



Befragung von Verbrauchern zur Cybersicherheit

Die zunehmende Notwendigkeit eines angemessenen Datenschutzes

Inhalt

Einführung	3
Ergebnisse	4
Erkenntnis 1: Die Verbraucher interessieren sich für Datenschutz und ein überraschend hoher Anteil von ihnen hat bereits Maßnahmen zum Datenschutz ergriffen	4
Erkenntnis 2: Die Datenschutzrichtlinie bildet die Grundlage für Innovation und hilft dabei, Vertrauen aufzubauen.	7
Erkenntnis 3: Die Verbraucher wissen die Rolle der Regierung bei der Regulierung der Verwendung personenbezogener Daten zu schätzen. Die DSGVO ist in ihren Augen eine gute Sache	9
Erkenntnis 4: Viele Verbraucher glauben, sie seien nicht in der Lage, ihre personenbezogenen Daten zu schützen. Für sie besteht die größte Herausforderung darin, herauszufinden, was genau die Unternehmen mit ihren Daten machen	11
Fazit	13
Über die Cisco Reihe zur Cybersicherheit	14

Einführung

Die meisten Nutzer verstehen, dass es heute von Vorteil und häufig notwendig ist, Unternehmen und Anwendungen bestimmte persönliche Informationen zur Verfügung zu stellen, um die Vorteile von Produkten, Services und Geschäftsbeziehungen zu genießen. Gleichzeitig zeigen sie sich zunehmend um den Schutz ihrer Privatsphäre und personenbezogener Daten besorgt.

Es gab immer wieder Schlagzeilen, die vermeldeten, es seien hunderte Millionen personenbezogener Datensätze durch Daten-schutzverletzung offengelegt worden. Unternehmen hatten die personenbezogenen Daten ihrer Kunden verarbeitet, ohne diese vorher zu informieren oder um ihr Einverständnis zu bitten. Vor diesem Hintergrund hat das Cisco Privacy Office erforscht, was Unternehmen, die Regierung und Einzelpersonen aus Sicht des Endkunden (In diesem Text „Verbraucher“ genannt), unternommen haben oder noch unternommen werden, um deren Privatsphäre zu respektieren und zu schützen.

Die Cisco Studie zum Verbraucherdatenschutz verwendet Daten, die im Mai 2019 im Rahmen einer Doppelblindstudie erfasst wurden. An der Umfrage haben 2600 Erwachsene in 12 der weltweit größten Volkswirtschaften teilgenommen – davon fünf in Europa, vier im asiatisch-pazifischen Raum und drei in Nord- und Südamerika.¹ Das Profil der Befragten umfasst verschiedene Altersgruppen, Geschlechter und Einkommensstufen. Die Teilnehmer wurden zu ihren Einstellungen und Verhaltensweisen in Bezug auf personenbezogene Daten, die Produkte und Services, die sie nutzen, ihr Vertrauen in potenzielle neue Geschäftsmodelle und die Auswirkungen der Datenschutzbestimmungen auf ihr Verhalten befragt.

Die Ergebnisse dieser Studie sowie frühere Untersuchungen von Cisco zeigen eine neue Landschaft, in der Datenschutz zu einem absoluten Muss bei jeglicher Geschäftstätigkeit geworden ist und auch beim Verhalten der Kunden eine entscheidende Rolle spielt. In dieser Abhandlung geht es um vier verschiedene Erkenntnisse:

- Die Verbraucher interessieren sich für Datenschutz. Eine überraschende Mehrheit hat bereits Maßnahmen zum Datenschutz ergriffen.

- Datenschutzbestimmungen bilden die Grundlage für Innovation und helfen, Vertrauen aufzubauen.
- Die Verbraucher wertschätzen die Rolle der Regierung bei der Regulierung der Nutzung personenbezogener Daten und sehen die Datenschutzgrundverordnung (DSGVO) der EU als Gewinn an.
- Viele Verbraucher glauben, sie seien nicht in der Lage, ihre personenbezogenen Daten zu schützen. Für sie besteht die größte Herausforderung darin, herauszufinden, was genau die Unternehmen mit ihren Daten machen.

Die Studie schlägt daher ein neues Rahmenwerk vor, das die Vorteile und die Rendite von Investitionen in den Datenschutz misst, und über die gesetzlichen Anforderungen und die Compliance-Anforderungen hinausgeht.

Da immer mehr Kunden dazu bereit sind, einen Aufpreis für den angemessenen Schutz ihrer personenbezogenen Daten zu zahlen, bietet sich Unternehmen die Möglichkeit, den gesetzlichen Anforderungen zu entsprechen und gleichzeitig wirtschaftliche Vorteile zu erlangen sowie ein Vertrauensverhältnis zu ihren Kunden aufzubauen.



Unternehmen haben die Möglichkeit, erhebliche geschäftliche Vorteile zu erlangen und gleichzeitig bei den Kunden Vertrauen und ein Markenbewusstsein aufzubauen.

„Datenschutz ist ein geschäftliches Muss und eine ethische Verantwortung und nicht nur eine Compliance-Anforderung.“

Harvey Jang Chief Privacy Officer & Counsel, Cisco

Ergebnisse

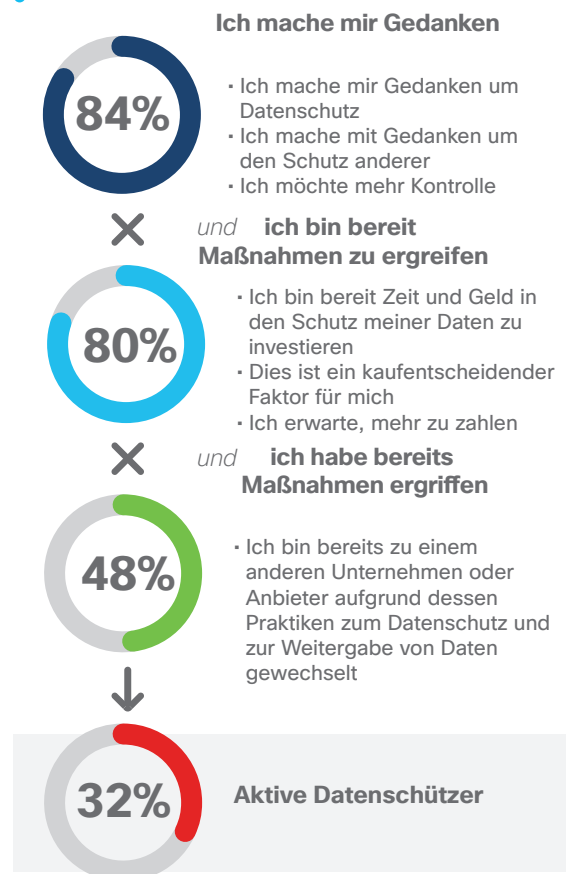
Erkenntnis 1: Die Verbraucher interessieren sich für Datenschutz. Eine überraschend große Mehrheit hat bereits Maßnahmen zum Datenschutz ergriffen.

In den letzten Jahren hat sich die Öffentlichkeit laut für den Datenschutz ausgesprochen. Die große Frage war, ob die Verbraucher dazu bereit sind, zu handeln und beispielsweise freiwillig einige Vergünstigungen aufzugeben und mehr für einen besseren Schutz und eine bessere Kontrolle ihrer personenbezogenen Daten zu zahlen. Auf der einen Seite haben viele Experten und die Medien die Ansicht geäußert, dass es nur wenige Benutzer gebe, die Maßnahmen ergreifen, um ihre Privatsphäre zu schützen.² Auf der anderen Seite ist das Bewusstsein im Hinblick auf Datenschutz durch die DSGVO der EU gestiegen. Die Nutzer müssen über ihre Rechte aufgeklärt werden. Es gab andauernd Schlagzeilen zu Datenschutzverletzungen, von denen Milliarden von Datensätzen und Millionen von Nutzern betroffen waren. Mit dieser Umfrage von Cisco Consumer Privacy aus dem Jahr 2019 haben wir versucht, das Benutzerverhalten besser zu verstehen und zu erfahren, was die Nutzer für einen besseren Schutz ihrer Daten tun würden oder bereits getan haben. Auf Grundlage der Antworten auf die Befragung haben wir eine überraschend große Bevölkerungsgruppe ausgemacht, die aussagt, sie kümmere sich um Datenschutz, sei bereit zu handeln und habe auch bereits gehandelt. Dieses Segment, das wir als „Aktive Datenschützer“ bezeichnen macht fast ein Drittel aller Befragten aus.

Wir haben dieses Ergebnis erreicht, indem wir zunächst eine große Mehrheit der Befragten (84 %) ausgemacht haben, die angab, sie mache sich Gedanken um Datenschutz. Diese Befragten machen sich Gedanken um ihre eigenen Daten und um die Daten anderer. Sie möchten genauer kontrollieren können, wie ihre Daten verwendet und verarbeitet werden. 80 % dieser Gruppe gaben an, sie seien bereit, Maßnahmen zum Datenschutz zu ergreifen. Diese Nutzer sind bereit, Zeit und Geld zu investieren, um ihre Daten zu schützen. Sie sehen den Datenschutz als wichtigen Faktor an, der zu Geschäftsentscheidungen beiträgt. Sie wissen, dass sie für Produkte

und Dienstleistungen mit einem besseren Datenschutz auch mehr zahlen müssen. Von diesen Befragten haben nahezu die Hälfte (48 %) angegeben, sie seien bereits zu Unternehmen gewechselt, die einen verantwortungsvollen Datenschutz praktizieren und Sorgfalt bei der Weitergabe von Daten walten lassen. All dies zusammengenommen, kommen wir auf einen Anteil von 32 % aller Befragten, die sich Gedanken um Datenschutz machen und bereit sind, zu handeln oder bereits Maßnahmen zum Datenschutz ergriffen haben. (siehe Abbildung 1).

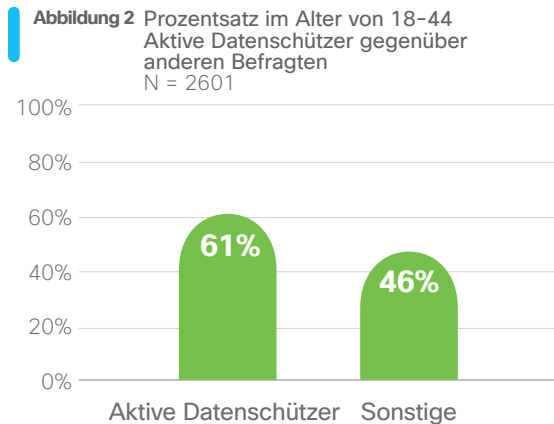
Abbildung 1 Segment Aktive Datenschützer
N = 2601



Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

Diese Datenschutzaktivitäten sind nicht nur beträchtlich, sondern auch demografisch für Unternehmen interessant. Im Vergleich zu den übrigen Befragten sind die aktiven

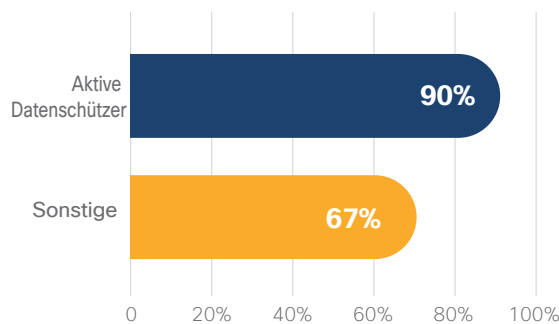
Datenschützer jünger: 61 % von ihnen sind unter 45 Jahre alt, gegenüber 46 % der anderen Befragten. (siehe Abbildung 2) Sie tätigen auch häufiger Online-Einkäufe (32 % gegenüber 23 %).



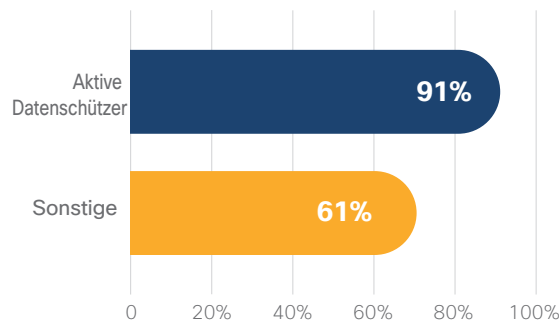
Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

Abbildung 3 Einstellungen der aktiven Datenschützer im Vergleich zu anderen Befragungsteilnehmern
N = 2601

Sie behandeln mich so, wie sie Daten behandeln



Kein Kauf, wenn ich nicht darauf vertraue, wie Daten behandelt werden



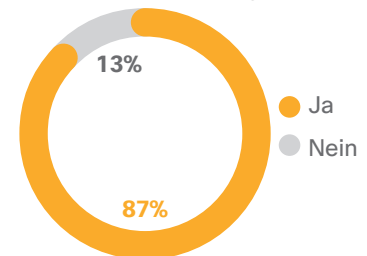
Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

Es ist vielleicht noch wichtiger, dass die aktiven Datenschützer Datenschutz als wichtigstes Kriterium eines Unternehmens und einer Marke ansehen, mit der sie Handel treiben.

90 % sagen, sie glauben, dass die Art und Weise, wie ein Unternehmen die personenbezogenen Daten seiner Kunden behandelt, etwas darüber aussagt, wie das Unternehmen mit den Kunden selbst umgeht; 91 % der Befragten würden nicht bei einem Unternehmen kaufen, dessen Datenschutzpolitik sie kein Vertrauen schenken. (siehe Abbildung 3).

Die Entstehung des Bereichs Datenschutz hilft auch dabei, einige der interessanten Erkenntnisse aus der [Cisco Datenschutz-Benchmarkstudie aus dem Jahr 2019](#) zu verstehen. In dieser Studie wurde hervorgehoben, dass 87 % der Unternehmen aufgrund der Bedenken ihrer Kunden im Hinblick auf mangelnden Datenschutz, Verzögerungen bei ihren Verkaufsaktivitäten verzeichnen. (siehe Abbildung 4). Heutzutage machen sich die Menschen mehr Gedanken um den Datenschutz; sie stellen häufiger Fragen zur Sammlung und Verwendung ihrer Daten. Sie möchten wissen, wer Zugriff auf ihre Daten hat und wie lange die Daten im Unternehmen vorgehalten werden. Die Tatsache, dass immer mehr Verbraucher bereit sind, neue Anbieter zu wählen (oder den Anbieter zu wechseln), steht in Einklang mit diesem Trend.

Abbildung 4 Befragte aus Unternehmen, die aufgrund von Datenschutzbedenken der Kunden Verzögerungen in ihren Vertriebszyklen verzeichneten
Prozentsatz der Befragten, N=2064



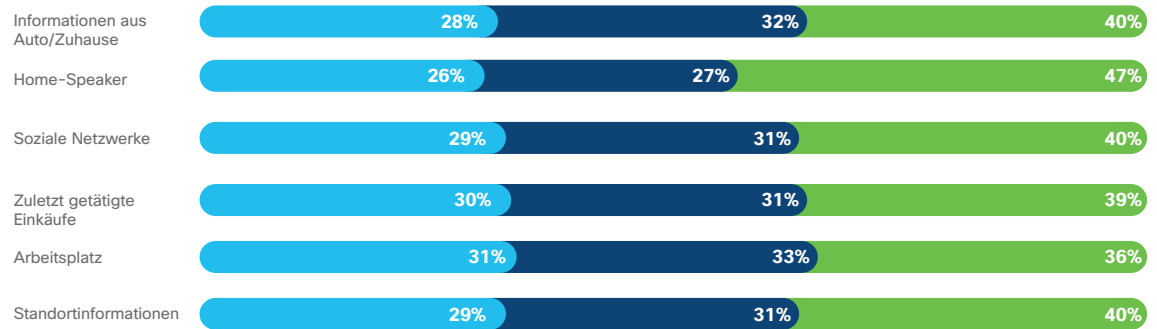
Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

Darüber hinaus haben wir festgestellt, dass 97 % der Unternehmen erkannt haben, dass sie durch ihre Investitionen in den Datenschutz durchaus Vorteile genießen. Sie haben dadurch möglicherweise einen Wettbewerbsvorteil gegenüber Konkurrenten oder sind attraktiver für Investoren. Da viele Verbraucher die Datenschutzpraktiken eines Unternehmens eng mit dessen Marke verbinden, ist es sinnvoll, dass Unternehmen diese geschäftlichen Vorteile weit über alle üblichen Compliance-Anforderungen stellen.

„Diese Untersuchungen von Cisco zeigen, dass sich die Kunden Ihrer Datenschutzrechte bewusst sind. Sie wählen bewusst Unternehmen aus, denen sie vertrauen und die ihrer Ansicht nach verantwortungsvoll mit den Daten umgehen. Daher ist es ein geschäftliches Muss und ein Wettbewerbsvorteil für Unternehmen, wenn sie für Transparenz sorgen und dafür verantwortlich zeichnen, wie mit personenbezogenen Daten umgegangen wird. Unternehmen sollten sich darauf konzentrieren, „digitales Vertrauen“ zu den Kunden aufzubauen.“

Bojana Bellamy President, Centre of Information Policy Leadership (CIPL)

Abbildung 5 Zustimmung der Benutzer zu neuen Geschäftsmodellen
N = 2601



Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019 ● Fühle mich wohl ● Neutral ● Fühle mich unwohl

Auch in zukünftigen Studien werden wir das Datenschutz-Segment, einschließlich dessen Größe, der geografischen Struktur und des Nutzerverhaltens beobachten.

Erkenntnis 2: Datenschutzbestimmungen bilden die Grundlage für Innovation und helfen, Vertrauen aufzubauen

Die Studie hat einen zweiten Schwerpunkt darauf gelegt, das Interesse der Kunden und deren Akzeptanz neuer Geschäftsmodelle zu erkennen, wenn diese Geschäftsmodelle personenbezogenen Daten in einer neuen – noch nicht dagewesenen – Weise verwenden, die für die Einzelperson oder die Gesellschaft als Ganzes von großem Nutzen sein könnte. Einige Benutzer finden, dass diese Geschäftsmodelle in ihre Privatsphäre eingreifen, andere hingegen finden die Modelle akzeptabel und vertrauenswürdig. Wir wollten diese Dynamik besser verstehen. Außerdem wollten wir erkennen, ob Datenschutzvorschriften bei der Nutzerakzeptanz eine Rolle spielen. Während bei jedem der Modelle, die wir getestet haben, personenbezogene Daten in einer noch nie dagewesenen Weise verwendet wurden, bot doch jedes Modell auch einen Vorteil für die Einzelpersonen oder die Gesellschaft als Ganzes. Die Modelle umfassten Folgendes:

- Das Teilen personenbezogener Informationen aus dem Zuhause oder dem Auto, wobei als Gegenleistung Gesundheits- oder Sicherheitswarnungen empfangen wurden, die dem einzelnen Nutzer und der Familie zugute kommen.
- Es wurde einem Smart-Home-Speaker (z.B. Alexa, Echo) das Mithören persönlicher

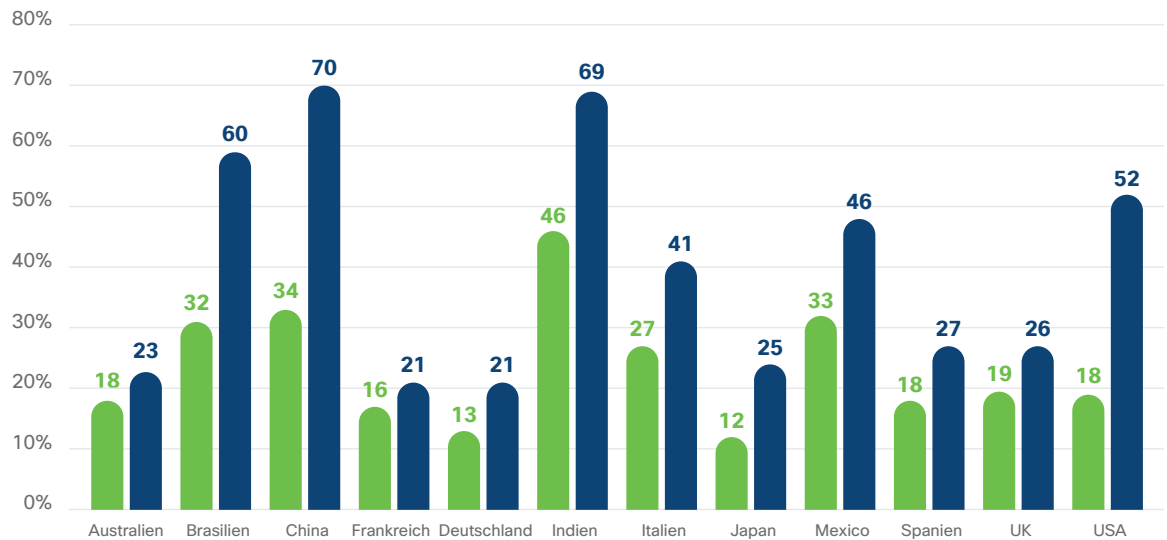
gestattet. Im Gegenzug wurden Gesundheits- oder Sicherheitswarnungen empfangen, die dem einzelnen Nutzer oder der Familie zugute kommen.

- Das Teilen personenbezogener Informationen aus sozialen Netzwerken (z.B. Facebook, Twitter), die gesammelt und anonymisiert wurden und zur Verbesserung der Gesundheit der gesamten Bevölkerung beitragen können.
- Das Teilen personenbezogener Informationen zu den zuletzt getätigten Einkäufen in Kombination mit relevanten Informationen zur Gesundheit. So können Händler Produkte vorschlagen (z.B. bestimmte Gesundheitsschuhe), die perfekt auf die Bedürfnisse des einzelnen Kunden angepasst sind.

„Datenschutz ist heutzutage ein Differenzierungsmerkmal von Unternehmen. Machen Sie es richtig, haben die Erfolg. Mangelnder Datenschutz kostet Sie den Kopf.“

John N. Stewart SVP, Chief Security and Trust Officer, Cisco

Abbildung 6 Durchschnittliche Zustimmung zu neuen Geschäftsmodellen, nach Land.
N = 2601



Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019 ● Teilnehmer mit Kenntnis der DSGVO ● Teilnehmer ohne Kenntnis der DSGVO

- Das Teilen personenbezogener Informationen vom Arbeitsplatz (z.B. Standort und Bewegungen), die dazu beitragen können, Sicherheit und Ergonomie für alle zu verbessern.
- Das Teilen personenbezogener Informationen zum aktuellen Standort, um im Gegenzug Werbeangebote und Rabatte lokaler Händler zu erhalten.

Die Umfrageteilnehmer haben diese neuen Geschäftsmodelle generell nicht unterstützt. Trotz der klar ersichtlichen möglichen Vorteile für Sicherheit und Gesundheit, die diese Modelle bieten, gaben 36 % bis 47 % (abhängig vom jeweiligen Geschäftsmodell) an, es sei ihnen nicht wohl dabei, wenn ihre Daten auf diese Weise verwendet und verarbeitet werden. Nur 26 % bis 31 % gaben an, sie hätten keine Probleme mit einer solchen Datenverarbeitung. (Siehe Abbildung 5.) Daher sollten Unternehmen, die neue Produkte und Dienstleistungen einführen möchten, welche die neue Methoden der Datennutzung einsetzen, gewährleisten, dass sie die möglichen Bedenken der Kunden im Hinblick auf Datenschutz berücksichtigen.

Datenschutzrichtlinien scheinen dazu beizutragen, den Kunden ein gutes Gefühl bei der Nutzung ihrer Daten zu vermitteln, vorausgesetzt, dass die Nutzer von der Existenz solcher Richtlinien wissen. Die Umfrageteilnehmer, die die Datenschutzgrundverordnung (DSGVO) kannten, gaben an, dass sie die neuen Geschäftsmodelle viel eher akzeptierten als diejenigen, die keine Kenntnis von der Existenz der DSGVO hatten. Im Durchschnitt, über all die sechs neuen Modelle hinweg, gaben 38 % der Befragten, die die DSGVO kannten, an, dass sie sich angesichts dieser neuen Modelle nicht unwohl fühlten. Dies sagten jedoch nur 24 % derjenigen Befragten, die keine Kenntnis von der Existenz der DSGVO hatten.

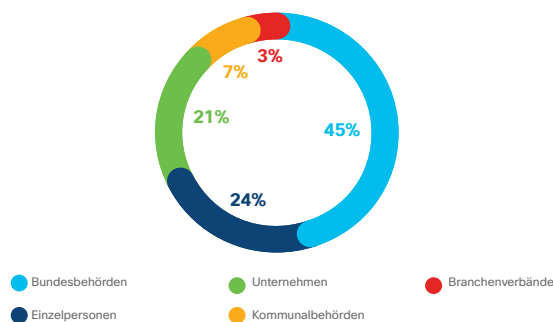
Interessanterweise ist die Akzeptanz in allen Ländern gleichermaßen angestiegen. Es gibt zwar Unterschiede, was die absolute positive Stimmungslage angeht, in allen Ländern war jedoch die Akzeptanz gegenüber den neuen Modellen bei denjenigen positiver, die Kenntnis von der DSGVO hatten. Wenn Datenschutzkontrollen klar definiert werden (z.B. in einem Gesetz oder einer Norm), scheinen sie sowohl den Verbrauchern als auch den Unternehmensaktivitäten zuträglich zu sein. (Siehe Abbildung 6.)

In der [Cisco-Benchmarkstudie zum Datenschutz von 2019](#) gaben 42 % der Unternehmen an, dass die Investitionen in den Datenschutz die Beweglichkeit und Innovationsfähigkeit im Unternehmen angetrieben haben. Da sie wussten, was aus Datenschutzsicht nicht realisiert werden konnte, waren sie sehr viel freier darin (und manchmal auch gezwungen), neue Ideen zu verfolgen. Dieses Ergebnis deutet darauf hin, dass nicht notwendigerweise jede Verordnung zum Datenschutz Vorteile für Verbraucher und Unternehmen mit sich bringt. Zu viele, zu normative und inkonsistente Verordnungen könnten zu kostspielig, zu belastend und verwirrend für Unternehmen und Verbraucher sein. Dennoch scheint es, dass zumindest ein gewisses Maß an Regulierung in einer sonst unübersichtlichen Landschaft Vorteile für alle bietet.

Erkenntnis 3: Die Verbraucher wissen die Rolle der Regierung bei der Regulierung der Verwendung personenbezogener Daten zu schätzen. Die DSGVO ist in ihren Augen eine gute Sache

Die Umfrageteilnehmer wurden befragt, welche Einheit-, Bundes- oder Kommunalbehörden, Unternehmen, Branchenverbände oder Einzelpersonen – in erster Linie für den Schutz personenbezogener Daten verantwortlich sein sollte. Regierungen können Regulierung und Kontrolle bieten. Übermäßige Bürokratie kann allerdings eine Belastung für Unternehmen

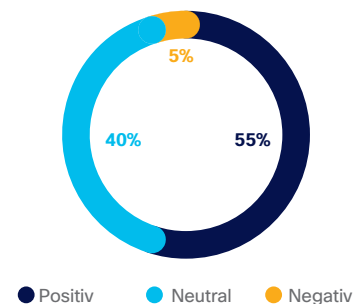
Abbildung 7 Wer hauptverantwortlich für den Datenschutz ist.
N = 2601



Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

und Privatpersonen darstellen. Es liegt in der Verantwortung der Unternehmen, die Daten ihrer Kunden zu schützen. Manchmal kommen allerdings kurzfristige Geschäftsziele dazwischen und der Unternehmensgewinn geht vor. Viele Verbraucher akzeptieren möglicherweise, dass auch sie zu einem Teil dafür verantwortlich sind, wann und wie sie ihre Daten teilen, verstehen jedoch nicht, was genau mit ihren Daten weiter geschieht. Die Befragten waren in der Frage, wer für den Datenschutz verantwortlich ist, gespalten. Die meisten Umfrageteilnehmer hielten die Regierungsbehörden (45 %)

Abbildung 8 Stimmungslage zum Einfluss der DSGVO
N = 941



Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

für verantwortlich, gefolgt vom einzelnen Benutzer (24 %) und den Unternehmen (21 %). (Siehe Abbildung 7.)

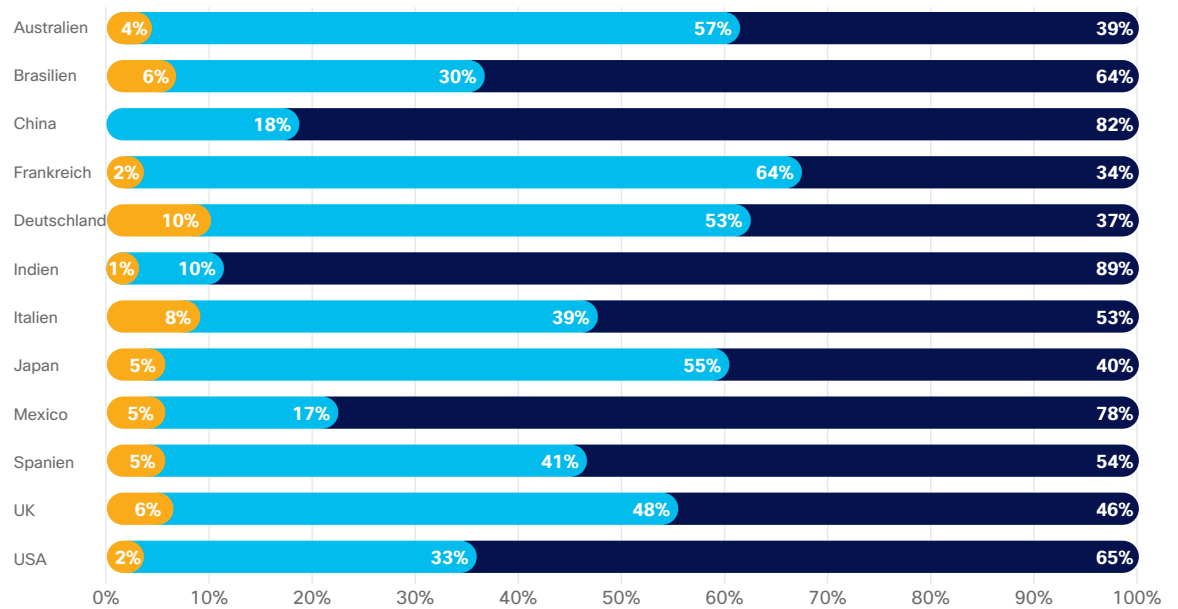
In der Tat scheinen alle drei genannten Instanzen beim Schutz personenbezogener Daten eine wichtige Rolle zu spielen. Regierungen können überwachen, was Unternehmen tun, Unternehmen können geeignete Datenschutzrichtlinien festlegen und befolgen, die den Grundsätzen der Transparenz, Fairness und Rechenschaftspflicht folgen. Einzelpersonen können Maßnahmen ergreifen, um ihre Privatsphäre zu schützen und Verantwortung für ihre Entscheidungen übernehmen. Die meisten Befragten gaben an, dass sie die Verantwortung bei den Regierungsbehörden sehen. Es ist nicht überraschend, dass diejenigen, die mit der DSGVO vertraut sind, der Ansicht sind, diese habe einen positiven

Einfluss. Eine überwältigende Mehrheit der Befragten, ganze 55 %, sahen die DSGVO positiv. Nur 5 % der Befragten lehnten die DSGVO ab. (Siehe Abbildung 8.)

Obwohl es je nach Land einige Abweichungen gab, so wird die DSGVO von den Verbrauchern doch weltweit als positiv angesehen. (Siehe Abbildung 9.) Die

Umfrageteilnehmer wurden auch gefragt, ob die DSGVO Einzelpersonen beim Datenschutz unterstützen könne. 52 % gaben an, dass sie dank der DSGVO mehr Kontrolle über ihre personenbezogenen Daten hätten. 59 % gaben an, sie könnten ihre Rechte in Bezug auf Daten besser durchsetzen. 47 % gaben an, sie hätten nun mehr Vertrauen in Unternehmen, die ihre Daten

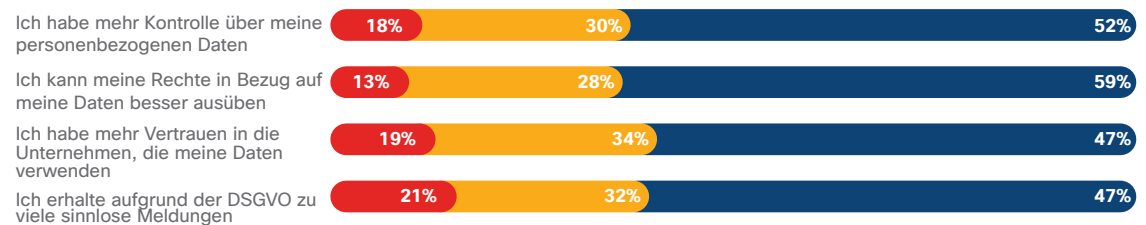
Abbildung 9 Stimmungslage zum Einfluss der DSGVO nach Land.
N = 941



Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

Hinweis: Für Australien, Brasilien und Japan ist die Zahl der Befragten, die mit der DSGVO vertraut sind, relativ gering, sodass die Fehlerspanne erheblich ist. Die Ergebnisse sind dennoch enthalten, da die Fehlerspanne immer noch erheblich geringer ist als die prozentuale Abweichung zwischen Befragten mit einer positiven oder negativen Stimmung.

Abbildung 10 Auswirkungen der DSGVO auf Einzelpersonen.
N = 941

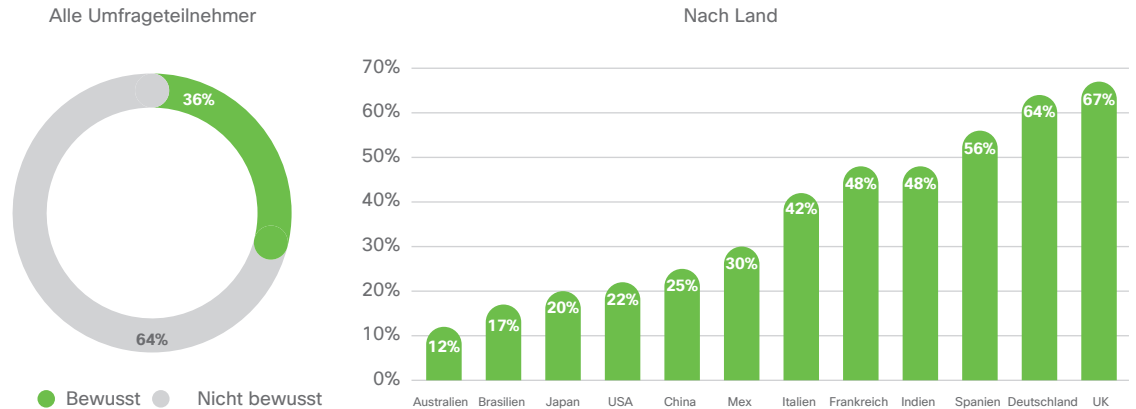


Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

Stimme nicht zu Neutral Stimme zu

Abbildung 11 Kenntnis der DSGVO

N = 2601



Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

verwenden. 47 % gaben an, sie seien der ganzen Benachrichtigungen, die aufgrund der DSGVO im Hinblick auf den Datenschutz versendet werden, langsam überdrüssig. (siehe Abbildung 10).

Unsere Umfrage ergab, dass sich die breite Öffentlichkeit noch immer nicht vollumfänglich des Themas Datenschutzrichtlinien bewusst ist. Nur ein Teil der Verbraucher ist über das Thema Datenschutzrichtlinien aufgeklärt. Es ist in Zukunft noch einige Aufklärungsarbeit notwendig. Insgesamt ist nur etwa ein Drittel der Befragten in den zwölf Ländern unserer Umfrage mit diesen neuen Bestimmungen vertraut. Sogar in Westeuropa, wo die DSGVO bereits im Jahr 2018 in Kraft trat und deutlich von Presse und Unternehmen kommuniziert wurde, kennen ein Drittel der Befragten die Verordnung nicht. Eine Minderheit steht den Vorteilen der Verordnung neutral gegenüber. (siehe Abbildung 11).

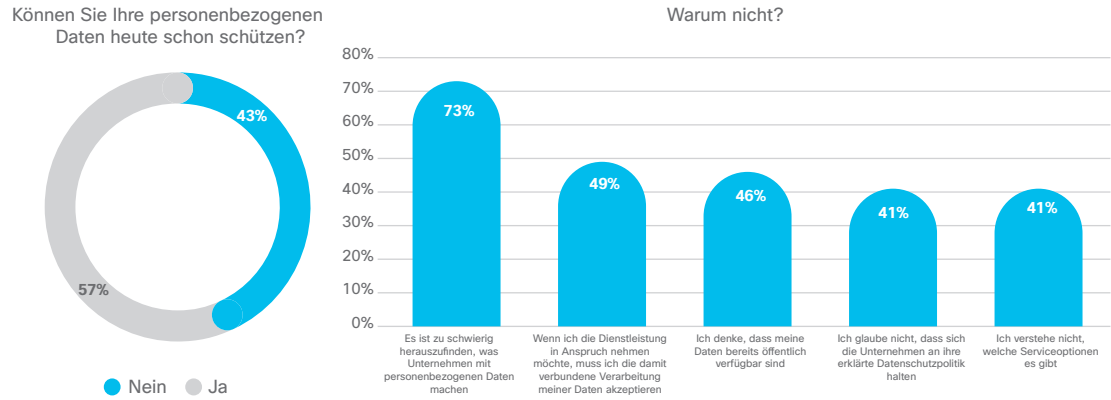
Erkenntnis 4: Viele Verbraucher glauben, sie seien nicht in der Lage, ihre personenbezogenen Daten zu schützen. Für sie besteht die größte Herausforderung darin, herauszufinden, was genau die Unternehmen mit ihren Daten machen

Die zunehmende Fokussierung auf den Datenschutz bringt eine ganze Anzahl neuer Herausforderungen mit sich. Die meisten

„Diese Untersuchungen von Cisco zeigen, dass Datenschutz für Einzelpersonen weltweit zu einem kritischen Thema geworden ist und dass Firmen (wie Cisco) die Daten der Kunden weiterhin vorschriftsmäßig behandeln müssen, um Vertrauen zu den Kunden aufzubauen. und eben dieses Vertrauen aufrecht zu erhalten.“

Tom Moore Chief Privacy Officer und SVP bei AT&T

Abbildung 12 Fähigkeit der Nutzer, ihre Daten zu schützen und Gründe, warum sie denken, dass sie nicht dazu in der Lage sind Links: N = 2601 Rechts: n = 1129



Quelle: Cisco Studie zum Verbraucherdatenschutz - 2019

Befragten wünschen sich eine einfache und transparente Einsicht in die Nutzung ihrer Daten. 43 % glauben, sie seien nicht in der Lage, ihre Daten angemessen zu schützen. Diese Bedenken sind bei den Befragten im Alter ab 55 Jahren höher. 52 % dieser Altersgruppe geben an, dass sie ihre personenbezogenen Daten heute nicht schützen können. Diejenigen Befragten, die der Ansicht sind, sie können ihre Daten nicht schützen, wurden auch nach der Ursache dieses Problems befragt. Die meist gegebene Antwort, die von nahezu drei Vierteln der Befragten gegeben wurde, war, es sei einfach zu schwierig herauszufinden, was Unternehmen mit den personenbezogenen Daten machen. Weitere wichtige Antworten waren beispielsweise: „Wenn ich die Dienstleistung in Anspruch nehmen möchte, muss ich die damit verbundene Verarbeitung meiner Daten akzeptieren“ (49 %); und „Ich denke, dass meine Daten bereits öffentlich verfügbar sind“ (49 %) und „Ich glaube nicht, dass sich die Unternehmen an ihre erklärte Datenschutzpolitik halten“ (41 %). (Siehe Abbildung 12).

den Erwartungen der Verbraucher und den erklärten und tatsächlichen Praktiken der Unternehmen. Es hat den Anschein, als hätten Unternehmen nicht genug dafür getan, den Kunden deutlich zu erklären, wie personenbezogene Daten verwendet werden. Sie haben nicht genug unternommen, um den Verbrauchern zu demonstrieren, dass sie sich auch wirklich an die erklärten Richtlinien zum Datenschutz halten.

Diese Antworten zeigen eine Lücke zwischen

Fazit

Die Ergebnisse der Umfrage, in Kombination mit den vorangegangenen Cisco-Studien zum Datenschutz, lassen darauf schließen, dass ein neues Modell zum Messen der Vorteile und der Rendite der Investitionen in den Datenschutz eingeführt werden sollte. Interviews mit Entscheidungsträgern im Bereich Datenschutz zeigen, dass Unternehmen und ihre Führungsriege sich im Allgemeinen auf die Einhaltung gesetzlicher Bestimmungen und die Vermeidung von Bußgeldern und Strafen konzentrieren. Unsere jüngsten Erkenntnisse lassen auf die Notwendigkeit eines noch umfassenderen Modells zur Ermittlung der Wertschöpfung schließen, in dessen Rahmen die geschäftlichen Vorteile des Datenschutzes einschließlich der folgenden Faktoren erfasst werden sollten.

1. Gewinnung und Bindung von Kunden, die sich um den Datenschutz kümmern und bereit sind, zu handeln.

Die Untersuchungen zeigen, dass die Mehrheit der Verbraucher sich Gedanken zum Thema Datenschutz macht. Ein Drittel hat bereits gehandelt und den Dienstleister gewechselt, wenn dieser die Erwartungen nicht erfüllt hat. Dieses Segment bildet einen interessanten Anteil der Nutzer. Diese Nutzer sind jünger und wohlhabender und haben öfter einen Internetzugang als der Rest der Bevölkerung. Kunden sehen zunehmend den Datenschutz als wichtigen Bestandteil der Marke eines Unternehmens an. Unternehmen müssen in den Datenschutz investieren, um zu gewährleisten, dass ihre Kunden ihre Datenpraktiken und -richtlinien verstehen und diesen Vertrauen entgegenbringen. Ist dies nicht der Fall, wechseln Kunden zu anderen Unternehmen, denen sie mehr Vertrauen entgegenbringen.

2. Erhöhen der geschäftlichen Flexibilität und der Innovationsleistung

In dieser Studie haben Kunden eine verstärkte Bereitschaft gezeigt, neue Nutzungsmethoden ihrer Daten zu akzeptieren, wenn sie davon überzeugt sind, dass ein angemessener Datenschutz gewährleistet ist. Sie erwarten von Regierungen und Unternehmen, dass diese

Vorschriften und Richtlinien einführen, die einen solchen Datenschutz bieten. Wenn dieser „Unterbau“ gewährleistet ist, sind Unternehmen flexibler bei der Einführung von Innovationen. Die Kunden akzeptieren dann eher neue Geschäftsmodelle. Dies bestätigt unsere bisherigen Forschungsergebnisse, die zeigen, dass Unternehmen aus ihren Investitionen in den Datenschutz die folgenden Vorteile ziehen.

3. Weniger verpasste Verkaufsoptionen

Wenn sich immer mehr Kunden Gedanken um den Datenschutz machen und auch entsprechende Maßnahmen ergreifen möchten, kann es dadurch durchaus zu verpassten Verkaufsoptionen kommen. Potenziellen Kunden fragen die Dienstleister vermehrt nach der Art der Verwendung ihrer personenbezogenen Daten. Wenn Unternehmen keine transparenten und gut verständlichen Informationen liefern können, führt dies zu Verzögerungen und verpassten Verkaufsoptionen.

4. Steigern der Attraktivität des Unternehmens für Kunden und Aktionäre

Aktionäre und Investoren erkennen die zunehmende Bedeutung des Datenschutzes für eine Marke und den Wert eines Unternehmens. Sie investieren in die Unternehmen, die dem Datenschutz eine hohe Bedeutung beimessen.

Daraus ergibt sich, dass Unternehmen den Wert des Datenschutzes voranstellen sollten, noch vor Compliance und Risikovermeidung. Für viele Unternehmen ist Datenschutz mittlerweile unabdingbar.

Über die Cisco Reihe zur Cybersicherheit

Im vergangenen Jahrzehnt hat Cisco eine Fülle an maßgeblichen Sicherheits- und Bedrohungsinformationen für Sicherheitsexperten veröffentlicht, die sich für den aktuellen Stand der globalen Cybersicherheit interessieren. Diese umfassenden Berichte enthielten detaillierte Beschreibungen von Bedrohungslandschaften und ihren organisatorischen Auswirkungen sowie Best Practices zum Schutz vor den negativen Folgen von Daten-sicherheitsverletzungen.

In unserem neuen Ansatz für unsere Vordenkerposition veröffentlicht Cisco Security eine Reihe von forschungsbasierten, datengesteuerten Publikationen unter der Überschrift Cisco Reihe zur Cybersicherheit. Wir haben die Anzahl der Titel erweitert, sodass sie jetzt auch verschiedene Berichte für Sicherheitsexperten mit anderen Interessen enthalten. Diese Berichte für 2019 greifen auf die tiefgreifenden und umfangreichen Kenntnisse von Bedrohungsforschern und Innovatoren in der Sicherheitsbranche zurück und enthalten die Benchmark-Studie zum Datenschutz, den Bedrohungsbericht und die Cisco Benchmark-Studien. Weitere Berichte sollen im Verlauf des Jahres veröffentlicht werden.

Weitere Informationen und Zugriff auf alle Berichte und archivierte Kopien finden Sie auf



www.cisco.com/go/securityreports.



Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Eine Liste der Adressen, Telefon- und Faxnummern finden Sie auf der Cisco-Website unter www.cisco.com/go/offices.

Veröffentlicht im November 2019

PRIV_07_1119_FINAL

© 2019 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1876404)