VERBRAUCHERUMFRAGE 2019:

VERTRAUEN UND RECHENSCHAFTSPFLICHT IM ZEITALTER DES DATENMISSBRAUCHS

EINLEITUNG

Datenschutz und Sicherheit werden immer wichtiger für die moderne Online-Erfahrung. Die Verbraucher werden weltweit mit Schlagzeilen über den grassierenden Missbrauch von Daten bombardiert, während umfangreiche Sicherheitsverletzungen weiterhin an der Tagesordnung sind. Ping Identity wollte einen tieferen Einblick erhalten, welche Auswirkungen dieses turbulente Umfeld auf die Beziehungen der Verbraucher zu ihren Dienstleistern und damit auch auf das Sicherheitsverhalten der Kunden im Allgemeinen hat, und startete zu diesem Zweck eine Umfrage mit mehr als 4000 Personen in den USA, Großbritannien, Australien, Frankreich und Deutschland.

Die Ergebnisse zeigen, dass die Verbraucher den Unternehmen den Schutz ihrer Online-Informationen nicht mehr wirklich zutrauen und ohne Weiteres bereit wären, diese Unternehmen für Sicherheitslücken und andere Vertrauensbrüche, wie z. B. Datenschutzverletzungen, zur Verantwortung zu ziehen. Gleichzeitig zeigen die Verbraucher jedoch auch ein generelles Unverständnis für die Risiken, denen sie ausgesetzt sind, und eine begrenzte Kenntnis der bewährten Verfahren zum Schutz ihrer Daten im Internet. Durch diesen Widerspruch in Haltungen und Handlungsweisen sind sie möglicherweise schlecht geschützt und setzen sich einer nicht zu unterschätzenden Gefahr aus.

WICHTIGSTE ERKENNTNISSE

- **81 % aller Befragten würden nach einer Datenschutzverletzung von einer Marke Abstand nehmen**. Diese Zahl ist gegenüber 2018 leicht gestiegen (78 %), wobei 25 % sich vollständig von der Marke abwenden würden.
- **63 % der Teilnehmer waren der Meinung, ein Unternehmen sei selbst dann für den Schutz der Benutzerdaten verantwortlich,** wenn Benutzer Opfer von Phishing-Betrug werden oder unverschlüsselte WiFi-Verbindungen verwenden.
- **Mehr als die Hälfte (55 %) aller Befragten erklärte, dass wenn ein Unternehmen ihre personenbezogenen Daten ohne Erlaubnis weitergäbe, sie dies mehr als alles andere davon abhalten würde, die Produkte dieser Marke weiterhin zu nutzen,** sogar noch mehr als eine Datenschutzverletzung (27 %).
- **Fast die Hälfte (47 %) der Gruppe gab zu, anderen ihr Passwort für einen Unterhaltungs- oder E-Commerce-Dienst weitergegeben zu haben.** 24 % der Befragten gab an, sie würden ihre Passwörter für Unterhaltungs- und E-Commerce-Websites wahrscheinlich auch für einen Dienst wiederverwenden, der mehr persönliche Informationen, wie E-Mail und Banking, freischalten kann.
- **65 % der Menschen empfinden die Anmelde-Verfahren als frustrierend,** was nicht überraschend ist, wenn man bedenkt, dass ein genau so hoher Anteil der Befragten mindestens einmal pro Jahr aus ihren Konten ausgesperrt werden. Dieser Verdruss hat Folgen: Ein Drittel (33 %) der Personen haben die Nutzung eines Gerätes, einer App oder eines Dienstes eingestellt oder aber eine schlechte Bewertung nach einer nicht zufriedenstellenden Anmeldeerfahrung abgegeben.

KUNDEN MACHEN DIE UNTERNEHMEN FÜR DATENSICHERHEIT VERANTWORTLICH

WICHTIGSTE BOTSCHAFT

In den letzten Jahren ist die Datensicherheit zu einem wichtigen Anliegen der Verbraucher geworden. Heutzutage lasten die Menschen den Unternehmen die gesamte Bürde des Datenschutzes auf und ziehen sie stärker zur Verantwortung. Datenverletzungen veranlassen immer mehr Menschen zu einer Veränderung ihres Verhaltens gegenüber ihren favorisierten Firmen und dazu, nach einer Datenschutzverletzung vollständig Abstand zu nehmen. Die nachstehenden Ergebnisse zeigen das Ausmaß, in dem eine Datenschutzverletzung potenzielle Kunden von der Interaktion mit einer Marke abschrecken, was sich letztendlich negativ auf den Gewinn eines Unternehmen auswirken kann.

UNTERSTÜTZENDE INFORMATIONEN

STÄRKERE SICHERHEITSBEDENKEN

- 49 % der Menschen erklären, sie seien heute stärker um den Schutz ihrer personenbezogenen Daten besorgt, als noch vor einem Jahr, wohingegen weitere 49 % ebenso besorgt sind, wie sie es auch im vergangenen Jahr waren.
- In den USA ist die Befürchtung am weitesten verbreitet, wo 60 % aller Befragten angeben, ihre Sorge sei seit dem letzten Jahr gestiegen. In anderen Ländern sind es hingegen durchweg weniger als 50 %.

DIE EINSÄTZE FÜR GEHACKTE UNTERNEHMEN SIND HOCH.

- 63 % der Befragten sind der Meinung, ein Unternehmen sei **immer** für den Schutz der Benutzerdaten verantwortlich, selbst dann, wenn Benutzer Opfer von Phishing-E-Mails werden oder unsichere Verfahren benutzen, wie beispielsweise unverschlüsselte Wi-Fi-Verbindungen oder die Mehrfachverwendung von Passwörtern. In vielen dieser Fälle wird den Unternehmen die Schuld gegeben, obwohl sie wenige oder gar keine Möglichkeiten hatten, um dies zu verhindern.
- Nur 14 % der Befragten würden sich nach einer Datenschutzverletzung bei einer Anwendung/einem Dienst zu Nutzung anmelden.
- 81 % würden nach einer Datenschutzverletzung keine Geschäft mehr mit einer Marke tätigen (bis zu 3 % von 2018), und 25 % würden jegliche Interaktionen einstellen.

PROBLEME MIT DATENSICHERHEIT UND DATENSCHUTZ SCHÜREN DAS MISSTRAUEN DER VERBRAUCHER

SICHERHEIT = SCHUTZ DER EIGENEN PERSON

Lasst nicht zu, dass andere meine Daten stehlen!

DATENSCHUTZ = RESPEKT FÜR DIE EIGENE PERSON

Verkauft oder verbreitet meine Daten nicht ohne meine Zustimmung.

WICHTIGSTE BOTSCHAFT

Das Vertrauen in die Fähigkeit von Unternehmen, personenbezogene Daten und Privatsphäre zu schützen, nimmt ab. Das Vertrauen in die Social Media-Unternehmen ist am geringsten, aber sogar Finanzdienstleister und Gesundheitsunternehmen (die Hüter der heiligsten Daten) haben ihre Sicherheitszyniker. Dass man sogar den Banken nicht mehr vertraut, ist doch etwas verwunderlich angesichts ihrer Vorreiterrolle bei der Datensicherheit. Bei den Gesundheitsdienstleistern könnten Angriffe durch Erpressungstrojaner das Verbrauchervertrauen zersetzen.

UNTERSTÜTZENDE INFORMATIONEN

KUNDENVERTRAUEN NACH MARKTSEKTOR

- Von den fünf großen Marktsektoren wird den Social Media-Unternehmen das geringste Vertrauen entgegengebracht: Nur etwa 28 % der Teilnehmer fühlen sich auf diesen Plattformen mit dem dort geleisteten Schutz ihrer personenbezogenen Daten sicher aufgehoben – in Anbetracht der Datenschutz-Ausrutscher der letzten Jahren ist dies nicht weiter verwunderlich.
- Weniger als zwei Drittel der Menschen (63 %) sind zuversichtlich, dass die Finanzdienstleister ihre Daten schützen können, während die Gesundheitsversorgung mit 61 % etwas schlechter abschneidet.
- Das Vertrauen in Gastgewerbe und Einzelhandel rangiert mit 38 % bzw. 36 % in der Mitte zwischen den oben genannten Sektoren.

WACHSENDE TECHNOLOGISCHE BEDENKEN

- Von den drei Schlüsselthemen – Online-Datensicherheit, Online-Datenauswertung und Online-Kontozugriff – ist die Mehrheit (57 %) der Befragten vorrangig um die Sicherheit ihrer Online-Daten besorgt, gefolgt von einem weiteren Viertel (25 %), die nicht möchten, dass die Unternehmen ihre Daten für Marketing- und Werbezwecke nutzen. Dem gegenüber stehen nur 12 %, die vor allem befürchten, auf den schnellen und problemlosen Zugang zu ihren Online-Konten verzichten zu müssen und nur 5 % die sich um keines der drei Themen Gedanken machen.
- Die Menschen gehen davon aus, dass die Datenschutzprobleme zunehmen werden: Für 39 % liegt das wichtigste technische Anliegen im kommenden Jahr beim Datenschutz, erst danach folgen Sicherheit, Überwachung, Falschinformationen im Internet oder Automatisierung.
- Der Missbrauch von Daten durch Unternehmen wird generell kritischer gesehen als das Hacking: 54 % erklären, wenn ein Unternehmen ihre Daten ohne Zustimmung weitergäbe, würde sich dies negativ auf ihre Haltung gegenüber dieser Organisation auswirken, während nur 29 % dies auch für einen Hack angeben.

Interessanterweise machen sich die Deutschen tendenziell mehr Sorgen wegen der Überwachung als andere Länder, während die USA sich mehr für den Datenschutz interessiert. So waren die Befragten in den Ländern der Europäischen Union (Großbritannien, Deutschland und Frankreich) weniger wegen des Datenschutzes besorgt als die Teilnehmer in den USA, was wahrscheinlich auf die Auswirkungen der DSGVO zurückzuführen ist.

DATENSCHUTZ TRIUMPHIERT ÜBER KOMFORT (UND SOGAR ÜBER DATENSICHERHEIT)

WICHTIGSTE BOTSCHAFT

Die Verbraucher tendieren eher zu den Datenschutztechniken und -praktiken, die sie als sicherer einstufen, statt die bequemste Option zu wählen. Der Datenschutz hat also Vorrang, und Verbraucher verzichten auf Optionen, die sie für sicherer halten, wenn diese eine Gefährdung des Datenschutzes darstellen. Dennoch sind die Verbraucher nach wie vor über Anmeldeerfahrungen und die Sperrung ihrer Online-Konten genervt und handeln, wenn ihnen das Anmeldeverfahren zu unbequem wird.

UNTERSTÜTZENDE INFORMATIONEN

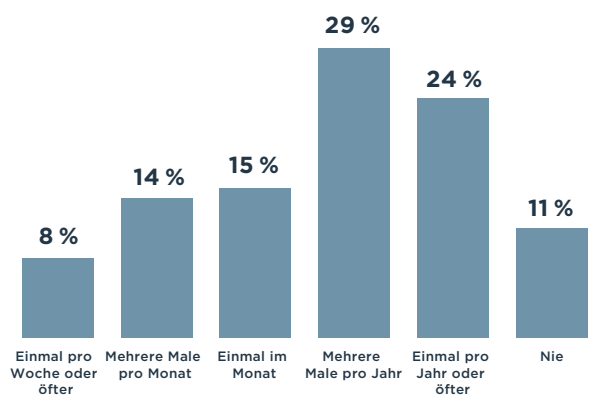
SICHERHEIT, DATENSCHUTZ UND KOMFORT IM VERGLEICH

- In einem Umfeld wachsender Sicherheitsbedenken ziehen die Menschen zwar die Datensicherheit dem Komfort vor, legen aber allerhöchsten Wert auf den Datenschutz.
- Die Multifaktor-Authentifizierung gehört zur am häufigsten verwendeten Anmeldemethode und wird von den Befragten als sicherste Lösung priorisiert.
- Das Einrichten eines eindeutigen und sicheren Passworts für jedes Konto wurde als dritthöchste Sicherheitsoption eingestuft und mit der Multifaktor-Authentifizierung als der am häufigsten verwendeten Methode in Verbindung gebracht. Dennoch wurde der mangelnde Komfort gemeinhin als Hemmschuh angeführt: 38 % derjenigen, die keine sicheren und eindeutigen Passwörter verwenden, begründeten dies mit der Umständlichkeit, und auch 30 % derjenigen, die keine Multifaktor-Authentifizierung verwenden, führten diesen Grund an.
- Bei der Wahl der Anmeldemethode wiegen Argumente des Datenschutzes bei den Verbrauchern schwerer als die Sicherheit. So rangiert beispielsweise die Biometrie an zweiter Stelle in puncto Sicherheit und Komfort. Diesbezüglich zweifelten 49 % den Datenschutz bei der Gesichtserkennung an, die zwar eine gängige Form der Technologie ist, jedoch nur von 31 % der Befragten genutzt wird.
    - > Bei denjenigen, die Datenschutzbedenken hinsichtlich der Gesichtserkennung geäußert haben, bestand die größte Befürchtung darin, die App könne ihre Daten an andere weiterleiten oder die Regierung könne sie zu Überwachungszwecken verwenden.

KRITISCHE ASPEKTE DER ANMELDUNG

- Obwohl der Komfort für die Verbraucher nicht länger an erster Stelle steht, empfinden doch (65 %) die Anmeldungsmethoden als lästig.
- 65 % der Beteiligten berichten, sie müssten ihre Passwörter mindestens eine paar Male pro Jahr ändern, nachdem sie von den Konten ausgeschlossen wurden, und 22 % erleben dies sogar mehrmals im Monat.
- Ein Drittel (33 %) der Personen haben die Nutzung eines Gerätes, einer App oder eines Dienstes eingestellt oder aber eine schlechte Bewertung nach einer nicht zufriedenstellenden Anmeldeerfahrung abgegeben.

Wie oft müssen Sie Ihr Passwort ändern, nachdem Sie aus Ihrem Konto ausgeschlossen wurden (z.B weil Sie Ihr Passwort vergessen haben)?



DIE VERBRAUCHER VERWENDEN NOCH IMMER RISKANTE SICHERHEITSPRAKTIKEN

WICHTIGSTE BOTSCHAFT

Obwohl die Verbraucher also wegen Datensicherheit und -schutz Sorge haben, treffen sie doch riskante Entscheidungen hinsichtlich der Datensicherheit. Jüngere Menschen gehen bei der Datensicherheit im Allgemeinen mehr Risiken ein. Da Unternehmen häufig selbst dann für Betrug und Datenschutzverletzungen verantwortlich gemacht werden, wenn diese auf potenziell unsichere Verbraucherentscheidungen zurückzuführen sind, müssen sie zum Schutz ihrer Kundendaten zusätzliche Anstrengungen unternehmen.

UNTERSTÜTZENDE INFORMATIONEN

DIE WICHTIGSTEN SICHERHEITSFEHLER

- 43 % verwenden kein starkes und eindeutiges Passwort für jedes Konto.
- Fast die Hälfte (47 %) der Befragten ließ zu, dass andere ihr Passwort für einen Unterhaltungs- oder E-Commerce-Dienst nutzen. und bei 18 % geschah dies sogar häufig. Fast einen Viertel (24 %) derer, die ein Passwort weitergegeben hatten, tendieren dazu, das gleiche Passwort auch für einen Dienst zu verwenden, bei dem personenbezogene Informationen freigegeben werden, wie eine Bank oder ein E-Mail-Konto.
- Ein Viertel (26 %) der Teilnehmer versäumen es, ihr Passwort für einen Onlinedienst sofort zu ändern, nachdem dessen Anbieter gehackt wurde.

JEDE GENERATION HAT IHRE SCHLECHTEN GEWOHNHEITEN

Die Bereitschaft, Passwörter weiterzugeben, ist bei der Boomer-Generation am geringsten (nur 20 %), bei der GenZ sind es 71 % und bei den Millennials dann 58 %.

Für die Mehrfachverwendung von Passwörtern findet man die meisten Übeltäter in der GenZ (34 %) und bei den Millennials (31 %).

DIE DISKREPANZ: DAS DENKEN UND HANDELN DER VERBRAUCHER GEHT NICHT IMMER HAND IN HAND

- Die Schwierigkeit, ein starkes und eindeutiges Passwort für jedes Konto zu verwalten, wird generell unterschätzt (oder man überschätzt seine eigene Fähigkeit, dies zu meistern).
  - > 46 % der Menschen bezeichnen dies als die Option mit der höchsten oder zweithöchsten Bequemlichkeit, noch vor Biometrie, einem Passwortmanager und Single-Sign-On-Lösungen, die tatsächlich einfacher zu bedienen und zu verwalten sind.
  - > Und zwar obwohl 65 % der Befragten angeben, mehrere Male pro Jahr ihr Passwörter ändern zu müssen, weil sie zu Ihrem Konto nicht mehr zugreifen können. Dies bedeutet, dass sie mehr als sicher sind, sich ihre eindeutigen Passwörter für jedes einzelne Konto selbst merken zu können.

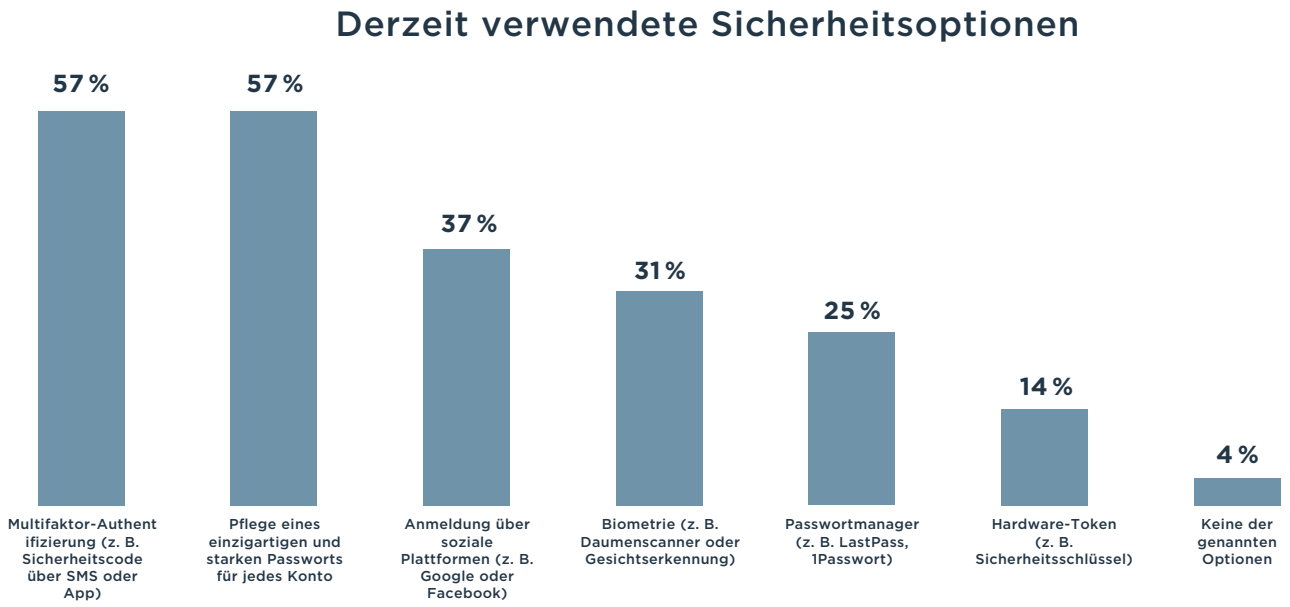
WIE ERKLÄRT SICH DIESER MANGEL AN SICHERHEITSBEWUSSTSEIN?

WICHTIGSTE BOTSCHAFT

Missverständnisse und mangelndes Bewusstsein führen dazu, dass sich die Verbraucher weiterhin riskanter Sicherheitspraktiken bedienen, obwohl sie sehr um die Sicherheit besorgt sind. Die Menschen kennen viele der sicheren Anmeldemethoden nicht oder wissen nicht, wie sie verwendet werden.

VERKANNTE DATENSICHERHEIT

- Die Sicherheit der Multifaktor-Authentifizierung wird von 56 % der Befragten an erster oder zweiter Stelle eingestuft. Trotzdem wird sie bisher von 43 % nicht verwendet. Von dieser Gruppe wiederum haben 16 % keine Ahnung, wie man sie benutzt, 19 % denken, es sei für sie nicht verfügbar und 11 % haben noch nie davon gehört.
- Nur 25 % aller Befragten verwenden aktuell einen Passwortmanager. Von denjenigen ohne Passwortmanager wissen 22 % nicht, wie man diese Anmeldemethode verwendet, und 17 % haben noch nie davon gehört.
- Hardware-Token verstehen und nutzen die wenigsten der Befragten. Nur 14 % geben an, diese Option zu nutzen, und von den anderen haben 20 % noch nie von einem Hardware-Token gehört und 24 % wissen nicht, wie man damit umgeht.



Die Menschen vertrauen mehr auf Passwörter als auf andere Sicherheitsvorkehrungen, bei denen das Gelingen eines Angriffs oder einer Kompromittierung der Daten weniger wahrscheinlich ist. So gingen die Befragten davon aus, dass die Pflege eines eindeutigen und sicheren Passworts für jedes Konto sicherer sei als ein Hardware-Token oder ein Passwortmanager. Tatsächlich sind aber die risikobehafteten Passwortpraktiken die Grundursache für die umfangreichen Schäden durch Datenschutzverletzungen. Zum einen sind die Praktiken der Verbraucher zu lasch, zum anderen lassen sich ihre Passwörter mit Hilfe automatisierter Tools auch leicht knacken. Die Wiederverwendung von Passwörtern ermöglicht Kriminellen den problemlosen Zugriff auf weitere Websites und Benutzerkonten.

SCHLUSSFOLGERUNG:

Verbraucher in aller Welt verlangen von den Unternehmen höhere Standards, wenn es um Datenschutz und -sicherheit geht. Gleichzeitig haben die Verbraucher nur geringes Vertrauen in die Fähigkeit der Unternehmen, ihre Daten und ihre Privatsphäre zu schützen, während ihre eigenen persönlichen Sicherheitsmaßnahmen und -praktiken alles andere als perfekt sind. Für Unternehmen, die gegenüber den modernen Realitäten einer digitalen Landschaft nach den Datenschutzverletzungen offen sind, bietet sich eine nie da gewesene Gelegenheit, Kundenvertrauen und -loyalität zu gewinnen – angefangen bei der Schaffung der richtigen Balance von Datenschutz, Sicherheit und Komfort.

Erfahren Sie mehr darüber, wie Ihnen Identitäts- und Zugriffsmanagement helfen kann, Kundendaten zu schützen, ohne den Komfort zu beeinträchtigen. Besuchen Sie pingidentity.com.

METHODIK

Ping Identity hat Market Cube mit der Befragung von 4017 Verbrauchern in den USA, Großbritannien, Frankreich und Deutschland beauftragt, die mindestens 18 Jahre alt sind und mindestens eine der folgenden Online-Sites oder -Dienste nutzen: Online-Shopping, Online-Banking, Film/TV-Dienstleistungen, Musikdienste, Behördendienste, Reise-Websites oder Transportdienstleistungen. Darüber hinaus müssen die Befragten in den letzten zwölf Monaten mindestens eine der folgenden Informationen auf einer Website oder App eingegeben haben: Adresse, Geburtsdatum, Telefonnummer, Kreditkartennummer, Bankverbindung, Sozialversicherungsnummer oder Führerscheinnummer. Die geografische Aufteilung der Befragten stellte sich dar wie folgt: Vereinigte Staaten: 1004, Großbritannien: 753, Australien: 755, Frankreich: 751, Deutschland: 754. Die Umfrage wurde online zwischen dem 31. Juli und dem 6. August 2019 durchgeführt. Die Fehlerspanne beträgt plus oder minus 1,6 Prozentpunkte.

#3464 | 10.08.19 | v003