Ping Identity

VERBRAUCHERUMFRAGE 2018:

WIE TICKEN VERBRAUCHER IM ZEITALTER DER DATENSCHUTZVERLETZUNGEN?

EINLEITUNG

Datenschutzverletzungen, die Verbraucher betreffen, sind heute fast schon an der Tagesordnung. 2018 waren vor allem der Cambridge Analytica/Facebook-Skandal und das Google+ Datenleck in den Schlagzeilen – Fälle, bei denen es um die persönlichen Daten von Millionen Menschen ging und die unser Vertrauen in große Marken nachhaltig erschüttert haben. Viele Verbraucher ändern mittlerweile drastisch die Art, wie sie mit Marken online interagieren und vertreten die Ansicht, dass letztlich die Unternehmen die Verantwortung für den Schutz ihrer Daten übernehmen müssten. Um Unternehmen zu helfen, das Verbrauchervertrauen zu wahren und die Erwartungen ihrer Kunden zu erfüllen, befragte Ping über 3.000 Personen in den USA, sowie in Großbritannien, Frankreich und Deutschland zu ihren Einstellungen und Ansichten im Zeitalter der Datenschutzverletzungen.

HAUPTERKENNTNISSE

- Einer von fünf Befragten (21%) wurde bereits Opfer einer Datenschutzverletzung. Davon erlitten 34% zudem einen finanziellen Verlust.

- 78% der Befragten würden nach einer Datenschutzverletzung mit der jeweiligen Marke nicht mehr online interagieren. Zudem würde sich fast die Hälfte (49%) bei Online-Services oder -Apps, die kürzlich gehackt wurden, nicht anmelden.

- Über die Hälfte der Verbraucher (56%) sind überhaupt nicht bereit, Anbieter von Apps und Online-Services für den zusätzlichen Schutz ihrer persönlichen Daten zu bezahlen.

- Für 59% der Umfrageteilnehmer steht bei der Interaktion mit Online-Apps und -Services der Schutz ihrer persönlichen Daten im Mittelpunkt. Lediglich 12% priorisieren ein komfortables, angenehmes Erlebnis, während für 7% eine personalisierte Benutzeroberfläche am wichtigsten ist.

AUSWIRKUNGEN EINER DATENSCHUTZVERLETZUNG

DIE WICHTIGSTEN ERKENNTNISSE

Die überwiegende Mehrzahl der Teilnehmer würde nach einer Datenschutzverletzung nicht mehr mit der betroffenen Marke interagieren und schätzt Sicherheit mehr als alles andere. Über die Hälfte der befragten Personen unternimmt nach einer Datenschutzverletzung nichts, um ihre persönlichen Daten zu sichern. Das legt nahe, dass Verbraucher die Verantwortung für den Schutz persönlicher Daten eher bei den Unternehmen sehen und nicht bei sich selbst.

UNTERSTÜTZENDE DATEN

- Einer von fünf Befragen (21%) wurde bereits Opfer einer Datenschutzverletzung. Davon erlitten 34% zudem einen finanziellen Verlust. Bei 41% der Personen aus dieser Gruppe lag dieser zwischen US$ 300 und US$ 999.

- 78% der Befragten würden nach einer Datenschutzverletzung mit der jeweiligen Marke nicht mehr online interagieren. Über ein Drittel (36%) würde die Interaktion sogar komplett einstellen.

- Fast die Hälfte (49%) würde keine Online-Services oder -Apps nutzen, die kürzlich gehackt wurden. Über ein Drittel (37%) würden einen kürzlich gehackten Online-Service nur dann nutzen, wenn es keine andere Möglichkeit gäbe, den entsprechenden Service zu beziehen.

- 47% der Personen haben nach einer Datenschutzverletzung bei der Sicherung ihrer persönlichen Daten Änderungen vorgenommen, während 53% keinerlei Maßnahmen eingeleitet haben. Siehe Abbildungen 1 & 2 unten.

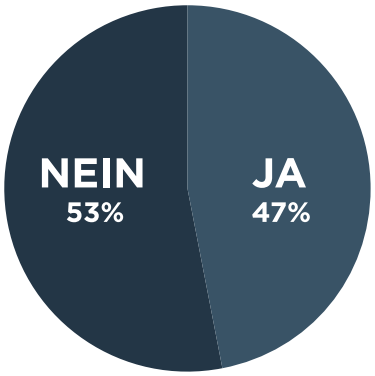


Abbildung 1

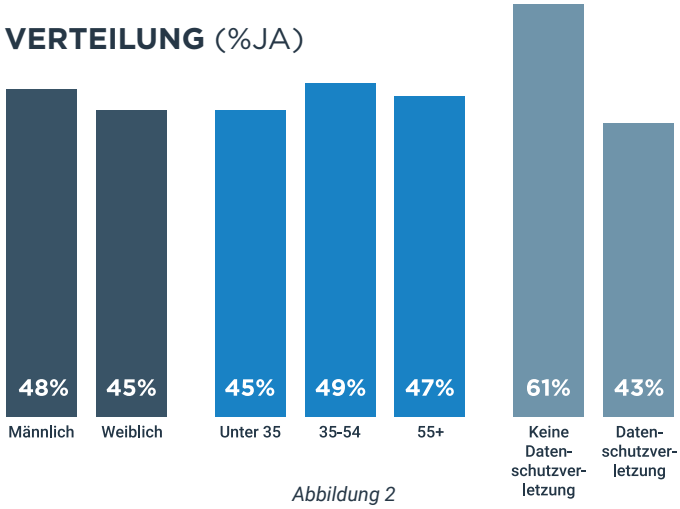


Abbildung 2

- Über die Hälfte (54%) der Verbraucher macht sich heute um den Schutz ihrer persönlichen Daten größere Sorgen, als noch vor einem Jahr. 2% sagen, sie sind eher weniger besorgt, während 44% keinen Unterschied zum Vorjahr sehen.

- Über ein Viertel (28%) plant, als Folge der Facebook-/Cambridge Analytica-Enthüllungen an der Online-Anmeldung über Social-Media-Plattformen etwas zu ändern. Ein Drittel (32%) meldet sich nach den Facebook-/Cambridge Analytica-Enthüllungen weiterhin unverändert über Social-Media-Plattformen an.

WER IST VERANTWORTLICH?

DIE WICHTIGSTEN ERKENNTNISSE

Die meisten Teilnehmer sind der Ansicht, dass es die Aufgabe der jeweiligen Anbieter ist, ihre persönlichen Daten zu schützen. Deshalb sind sie nicht bereit, für den Schutz ihrer Daten mehr zu bezahlen. Während die Mehrzahl der Teilnehmer nicht bereit ist, Betreibern von Online-Apps und -Services für zusätzliche Sicherheit überhaupt etwas zu bezahlen, ist lediglich ein Viertel bereit, einen geringen Beitrag zu leisten. Vergleicht man das mit der Summe, die Personen generell zu zahlen bereit sind, um ihre persönlichen Daten vor unberechtigtem Zugriff zu schützen (nicht notwendigerweise an Anbieter von Online-Apps und -Services), fällt die Investitionsbereitschaft geringfügig höher aus.

UNTERSTÜTZENDE DATEN

- Über die Hälfte der Befragten (56%) sind überhaupt nicht bereit, Anbieter von Apps und Online-Services für den zusätzlichen Schutz ihrer persönlichen Daten zu bezahlen. Etwa ein Viertel (24%) ist nicht bereit, mehr als US$ 5 zu bezahlen, während 2% bereit sind, mehr als US$ 20 zu bezahlen. Siehe Abbildung 3.

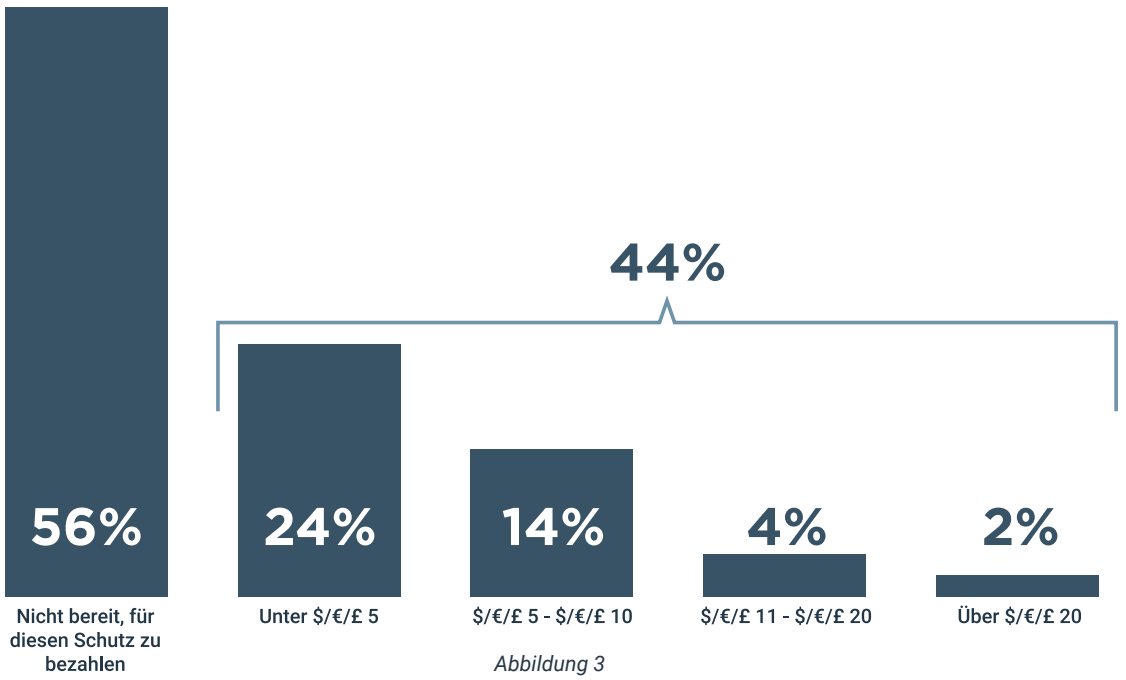


Abbildung 3

- 48% der Befragten sind nicht bereit, überhaupt zu bezahlen, um ihre persönlichen Daten vor unberechtigtem Zugriff zu schützen. 38% wären bereit, dafür bis zu US$ 49 zu bezahlen.

SICHERHEIT UND BENUTZERERFAHRUNG

DIE WICHTIGSTEN ERKENNTNISSE

Verbraucher sagen, Sicherheit sei ihnen bei der Interaktion mit einer Marke wichtiger als ein komfortables, personalisiertes Benutzererlebnis. Aber immer mehr Menschen melden sich über ihre Social-Media-Konten auf Websites an. Der Stellenwert von Schnelligkeit und Komfort bei der Anmeldung ist nicht zu unterschätzen, während bei der Interaktion mit Marken eher die Sicherheit zählt.

UNTERSTÜTZENDE DATEN

- Für 59% steht bei der Interaktion mit Online-Apps und -Services der Schutz ihrer persönlichen Daten im Mittelpunkt. 12% priorisieren ein komfortables, angenehmes Erlebnis, während für 7% eine personalisierte Benutzeroberfläche am wichtigsten ist. (Für 22% stehen die Kosten im Vordergrund [kostenloser ggü. kostenpflichtiger Service]). Siehe Abbildung 4.

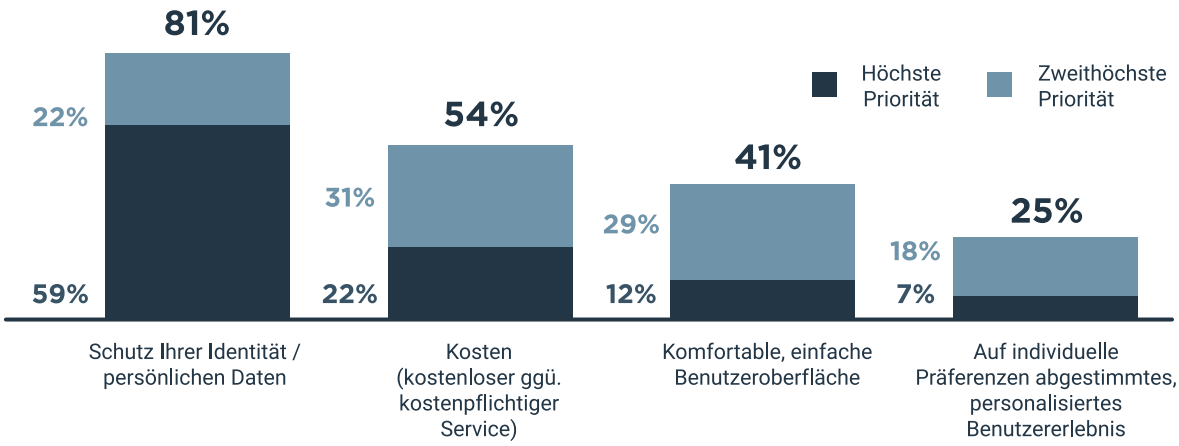


Abbildung 4

- 70% der Nutzer melden sich nach wie vor primär mit Benutzernamen und Passwort an. 13% der Teilnehmer melden sich in der Regel über ihre Social-Media-Konten auf anderen Websites an. Von allen Personen, die sich über die sozialen Medien anmelden, tun das 84%, weil es bequemer ist (40%) oder weil es Zeit spart (44%).

Zwar steigt die Akzeptanz von Fingerabdruckscannern und Gesichtserkennung, aber der überwiegende Teil der Anwender nutzt weiterhin traditionelle Anmeldemethoden.

Die Nutzung neuer Technologien wie Fingerabdruckscanner und Gesichtserkennung für die Anmeldung wird immer beliebter, dennoch wird es noch lange dauern, bis Passwörter endgültig aus unserem Leben verschwunden sind. Alles beginnt damit, die Verbraucher über den Nutzen und die Vorteile biometrischer Anmeldetechniken zu informieren.

- 51% glauben, dass die Anmeldung über Fingerabdruckscanner und Gesichtserkennung sicherer ist, als die Verwendung von Benutzernamen und Passwörtern. (40% halten beide Methoden für gleich sicher.) Nur 10% der Anwender nutzen biometrische Technologien, wie Fingerabdruckscanner und Gesichtserkennung, als primäre Anmeldemethode. Vermutlich liegt das daran, dass diese neue Technologie von den meisten Plattformen noch nicht angeboten wird.

SPOTLIGHT: RESULTATE NACH ALTERSGRUPPE

UNTER 35	ÜBER 55
Das in Marken gesetzte Vertrauen ist eher stark. • 53% sind sich sicher oder sehr sicher, dass Anbieter von Online-Apps und -Services in der Lage sind, ihre persönlichen Daten zu schützen.	**Das in Marken gesetzte Vertrauen ist eher schwach.** • Nur 27% sind sich sicher oder sehr sicher, dass Anbieter von Online-Apps und -Services in der Lage sind, ihre persönlichen Daten zu schützen.
Eher unbesorgt bezüglich ihrer sensiblen persönlichen Daten • 54% sind bereit, ihre Kontodaten auf einer Website oder in einer App einzugeben.	**Schützen ihre sensiblen persönlichen Daten sorgfältiger** • 41% sind bereit, ihre Kontodaten auf einer Website oder in einer App einzugeben.
Finanzielle Verluste aufgrund einer Datenschutzverletzung sind wahrscheinlicher. • 41% mussten bereits aufgrund einer Datenschutzverletzung finanzielle Verluste hinnehmen.	**Finanzielle Verluste aufgrund einer Datenschutzverletzung sind eher unwahrscheinlich.** • 27% mussten bereits aufgrund einer Datenschutzverletzung finanzielle Verluste hinnehmen.
Die Bereitschaft, mehr für den Schutz ihrer persönlichen Daten auszugeben, ist eher stärker ausgeprägt. • 42% sind nicht bereit, für den zusätzlichen Schutz ihrer persönlichen Daten mehr Geld an Online-Apps und -Services zu zahlen. • 37% sind nicht bereit, überhaupt dafür zu bezahlen, dass ihre persönlichen Daten vor unbefugtem Zugriff geschützt werden. • 42% sind bereit, zwischen US$ 1 und US$ 49 zu bezahlen, um ihre persönlichen Daten vor unbefugtem Zugriff zu schützen.	**Die Bereitschaft, mehr für den Schutz ihrer persönlichen Daten auszugeben, ist nicht sehr ausgeprägt.** • 75% sind nicht bereit, für den zusätzlichen Schutz ihrer persönlichen Daten mehr Geld an Online-Apps und -Services zu zahlen. • 62% sind nicht bereit, überhaupt dafür zu bezahlen, dass ihre persönlichen Daten vor unbefugtem Zugriff geschützt werden. • 32% sind bereit, zwischen US$ 1 und US$ 49 zu bezahlen, um ihre persönlichen Daten vor unbefugtem Zugriff zu schützen.
Nach dem Cambridge Analytica-Skandal verlor Facebook Connect einen erheblichen Teil seiner Nutzer über alle Altersgruppen hinweg. • 37% werden Facebook Connect nicht mehr nutzen, um sich bei Online-Apps und -Services anzumelden. Zwar sind die Zahlen nicht so hoch, wie bei der älteren Generation, dennoch wird Facebook Connect ein Drittel seiner Kundenbasis verlieren.	**Nach dem Cambridge Analytica-Skandal verliert Facebook Connect eine substanzielle Zahl von Nutzern aller Altersgruppen.** • 56% werden Facebook Connect nicht mehr nutzen, um sich bei Online-Apps und -Services anzumelden.
Offener gegenüber der Nutzung biometrischer Lösungen • 46% nutzen für die Anmeldung bei Online-Apps und -Services biometrische Tools wie Fingerabdruckscans oder Gesichtserkennung.	**Die Akzeptanz biometrischer Sicherheitslösungen ist eher niedrig.** • 13% nutzen für die Anmeldung bei Online-Apps und -Services biometrische Tools wie Fingerabdruckscans oder Gesichtserkennung.

SPOTLIGHT: RESULTATE NACH LÄNDERN

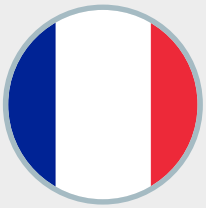
Hohe Bereitschaft zur Weitergabe persönlicher Daten:

Höhere Wahrscheinlichkeit, sensible persönliche Daten mit Marken zu teilen als in anderen Ländern:

- Sozialversicherungsnummer (16% in den USA, 9% in Frankreich, 6% in Deutschland und 4% in Großbritannien)
- Kreditkartendaten (40% in den USA, 36% in Frankreich, 26% in Großbritannien und 13% in Deutschland)

Hohe Ausgabebereitschaft – für Services, nicht für die Sicherheit:

- Amerikaner geben für Online-Apps und -Services wie Spotify, Netflix, etc. mehr aus, als die Bürger anderer Staaten (62% der US-Bürger geben Geld für Services/Apps aus, im Vergleich zu 53% in Großbritannien, 49% in Deutschland und 47% in Frankreich).
- Amerikaner zeigen die geringste Bereitschaft, Geld auszugeben, um ihre persönlichen Daten vor unberechtigtem Zugriff zu schützen (USA: 36%, Deutschland: 46%, Großbritannien: 54% und Frankreich: 60%).



Geringes Vertrauen:

- Die Franzosen sind am wenigsten davon überzeugt, dass Anbieter von Online-Apps und -Services in der Lage sind, persönliche Daten zu schützen. (Nur 38% sind sich sicher oder sehr sicher im Vergleich zu 48% in den USA und Großbritannien und 42% in Deutschland).

Geringste Wahrscheinlichkeit einer Datenschutzverletzung:

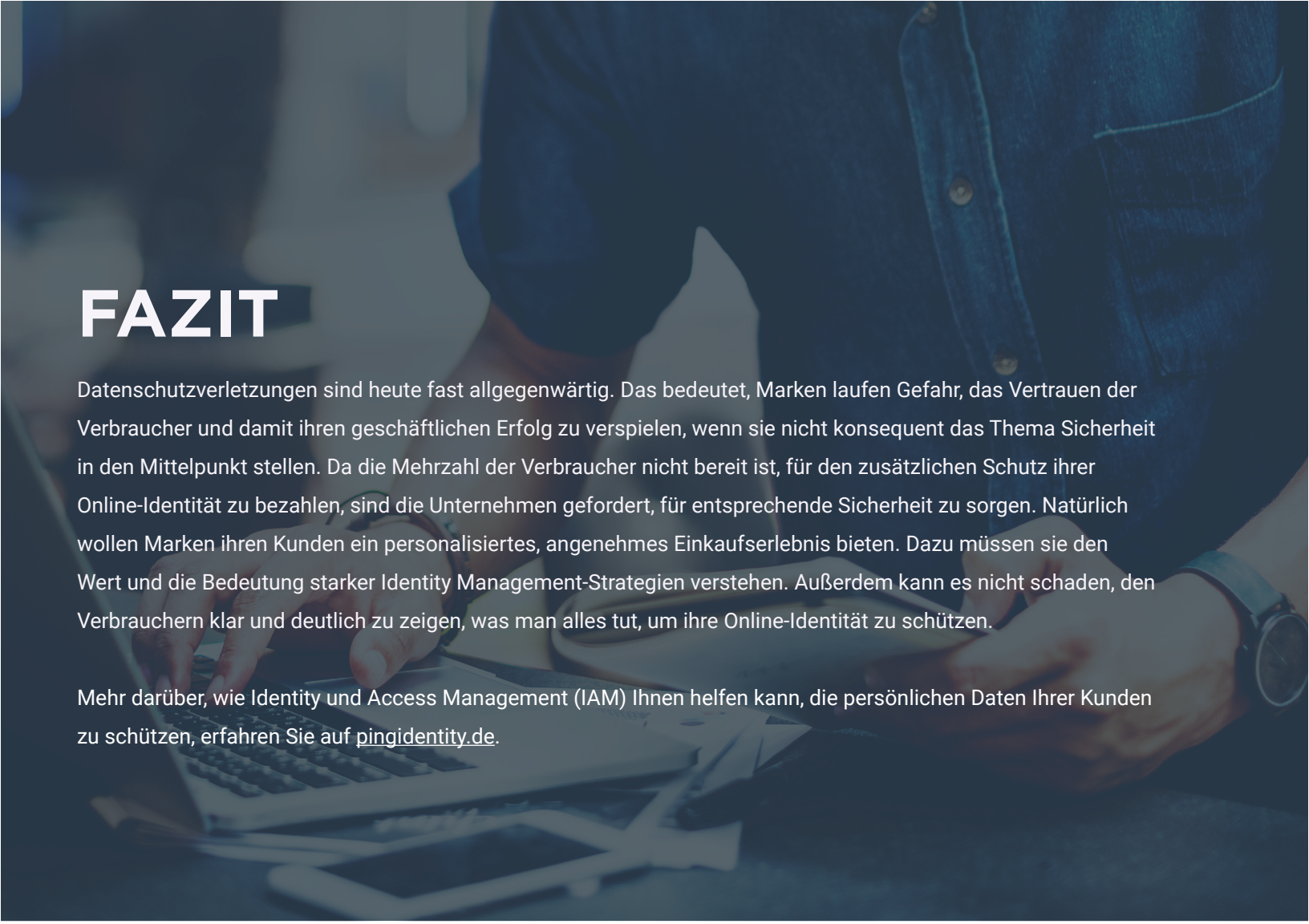
- Bei Briten ist die Häufigkeit von Datenschutzverletzungen (15%) geringer als in den USA (27%), Frankreich (21%) oder Deutschland (17%). Allerdings mussten 42% der britischen Teilnehmer, die von einer Datenschutzverletzung betroffen waren, auch finanzielle Einbußen hinnehmen. In den USA waren es 24%, in Deutschland 38% und in Frankreich 43%.

Nicht bereit, für Sicherheit mehr zu bezahlen:

- Briten zeigen die geringste Bereitschaft, Anbietern von Online-Apps und -Services für den Schutz ihrer persönlichen Daten mehr zu bezahlen (64%), im Vergleich zu 61% in Frankreich, 52% in Deutschland und 48% in den USA.

Massive Abwanderung von Facebook Connect:

- Die Deutschen fahren eine klarere Linie, wenn es um Änderungen nach dem Cambridge Analytica-Skandal geht. 50% werden sich aufgrund der Enthüllungen künftig nicht mehr über Facebook Connect bei anderen Online-Apps und -Services anmelden (im Vergleich zu 42% in den USA, 41% in Frankreich und 39% in Großbritannien).



FAZIT

Datenschutzverletzungen sind heute fast allgegenwärtig. Das bedeutet, Marken laufen Gefahr, das Vertrauen der Verbraucher und damit ihren geschäftlichen Erfolg zu verspielen, wenn sie nicht konsequent das Thema Sicherheit in den Mittelpunkt stellen. Da die Mehrzahl der Verbraucher nicht bereit ist, für den zusätzlichen Schutz ihrer Online-Identität zu bezahlen, sind die Unternehmen gefordert, für entsprechende Sicherheit zu sorgen. Natürlich wollen Marken ihren Kunden ein personalisiertes, angenehmes Einkaufserlebnis bieten. Dazu müssen sie den Wert und die Bedeutung starker Identity Management-Strategien verstehen. Außerdem kann es nicht schaden, den Verbrauchern klar und deutlich zu zeigen, was man alles tut, um ihre Online-Identität zu schützen.

Mehr darüber, wie Identity und Access Management (IAM) Ihnen helfen kann, die persönlichen Daten Ihrer Kunden zu schützen, erfahren Sie auf pingidentity.de.

METHODIK

Ping Identity hat über das Marktforschungsunternehmen MarketCube in den USA sowie in Großbritannien, Frankreich und Deutschland ein repräsentatives Teilnehmer-Panel von 3.264 Erwachsenen befragt. Diese waren älter als 18 Jahre und nutzen zumindest eine Website/einen Online-Service der folgenden Kategorien: Shopping, Banking, Film/TV, Musik, Behördenservices und Reise oder Apps wie Uber und Lyft. Zudem mussten die Teilnehmer in den letzten zwölf Monaten auf einer Website oder in einer App mindestens eine der folgenden Angaben gemacht haben: Anschrift, Geburtsdatum, Rufnummer, Kreditkartennummer, Bankverbindung, Sozialversicherungsnummer oder Führerscheinnummer. Die regionale Verteilung der Befragten stellt sich folgendermaßen dar: USA: 1.004, Großbritannien: 753, Frankreich: 754, Deutschland: 753. Die Umfrage wurde zwischen dem 21. und dem 25. Mai 2018 online durchgeführt. Die Fehlerspanne beträgt +/- 1,7 Prozentpunkte.

#3375 (DE) | 11.18 | v001