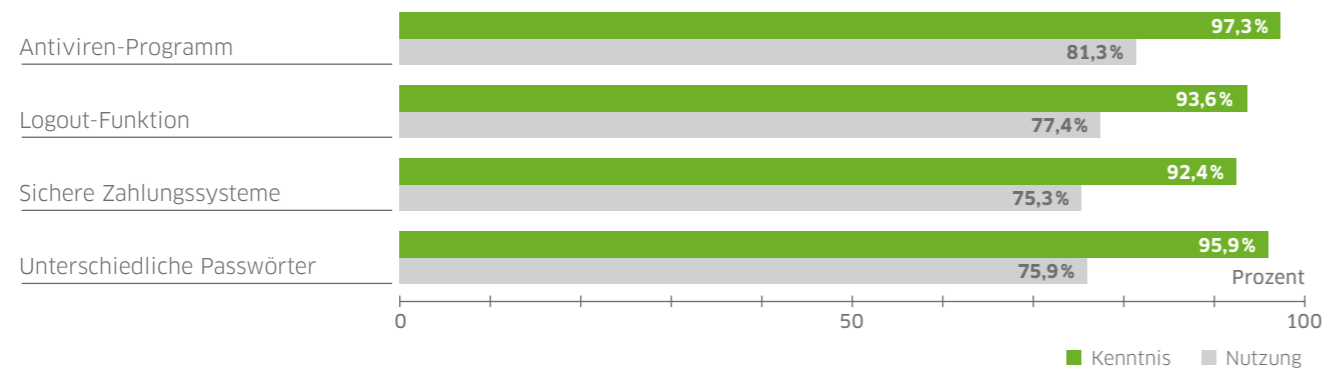


Abb. 30 Nutzung versus Kenntnis von Schutzmaßnahmen - vordere Plätze

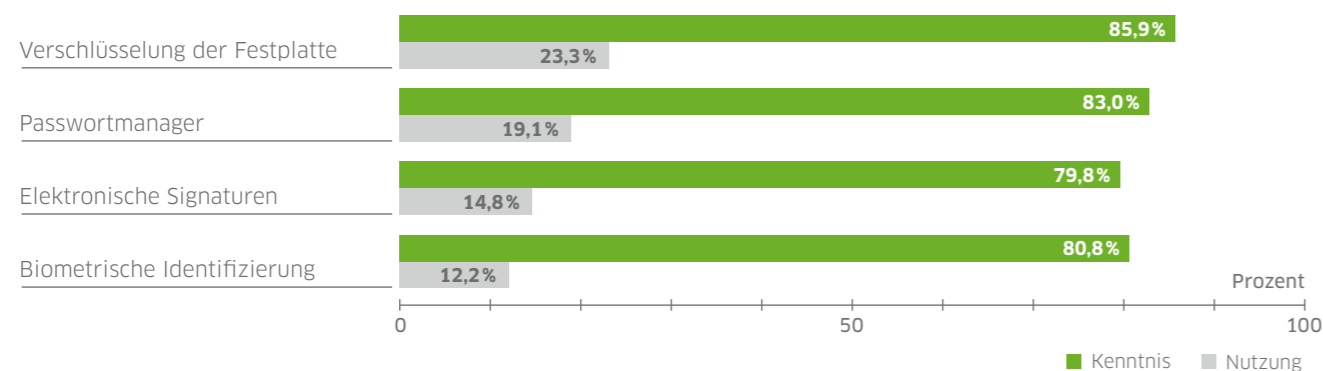


Abb. 31 Nutzung versus Kenntnis von Schutzmaßnahmen - hintere Plätze

Diskrepanz von Wissen und Verhalten

Um das Schutzniveau effektiv zu verbessern, müssen Sicherheitsmaßnahmen nicht nur gut bekannt sein, sondern im digitalen Alltag auch angewendet werden. Hier klafft – wie schon 2014 – eine Lücke zwischen Kenntnis und Umsetzung bei allen Nutzergruppen. Bei den Fatalisten wie auch bei den Gutgläubigen ist diese Diskrepanz besonders stark ausgeprägt.

Komplexe Schutzmechanismen im Nachteil

Besonders auffällig aber auch nachvollziehbar ist: Je komplexer oder je unbekannter eine Sicherheitsmaßnahme ist, desto seltener erfolgt ihre Anwendung. Schlusslichter bilden wirksame Verschlüsselungstechniken – noch vor dem Passwortmanager, elektroni-

schen Signaturen und biometrischer Identifizierung. Letztere wird nur von 12 Prozent der Verbraucher genutzt – bei 80 Prozent Kenntnis.

Zur Nutzung von Schutzmaßnahmen anregen

Hier setzt das Training zur Umsetzung des Wissens an, um die Anwendung von Sicherheitsmaßnahmen zur Routine werden zu lassen. Dabei geht es auch um die Kommunikation und Anleitung, wie komplizierte Mechanismen im Gebrauch vereinfacht werden können – beispielsweise die regelmäßige Passwort-änderung durch Passwort-Manager. Die Aufklärung muss hier auf die Praxistauglichkeit fokussiert werden.

Sicherheitspraxis: Motivieren

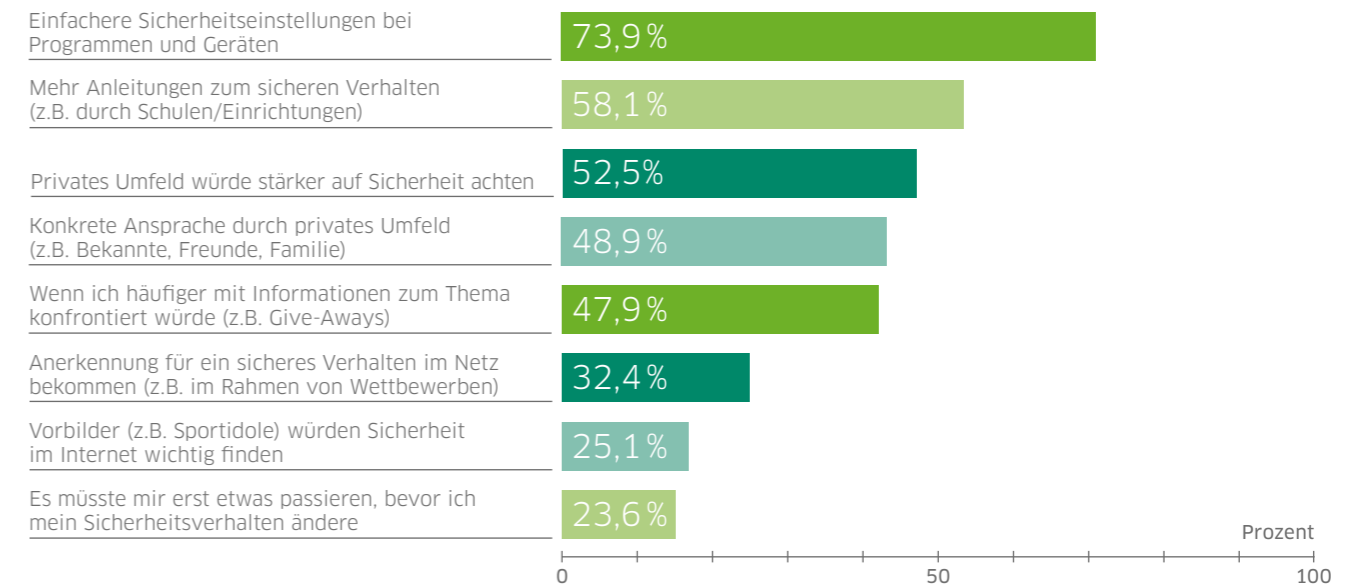


Abb. 32 Möglichkeiten zur Reduzierung der Sicherheitsvorfälle

Souverän im Netz handeln

Oftmals scheitert der letzte Schritt zur Anwendung an der Bequemlichkeit oder an mangelnder Einsicht. Im Index geben drei von vier Verbrauchern im Internet an, selbst einen höheren Beitrag zum Abbau sicherheitsrelevanter Vorfälle leisten zu können. Damit bestätigt die überwiegende Mehrheit, dass sie den Schlüssel für IT-Sicherheit mit in der Hand haben.

Ein Schwerpunkt der Aufklärung sollte daher Routinetraining sein, um Maßnahmen zu verinnerlichen. Relevant ist aber auch die Vermittlung einer Haltung, die jeden Einzelnen selbst zum sicheren Umgang im Netz auffordert. Dadurch können sich Verbraucher in neuen Situationen eigenständig zurechtfinden. Motivieren lassen sich die deutschen Onliner dabei durch ihr direktes persönliches Umfeld (48,9 Prozent) sowie durch häufigeren Kontakt mit Informationen zu Internetsicherheit (48 Prozent der Befragten, s. Abb. 32).



- **Umsetzungsmotivation fördern:**
Schulung von Multiplikatoren im persönlichen Umfeld „Peergroup“
- **DsiN-Tools zur Umsetzung:**
 - Digitale Nachbarschaft für Ehrenämter
 - Passwort-Wechsel-App
 - Sicherheitsbarometer

Diskrepanz von Wissen und Handeln konkret entgegenwirken

Fazit – Digitale Aufklärung 2.0 verbessert Sicherheitslage

Aufklärung tut not! Damit Schutz, Sicherheit und Vertrauen im Internet für alle Verbraucher gleichmäßig gelebt werden kann, muss das Digitale Sicherheitsgefälle abgebaut werden – zügig und nachhaltig. Denn eine digitale Zukunft, in der 60 Prozent der Verbraucher relevante Sicherheitsdefizite in der eigenen Lebenswelt aufweisen, kann ihre Chancen nicht wirklich entfalten.

Leichte Verbesserungen im Index 2015 zeigen, dass die Sicherheitslage der Verbraucher dynamisch ist und tatsächlich verändert werden kann. Positiv hervorzuheben ist auch, dass die Schere zwischen den „sicheren“ und „unsicheren“ Nutzergruppen nicht größer geworden ist. Insgesamt aber haben sich Defizite in allen subjektiven Sicherheitsfaktoren bestätigt – vom Sicherheitsgefühl über Kenntnisse bis zum Sicherheitsverhalten.

Um die Internetnutzer zum souveränen Umgang mit dem Netz zu befähigen, müssen Aufklärungsaktivitäten verstärkt werden. Mit dem Ziel einer „Digitalen Aufklärung 2.0“ werden dazu drei Schwerpunkte gesetzt, um eine breite und nachhaltige Verbesserung der Sicherheitslage zu erreichen:

• Individuelle Aufklärungsmaßnahmen

Um Sicherheitskompetenzen und -verhalten bei Verbrauchern zu verbessern, müssen die individuellen Bedürfnisse berücksichtigt werden. Ein Mix an Aufklärungsarbeit wird angestrebt. Deutschland sicher im Netz bietet dazu zielgruppenspezifische Unterstützungsangebote für Verbraucher: neue Projekte, die bundesweit konkrete Beratung und Unterstützung vor Ort bieten. Dazu sind auch Angebote für Berufsschüler, Vereine, Senioren und Kleinunternehmen geplant.

• Aufklärungsinitiativen vernetzen

Zahlreiche Initiativen bieten heute gute Aufklärungsangebote. Für eine wirksame Aufklärung, die Verbraucher wirklich erreicht, sollten diese Angebote vernetzt und für Verbraucher auf diesem Wege besser zugänglich gemacht werden. Ein Aktionsbund „Digitale Sicherheit“ kann die Zugangswege der Verbraucher zu Aufklärungsangeboten verkürzen. Er ist ein Baustein, um guten Aufklärungsinitiativen zu mehr Breitenwirkung in Gesellschaft, Politik und Wirtschaft zu verhelfen.

• Dialog mit allen Beteiligten verstärken

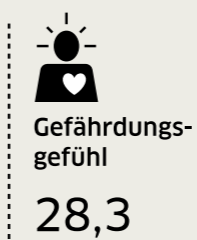
Dort, wo Aufklärungsarbeit an ihre Grenzen stößt, muss der Dialog mit allen Beteiligten verstärkt werden. So können technologische Innovationen dort ansetzen, wo Aufklärungsbemühungen wenig Wirkung entfalten können – beispielsweise durch ein höheres Maß an Nutzerfreundlichkeit. Auch die Politik kann das Engagement für Aufklärung unterstützen.

Das Zusammenwirken dieser drei Faktoren der Digitalen Aufklärung 2.0 ist eine notwendige Voraussetzung, um Souveränität für Verbraucher im digitalisierten Alltag zu erreichen. Die Erkenntnisse der Studie werden dazu beitragen, diesen Prozess zu vertiefen und im Dialog mit allen Beteiligten zu verstetigen.

DsiN-Sicherheitsindex 2015

Digitale Sicherheitslage der Verbraucher in Deutschland

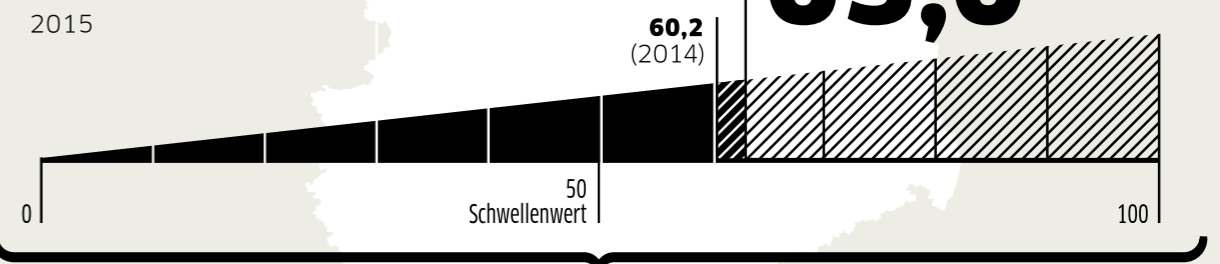
BEDROHUNGSLAGE



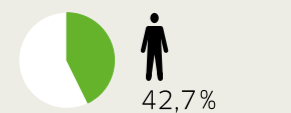
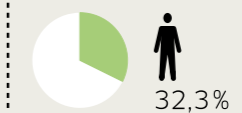
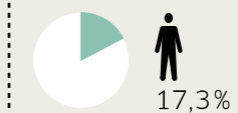
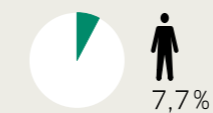
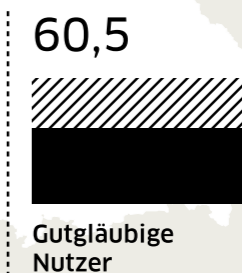
SCHUTZNIVEAU



DIGITALE SICHERHEITSGEFÄLLE



VIER VERBRAUCHERTYPEN



Digitale Aufklärung 2.0

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

Risikokompetenz-
einschätzung stärken

Sicherheitswissen
ausbauen und vertiefen

Umsetzungs-
kompetenz trainieren

Zur Sicherheitspraxis
motivieren

Abb. 33: DsiN-Sicherheitsindex 2015

Glossar

Aufklärung 2.0	Um die digitale Sicherheitslage zu verbessern, werden Aufklärungsangebote stärker auf die Bedürfnisse der Verbraucher zugeschnitten – gemeinsam mit allen Stakeholdern.
Gefährdungsgefühl	Das von den Onlinern selbst eingeschätzte Risiko bei der Nutzung ausgesuchter Technologien und Anwendungen.
Bedrohungslage	Zusammenfassung der Faktoren sicherheitsrelevanter Vorfälle und Bedrohungsempfinden.
Der DsiN-Index	Die Sicherheitslage der deutschen Onliner in einer Zahl. Gewichteter Mittelwert aus den vier Faktoren Sicherheitsvorfälle, Bedrohungsempfinden, Bekanntheit und Nutzung von Schutzmaßnahmen.
DsiN-Nutzertypen	<p>Eine Clusterung der deutschen Onliner. Es gibt 4 Nutzertypen, die sich durch typische Verhaltensweisen auszeichnen.</p> <p>Außenstehende Nutzer: Haben im Vergleich zu den anderen Nutzergruppen deutliche Defizite bei der Kenntnis und der Nutzung von Schutzmaßnahmen.</p> <p>Fatalistische Nutzer: Sie unterlassen Sicherheitsmaßnahmen, obwohl sie Risiken und Schutzmaßnahmen überdurchschnittlich gut kennen, geringes Gefährdungsempfinden.</p> <p>Gutgläubige Nutzer: Sie verfügen über ein nur sehr gering ausgeprägtes Gefährdungsempfinden und nutzen Schutzmaßnahmen kaum.</p> <p>Souveräne Nutzer: Sie verfügen bereits über eine hohe Kompetenz und wenden Schutzmaßnahmen meist auch an.</p>
Indexpunkte	Der DsiN-Index wird auf einer Skala von 1 bis 100 gemessen. Der Wert 50 stellt dabei den Punkt dar, an dem die Sicherheitslage kippt.
Kenntnis von Schutzmaßnahmen	Selbstauskunft der Nutzer, ob sie bestimmte Schutzmaßnahmen kennen oder nicht.
Nutzung von Schutzmaßnahmen	Selbstauskunft der Nutzer, ob sie ausgesuchte Schutzmaßnahmen auch tatsächlich anwenden.
Sicherheitsvorfälle	Für die Sicherheit der Nutzer relevante Vorfälle, die von den Onlinern bemerkt wurden, z. B. Passwortdiebstahl, Virenbefall, o. ä. Schutzniveau ist ein eigenständiger Begriff im Glossar.
Schwellenwert	Bei Werten unter 50 Indexpunkten ist die Bedrohungslage höher als das Schutzniveau, bei Werten über 50 ist es umgekehrt.

DEUTSCHLAND SICHER IM NETZ (DSiN)

Unsere Mission ist die Verbesserung des Sicherheitsbewusstseins und Verhaltens von Verbrauchern sowie kleinen und mittleren Unternehmen im Netz durch konkrete Hilfestellungen – im Verbund mit Unternehmen, Verbänden und Vereinen. Dafür bietet DsiN praktische Orientierungshilfen und Anleitungen. Als produktunabhängige Plattform für Aufklärungsinitiativen ist DsiN für neue Mitglieder offen.

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 Anleitungen zum souveränen digitalen Umgang im Netz im Mittelpunkt wie die Passwort Wechsel App für Verbraucher sowie das neue 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 2015 | Digitale Sicherheitslage der Verbraucher in Deutschland

Verantwortlich: Dr. Michael Littger

Verfasser: Tobias Weber (TNS Infratest) und Tina Leusbrock (DsiN)

Eine Studie von TNS Infratest (Studienpartner)
im Auftrag von Deutschland sicher im Netz e.V.

Gestaltung: ideengut | Agentur für Kommunikation
Infografiken: Carsten Raffel (USOTA)

Stand: Juni 2015

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, SAP, DsiN

© vege / fotolia.com, © ptnphotof / fotolia.com, © Maridav / fotolia.com,
© annebaek / iStock, © mediaphotos / iStock