

INITI@TIVE D²¹

Eine Studie der Initiative D21, durchgeführt von TNS Infratest

Eine Sonderstudie im Rahmen des

(N)ONLINER Atlas 2008



**Sicher Surfen 2008:
Wie schützen sich Onliner im Internet?**

mit freundlicher Unterstützung von

Microsoft®

Sicher Surfen 2008:

Wie schützen sich Onliner im Internet?





Ob für E-Mail, Informationen, Einkäufe, Behördengänge oder rein zur Unterhaltung: Das Internet ist auch im privaten Umfeld nicht mehr wegzudenken.

Über 65 Prozent der Menschen in Deutschland sind mittlerweile online und nutzen die unzähligen Angebote der Datenautobahn. Tendenz weiter steigend.

Tendenz weiter steigend.

Dabei ist erfreulich: Parallel wächst das Bewusstsein für das Thema Sicherheit. Denn bei jedem Ausflug ins Web gibt es nach wie vor zahlreiche Wegelagerer, die nur darauf warten, heimlich mitzufahren oder gleich ganz den heimischen Computer in Besitz zu nehmen. Unsere aktuelle IT-Sicherheitsstudie als Sonderteil des *(N)ONLINER Atlas 2008* der Initiative D21 zeigt: Privatanwender wissen zunehmend, dass auch ihr persönliches Verhalten beim Schutz vor Viren, Trojanern und Co eine entscheidende Rolle spielt.

So ist bei der Aktualisierung von Betriebssystemen und Software zum Schutz vor Schadprogrammen ein klarer Trend sichtbar. 74 Prozent der Internetnutzer bringen ihr Betriebssystem auf den neusten Stand, sobald ein Update verfügbar ist. Das sind knapp 18 Prozentpunkte mehr als im Vorjahr. Auf der anderen Seite liegt der Anteil derjenigen, die ihre Software nie aktualisieren, bei weniger als vier Prozent.

Diese Zahlen spiegeln sich auch im Sicherheitsempfinden der Nutzer: 83 Prozent glauben, dass ihr Computer gut geschützt ist. Die Zahl der Internetnutzer, die angeben, sich schon einmal einen Virus oder Schadstoffsoftware auf ihrem Computer eingefangen zu haben, ist im vergangenen Jahr um ca. sieben Prozentpunkte gesunken.

So erfreulich diese Momentaufnahmen sind: Das Thema Sicherheit bleibt eine Daueraufgabe für Politik, Gesellschaft und Wirtschaft. So wächst beispielsweise der Wunsch der Anwender nach verständlichen und kompakten Informationen zum Thema Sicherheit insgesamt. Dabei herrscht ein besonderer Informationsbedarf im Bereich Datensicherheit. Etwa jeder vierte Anwender mit Informationsbedürfnis möchte zu diesem Thema gerne mehr wissen. Das entspricht einem Anstieg um etwa 15 Prozentpunkte. Meldungen der letzten Monate über den Missbrauch persönlicher Daten dürften hier ihren Niederschlag finden.

Auch beim Thema Kinderschutz gibt es ambivalente Entwicklungen. Zwar setzen immer mehr Eltern auf spezielle Software und Browsereinstellungen, um ihren Nachwuchs von schädlichen Inhalten fernzuhalten. Gleichzeitig sinkt aber die persönliche Kontrolle durch die Eltern, und zeitliche Limits für die Nutzung werden seltener gesetzt. Speziell bei der Vermittlung von Medienkompetenz müssen die Eltern also künftig wieder eine stärkere Rolle spielen. In Schulen nimmt Microsoft diese Verantwortung bereits wahr. Unter dem Motto „Sicherheit macht Schule“ stellen wir Unterrichtsideen und Materialien zur Verfügung, um das Sicherheitsbewusstsein der jungen Generation zu schärfen.

Permanente technologische Verbesserungen und inhaltliche Aufklärung bleiben also die wichtigsten Schlüssel für mehr Sicherheit im Web. Nur so wird es uns gelingen, das Vertrauen weiter zu stärken und die Voraussetzung für künftige Innovationen und wirtschaftliches Wachstum zu schaffen.

Achim Berg

General Manager Microsoft Deutschland GmbH

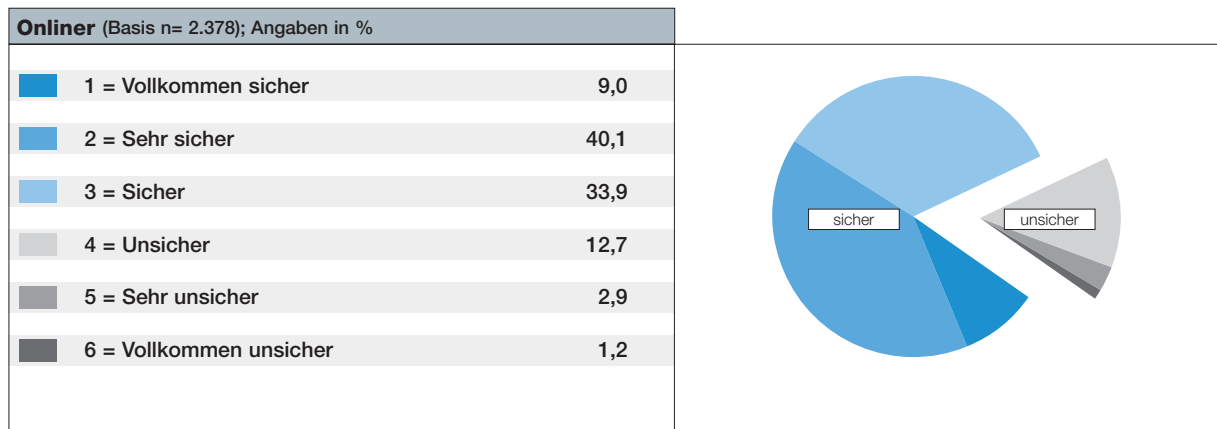
Zur Studie: Methodensteckbrief

- Stichprobe: Repräsentativ mit 2.378 Interviews
- Grundgesamtheit: Deutschsprachige Onliner in Privathaushalten in Deutschland im Alter ab 14 Jahren, die das Internet privat nutzen
- Auswahl: TNS Onlinepanel; gewichtet nach zentralen Merkmalen (Geschlecht, Alter, formale Bildung, Region und Zugangsart zum Internet)
- Repräsentative Erhebung, Ergebnisse auf die Grundgesamtheit übertragbar
- Durchführung als Onlinebefragung (computergestütztes Webinterview CAWI), in KW 19/2008 und KW 20/2008
- Zentrale Themen/Fragestellungen unter anderem:
 - Allgemeine Einschätzung der Computer-Sicherheit, Einstellungen zum Thema
 - Betriebssystempflege, genutzte Sicherheitssysteme
 - Opfer von Viren/Schadsoftware, Aufwand der Viren-Beseitigung
 - Kenntnisse, Informationsstand, Informationsbedarf
 - Verantwortung für Sicherheit im Internet
 - Zugang zum Internet
 - Kinderschutz

Allgemeine Einschätzung der Computer-Sicherheit

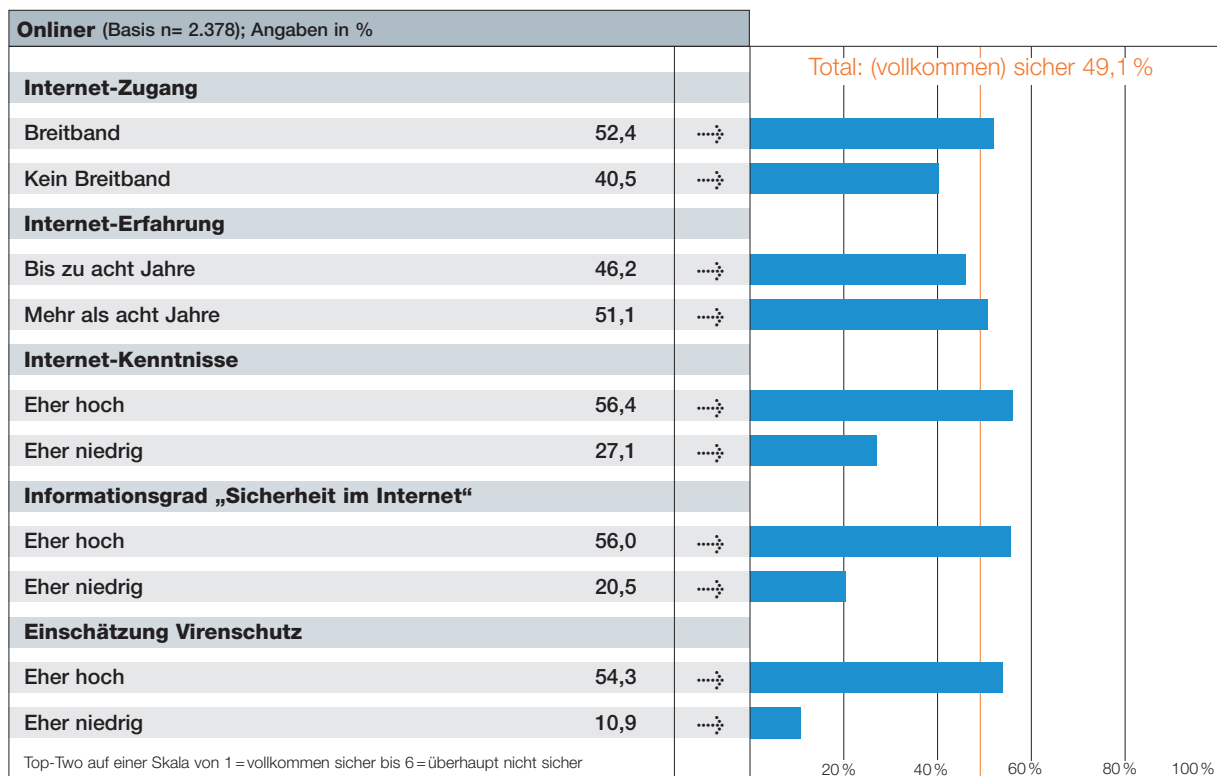
Frage: Wie schätzen Sie allgemein die Sicherheit Ihres Computers ein?

Auf einer Skala von 1 = vollkommen sicher bis 6 = überhaupt nicht sicher, wie sicher ist Ihr Computer?



Die Mehrheit der Onliner in Deutschland schätzt ihren eigenen Computer als sicher bis vollkommen sicher ein. Über 80 Prozent der Befragten gehören zu dieser Gruppe. Daraus ergibt sich allerdings auch, dass etwa jeder sechste Onliner seinen Computer als unsicher bis sehr unsicher einschätzt. Die folgende Grafik zeigt darüber hinaus, dass insbesondere Wissen über die Sicherheit im Internet zu einem gesteigerten Sicherheitsempfinden führt.

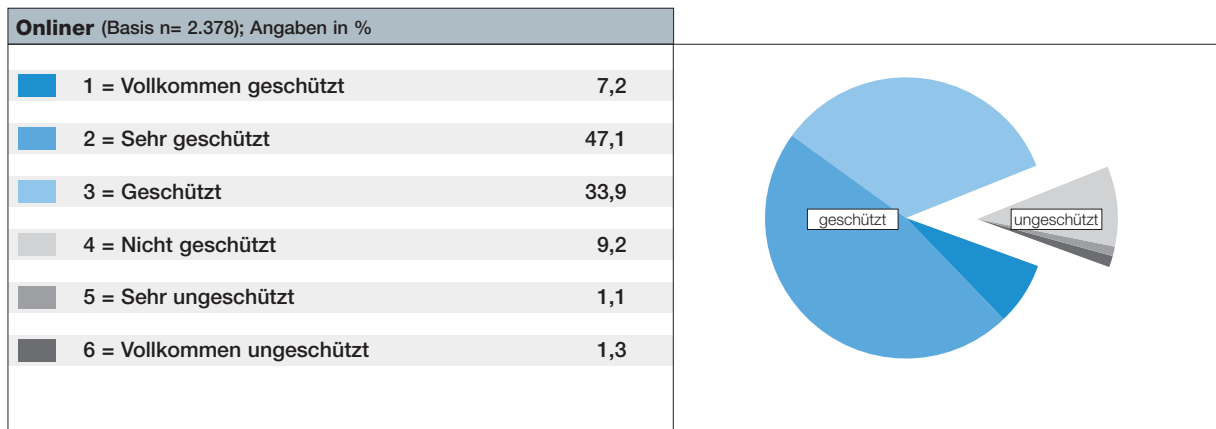
Allgemeine Einschätzung der Computer-Sicherheit – Top-Two* nach Merkmalen



Die Einschätzung des Virenschutzes, die Internet-Kenntnisse und dabei insbesondere die Kenntnisse zur Sicherheit im Internet führen zu einer erhöhten Einschätzung der Computersicherheit. Demnach wird das Internet als größte Gefahrenquelle gesehen. Am besten lässt sich diesem Gefahrenpotenzial mit einem guten Virenschutz und gezielter Informationsbeschaffung zum Thema „Internetsicherheit“ entgegenwirken. Eine Reihe wichtiger Informationen erhalten Sie in dieser Sonderstudie.

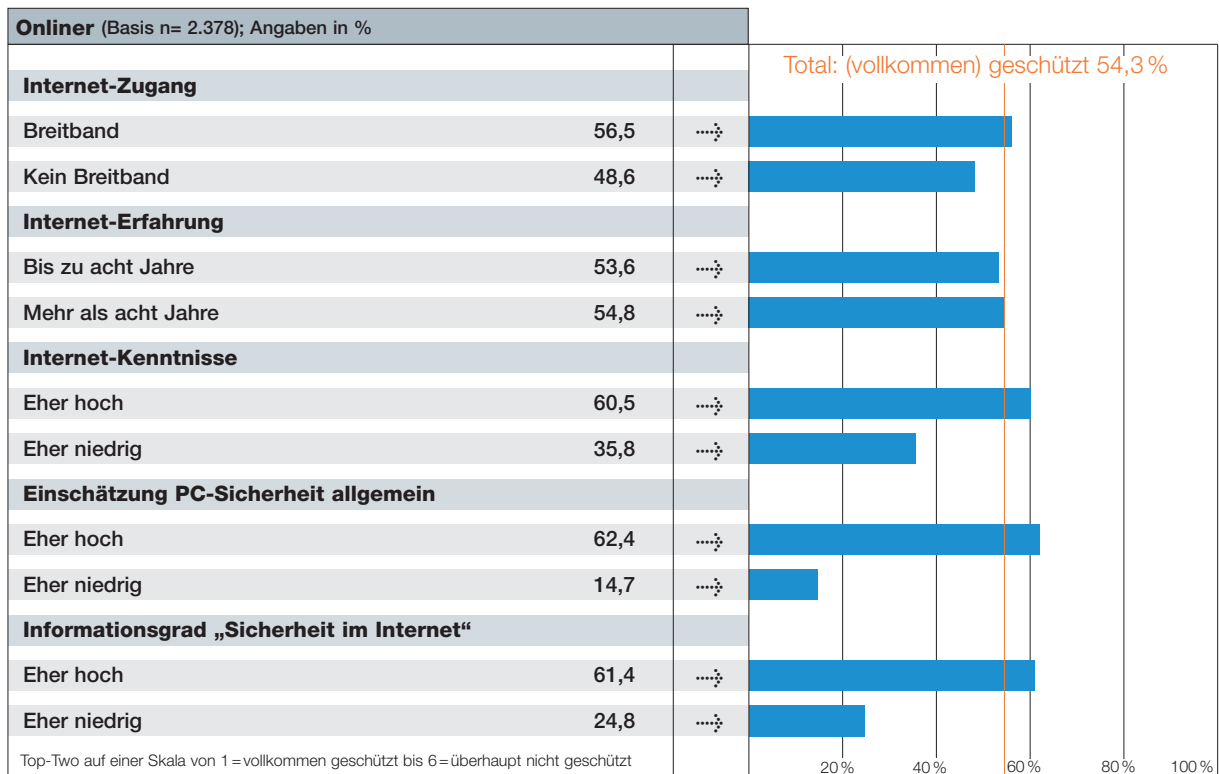
Schutz vor Viren / Schadsoftware

Frage: Was denken Sie, auf einer Skala von 1 = vollkommen geschützt bis 6 = überhaupt nicht geschützt: Wie gut ist Ihr Computer vor Viren und anderer Schadsoftware geschützt?



Vor Computerviren und anderer Schadsoftware fühlen sich immerhin 88,2 Prozent der befragten Onliner geschützt. Etwa jeder Zehnte ist durch die Existenz von Viren und Schadsoftware verunsichert. Verglichen mit der allgemeinen Einschätzung zur Sicherheit des Computers fühlen sich weniger Onliner vor Viren ungeschützt. Die Sicherheit des Computers hängt folglich von mehr als nur einem perfekten Virenschutz ab.

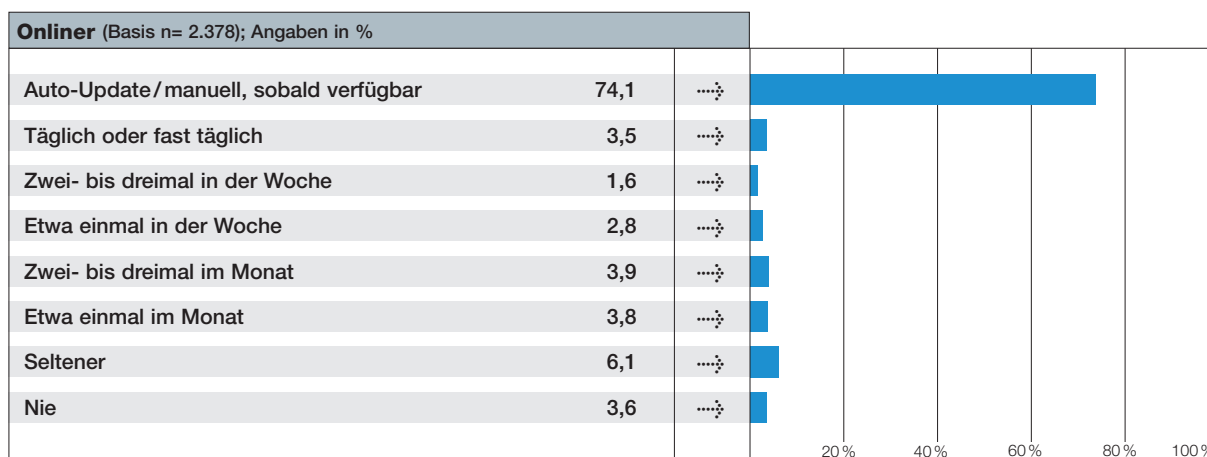
Schutz vor Viren / Schadsoftware – Top-Two* nach Merkmalen



Personen, die sich vor Viren und Schadsoftware geschützt fühlen, schätzen auch ihre allgemeine Computersicherheit positiver ein. Zudem spielt beim Thema „Viren und Schadsoftware“ der Wissensstand zum Internet und besonders zur Sicherheit im Internet eine wichtige Rolle.

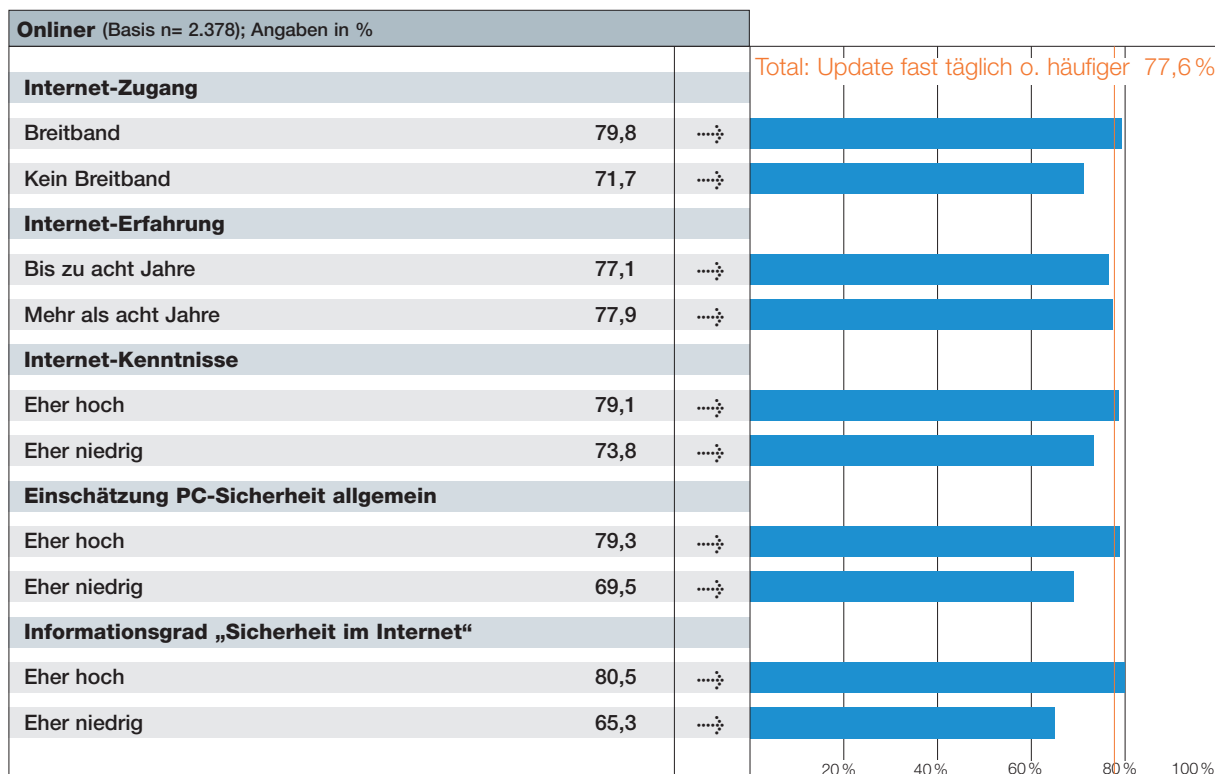
Pflege des Betriebssystems

Frage: Wie häufig führen Sie eine Aktualisierung (ein Update) Ihres Betriebssystems aus?



Die zeitnahe Aktualisierung des Betriebssystems ist äußerst wichtig, um gegen Angriffe durch Viren und Schadsoftware gewappnet zu sein. Daher ist es sehr erfreulich, dass sich die automatische bzw. zeitnahe Aktualisierung zum allgemein akzeptierten Standard entwickelt. Aktualisierungen in größeren Zyklen werden eher von einer Minderheit vorgenommen.

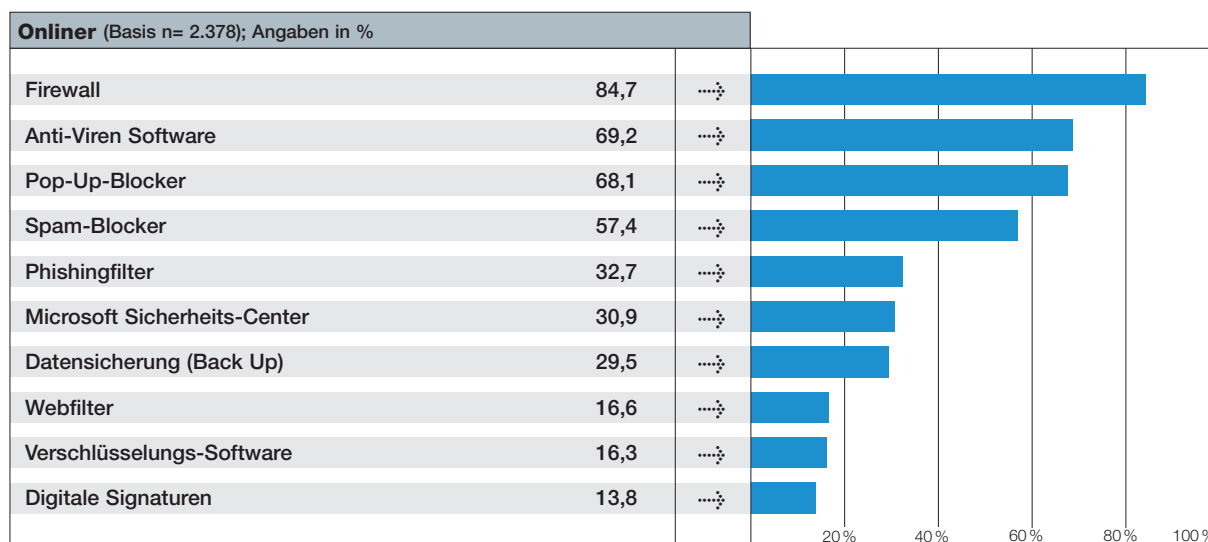
Pflege des Betriebssystems – „Update fast täglich oder häufiger“ nach Merkmalen



Zusätzlich zum Informationsgrad „Sicherheit im Internet“, der Sicherheitseinschätzung des PCs und den allgemeinen Internetkenntnissen hat die Zugangsform zum Internet einen Einfluss auf das Aktualisierungsverhalten. Die Breitbandnutzer aktualisieren ihr Betriebssystem häufiger als Befragte, die sich beispielsweise über Modem ins Internet einwählen. Die zunehmende Verbreitung von Breitbandanschlüssen hat somit auch einen positiven Effekt auf die Sicherheit der genutzten Betriebssysteme.

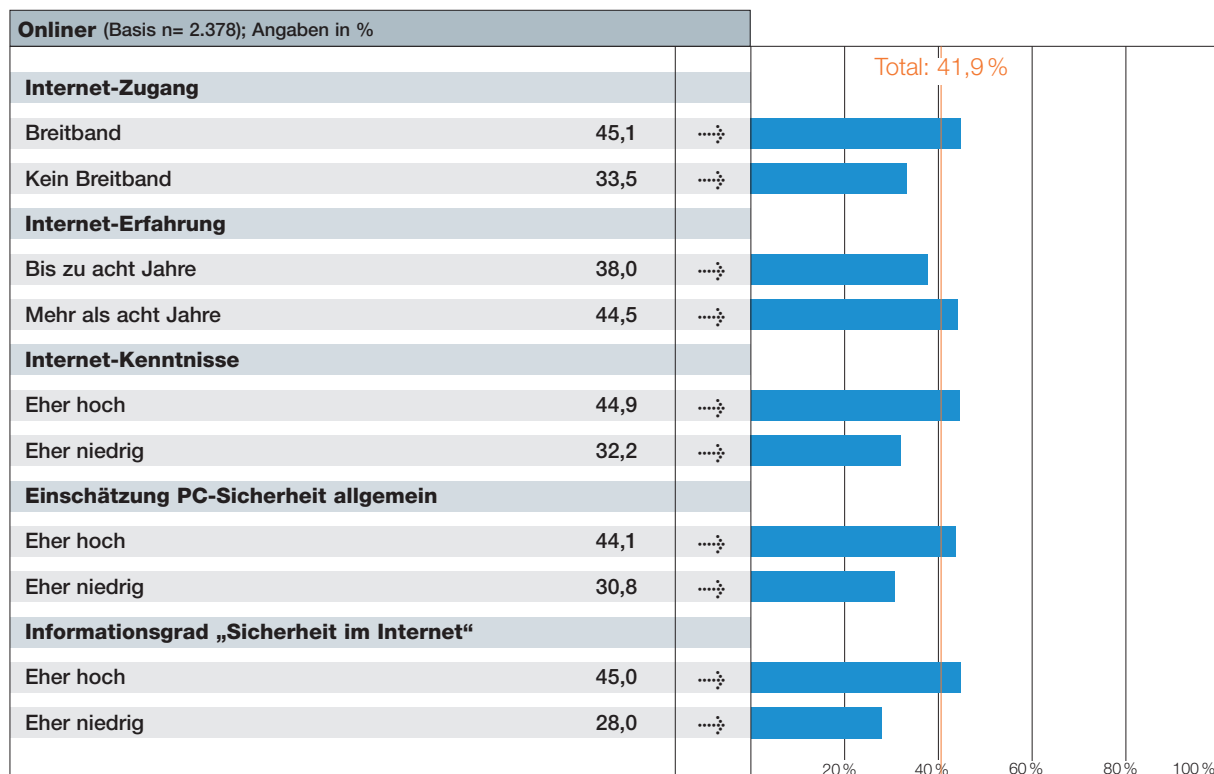
Nutzung von Sicherheitssystemen

Frage: Bitte geben Sie zu jedem Sicherheitssystem an, ob Sie dieses derzeit aktiv nutzen.



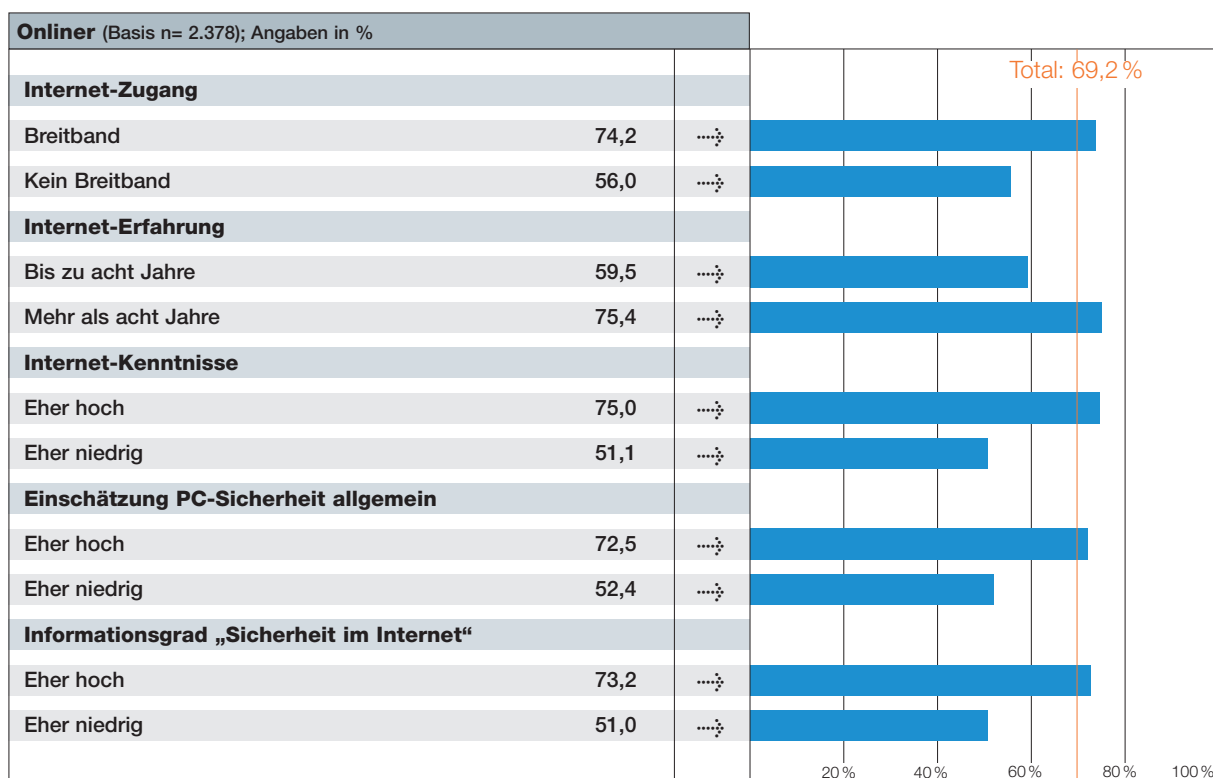
Auch bei der Nutzung der Sicherheitssysteme ist ein sehr positiver Trend zu beobachten. Knapp 85 Prozent der Onliner nutzen eine Firewall und ca. 70 Prozent haben eine Anti-Viren-Software auf ihrem Computer installiert. Der Unterschied von etwa 15 Prozentpunkten zwischen Firewall und Anti-Viren-Software ließe sich unter anderem damit erklären, dass in modernen Betriebssystemen bereits eine Firewall integriert ist. Digitale Signaturen und Verschlüsselungssoftware werden bisher nur selten genutzt.

Nutzung von Sicherheitssystemen – alle Sicherheitssysteme



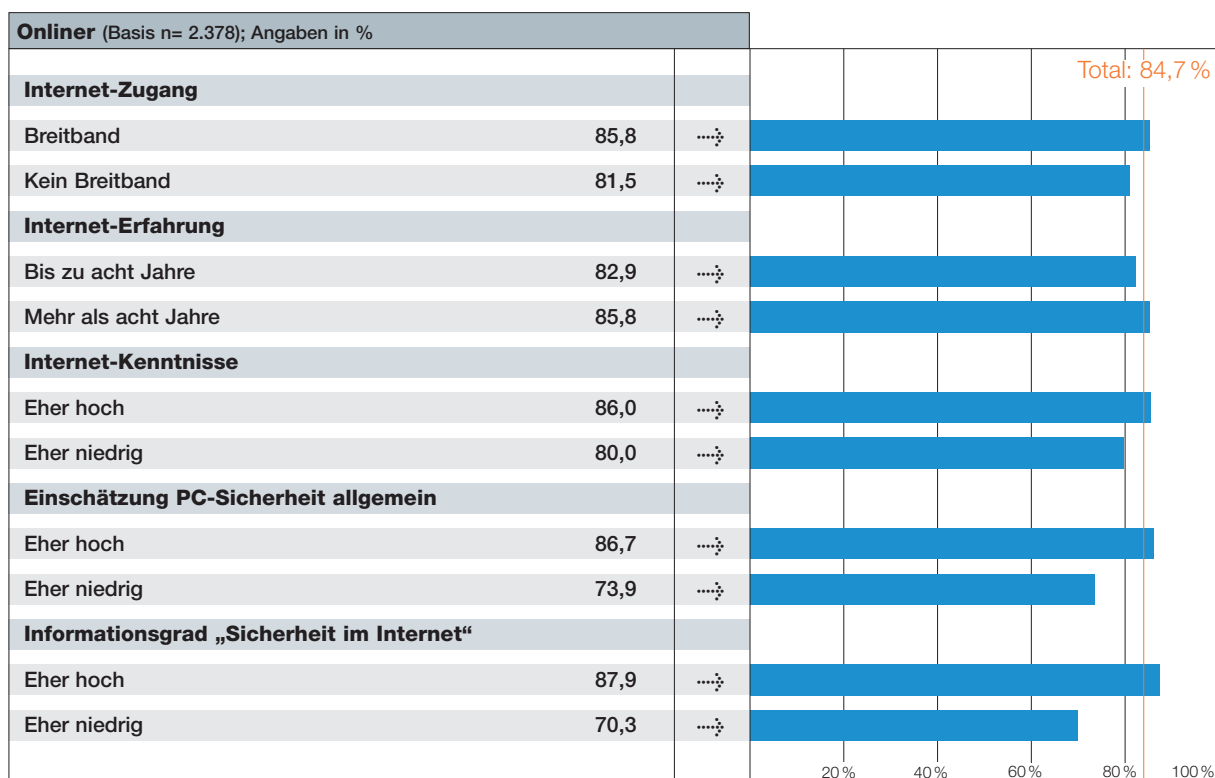
Bei der Verwendung von Sicherheitssystemen zeigt sich in der Gesamtbetrachtung, dass der Informationsgrad „Sicherheit im Internet“ zum größten Unterschied in der Nutzung von Sicherheitssystemen führt. Aber auch die übrigen Segmentierungsansätze zeigen deutliche Unterschiede bei der Nutzung der Sicherheitssysteme.

Nutzung von Sicherheitssystemen – Software zum Schutz vor Viren



In der gezielten Auswertung zur Nutzung eines Virenschutzes ergeben sich für alle analysierten Einflussfaktoren deutliche Nutzungsunterschiede. Eher hohe bzw. eher niedrige Internet-Kenntnisse führen zu den größten Unterschieden in der Nutzung von Sicherheitssoftware gegen Viren.

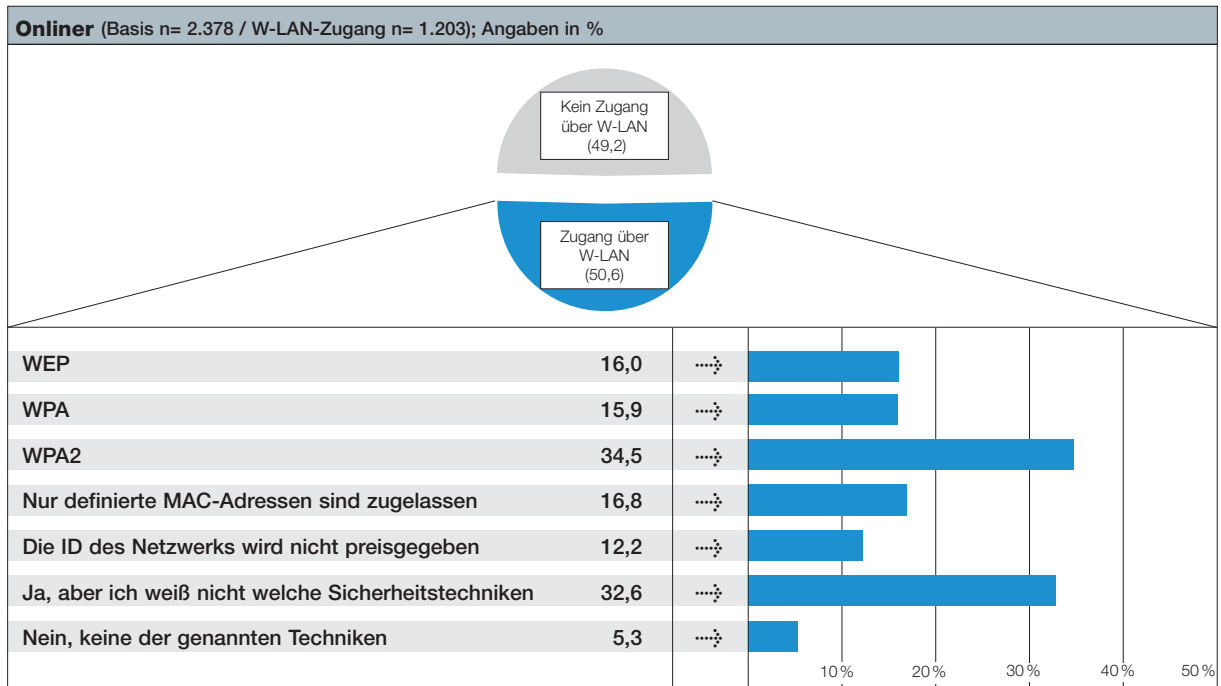
Nutzung von Sicherheitssystemen – Firewall



Die Nutzung einer Firewall wird vom Wissen über Internetsicherheit am deutlichsten beeinflusst. Bemerkenswert ist hier, dass die Breitbandnutzung – die häufig einen Router mit integrierter Firewall nach sich zieht – nur einen geringen Einfluss auf die Nutzung einer Firewall ausübt. Daher ist davon auszugehen, dass die Firewall des Betriebssystems eine größere Rolle im Bewusstsein der Befragten einnimmt.

Zugangsgeschwindigkeit / Nutzung von W-LAN-Sicherheitstechniken

Frage: Bitte geben Sie zu jedem Sicherheitssystem an, ob Sie dieses derzeit aktiv nutzen.

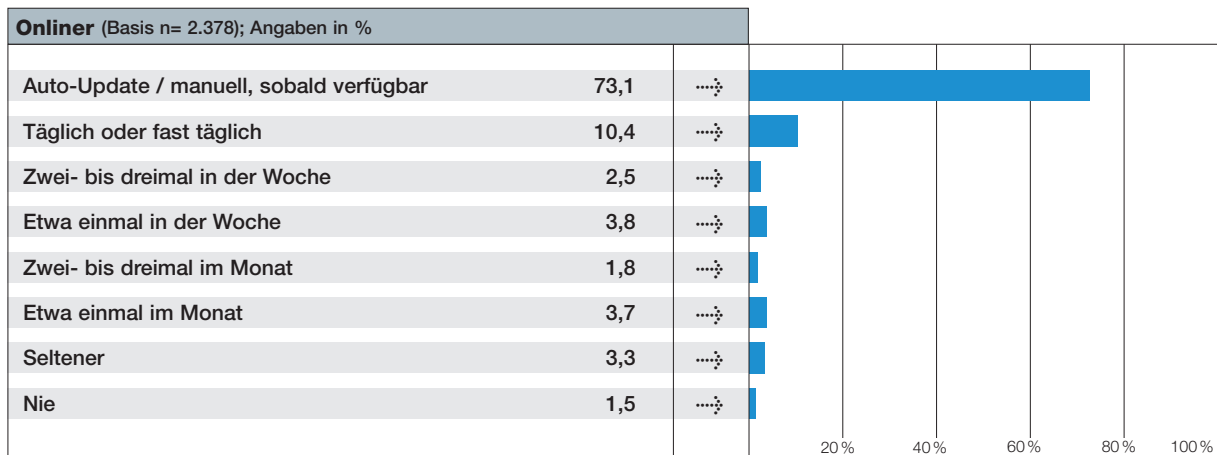


Über die Hälfte der Onliner (50,6 Prozent) nutzen ein W-LAN, um eine Verbindung mit dem Internet herzustellen. Beim W-LAN kommen nun die Sicherheitstechniken des Routers zum Einsatz. Ungeschützte Funknetzwerke sind 2008 beinahe die Ausnahme (5,3 Prozent). Immerhin 66,4 Prozent der Befragten wissen, dass ihr W-LAN mit einem Passwortschutz belegt ist. Weitere 32,6 Prozent wissen zwar, dass ihr drahtloses Netzwerk geschützt ist, können jedoch die genutzten Sicherheitstechniken nicht benennen. Hier ist anzunehmen, dass sie das W-LAN nicht selbst eingerichtet haben.

Auch wenn das Gesamtergebnis sehr erfreulich ist, sollte es Ziel sein, die derzeit verbleibenden fünf Prozent ohne Sicherheitstechniken von einem sicheren Umgang mit dem Computer zu überzeugen.

Aktualisierung der Software zum Schutz vor Viren / Schadsoftware

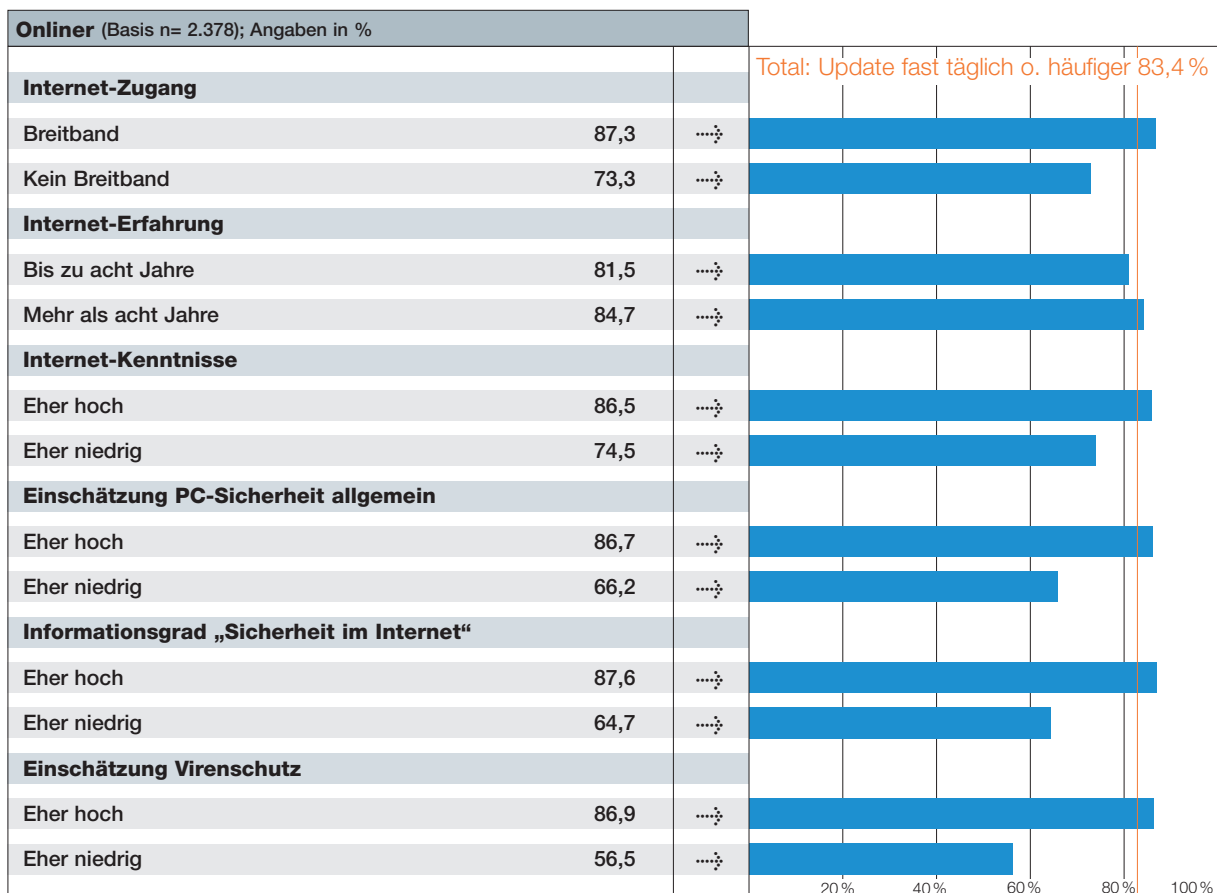
Frage: Wie oft aktualisieren Sie die Software zum Schutz vor Viren und anderer Schadsoftware durch Updates?



Ähnlich wie beim Betriebssystem lässt sich bei der Aktualisierung von Virenschutz und Programmen zur Bekämpfung von Schadsoftware ein sehr positiver Trend ablesen. Insgesamt 73,1 Prozent der Onliner aktualisieren ihre Schutzsoftware entweder sobald ein Update vorhanden ist oder sogar automatisch. Ein weiterer Anteil von 10,4 Prozent gibt an, täglich oder fast jeden Tag die Schutzprogramme zu aktualisieren. Damit sind insgesamt 83,5 Prozent der Onliner meist auf dem aktuellsten Stand.

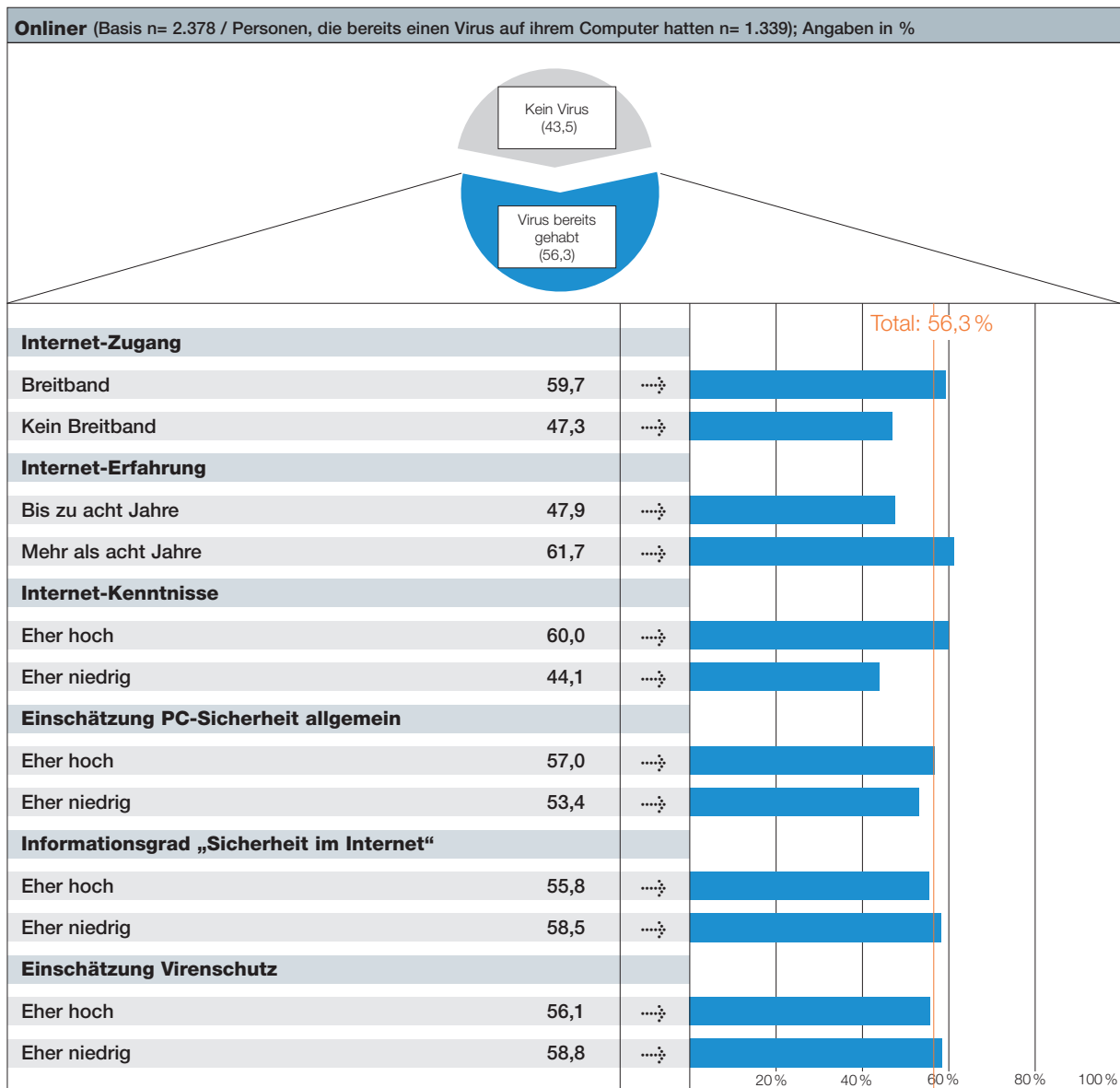
Diese Personen schätzen tendenziell sowohl ihre Computersicherheit als auch ihren Virenschutz höher ein. Sie nutzen häufiger einen Breitbandanschluss und sind über Sicherheitsthemen besser informiert.

Aktualisierung der Software zum Schutz vor Viren / Schadsoftware – „Update fast täglich oder häufiger“ nach Merkmalen



Vorhandensein eines Virus / Schadsoftware

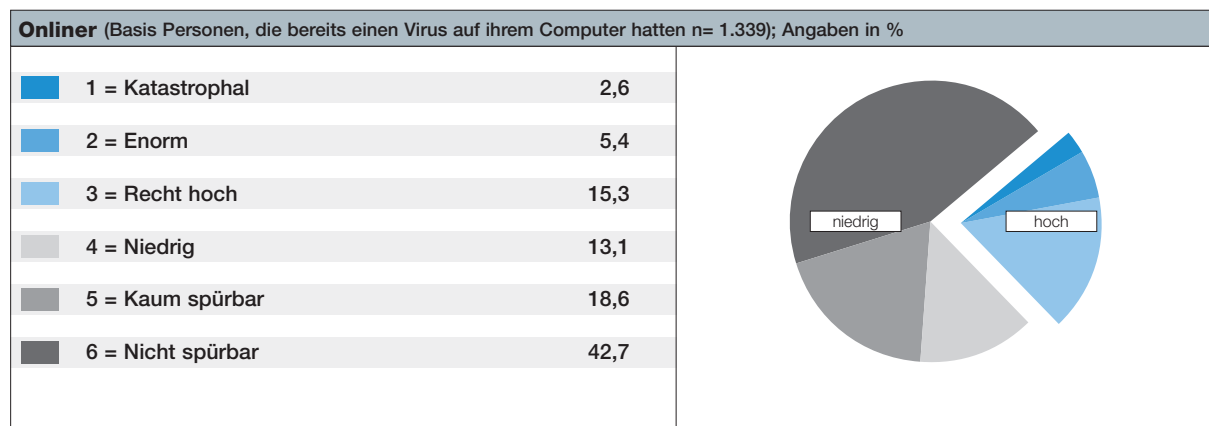
Frage: Hatten Sie schon einmal einen Virus oder eine andere Schadsoftware (ein „Schadprogramm“) auf Ihrem Computer?



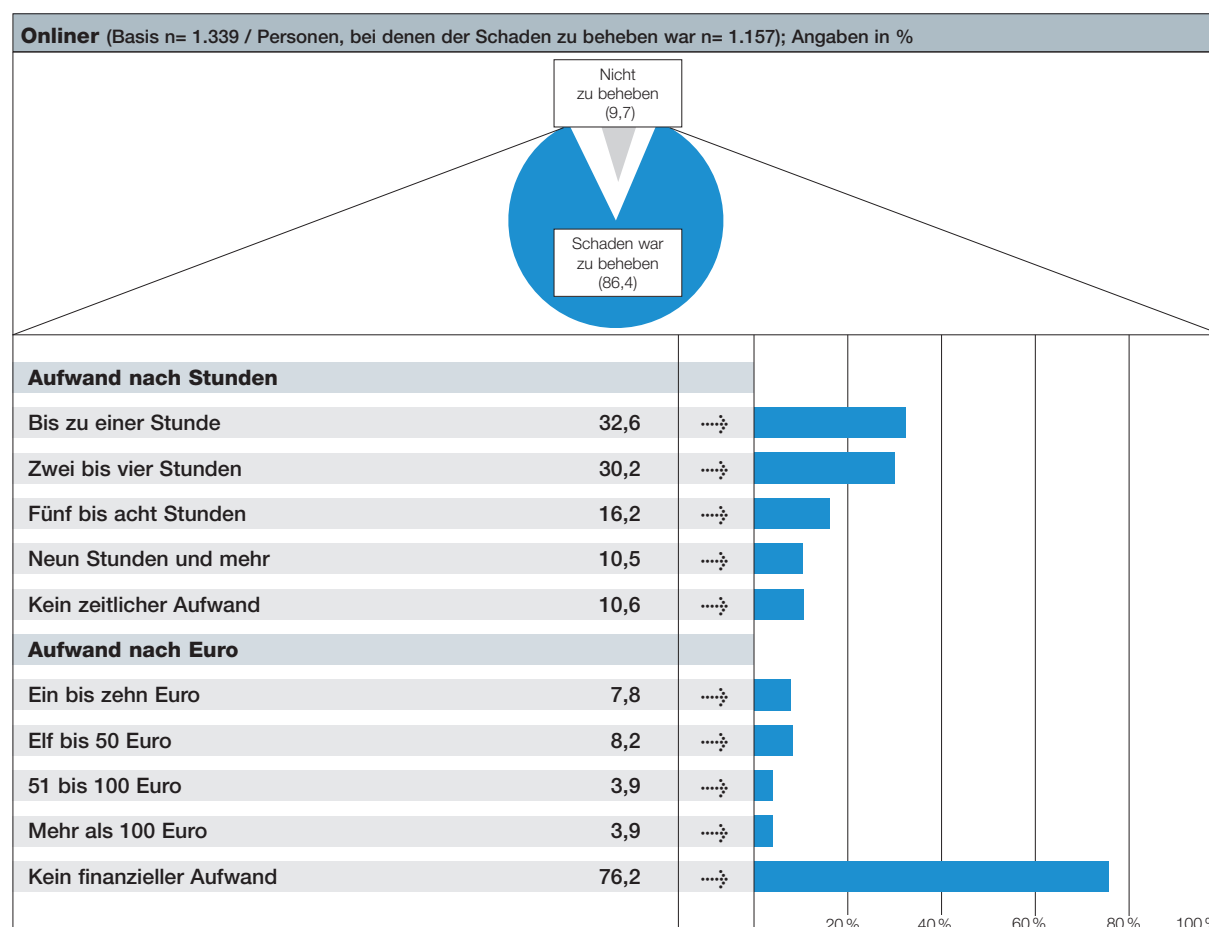
Die Zunahme der genutzten Schutzmaßnahmen und die häufigere Aktualisierung der Sicherheitssoftware sind mögliche Gründe dafür, dass der Anteil von Personen, die bereits einen Virus auf ihrem derzeitigen Rechner hatten, erneut zurückgeht. In diesem Jahr geben 56,3 Prozent der Befragten an, bereits einen Virus auf ihrem Rechner gehabt zu haben. In den Jahren zuvor waren es noch 63,4 Prozent (2007) und 64,8 Prozent (2006). Personen, die bereits einen Virus oder Schadsoftware hatten, scheinen sich häufiger im Internet zu bewegen. Sie verfügen eher über einen Breitbandanschluss, nutzen das Internet meist länger als acht Jahre und schätzen ihre Internetkenntnisse überdurchschnittlich hoch ein.

Höhe des Schadens / Aufwand für Schadensbeseitigung

Frage: Wie hoch war der für Sie persönlich entstandene Schaden durch dieses Schadprogramm? / Welcher Aufwand an Zeit und Geld war mit der Behebung dieses Schadens für Sie persönlich verbunden? (Selektion: Personen, die bereits Virus / Schadprogramme auf ihrem Computer hatten)



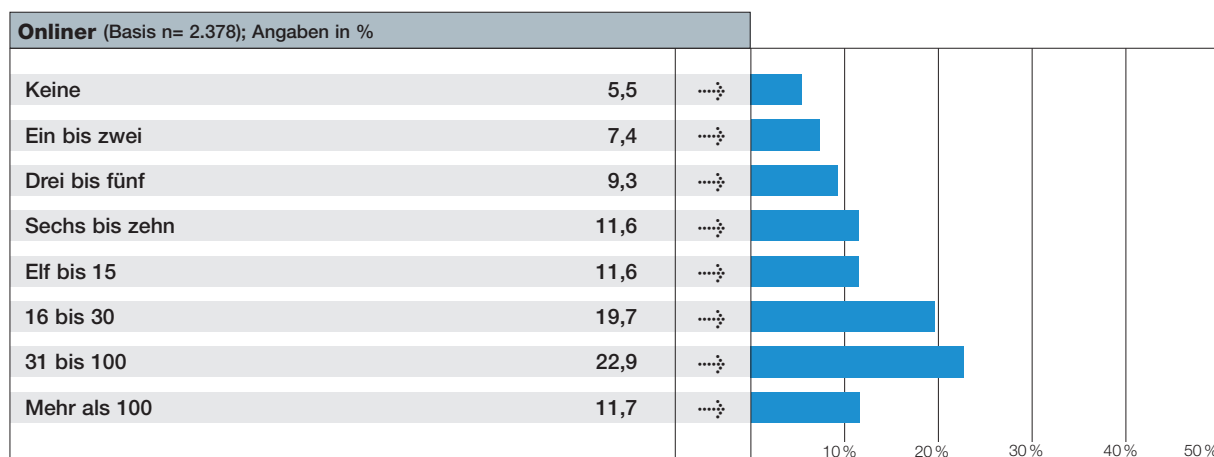
Ein großer Teil der Befragten (42,7 Prozent) gibt an, dass der Schaden durch den letzten Virus bzw. die letzte Schadsoftware nicht spürbar war. Dieser Anteil ist im Vergleich zu 2007 gestiegen. Es ist jedoch voreilig anzunehmen, Viren und Schadsoftware seien ungefährlicher geworden, nur weil in vielen Fällen kein Schaden zu spüren war. Die Wirkungsweise der Viren hat sich entscheidend geändert. Aktuell werden Viren so programmiert, dass sie möglichst unerkannt bleiben, um ungehindert auf Ressourcen zuzugreifen oder Nutzerinformationen auszuspähen. Es gibt keinen Grund zur Entwarnung, denn für 23,3 Prozent der Onliner war der Schaden recht hoch und für 2,6 Prozent sogar katastrophal (2,7 Prozent in 2007).



In knapp zehn Prozent der Fälle ließ sich der Schaden durch Computerviren und Schadsoftware nicht wieder beheben! War der Schaden durch Zeitaufwand wieder gut zu machen, wurden im Durchschnitt 5,2 Stunden für die Beseitigung benötigt. Wenn bei der Beseitigung finanzieller Aufwand entstand, betrug dieser im Durchschnitt 69 Euro.

Schätzung Anzahl Spam-Mails

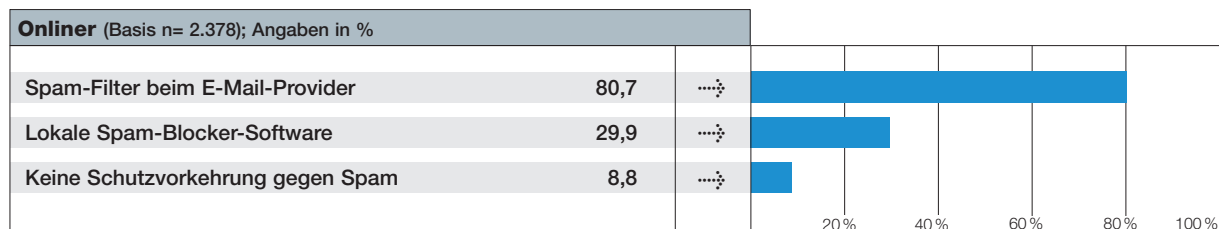
Frage: Spam-Mails sind Werbe-E-Mails, die unaufgefordert und massenhaft versendet werden. Was schätzen Sie, wie viele so genannte Spam-Mails bekommen Sie durchschnittlich in einer Woche an Ihre private(n) E-Mail-Adresse(n)?



Die Spam-Problematik hat sich im Vergleich zum Vorjahr leicht entspannt. Dennoch werden bei 11,7 Prozent der Onliner die Postfächer mit über 100 Spam-Mails pro Woche überflutet. 34,6 Prozent der Befragten geben an, 30 und mehr unerwünschte E-Mails in der Woche zu erhalten.

Schutzvorkehrungen gegen Spam-Mails

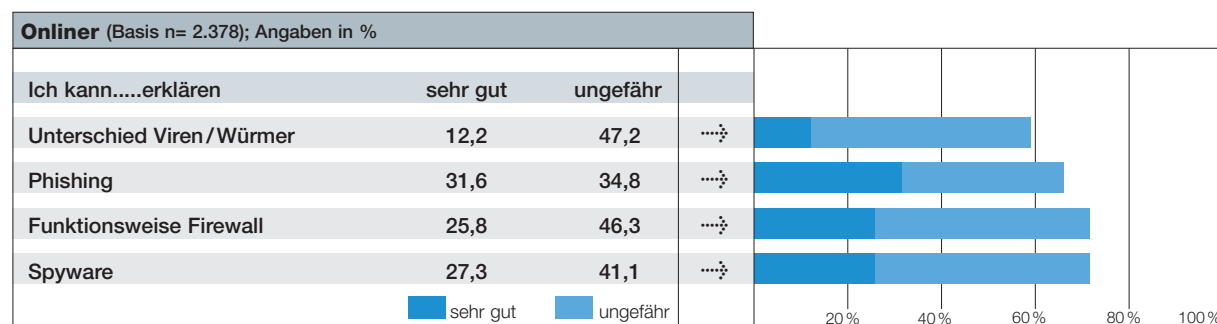
Frage: Welche Schutzvorkehrungen gegen Spam-E-Mails nutzen Sie?



Lediglich 8,8 Prozent der Onliner ergreifen keine Maßnahmen gegen Spam. Insgesamt 80,7 Prozent nutzen den Spam-Schutz ihres Providers und 29,9 Prozent haben einen Spam-Blocker lokal auf dem Rechner installiert. Dennoch erhalten über drei Viertel der Onliner mindestens sechs – meist jedoch deutlich mehr – unerwünschte E-Mails pro Woche.

Kenntnisse IT-Sicherheit

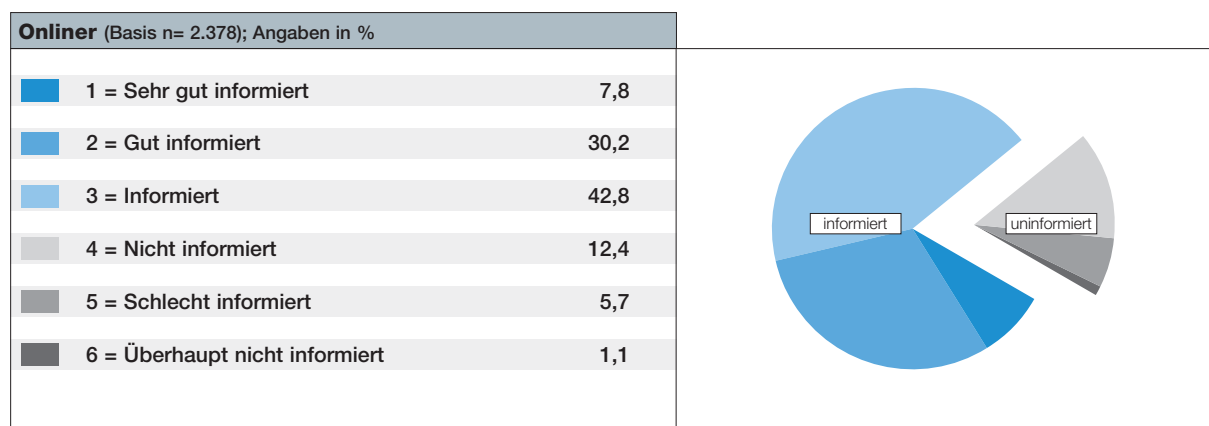
Frage: Die für die IT-Sicherheit wichtigen Begriffe sind ja nicht immer leicht zu verstehen und oft noch schwerer zu erklären. Was meinen Sie, welche Aussagen treffen am ehesten auf Sie zu? Könnten Sie die folgenden Begriffe einem Bekannten oder einer Bekannten erklären, ohne vorher entsprechende Unterlagen zu Rate zu ziehen?



Die Firewall liegt nicht nur bei der Nutzung vorne, auch die Kenntnisse zum Thema Firewall sind am weitesten verbreitet. Viele Onliner (72,1 Prozent) können ungefähr erklären, wie eine Firewall funktioniert. Was Spyware (68,4 Prozent) und Phishing (66,4 Prozent) sind, können noch immer etwa zwei Drittel der Onliner erklären. Spezialfragen, wie z. B. der Unterschied zwischen Würmern und Viren, sind schwieriger. Nur 12,2 Prozent der Onliner können diesen Unterschied sehr gut erklären, 47,2 Prozent trauen sich eine ungefähre Erklärung zu.

Informationsgrad „Sicherheit im Internet“

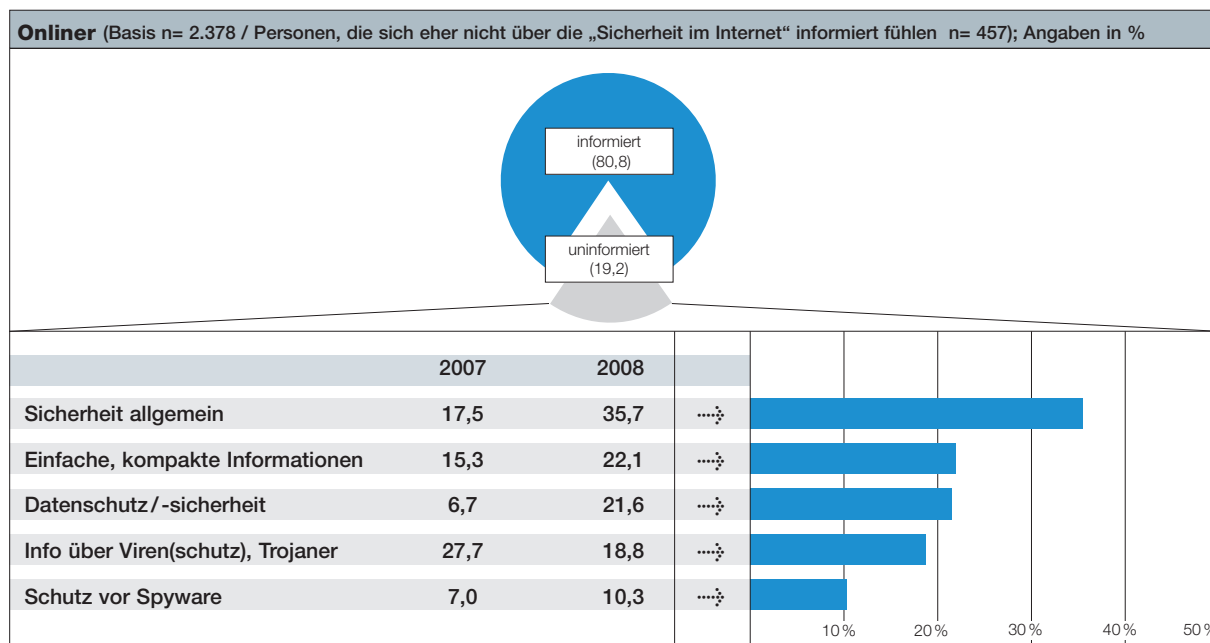
Frage: Wie gut fühlen Sie sich persönlich über das Thema „Sicherheit im Internet“ informiert?



Während sich 38,0 Prozent der Onliner gut bis sehr gut über das Thema „Sicherheit im Internet“ informiert fühlen, gibt die Mehrheit an, nur mittelmäßig oder schlecht informiert zu sein (62,0 Prozent). Im Vergleich zum Vorjahr sind tendenziell weniger Onliner gut informiert.

Informationsbedarf „Sicherheit im Internet“

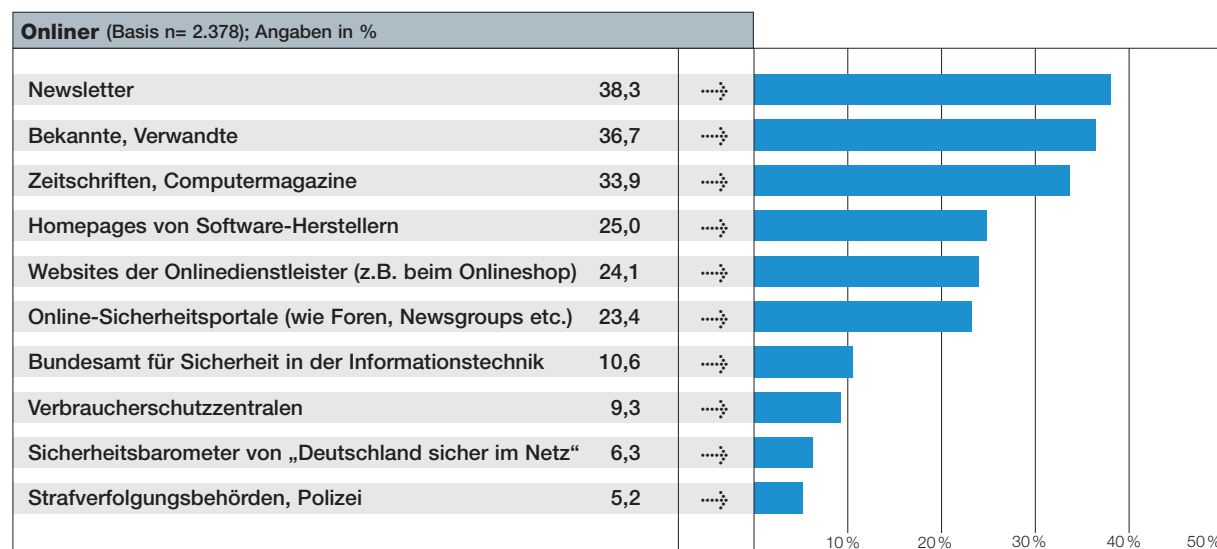
Frage: Sie haben gerade angegeben, dass Sie sich nicht so gut über das Thema „Sicherheit im Internet“ informiert fühlen. Worüber würden Sie bei diesem Thema gerne mehr wissen? Notieren Sie bitte alles, was Ihnen einfällt.



Die sinkende Tendenz des Informationsgrades erklärt sich zumindest teilweise aus einem veränderten Informationsbedürfnis. Im Vergleich zum Vorjahr steigt das Interesse zum Thema Datenschutz sehr deutlich (Unterschied: 14,9 Prozentpunkte). Auch wird die Sicherheit im Allgemeinen stärker thematisiert. Bei 35,7 Prozent der Befragten herrscht ein Informationsdefizit zur allgemeinen Sicherheit. Zudem wünschen sich 22,1 Prozent der Befragten einfache und kompakte Informationen. Einzig die Bedeutung von Viren und Trojanern nimmt im Vergleich zum Vorjahr ab.

Nutzungshäufigkeit von Informationskanälen

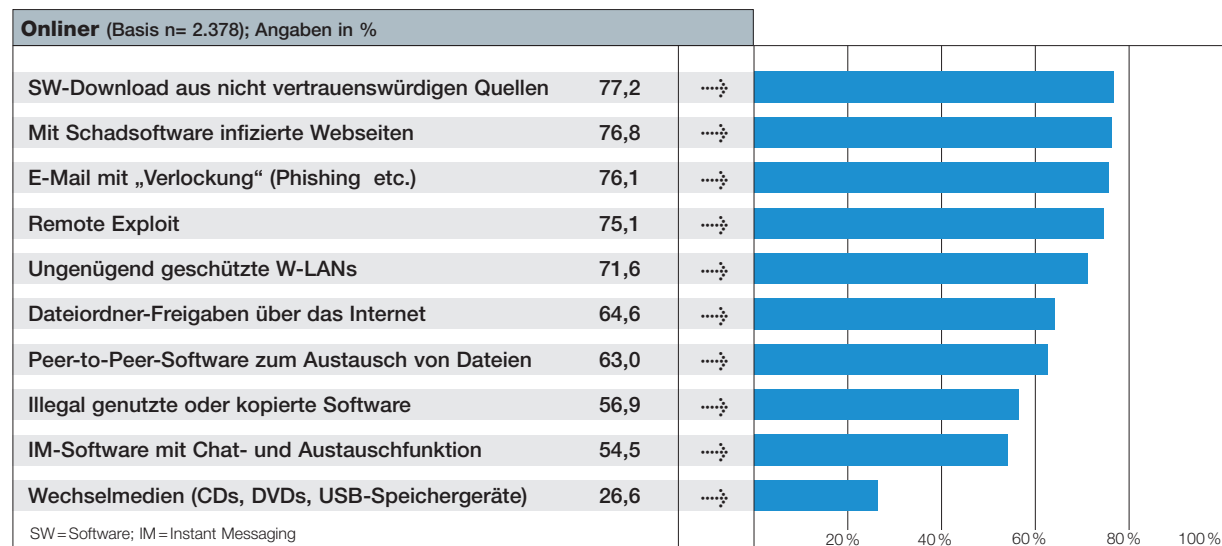
Frage: Wie häufig nutzen Sie jede der folgenden Informationsquellen, um sich über aktuelle Sicherheitsprobleme wie Viren, Würmer, Tricks von Betrügern usw. zu informieren?



Die wichtigsten Informationskanäle zum Thema „Sicherheit im Internet“ sind Newsletter, Bekannte, Verwandte und themenspezifische Zeitschriften. Die Bedeutung der Newsletter gewinnt verglichen mit dem Vorjahr an Bedeutung. Die Relevanz von Bekannten und Verwandten nimmt leicht ab. Im Mittelfeld liegen Websites verschiedener Anbieter, die gezielt zur Informationssuche aufgesucht werden. Weniger als zehn Prozent der Onliner nutzen die Informationsquellen von Verbraucherschutzzentralen oder der Polizei.

Top-Two-Risikoeinschätzung bzgl. Gefährdungen

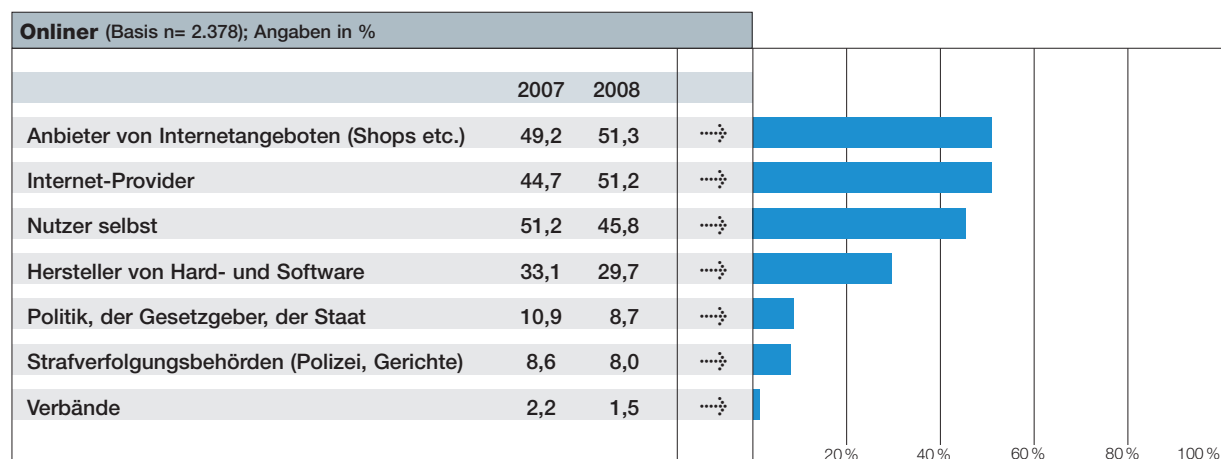
Frage: Sie sehen nun eine Liste, auf der verschiedene Gefährdungen der Computersicherheit. Bitte geben Sie auf einer Skala von 1 = geringes Risiko bis 6 = hohes Risiko an, für wie riskant Sie persönlich diese halten.



Die Risikoeinschätzung der deutschen Onliner zu den abgefragten Gefährdungen ist – wie schon im Vorjahr – plausibel. Die größten Risiken werden dem Softwaredownload aus vertrauensunwürdigen Quellen, Besuchen von infizierten Webseiten, per E-Mail verschickten „Verlockungen“ und Remote Exploits (gezielte Attacken aus dem Internet) zugeschrieben. Bei diesen Gefahren handelt es sich stets um bösartige Angriffe, die gezielt menschliche oder technische Schwächen ausnutzen. Darauf folgen Attacken auf „selbst verschuldete“ Sicherheitslücken. Ungeschützte W-LANs, versehentlich für das Internet freigegebene Ordner und Peer-to-Peer-Software lassen sich vermeiden und gehören ebenfalls zu den äußerst gefährlichen Risiken. Eine geringe Risikoeinschätzung für Wechseldatenträger setzt voraus, dass nur Medien von vertrauenswürdigen Personen oder Anbietern genutzt werden. Aus technischer Sicht können auch USB-Sticks, CDs und DVDs erheblichen Schaden anrichten. In der Regel werden solche Medien jedoch nur aus sicheren Quellen bezogen.

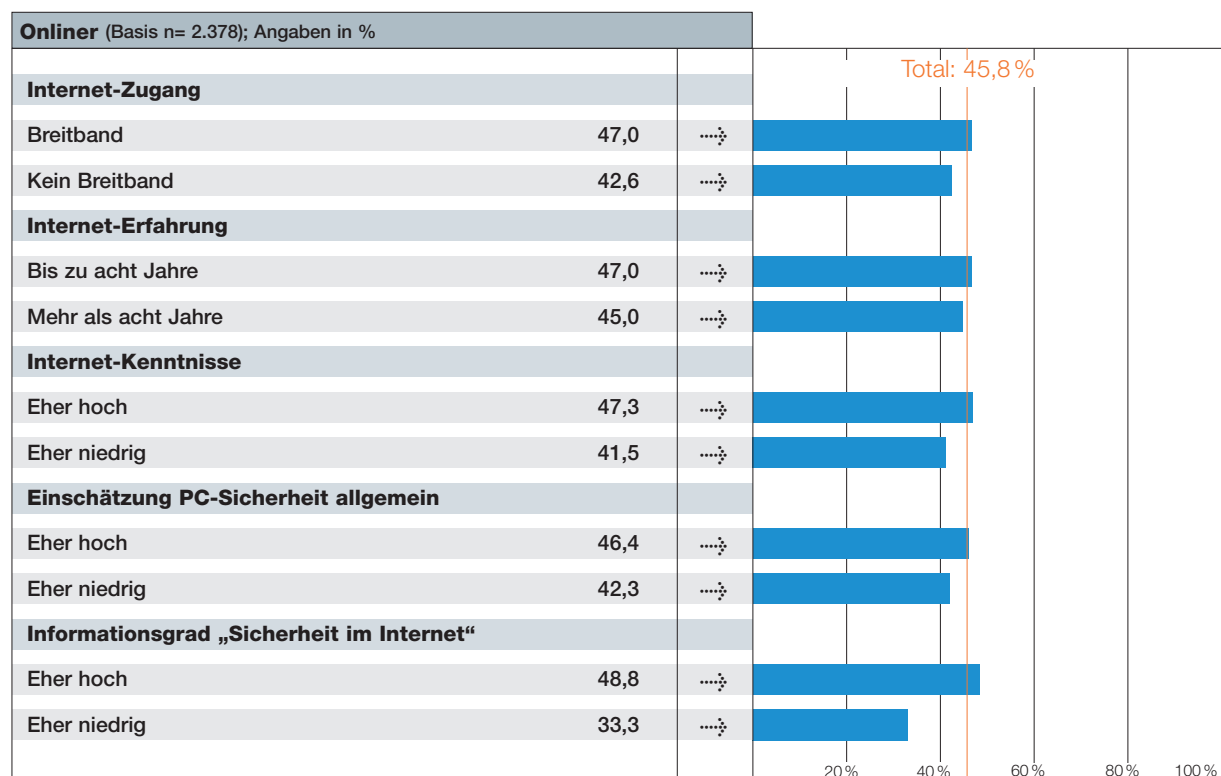
Verantwortung für Sicherheit im Internet – Rang 1 oder 2

Frage: Inwieweit sind die folgenden Institutionen, Betreiber oder Personen für die allgemeine Sicherheit im Internet verantwortlich? Bitte vergeben Sie die Werte 1, 2, 3, 4, 5, 6, 7. Eine 1 bedeutet: ist am meisten für die Sicherheit im Internet verantwortlich, eine 2 bedeutet: besitzt die zweitgrößte Verantwortung usw.



Im Verantwortungsbewusstsein der deutschen Onliner lassen sich Veränderungen erkennen. Wurde 2007 noch dem Nutzer selbst die größte Verantwortung für Computersicherheit zugeschrieben, treten 2008 die Anbieter von Internetangeboten und die Internet-Provider an diese Stelle. Die größten Gefahren resultieren aus der Vernetzung der Computer. Angriffe über das weltweite Netz sind wohl in der Zwischenzeit so komplex geworden, dass die Nutzer bereit sind, die Verantwortung für Sicherheit auf einen Dienstleister zu übertragen.

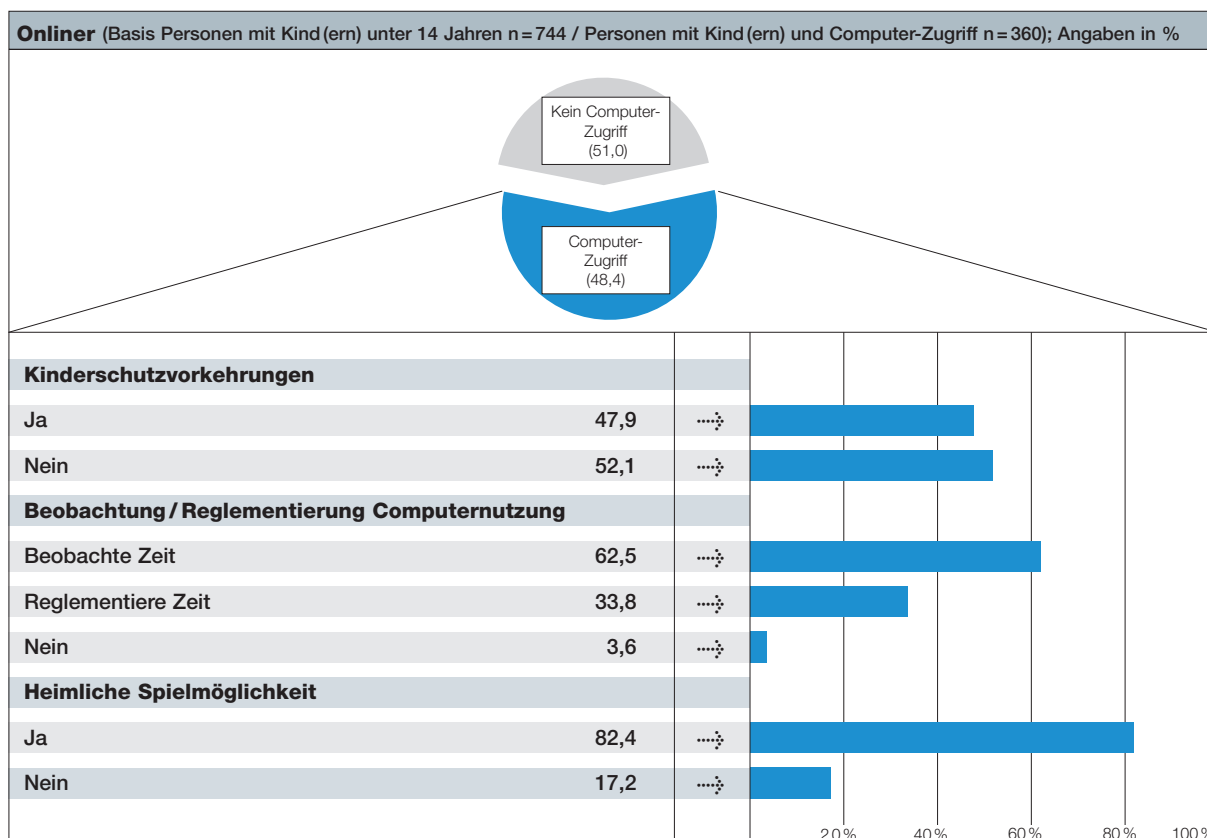
Verantwortung für Sicherheit im Internet – „Nutzer selbst“ nach Merkmalen



Je geringer der Informationsgrad „Sicherheit im Internet“, desto eher sind die deutschen Onliner bereit, die Verantwortung abzugeben. Lediglich 33,3 Prozent mit eher niedrigem Informationsgrad sehen hauptsächlich sich selbst in der Verantwortung für die Sicherheit im Internet. Auch Befragte mit niedrigen Internetkenntnissen, einem Modem- oder ISDN-Anschluss und einer niedrigen Einschätzung ihrer PC-Sicherheit sehen sich selbst weniger in der Verantwortung.

Kinder unter 14 Jahren mit Zugriff auf Computer / Schutz der Kinder

Frage: Hat Ihr Kind / mindestens eines Ihrer Kinder unter 14 Jahren Zugriff auf einen Computer in Ihrem Haushalt? Benutzen Sie spezielle Software oder Einstellungen im Browser zum Schutz Ihres Kindes / Ihrer Kinder, wenn es Ihren Computer nutzt / diese Ihren Computer nutzen?
Beobachten und reglementieren Sie die Zeit, die Ihr Kind / Ihre Kinder am Computer verbringt / verbringen? Glauben Sie, dass es einem durchschnittlichen Kind ohne das Wissen seiner Eltern möglich wäre, zuhause jugendgefährdende Computerspiele zu spielen?



Der Anteil der Eltern, die technische Vorkehrungen zum Schutz ihrer Kinder am Computer vornehmen, ist von 43,1 Prozent (2007) auf 47,9 Prozent (2008) gestiegen. Damit schützen nun beinahe die Hälfte der Eltern ihre Kinder mit Hilfe von spezieller Software oder bestimmten Browsereinstellungen.

Insgesamt 33,8 Prozent der befragten Eltern mit Kindern unter 14 Jahren reglementieren die Zeit ihrer Kinder vor dem Computer. Ein weit größerer Anteil (62,5 Prozent) beobachtet die Zeit ihrer Kinder vor dem Rechner. Nur ein sehr kleiner Teil der Kinder (3,6 Prozent) nutzt den Computer vollkommen unbeaufsichtigt.

Dennoch glauben 82,4 Prozent der befragten Eltern, dass ein durchschnittliches Kind jugendgefährdende Spiele am Computer spielen kann, ohne dass es die Eltern des Kindes bemerkt. Diese alarmierend hohe Zahl deutet darauf hin, dass sich viele Eltern mit der Regulierung des Nutzungsverhaltens der Kinder überfordert fühlen.

Ansprechpartner:

Presse- und Öffentlichkeitsarbeit:

Thomas Baumgärtner

Pressesprecher Security, Green IT, Issues
Microsoft Deutschland GmbH
Telefon 089 / 31 76 500
thomba@microsoft.com

Daniel Ott

Presse- und Öffentlichkeitsarbeit
Initiative D21 e.V.
Telefon 030 / 526 87 22 55
daniel.ott@initiated21.de

Projektleitung und Redaktion:

Matthias Peterhans

TNS Infratest GmbH
Telefon 089 / 56 00 1909
matthias.peterhans@tns-infratest.com

Impressum:

Herausgeber:

Microsoft Deutschland GmbH
www.microsoft.de

Initiative D21 e.V.
www.initiated21.de

Gestaltung und Produktion:

Kathleen Susan Hiller
viaduct b.
www.viaduct-b.de

Druck:

Königsdruck
www.koenigsdruck.de

