Maximierung des Nutzens von Datenschutzinvestitionen

Benchmark-Studie zum Datenschutz

CISCO

Zusammenfassung

Am 25. Mai 2018 trat die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union in Kraft, aber auch Datenschutzgesetze und Vorschriften auf der ganzen Welt werden laufend geändert und erweitert.

Kunden fragen während des Kaufzyklus häufiger nach, wie ihre Daten erfasst, verwendet, übertragen, geteilt, gespeichert und vernichtet werden.

Die meisten Organisationen haben in Mitarbeiter, Prozesse, Technologien und Richtlinien investiert, um Datenschutzanforderungen von Kunden zu erfüllen und erhebliche Geldstrafen und andere Sanktionen zu vermeiden, und das werden sie auch weiter tun. Trotzdem gelangen bei Datensicherheitsverletzungen weiterhin persönliche Daten von Millionen von Menschen an die Öffentlichkeit und Organisationen machen sich Gedanken über die Produkte, die sie kaufen, die Services, die sie nutzen, die Mitarbeiter, die sie beschäftigen und über die Tatsache, mit wem sie Partnerschaften eingehen und allgemein Geschäfte machen. Demzufolge haben Kunden während des Kaufzyklus mehr Fragen dazu, wie ihre Daten erfasst, verwendet, übertragen, geteilt, gespeichert und vernichtet werden. In der Studie vom letzten Jahr (Cisco Benchmark-Studie zum Fortschritt von Datenschutzbemühungen 2018) stellte Cisco Daten und Einblicke zu den negativen Auswirkungen dieser datenschutzrechtlichen Bedenken auf den Kaufzyklus und die Zeitpläne vor. In der diesjährigen Studie werden diese Ergebnisse aktualisiert und die Vorteile im Zusammenhang mit Datenschutzinvestitionen untersucht.

Die Benchmark-Studie zum Datenschutz von Cisco nutzt Daten aus der eigenen jährlichen Benchmark-Studie zum Thema Cybersicherheit. Dabei handelt es sich um eine Doppelblindstudie, die von über 3200 Sicherheitsexperten in 18 Ländern und aus allen wichtigen Industrien und Ländern durchgeführt wird. Viele der auf den Datenschutz bezogenen Fragen richteten sich an über 2.900 Teilnehmer, die mit den Datenschutzprozessen in ihren Organisationen vertraut sind. Die Teilnehmer wurden dazu befragt, inwieweit sie die Vorgaben der DSGVO erfüllen, ob es wegen Datenschutzbedenken von Kunden zu Verzögerungen im Vertriebszyklus kam, ob Verluste aus Datensicherheitsverletzungen entstanden sind und welche Praktiken sie aktuell anwenden, um das Potenzial ihrer Daten voll auszuschöpfen.

Die Ergebnisse dieser Studie zeigen deutlich, dass Organisationen von Datenschutzinvestitionen profitieren, die über bloße Compliance hinausgehen. Organisationen, welche die DSGVO-Vorgaben vollständig erfüllen, profitieren von geringeren Verzögerungen im Vertriebszyklus wegen Datenschutzbedenken von Kunden als diejenigen, die noch nicht so weit sind. Organisationen mit dem Siegel „DSGVO-ready“ verzeichneten auch weniger Datensicherheitsverletzungen, und falls doch welche auftraten, waren weniger Datensätze davon betroffen und die Systemausfallzeiten kürzer. Demzufolge fielen die Gesamtkosten für Datensicherheitsverletzungen geringer aus als in Organisationen, die nicht DSGVO-ready sind. Obwohl sich Unternehmen auf die Erfüllung der Datenschutzvorschriften und Anforderungen konzentrierten,

> **„Datenschutz ist eine entscheidende Komponente für den Unternehmenserfolg, was die Sicherung von Daten und die Förderung von Innovation angeht.“**
>
> **John N. Stewart, Senior Vice-President und Chief Security and Trust Officer, Cisco**

gaben fast alle Unternehmen an, dass sie aus diesen, über bloße Compliance hinausgehenden Investitionen, weiteren geschäftlichen Nutzen ziehen. Dieser mit dem Datenschutz zusammenhängende Nutzen bietet Organisationen Wettbewerbsvorteile und mithilfe dieser Studie können sie Entscheidungen bezüglich Investitionen treffen, während sie weiter an der Optimierung ihrer Datenschutzprozesse arbeiten.

„Diese Studie belegt, was Datenschutzexperten schon lange wissen: Organisationen profitieren von Datenschutzinvestitionen, die über bloße Compliance hinausgehen. Die Cisco Studie zeigt, dass eine strenge Einhaltung von Compliance-Vorschriften den Vertriebszyklus verkürzt und das Vertrauen von Kunden erhöht.“

Peter Lefkowitz, Chief Digital Risk Officer,
Citrix Systems and 2018 Board Chairman,
International Association of Privacy Professionals (IAPP)

Die Ergebnisse

59 % der Unternehmen geben an, dass sie jetzt alle oder die meisten DSGVO-Anforderungen erfüllen; 29 % erwarten, dieses Ziel innerhalb eines Jahres zu erreichen. Die größten Herausforderungen der DSGVO-Readiness sind: Datensicherheit, Mitarbeiterschulung und Schritthalten mit der Weiterentwicklung von Regelungen.

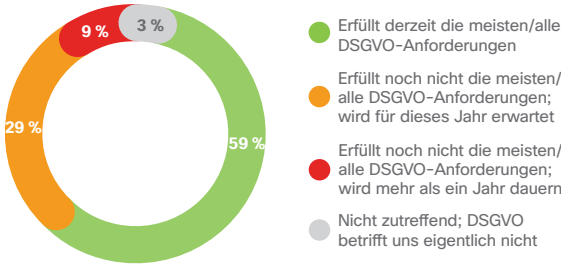
DSGVO-Readiness

Von den Teilnehmern an der Benchmark-Studie zum Datenschutz gaben 59 % an, dass sie heute alle oder die meisten DSGVO-Anforderungen erfüllen. (Siehe Abbildung 1) Weitere 29 % sagten, sie wollten innerhalb eines Jahres DSGVO-ready werden, und 9 % sagten, es würde länger als ein Jahr dauern, um dieses Ziel zu erreichen. Die DSGVO gilt für in der EU ansässige Unternehmen und für die Verarbeitung von personenbezogenen Daten, die über Einzelpersonen innerhalb der EU erfasst wurden. Das Interessante dabei ist, dass nur 3 % der Befragten in unserer globalen Studie der Meinung waren, die DSGVO beträfe ihre Organisation nicht.

Auf die einzelnen Länder bezogen lag die DSGVO-Readiness zwischen 42 % und 76 %. (Siehe Abbildung 2) Es ist wenig überraschend, dass die an der Studie beteiligten europäischen Länder (Spanien, Italien, Großbritannien, Frankreich, Deutschland) im Allgemeinen besser abschnitten.

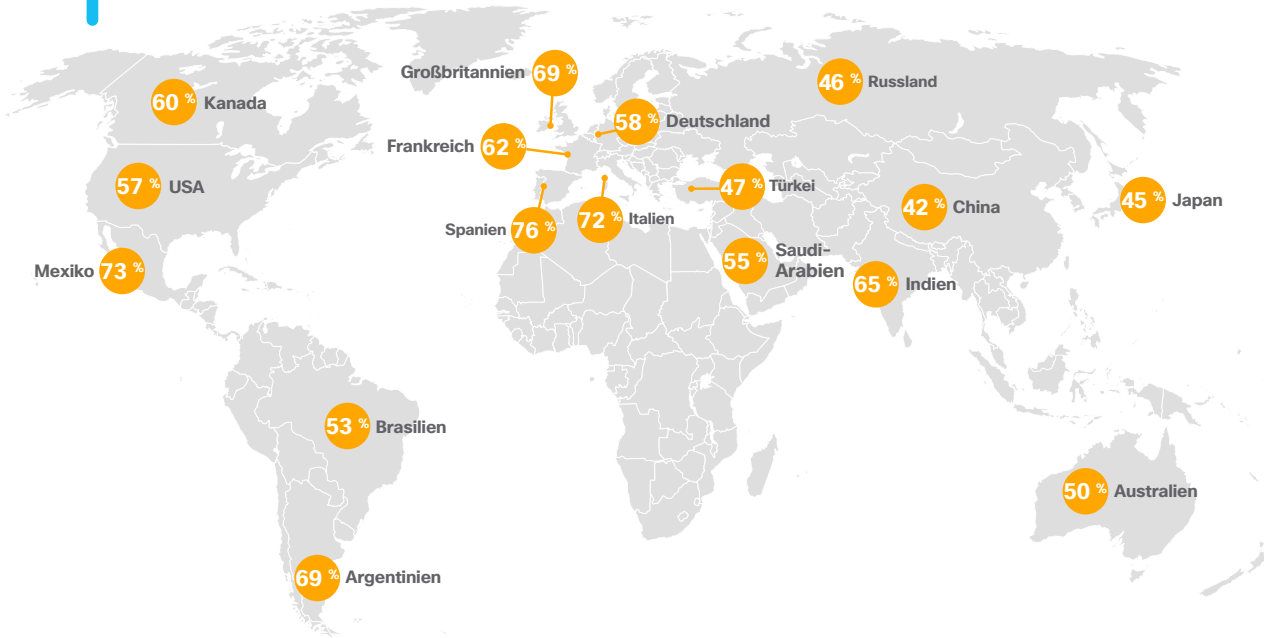
In unserer globalen Studie gaben nur 3 % der Befragten an, dass die DSGVO ihre Organisation ihrer Meinung nach nicht beträfe.

Abbildung 1 DSGVO-Readiness
Prozentsatz der Befragten, N=3206



Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019; N=3206

Abbildung 2 DSGVO-Readiness nach Land
Prozentsatz der Befragten, N=3206



Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

Die Befragten sollten die größten Herausforderungen ihrer Organisationen bei ihren Bemühungen zur Erlangung der DSGVO-Readiness nennen. Am häufigsten fielen Begriffe wie Datensicherheit, interne Schulungen, sich wandelnde Vorschriften und Privacy by Design-Anforderungen. (Siehe Abbildung 3).

Abbildung 3 Größte Herausforderungen bei der Erlangung der DSGVO-Readiness
(Prozentsatz der Befragten, N=3098

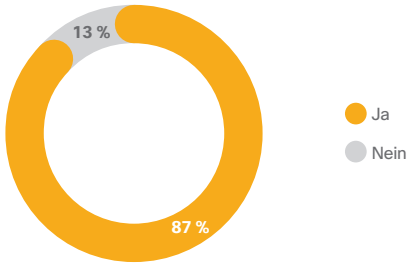
42 %	Erfüllung von Datensicherheitsanforderungen
39 %	Interne Schulungen
35 %	Schritt halten mit laufenden Weiterentwicklungen von Vorschriften
34 %	Einhaltung von Privacy By Design-Anforderungen
34 %	Erfüllung von Zugriffsanfragen für Datensubjekte
31 %	Katalogisierung und Inventarisierung von Daten
30 %	Ermöglichung von Anforderungen der Datenlöschung
29 %	Einstellung/Ernennung von Data Protection Officers für jedes relevante Land
28 %	Lieferantenmanagement

Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

Vertriebsverzögerungen aus Datenschutzgründen

Die Teilnehmer wurden gefragt, ob aufgrund von Datenschutzbedenken der Kunden Verzögerungen in ihren Vertriebszyklen auftreten. 87 % der Befragten gaben an, dass es bei bestehenden oder potenziellen Kunden zu Vertriebsverzögerungen kommt. (Siehe Abbildung 4) Dies ist deutlich höher als die 66 %, die in der Studie vom Vorjahr Vertriebsverzögerungen meldeten. Wahrscheinlich ist das Ergebnis auf eine zunehmende Sensibilisierung für den Datenschutz, die Umsetzung von DSGVO-Vorgaben und das Aufkommen von anderen Datenschutzgesetzen und Anforderungen zurückzuführen. Datenschutz ist in vielen Organisationen zur Chefsache geworden und Kunden sorgen dafür, dass ihre Anbieter und Geschäftspartner ihre Fragen zum Datenschutz zufriedenstellend beantworten können, bevor sie Geschäfte mit ihnen machen.

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



Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

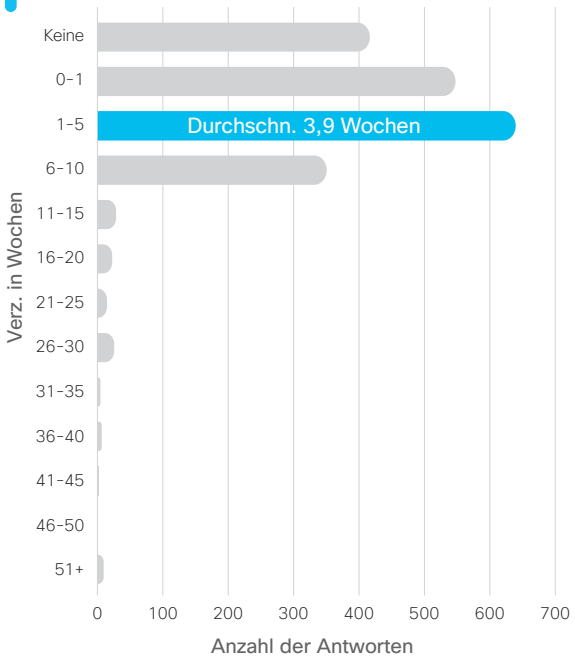
Bei der Frage zur Dauer der Verzögerungen gingen die Schätzungen weit auseinander. Durchschnittliche Vertriebsverzögerungen bei bestehenden Kunden betrugen 3,9 Wochen und mehr als 94 % der Organisationen meldeten Verzögerungen zwischen 0 und 10 Wochen. Gleichwohl gab es einige Organisationen, bei denen es zu Verzögerungen von bis zu 25 bis 50 Wochen oder noch länger kam. (Siehe Abbildung 5) Beachten Sie, dass durchschnittliche Verzögerungen beim Vertrieb an potenzielle Kunden 4,7 Wochen betrugen, was wahrscheinlich auf längere Zeiträume

Für die meisten Organisationen werden Verzögerungen des Vertriebs aufgrund von Datenschutzbedenken der Kunden weiterhin ein Problem bleiben.

87 % gaben an, dass es beim Verkauf an bestehende oder potenzielle Kunden zu Verzögerungen kommt, was im Vergleich zum Vorjahr deutlich mehr ist.

zurückzuführen ist, die für eine angemessene Behandlung von Datenschutzbedenken potenzieller Kunden nötig sind. Die üblichen Verzögerungen bei bestehenden und potenziellen Kunden sind deutlich kürzer als die durchschnittlichen 7,8 Wochen, die in der Studie vom vergangenen Jahr genannt wurden. Das liegt womöglich daran, dass Unternehmen Kundenfragen zum Thema Datenschutz jetzt besser beantworten können als im Vorjahr.

Abbildung 5 Verzögerungen bei der Behandlung von Datenschutzbedenken von Kunden
Prozentsatz der Befragten, N=2081



Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

Auf die einzelnen Länder bezogen betrugen Vertriebsverzögerungen bei bestehenden Kunden 2,2 bis 5,5 Wochen. Längere Verzögerungen gibt es in der Regel dort, wo Datenschutzanforderungen streng sind oder sich im Wandel befinden und Organisationen daran arbeiten, auf die Bedenken von Kunden einzugehen. (Siehe Abbildung 6.)

Die Hauptgründe für datenschutzbezogene Vertriebsverzögerungen:

- *Untersuchung spezifischer Kundenwünsche*
- *Übersetzung von Datenschutzinformationen in die Sprache des Kunden*
- *Informieren von Kunden über Datenschutzpraktiken und -prozesse des Unternehmens*
- *Neugestaltung von Produkten, um Datenschutzanforderungen von Kunden zu erfüllen*

Abbildung 6 Verteilung von Vertriebsverzögerungen nach Land
Prozentsatz der Befragten, N=2081

Land	Ø Verzög. (Wochen)
Argentinien	3,9
Australien	3,9
Brasilien	5,2
Kanada	5,1
China	3,5
Frankreich	4,2
Deutschland	3,1
Indien	4,9
Italien	2,6
Japan	4,1
Mexiko	2,9
Russland	2,5
Saudi-Arabien	4,8
Spanien	5,5
Türkei	2,2
Großbritannien	4,9
USA	3,7
Gesamt	3,9

Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

Vertriebsverzögerungen sorgen geringstenfalls dafür, dass Erlöse erst etwas später gebucht werden können. Das kann dazu führen, dass Umsatzziele nicht erreicht werden, und dies wiederum wirkt sich auf Entschädigungen, Finanzierungsbeschlüsse und Beziehungen mit Investoren aus. Darüber hinaus können Verzögerungen im Vertrieb zu entgangenen Umsätzen führen, etwa wenn Kunden aus diesem Grund das Produkt eines Mitbewerbers kaufen oder ganz auf den Kauf eines Produkts oder Service verzichten.

Die Teilnehmer wurden außerdem gebeten, die Gründe für datenschutzbezogene Vertriebsverzögerungen in ihren Organisationen zu nennen. Am häufigsten wurden folgende Punkte erwähnt: Bestimmte Kundenanforderungen wurden untersucht, Informationen zum Datenschutz wurden in die Sprache des Kunden übersetzt, Kunden wurden über die Datenschutzpraktiken oder -prozesse informiert oder das Produkt musste neu gestaltet werden, um die Datenschutzanforderungen des Kunden zu erfüllen. (Siehe Abbildung 7)

Abbildung 7 Gründe für Vertriebsverzögerungen
Prozentsatz der Befragten, N=1812

49 %	Wir müssen spezifische/ungewöhnliche Anforderungen von (potenziellen) Kunden untersuchen, bevor diese mit unseren Datenschutzpraktiken einverstanden sind.
42 %	Wir müssen Informationen über unsere Datenschutzrichtlinien und -prozesse in die Sprache des (potenziellen) Kunden übersetzen.
39 %	(Potenzielle) Kunden müssen mehr über unsere Datenschutzrichtlinien oder -prozesse erfahren.
38 %	Unser Produkt oder Service muss neu gestaltet werden, um Datenschutzanforderungen von (potenziellen) Kunden zu erfüllen.
33 %	Wir können oder wollen Datenschutzanforderungen von (potenziellen) Kunden nicht erfüllen (z. B. Richtlinien für Datensicherheitsverletzungen, Anforderungen zur Datenlöschung).
28 %	Es dauert, bis die richtige Person oder ein Team gefunden ist, das Fragen von (potenziellen) Kunden beantworten kann.
17 %	Wir müssen klären, welche Seite letztendlich für die Daten verantwortlich ist.
5 %	Wir müssen Anwälte hinzuziehen, um uns Klarheit bezüglich der Rechtslage zu verschaffen.

Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

Geschäftliche Vorteile von Datenschutzinvestitionen

Organisationen, die in Maßnahmen zur Erfüllung von DSGVO-Anforderungen investiert haben, wollten in erster Linie beträchtliche Geldbußen und andere Strafen für Datenschutzverstöße vermeiden. Allerdings zeigt die Studie auch, dass diese Datenschutzinvestitionen erhebliche geschäftliche Vorteile mit sich bringen.

Was Vertriebsverzögerungen aufgrund von Datenschutzproblemen angeht, betrug die durchschnittliche Vertriebsverzögerung bei bestehenden Kunden 3,9 Wochen. Jedoch berichteten Organisationen, die alle oder die meisten DSGVO-Anforderungen erfüllen, dass ihre Vertriebsverzögerung bei durchschnittlich 3,4 Wochen lag. Bei Organisationen, die dieses Ziel erst innerhalb eines Jahres erreichen werden, sind es 4,5 Wochen und bei Organisationen, die länger als ein Jahr brauchen werden, um DSGVO-Readiness zu erlangen, sind es 5,4 Wochen. Demzufolge sind Verzögerungen in Organisationen, die nicht so gut vorbereitet sind, knapp 60 % länger als bei gut vorbereiteten. (Siehe Abbildung 8)

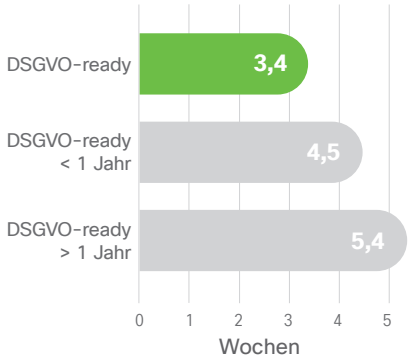
Die meisten Unternehmen berichteten im letzten Jahr von einer Datensicherheitsverletzung, allerdings war unter den Unternehmen mit DSGVO-Readiness ein niedrigerer Prozentsatz (74 %) betroffen. Bei den Organisationen, die noch ein Jahr bis zur Erreichung dieses Ziels brauchen, waren es 80 %, und unter den noch schlechter vorbereiteten Unternehmen 89 %.

Zusammenfassung der wichtigsten Ergebnisse

Unternehmen mit DSGVO-Readiness profitieren von ihren Datenschutzinvestitionen, die über bloße Compliance hinausgehen, auf verschiedene messbare Weisen. Es kam zu kürzeren Vertriebsverzögerungen aufgrund von Datenschutzbedenken von Kunden (3,4 statt 5,4 Wochen). Die Wahrscheinlichkeit einer Datensicherheitsverletzung war im letzten Jahr geringer (74 % im Vgl. zu 89 %) und falls ein Vorfall eintrat, waren weniger Datensätze betroffen (79.000 statt 212.000) und die Systemausfallzeit war kürzer (6,4 statt 9,4 Stunden). Infolgedessen fielen die Kosten im Zusammenhang mit Sicherheitsverletzungen geringer aus. Nur 37 % der Unternehmen mit DSGVO-Readiness verzeichneten im letzten Jahr Verluste von über 500.000 USD im Vergleich zu 64 % der am schlechtesten auf die DSGVO vorbereiteten Unternehmen.

Diese Ergebnisse zeigen, dass ausgereifte Datenschutzmaßnahmen für viele Unternehmen einen wichtigen Wettbewerbsvorteil darstellen. Organisationen sollten daran arbeiten, die geschäftlichen Vorteile ihrer Datenschutzinvestitionen zu maximieren, die über bestimmte Datenschutzbestimmungen hinausgehen können.

Abbildung 8 Durchschn. Wochen Verzögerung (bestehend)
Prozentsatz der Befragten, N=2081



Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

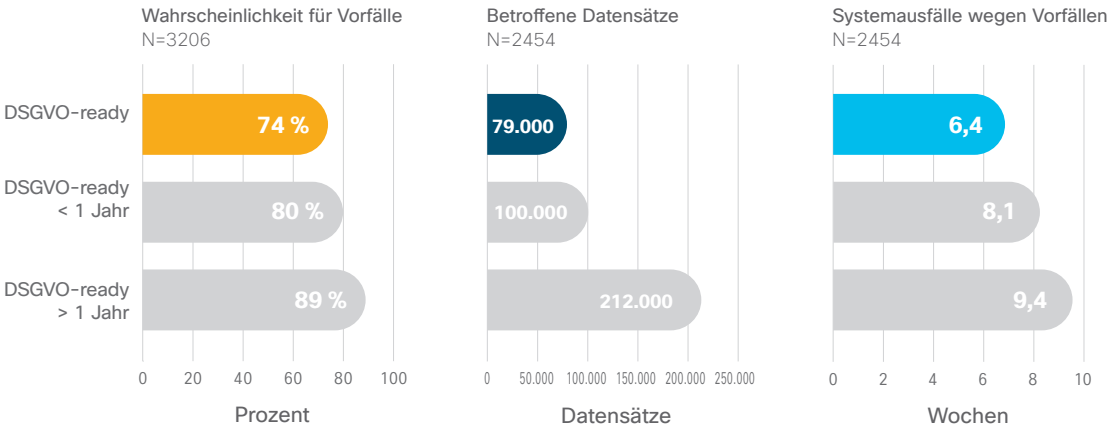
„Organisationen sind noch weit davon entfernt, den Nutzen ihrer Datenschutzinvestitionen zu maximieren. Unsere Studie zeigt, dass der Markt auf diejenigen vorbereitet ist, die in Datenbestände investieren möchten. Hierfür könnte der Datenschutz wegweisend sein.“

Michelle Dennedy, Chief Privacy Officer, Cisco

Ein weiterer messbarer Vorteil der DSGVO-Readiness liegt darin, dass sie die Häufigkeit und Auswirkungen von Sicherheitsverletzungen anscheinend verringert. Die DSGVO verlangt, dass Organisationen wissen, wo personenbezogene Daten gespeichert sind und dass sie diese angemessen schützen. Das kann dazu beigetragen haben, dass Organisationen ihre Daten und die damit verbundenen Risiken besser verstehen und dadurch Maßnahmen zum Schutz dieser Daten festlegen oder stärken können.

Die meisten Unternehmen berichteten im letzten Jahr von einer Datensicherheitsverletzung, allerdings war unter den Unternehmen mit DSGVO-Readiness ein niedrigerer Prozentsatz (74 %) betroffen. Bei den Organisationen, die noch ein Jahr bis zur Erreichung dieses Ziels brauchen, waren es 80 %, und unter den noch schlechter vorbereiteten Unternehmen 89 %. (Siehe Abbildung 9)

Abbildung 9 Geschäftliche Vorteile von Datenschutzinvestitionen



Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

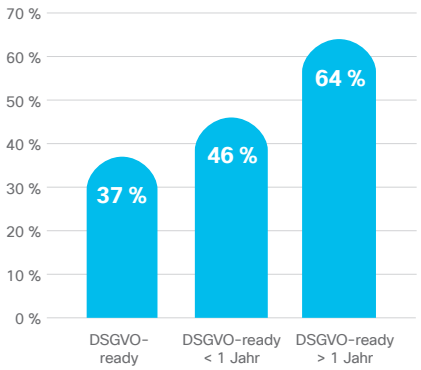
Fast alle Unternehmen (97 %) berichten, dass sie jetzt von zusätzlichen Vorteilen aus ihren Datenschutzinvestitionen profitieren, wie Flexibilität/Innovation, Wettbewerbsvorteile, betriebliche Effizienz, geringere Verluste bei Sicherheitsverletzungen, reduzierte Verzögerungen im Vertrieb und mehr Anreiz für Investoren.

Außerdem waren die Auswirkungen von Sicherheitsverletzungen in Unternehmen mit dem Siegel „DSGVO-ready“ nur gering. Bei diesen Unternehmen waren im Durchschnitt 79.000 Datensätze betroffen. Bei Unternehmen, die noch einen weiten Weg bis dahin haben, waren es hingegen 212.000 (siehe Abbildung 9).

Unternehmen mit DSGVO-Readiness hatten es infolge der Sicherheitsverletzung mit kürzeren Ausfallzeiten zu tun, was womöglich mit einer besseren Verwaltung ihrer Datenbestände zusammenhängt. In Unternehmen mit DSGVO-Readiness kam es zu einer durchschnittlichen Systemausfallzeit von 6,4 Stunden; in Organisationen, die DSGVO-Anforderungen noch lange nicht erfüllen können, waren es 9,4 Stunden. (Siehe Abbildung 9)

Da weniger Datensätze betroffen und Ausfallzeiten kürzer sind, ist es nicht verwunderlich, dass die Gesamtkosten für Unternehmen mit DSGVO-Readiness bei Datensicherheitsverletzungen geringer ausfielen. Nur 37 % dieser Unternehmen mussten bei Datensicherheitsverletzungen Verluste hinnehmen; im Vergleich dazu verloren 64 % der Unternehmen, die DSGVO-Anforderungen kaum erfüllen, mindestens 500.000 USD (siehe Abbildung 10).

Abbildung 10 Wahrsch. für Verlust von 500.000 USD nach Vorfall
Prozentsatz der Befragten, N=3206



Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

Da weniger Datensätze betroffen und Ausfallzeiten kürzer sind, ist es nicht verwunderlich, dass die Gesamtkosten für Unternehmen mit DSGVO-Readiness bei Datensicherheitsverletzungen geringer ausfielen.

Organisationen, die den Nutzen von Datenschutzinvestitionen erkennen

Die vorherigen beiden Abschnitte dieser Studie befassten sich mit den Zusammenhängen zwischen Datenschutzinvestitionen und geschäftlichen Vorteilen, wie kürzeren Vertriebsverzögerungen und weniger Datensicherheitsverletzungen, die sich finanziell weniger auswirken. Es ist interessant zu beobachten, dass die meisten Befragten viele dieser Vorteile jetzt erkennen. Auf die Frage hin, ob Datenschutzinvestitionen Vorteile mit sich bringen (z. B. höhere Flexibilität und Innovationskraft, Erreichen von Wettbewerbsvorteilen oder betrieblicher Effizienz usw.), gaben 75 % aller Befragten zwei oder mehr Vorteile an und fast alle Unternehmen (97 %) stellten mindestens einen Vorteil fest. (Siehe Abbildung 11)

Abbildung 11 Vorteile von Datenschutzinvestitionen
Prozentsatz der Befragten, N=3259

42 %	Mehr Flexibilität und Innovation dank geeigneter Datenkontrollen
41 %	Wettbewerbsvorteil gegenüber anderen Organisationen
41 %	Betriebliche Effizienz dank organisierter und katalogisierter Daten
39 %	Geringere Verluste bei Datensicherheitsverletzungen
37 %	Kürzere Vertriebsverzögerungen wegen Datenschutzbedenken von (potenziellen) Kunden
36 %	Mehr Anreize für Investoren
3 %	Keiner der oben genannten Punkte

Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

In Organisationen, die alle oder die meisten DSGVO-Anforderungen erfüllen, betrugen Vertriebsverzögerungen durchschnittlich 3,4 Wochen.

Maximierung des Werts von Daten

Datenschutz ist ein wichtiger Aspekt der Anstrengungen einer Organisation, den Wert ihrer Datenbestände während des Lebenszyklus von Daten zu maximieren. Wie jede andere Ressource sollten Daten effizient erfasst, gespeichert, geschützt, genutzt und archiviert bzw. gelöscht werden. Organisationen, die den Wert ihrer Daten auf geeignete Weise maximieren, können durch den Aufbau des Kundenvertrauens deutlich profitieren und sorgfältig geschützte und gepflegte Daten verwenden, um das Kundenerlebnis zu verbessern und Mehrwert für alle Beteiligten zu schöpfen.

Die Teilnehmer an dieser Studie wurden zu den diversen Merkmalen befragt, die in ausgereifteren Datenumgebungen beobachtet werden. Das gibt es beispielsweise das Vorliegen eines kompletten Datenkatalogs, die Vernetzung von Daten mit anderen Ressourcen, die Einstellung eines Chief Data Officers und die externe Monetarisierung von Daten. (Siehe Abbildung 12) Weniger als die Hälfte der Befragten zeigte jedes dieser Merkmale, deshalb wird dieser Bereich weiter untersucht um herauszufinden, wie Organisationen den Wert ihrer Datenbestände maximieren.

Auswirkungen

Diese Ergebnisse zeigen, dass Datenschutzinvestitionen einen geschäftlichen Mehrwert erzeugen, der über bloße Compliance hinausgeht, und für viele Unternehmen zu einem wichtigen Wettbewerbsvorteil geworden sind. Organisationen sollten sich daher bemühen, die Auswirkungen ihrer Datenschutzinvestitionen nachzuvollziehen, beispielsweise die Reduzierung von Verzögerungen im Vertriebszyklus, die Senkung von Risiken und Kosten im Zusammenhang mit Datensicherheitsverletzungen sowie andere potenzielle Vorteile wie Flexibilität/Innovation, Wettbewerbsvorteile und betriebliche Effizienz.

Die Analysen und Einblicke aus dieser Studie können von jeder Organisation als Framework und Ausgangspunkt verwendet werden, um den Wert ihrer Datenschutzinvestitionen zu maximieren.

Abbildung 12 Typische Merkmale von ausgereiften Datenumgebungen
Prozentsatz der Befragten, N=3259

42 %	Wir verstehen den Wert der meisten/aller unserer Datenbestände.
42 %	Wir wissen, wo die meisten/alle personenbezogenen Daten gespeichert sind und wie sie verwendet werden.
40 %	Wir verknüpfen verschiedenen Datenbestände effektiv, um Mehrwert für unsere Kunden und uns selbst zu schaffen.
37 %	Wir haben einen fast vollständigen Katalog an Datenbeständen.
32 %	Wir haben einen Chief Data Officer.
32 %	Wir betrachten uns als informationsorientiertes Unternehmen.
30 %	Wir können ausgewählte Datenbestände monetarisieren, indem wir sie extern verkaufen (oder tauschen).
2 %	Keiner der oben genannten Punkte

Quelle: Benchmark-Studie zum Datenschutz von Cisco 2019

Organisationen, die den Wert ihrer Daten auf geeignete Weise maximieren, können durch den Aufbau des Kundenvertrauens deutlich profitieren und sorgfältig geschützte und gepflegte Daten verwenden, um das Kundenerlebnis zu verbessern und Mehrwert für alle Beteiligten zu schöpfen.

„Eine gute unternehmenseigene Datenschutzrichtlinie kann finanzielle Verluste durch Datensicherheitsverletzungen abwehren, indem sie Kunden Transparenz und Kontrolle über ihre personenbezogenen Daten bietet. Eine unzureichende Richtlinie kann durch einen Vorfall verursachte Probleme hingegen noch verstärken.“

Harvard Business Review, „Mit einer starken Datenschutzrichtlinie kann Ihr Unternehmen Millionen einsparen“, 15. Februar 2018

Fazit

Datenschutzinvestitionen haben neben einem geschäftlichen Mehrwert, der über bloße Compliance hinausgeht, auch einen wichtigen Wettbewerbsvorteil für viele Unternehmen geschaffen.

In dieser Studie konnten die geschäftlichen Vorteile fortgeschrittener Datenschutzmaßnahmen in Zahlen ausgedrückt werden. Viele der Vorteile, die erstmals im Bericht des vergangenen Jahres erwähnt wurden, konnten bestätigt und weiter untersucht werden. Dazu gehörte die Reduzierung von Vertriebsverzögerungen aus Datenschutzgründen und die geringere Häufigkeit und Auswirkung von Datensicherheitsverletzungen. In zukünftigen Studien werden wir untersuchen, wie sich diese Vorteile im Laufe der Zeit verändern, da sich die Datenschutzbestimmungen und Kundenerwartungen in unterschiedlichen Industrien und Ländern laufend wandeln. Cisco wird weiterhin mit seinen Kunden und anderen führenden Unternehmen im Bereich Datenschutz zusammenarbeiten, um Entscheidungen bezüglich Investitionen zu verbessern und das Vertrauen unserer Kunden zu stärken.

Weitere Informationen finden Sie unter:
Datenschutz aus Sicht des Unternehmens

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 Datensicherheitsverletzungen.

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 Berichtsammlung für 2019 greift auf die tiefgreifenden und umfangreichen Kenntnisse von Bedrohungsforschern und Innovatoren in der Sicherheitsbranche zurück und enthält die Benchmark-Studie zum Datenschutz, den Bedrohungsbericht und die Cisco Benchmark-Studien. Weitere Berichte sollen im Jahresverlauf folgen.

Weitere Informationen finden Sie unter www.cisco.com/go/securityreports.

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

Hauptgeschäftsstelle Asien/Pazifik
Cisco Systems (USA) Pte.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

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

Veröffentlicht im Januar 2019 PRIV_01_0119_r1