STATE OF DIGITAL TRUST

PILLARS OF TRUST

C- LEVEL, DIRECTOR
MANAGER INSIGHTS

DIGITAL TRUST READINESS
SCORE
1245.56°
753234.72°

IDENTITY

AUTOMATION
433.6°
24567.76°

ID 7021.4

THREATS

XX
SECURITY ALERT

ZERO TRUST

NOVEMBER 2022

ENTERPRISES
EMPLOYEES
CUSTOMERS
6578.854°
6785.77°

GLOBAL STUDY

digicert®

DIGITALES VERTRAUEN: UMFRAGEERGEBNISSE 2022

Wir befinden uns in einem raschen Wandel weg von einer anwesenheitsorientierten hin zu einer digital vernetzten Welt. Die digitale Transformation beschleunigt diese Entwicklung und die Pandemie tut ihr Übriges. Wie können wir in diesem Umfeld Vertrauenswürdigkeit etablieren?
Wie können wir

- sichergehen, dass die Menschen (und Geräte), mit denen wir uns vernetzten, diejenigen sind, für die sie sich ausgeben?
- wissen, dass die Daten, die wir nutzen, sicher sind?
- dafür sorgen, nicht Opfer von Sicherheitslücken oder Denial-of-Service-Angriffen zu werden?
- sicher sein, dass die Anwendungen und Services, die wir ausführen, nicht manipuliert wurden?

Es ist nicht einfach. Die neue Situation hat unsere Angriffsflächen erheblich vergrößert und die Kosten von Sicherheitslücken explosionsartig in die Höhe getrieben. Denn neben den gesetzlichen und aufsichtsrechtlichen Folgen und den Kosten für die Behebung fallen hier vor allem verlorene Kundenbindung und der Reputationsverlust der Marke ins Gewicht. Ein Bericht von Forbes Insights ergab, dass es bei fast der Hälfte (46 %) aller Unternehmen bereits einmal aufgrund einer Datenschutzverletzung durch Dritte zu Schäden an Reputation und Marke gekommen ist.[1]

Digitales Vertrauen als Problem ist dadurch wesentlich sichtbarer geworden. Laut Jennifer Glenn, Research Director bei IDC, ist digitales Vertrauen die Grundlage für eine sichere vernetzte Welt, und Unternehmen müssen sich sicher sein können, dass ihre Kundschaft, Belegschaften und Partner auf die Sicherheit ihrer Online-Geschäftsprozesse und -Interaktionen vertrauen können.

Im Wesentlichen schafft digitales Vertrauen erst die Freiheit für eine uneingeschränkte Teilnahme an der digitalen Welt.

Als einer der weltweit führenden Anbieter digitaler Vertrauenslösungen sorgt DigiCert dafür, dass Unternehmen und Einzelpersonen digitalen Interaktionen in dem Wissen vertrauen können, dass ihre digitale Infrastruktur und ihre Anbindung an eine Welt voller Online-Transaktionen sicher und geschützt sind. Deshalb möchten wir weiter erforschen, wie globale Unternehmen digitales Vertrauen wahrnehmen und wie weit ihre Initiativen zur Schaffung digitalen Vertrauens bereits gediehen sind.

Die DigiCert-Umfrage „State of Digital Trust“ 2022 widmet sich der Frage, wo auf der Welt Unternehmen, Belegschaften und VerbraucherInnen digitales Vertrauen schaffen und nutzen.

[1] „The Reputational Impact of IT Risk“, Forbes Insights

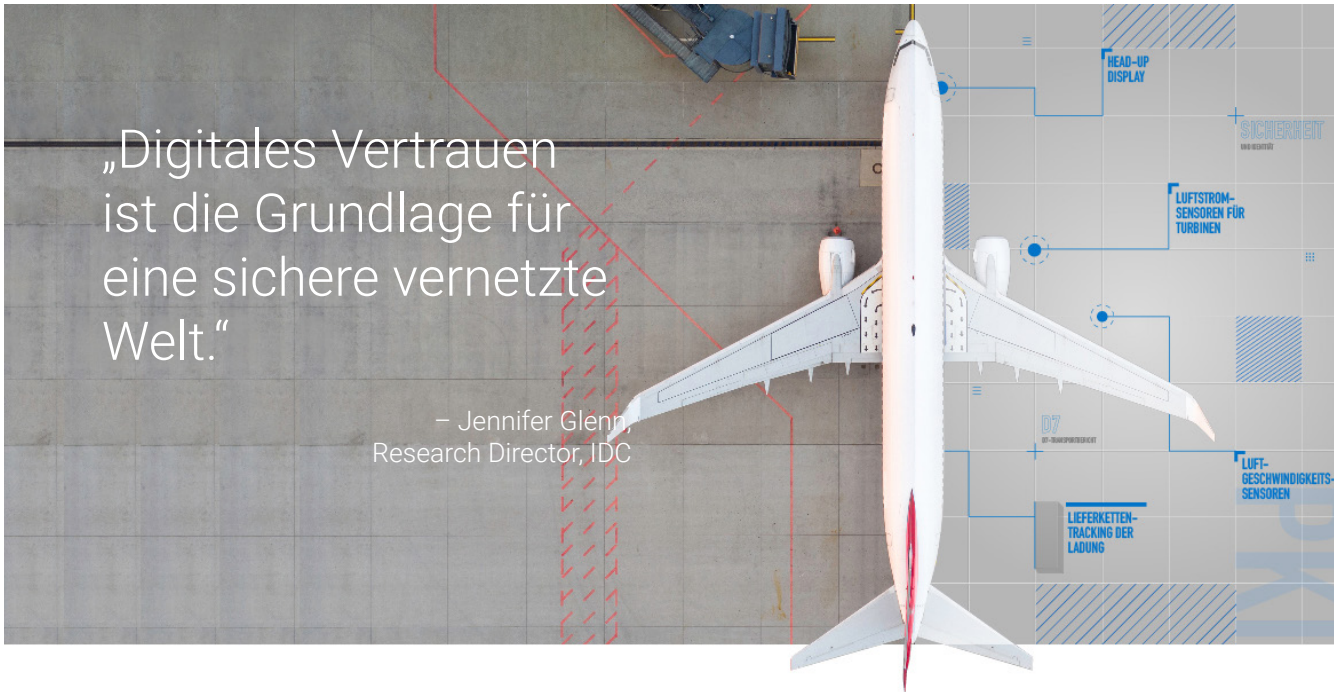
Was bedeutet digitales Vertrauen?

Laut Jennifer Glenn, Research Director bei IDC, ist digitales Vertrauen die Grundlage für eine sichere vernetzte Welt und Unternehmen müssen sich sicher sein können, dass ihre Kundschaft, Belegschaften und Partner auf die Sicherheit ihrer Online-Geschäftsprozesse und -Interaktionen vertrauen können.

Digitales Vertrauen kann nur dann entstehen, wenn die folgenden vier Voraussetzungen erfüllt sind:

1. Normen, in denen die Anforderungen an Vertrauen für eine bestimmte Technologie oder Branche festgelegt sind
2. Konformitäten und Abläufe für die Ausstellung und Verifizierung digitaler Zertifikate, die Vertrauen (durch Identität, Integrität und Verschlüsselung) herstellen und dabei gewährleisten, dass diese die von den Normungsgremien formulierten Anforderungen erfüllen
3. Vertrauensmanagement, das gewährleistet, dass Unternehmen die Zertifikats-Lebenszyklen erfolgreich verwalten und die Zertifikatsverwendung zentral einsehen und steuern können
4. Umfassendes, vernetztes Vertrauen auch für komplexere Lieferketten (wie beispielsweise bei Software, Geräten und Content)

Digitales Vertrauen baut auf diesen vier wichtigen Fundamenten auf. Unternehmen können sich für alle oder einen Teil dieser Prinzipien auf externe Anbieter verlassen oder sie intern verwalten.



„Digitales Vertrauen ist die Grundlage für eine sichere vernetzte Welt."

– Jennifer Glenn, Research Director, IDC

DIGITALES VERTRAUEN IST WICHTIG

Die Einigkeit unter den Befragten über die Notwendigkeit digitalen Vertrauens ist hoch: 100 % der Unternehmen stufen digitales Vertrauen als wichtig und die meisten (90 %) sogar als sehr wichtig ein. Fast zwei Drittel haben nach einem Vertrauensverlust sogar bereits einmal einen Lieferanten gewechselt. Und fast alle Unternehmen (99 %) halten es für möglich, dass auch ihre KundInnen zum Wettbewerb abwandern würden, wenn sie das Vertrauen verlören. Fast die Hälfte (47 %) hält das sogar für wahrscheinlich.

Auch die Belegschaften der Unternehmen messen digitalem Vertrauen einen hohen Wert bei: 100 % der befragten Mitarbeitenden halten es für wichtig und 86 % für extrem wichtig. In ihrem beruflichen Alltag im Unternehmen würden 99 % bei Vertrauensverlust einen Lieferantenwechsel in Erwägung ziehen, etwa die Hälfte (51 %) würden dies „wahrscheinlich" tun.

Bei den VerbraucherInnen schließlich geben zwei Drittel (68 %) digitales Vertrauen als wichtig an, ein Drittel (36 %) sogar als sehr wichtig. Etwa die Hälfte (47 %) hat tatsächlich bereits eine Geschäftsbeziehung mit einem Unternehmen abgebrochen, das ihr Vertrauen verloren hatte. Für die Zukunft würden 84 % dies in Erwägung ziehen, 57 % würden es wahrscheinlich tun. Je wohlhabender VerbraucherInnen im Übrigen sind, desto wichtiger ist ihnen digitales Vertrauen (58 % der VerbraucherInnen mit überdurchschnittlichem Einkommen geben an, dass digitales Vertrauen wichtig ist).

Methodik

Das Marktforschungsunternehmen Eleven Research in Dallas startete die Umfrage „State of Digital Trust" im September 2022. 400 Unternehmen sowie 400 VerbraucherInnen auf der ganzen Welt wurden telefonisch oder per E-Mail befragt.

Unternehmen

400 Führungskräfte und GeschäftsführerInnen in den Bereichen IT, Informationssicherheit und DevOps in Unternehmen mit mindestens 1.000 Mitarbeitenden wurden befragt. Die Befragten waren weltweit verteilt: Abbildung A (siehe S. 5)

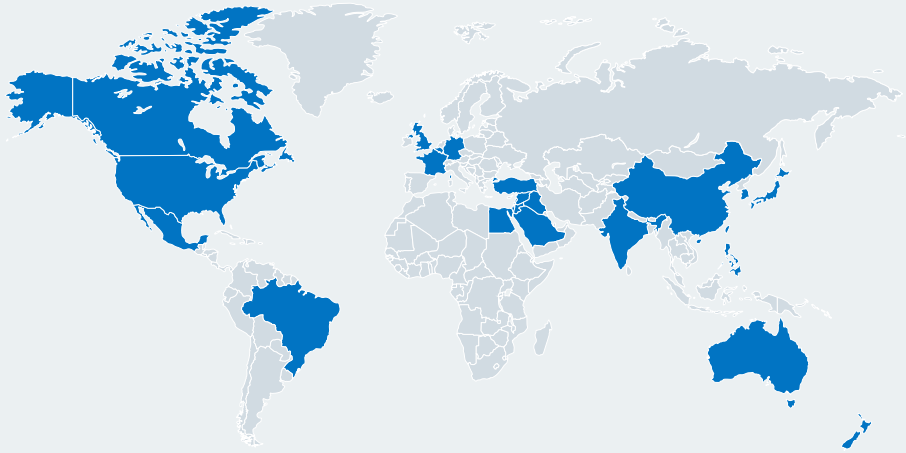
VerbraucherInnen

Wir befragten weltweit 400 VerbraucherInnen (selbe Regionen) aller Altersgruppen, Geschlechter, politischen Orientierungen und Einkommensklassen: Abbildung B (siehe S. 5)

100
Nordamerika

100
EMEA

50
Naher Osten



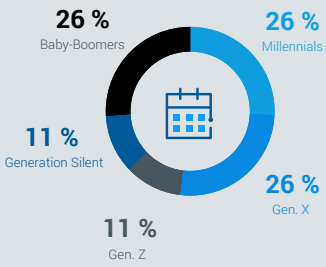
50
Lateinamerika

100
Asien-Pazifik

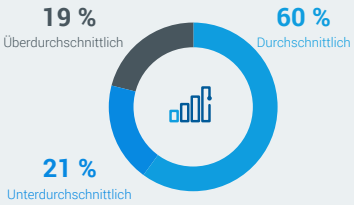
Abbildung A

Großes Altersspektrum

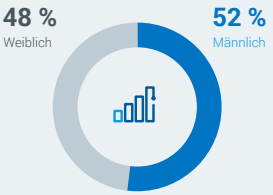
(entsprechend dem jeweiligen Bevölkerungsanteil)



Großes Einkommensspektrum



Nahezu gleiches Geschlechterverhältnis



Breites politisches Spektrum

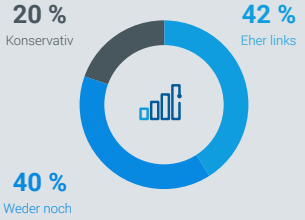
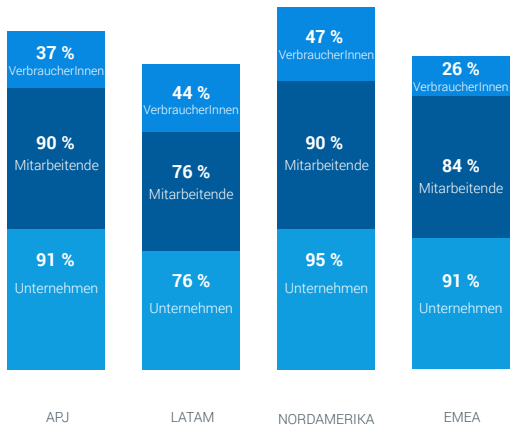


Abbildung B

DIE BEDEUTUNG DES DIGITALEN VERTRAUENS VARIIERT

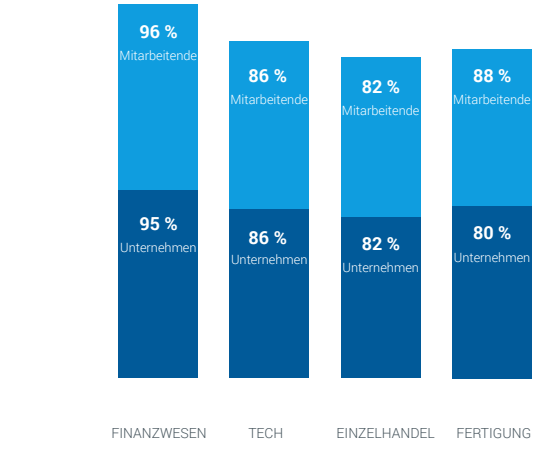
Dass digitales Vertrauen wichtig ist, sagen alle Unternehmen, Mitarbeitenden und VerbraucherInnen, aber wie wichtig genau, hängt von einer Reihe an Merkmalen ab.

DIGITALES VERTRAUEN IST EXTREM WICHTIG, NACH REGION



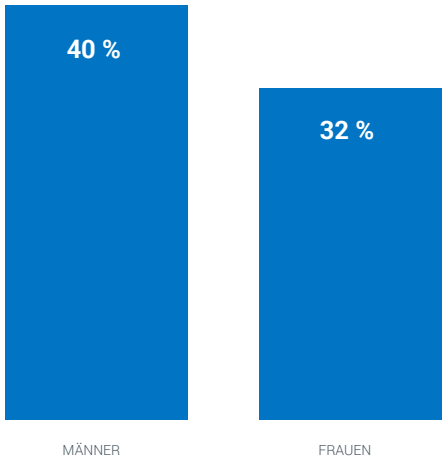
So stuften vergleichsweise weniger Unternehmen und Belegschaften in Lateinamerika das digitale Vertrauen als extrem wichtig ein. Bei den VerbraucherInnen gilt dies für APAC und EMEA. Der Anteil von 26 % der VerbraucherInnen in EMEA, die digitales Vertrauen als extrem wichtig angeben, ist angesichts der 2018 verabschiedeten strengen DSGVO überraschend.

DIGITALES VERTRAUEN IST EXTREM WICHTIG, NACH BRANCHE



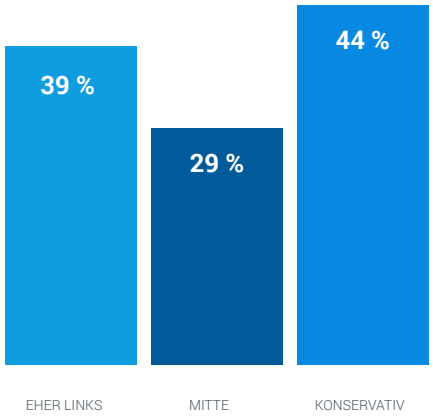
Wenig überraschend: In der Finanzbranche gibt es die meisten Befragten, die digitales Vertrauen für sehr wichtig halten.

DIGITALES VERTRAUEN IST EXTREM WICHTIG, NACH GESCHLECHT (VERBRAUCHERINNEN)



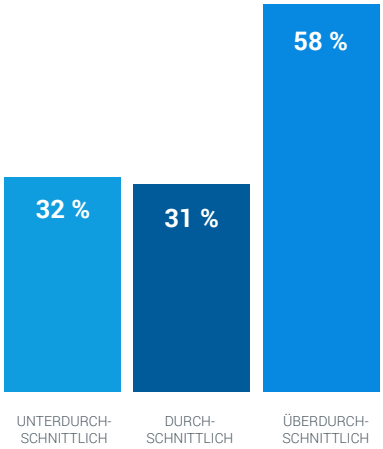
Verbraucher legen tendenziell mehr Wert auf digitales Vertrauen als Verbraucherinnen.

DIGITALES VERTRAUEN IST EXTREM WICHTIG, NACH POLITISCHER ORIENTIERUNG (VERBRAUCHERINNEN)



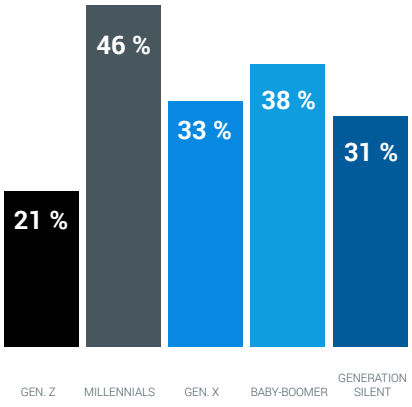
Politische Gegner sind sich hier ausnahmsweise einig: In großen Teilen beider Lager gilt digitales Vertrauen als extrem wichtig.

DIGITALES VERTRAUEN IST EXTREM WICHTIG, NACH EINKOMMEN (VERBRAUCHERINNEN)



VerbraucherInnen mit überdurchschnittlichem Einkommen ist digitales Vertrauen deutlich wichtiger.

DIGITALES VERTRAUEN IST EXTREM WICHTIG, NACH GENERATION (VERBRAUCHERINNEN)



Interessanterweise sind die jüngste und zweitjüngste Generation, also die einzigen „digital natives“, diejenige mit den jeweils wenigsten und meisten Befragten, die digitales Vertrauen für sehr wichtig halten.

WOHER RÜHRT DAS INTERESSE AN DIGITALEM VERTRAUEN?

Auf der Suche nach den Gründen für dieses universelle Interesse am digitalen Vertrauen stießen wir auf zahlreiche unterschiedliche Faktoren.

Daten gewinnen an Bedeutung. Unseren Umfrageteilnehmern zufolge war dies der Hauptgrund. Warum? Weil die Datenmenge eine durchschnittliche Zuwachsrate von 23 % hat.[2] Anders ausgedrückt: Die Welt hat 70 Jahre gebraucht, um die 97 Zettabyte Daten anzuhäufen, die Ende 2021 existierten. Doch dann wird sich das Datenvolumen in nur vier Jahren, nämlich bis Ende 2025, fast verdoppeln (auf 174 ZB). Das macht im Jahr 2025 für jeden Menschen auf der Erde mehr als 20.000 Gigabyte aus!

Es geht hier aber nicht nur um die schiere Menge der Daten, sondern auch um ihre Bedeutung. Sie enthalten wertvolle personenbezogene Daten, beispielsweise darüber, wie wir kaufen und wohin wir surfen, unsere Gesundheitsdaten, Einträge in sozialen Netzwerken, Fotos und vieles mehr.

Die Angriffsfläche wächst. Unternehmen haben die relativ statischen Netzwerke, die früher Rechenzentren, Büros und andere Niederlassungen miteinander verbanden, zu weitaus komplexeren Hybridnetzwerken ausgebaut. Diese neuen Netzwerke verbinden neben Rechenzentren, Büros und anderen Niederlassungen auch Tausende Home-Offices, mehrere Clouds, digitale Geräte, Edge-Netzwerke und IoT-Geräte miteinander.

Die Zahl der Angriffspunkte in diesem Netzwerktyp ohne definierten Perimeter ist um Größenordnungen höher.

Die Kundenerwartungen sind gestiegen. Wie im letzten Abschnitt erwähnt, stufen 100 % der Unternehmen und 68 % der VerbraucherInnen digitales Vertrauen als wichtig ein. Beide Gruppen würden wahrscheinlich bei Vertrauensverlust zu einem Mitbewerber wechseln. Digitales Vertrauen ist zu einem existenziellen Gut geworden.

Die Anzahl der potenziellen Angreifer steigt. Die Anzahl der potenziellen Angreifer steigt Jahr für Jahr. Dazu zählen:

- Hacker
- Cyber-Kriminelle
- Cyber-Terroristen
- Hacktivisten
- Insider
- staatlich gesponserte Akteure
- Trolle und Spaßakteure

Einen Beleg für die wachsende Zahl böswilliger Akteure liefert die Rekordzahl der 2021 beim IC3 eingegangenen Beschwerden, die mit 847.376 um 7 % über dem Vorjahreswert lag.[3]

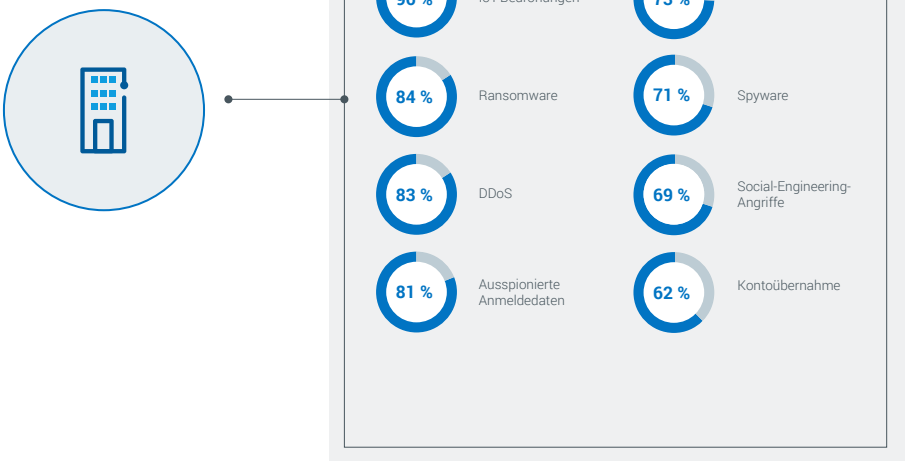
[2] „Big Growth Forecasted for Big Data", IDC
[3] FBI Internet Crime Complaint Center (IC3)

WAS STEHT AUF DEM SPIEL?

Was schützen Unternehmen? 100 % der befragten Führungskräfte nannten die Kundenbindung als wichtigen Aspekt. Das ergibt Sinn, wenn man bedenkt, wie wahrscheinlich ein Kunde bzw. eine Kundin zum Wettbewerb abwandert, wenn er oder sie das Vertrauen in ein Unternehmen verliert.

Laut Angaben der Befragten werden die folgen Angriffsarten am meisten gefürchtet:

FÜR UNTERNEHMEN ...



Mitarbeitende in Unternehmen sorgen sich dagegen hauptsächlich um ihre personenbezogenen Daten.

FÜR MITARBEITENDE ...

Und VerbraucherInnen haben zahlreiche verschiedene Bedenken:

GEFÜRCHTETE ANGRIFFE

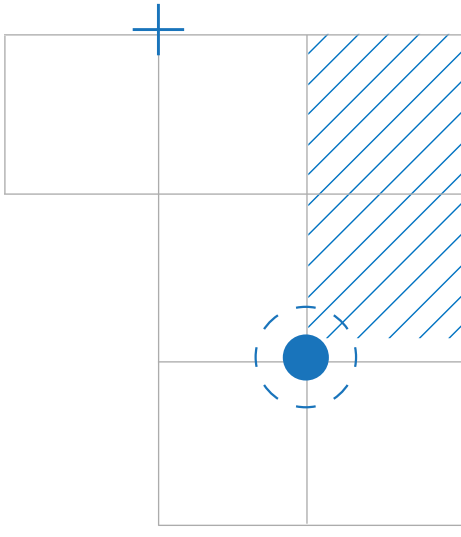
83 % Diebstahl von Bankkonto/Kreditkarte	83 % Verletzung persönlicher Daten
82 % Geldverlust	82 % Konto-übernahme
80 % Kreditschädigung durch Identitätsdiebstahl	74 % Veröffentlichung persönlicher Daten
74 % Cyber-Stalking	72 % Unternehmen sammeln persönliche Daten
72 % Behörden nutzen persönliche Daten	66 % Persönliche Daten gelangen zum Arbeitgeber

ZU SCHÜTZEN SIND ...

87 % Passwörter	85 % PD
84 % Geld	83 % Private Mitteilungen
81 % Gesundheitsdaten	80 % Private Fotos
73 % Standortdaten	73 % Browser-Verlauf
69 % Informationen aus sozialen Medien	68 % Kaufhistorie

Wir fragten uns, ob Unternehmen den Schutz dessen, was für VerbraucherInnen am wichtigsten ist, als genauso wichtig ansehen (Passwörter, personenbezogene Daten (PD) usw.) Nahezu alle Angriffe, die zum Diebstahl von Verbraucherdaten führen, beginnen mit E-Mail-Angriffen.[4] Doch trotz der großen Anstrengungen vieler Unternehmen zum Schutz von VerbraucherInnen lag der Schutz gegen Phishing-Angriffe beim Grad der Umsetzung auf dem zweitletzten Platz. Zudem wurde Phishing als die Angriffsform genannt, die Unternehmen am meisten Sorgen bereitet.

Man konzentriert sich in Unternehmen also durchaus auf die Dinge, die VerbraucherInnen am wichtigsten sind, aber das von den VerbraucherInnen gewünschte Sicherheitsniveau ist trotzdem noch nicht erreicht.

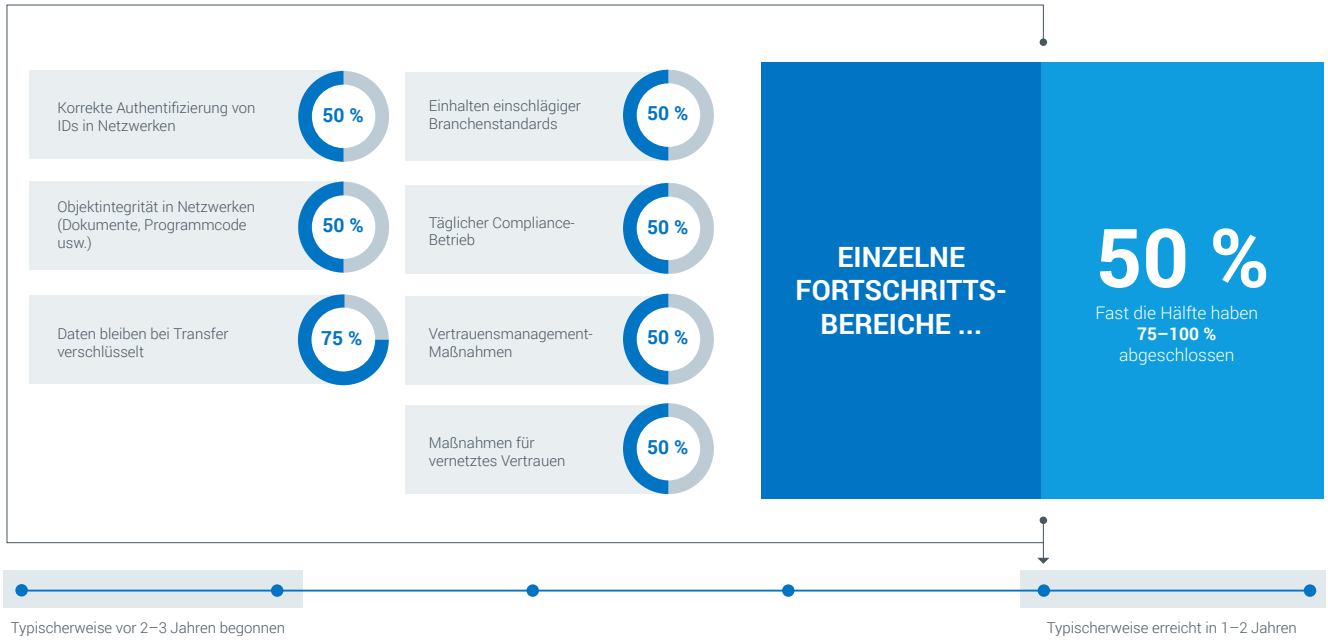


[4] „Why Your Business Needs Better Email Security", Guardian Digital

WIE OPTIMIEREN UNTERNEHMEN DIGITALES VERTRAUEN?

Unternehmen bemühen sich sehr um digitales Vertrauen. Eine typische Organisation hat vor zwei bis drei Jahren begonnen, daran zu arbeiten und hat bisher mindestens 75 % der Arbeit abgeschlossen. Die typische Organisation erreicht ihr gestecktes Ziel hinsichtlich des digitalen Vertrauens in den nächsten ein bis zwei Jahren.

Digitales Vertrauen hat viele Facetten. Wir haben näher aufgeschlüsselt, in welchen Bereichen Unternehmen schon Fortschritte gemacht haben.



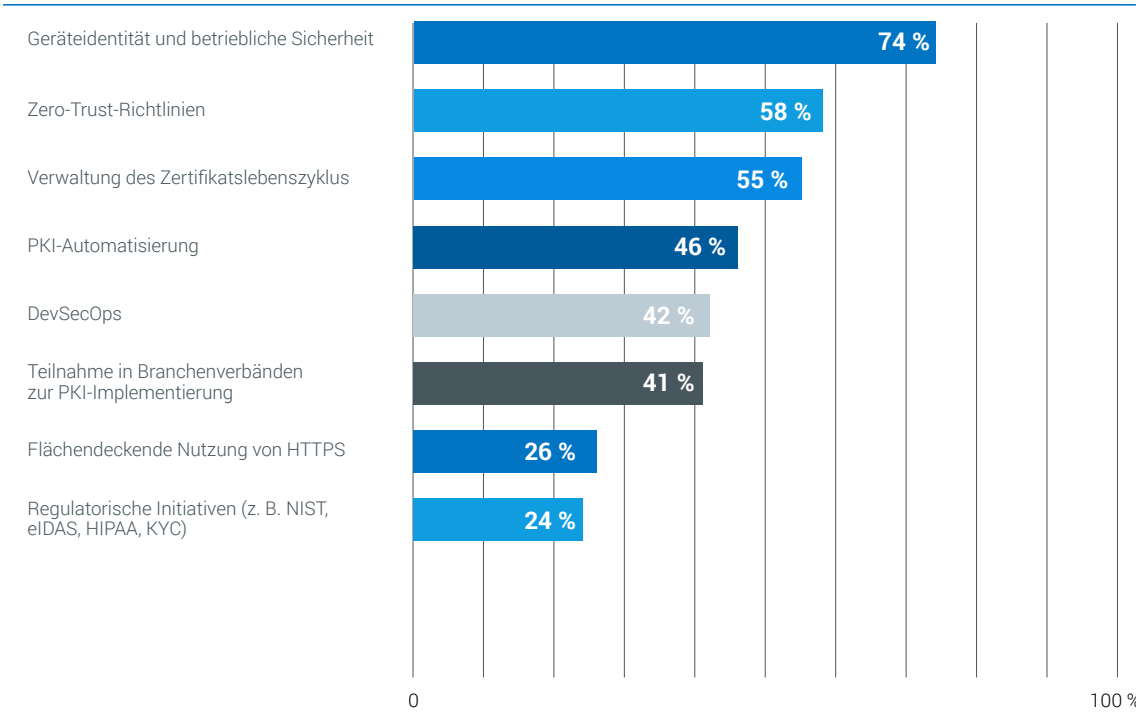
Ziele des digitalen Vertrauens: Unternehmen nannten die Kundenbindung als wichtigstes Ziel in Sachen digitales Vertrauen. 100 % stufen dieses Ziel als wichtig ein, wodurch es zum Top-Ziel der Unternehmen wird. Es gibt jedoch auch andere Ziele.

Herausforderungen beim digitalen Vertrauen: Obwohl viele Unternehmen schon gute Fortschritte erzielt haben, ist die Arbeit am digitalen Vertrauen nicht immer einfach. Als größte Herausforderung wird die Verwaltung der digitalen Zertifikate angegeben. Diese sind für 100 % der Unternehmen wichtig. Die Einhaltung von Compliance-Vorgaben und der Umgang mit der schieren Menge der zu schützenden Güter steht mit je 99 % gleich an zweiter Stelle. Schließlich werden noch die Komplexität, also die Sicherung eines komplexen, dynamischen Netzwerks mit mehreren Providern, und ein unzureichender Wissensstand in der Belegschaft genannt.

Maßnahmen für digitales Vertrauen: Es gibt zahlreiche verschiedene Initiativen für mehr digitales Vertrauen in einem Unternehmen. Die meisten befragten Unternehmen verfolgen diese Initiativen mindestens gelegentlich, aber es ist informativ zu sehen, welche Initiativen bereits vollständig umgesetzt wurden.

Ganz oben steht die Identität von Geräten und die operative Sicherheit; diese ist inzwischen von 74 % der Unternehmen umgesetzt. Als nächstes folgen Zero-Trust-Richtlinien, aber diese sind erst bei 58 % der Unternehmen vollständig umgesetzt. Die einzige andere von mehr als der Hälfte (55 %) der untersuchten Unternehmen implementierte Maßnahme ist die Verwaltung des Zertifikatslebenszyklus. Mit abnehmender Häufigkeit folgen dann:

Q22: Inwiefern setzen Sie die folgenden Initiativen zur Stärkung des digitalen Vertrauens um?
(Bereits implementiert)

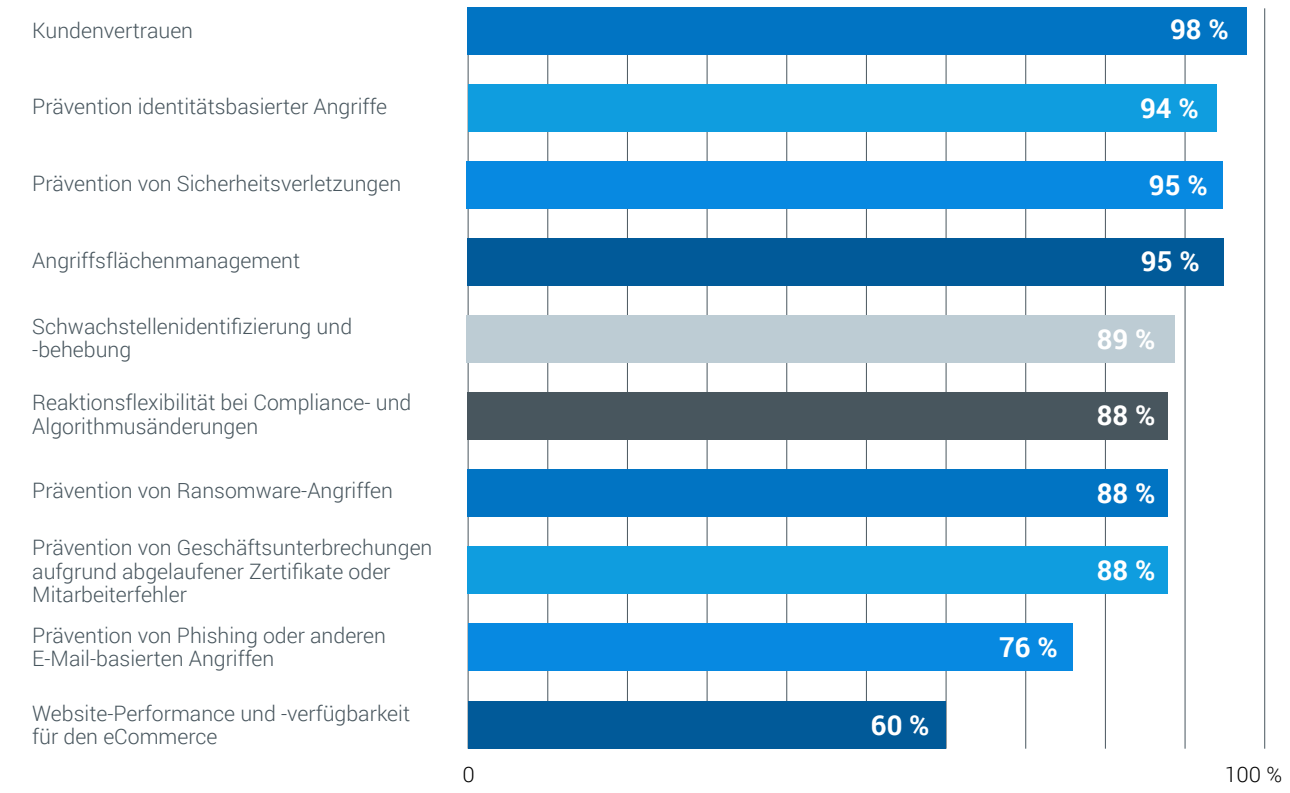


WIE STEHT ES UM DIE ZIELMETRIKEN FÜR DAS DIGITALE VERTRAUEN?

Bei zahlreichen Zielmetriken in Sachen digitales Vertrauen stehen die Unternehmen nicht schlecht da. Zum Beispiel hinsichtlich der Kundenbindung (was ja das wichtigste Ziel war). 98 % machen die Sache gut (und 61 % sogar extrem gut). Ebenso gut läuft es mit der Vermeidung von Datenschutzverletzungen (95 % gut, 51 % extrem gut) und identitätsbasierten Angriffen (94 % bzw. 50 %).

Tatsächlich sagen bei acht von zehn der von uns abgefragten Metriken mindestens sieben von acht Unternehmen, dass sie gut abschneiden. Nur bei der Prävention von Phishing und anderen E-Mail-basierten Angriffen sowie der Performance und Verfügbarkeit von eCommerce-Websites sieht es schlechter aus (76 % bzw. 60 %).

Q23: Wie gut sind Sie bezüglich jeder der folgenden Kennzahlen zum digitalen Vertrauen aufgestellt?
(Eher/Sehr gut)



KundInnen beobachten Verbesserungen

Alle (100 %) Unternehmen geben an, dass digitales Vertrauen für ihre Abnehmer wichtig ist, bei 91 % ist es sogar extrem wichtig.

Es wäre also interessant, festzustellen, wie die KundInnen selbst ihr digitales Vertrauen wahrnehmen. Aus Sicht der Unternehmen ist die Lage gut, denn 99 % der Unternehmen sagen, dass ihre Kundschaft das digitale Vertrauen des Unternehmens heute positiver wahrnimmt als in der Vergangenheit. Fast drei Viertel (73 %) sagen: sogar deutlich positiver.

Aber was sagen die Abnehmer? Sind sie auch so optimistisch? Die Zahlen sind hier fast identisch. Auf die Frage nach dem Vertrauen in ihre Partnerunternehmen antworteten 98 %, dass es größer als in der Vergangenheit sei (für 76 % sogar viel größer).

Aber das gilt für das B2B-Geschäft. Wie sieht es mit B2C aus? Hier sind die Zahlen nicht ganz so optimistisch. Bei weniger als der Hälfte ist das digitale Vertrauen zu den Unternehmen, mit denen sie zu tun haben, größer als in der Vergangenheit, während 54 % Luft nach oben sehen.

Ergebnisse für Nordamerika

In Nordamerika (USA und Kanada) gibt es weltweit die höchste Zahl der Antworten, die digitales Vertrauen als extrem wichtig einschätzen. Und zwar sowohl bei den Unternehmen, als auch bei den Mitarbeitenden und den VerbraucherInnen.

Insbesondere sind die VerbraucherInnen in Nordamerika nach denjenigen im Asien-Pazifikraum am besorgtesten über Cyber-Bedrohungen (wie Zugriffe auf Bankkonten oder Kreditkarten mit Diebstahl von Geld). (91 % der VerbraucherInnen im Asien-Pazifikraum sind über diese Bedrohungen besorgt. In Nordamerika sind es 85 %, in Lateinamerika 78 % und in der Region EMEA 77 %.)

All dies zeigt sich auch in der positiven Bewertung nordamerikanischer Unternehmen seitens der VerbraucherInnen. Zum Thema digitales Vertrauen sagen 31 % der nordamerikanischen VerbraucherInnen, dass ihr Vertrauen zu den Unternehmen, mit denen sie zu tun haben, erheblich gestiegen ist. VerbraucherInnen im Asien-Pazifikraum liegen mit 19 % im Mittelfeld. Dem gegenüber stehen 24 % für lateinamerikanische VerbraucherInnen und nur 15 % für diejenigen in EMEA.

Ergebnisse für APAC

Im Asien-Pazifikraum wird digitales Vertrauen durchweg als extrem wichtig angesehen. Dies ist neben Nordamerika diejenige Region, in der man digitalem Vertrauen den höchsten Wert beimisst.

Dies liegt zum Teil daran, dass die VerbraucherInnen in APAC besorgter über Cyber-Bedrohungen (wie Zugriffe auf Bankkonten oder Kreditkarten mit Diebstahl von Geld) sind als irgendwo sonst auf der Welt. (91 % der VerbraucherInnen im Asien-Pazifikraum sind über diese Bedrohungen besorgt. In Nordamerika sind es 85 %, in Lateinamerika 78 % und in der Region EMEA 77 %.)

Was den Erfolg der Bemühungen von Unternehmen um digitales Vertrauen betrifft, liegt der Asien-Pazifikraum im Mittelfeld: 19 % der VerbraucherInnen sagen, dass ihr Vertrauen zu den Unternehmen, mit denen sie zu tun haben, erheblich gestiegen ist. In Nord- und Lateinamerika stimmen 31 % bzw. 24 % der VerbraucherInnen dieser Aussage zu, in EMEA hingegen nur 15 %.

Ergebnisse für LATAM

In Lateinamerika gibt es weltweit die niedrigste Zahl der Antworten, die digitales Vertrauen als extrem wichtig einschätzen.

Das liegt zum Teil daran, dass lateinamerikanische VerbraucherInnen sich weniger Sorgen um Cyber-Bedrohungen (wie unbefugte Zugriffe auf und Diebstahl von Bankkonten oder Kreditkarten) machen als VerbraucherInnen in anderen Regionen. (Nur 78 % der lateinamerikanischen VerbraucherInnen sind über diese Bedrohungen besorgt. In APAC sind es 91 %, in Nordamerika 85 % und in EMEA 77 %.)

Die Bemühungen der Unternehmen um digitales Vertrauen sind in Lateinamerika relativ erfolgreich. 24 % der VerbraucherInnen in dieser Region haben eigenen Angaben zufolge erheblich mehr Vertrauen in die Unternehmen, mit denen sie zu tun haben, als früher. In Nordamerika sind es 31 %, in den Regionen APAC und EMEA hingegen 19 % bzw. 15 %.

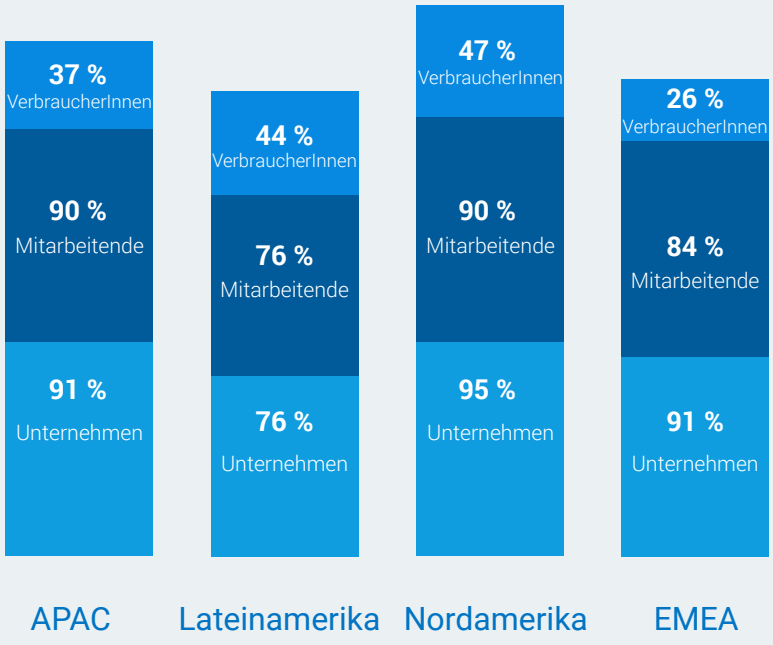
Ergebnisse für EMEA

Für eine Weltregion mit einer der strengsten Datenschutzbestimmungen (DSGVO) sind VerbraucherInnen in EMEA gegenüber dem digitalen Vertrauen erstaunlich nonchalant eingestellt. Insgesamt landet die Region auf Platz drei, wenn alle Bewertungen der Bedeutung des digitalen Vertrauens zusammengezählt werden. Wenn man sich die Daten jedoch näher ansieht, herrscht in EMEA auf Unternehmensebene starkes Interesse und auf der Arbeitnehmerebene immer noch mittleres Interesse. Nur bei den VerbraucherInnen liegt die Bedeutung des digitalen Vertrauens bei nahezu der Hälfte dessen, was in Nordamerika genannt wird.

Genauso sieht es bei der Besorgnis über Cyber-Bedrohungen aus. VerbraucherInnen in der Region EMEA sind am wenigsten besorgt über Cyber-Bedrohungen wie den Gelddiebstahl durch Zugriff auf Bankkonto oder Kreditkarte. Besorgt über diese Bedrohungen sind nur 77 % der VerbraucherInnen in der EMEA-Region, verglichen mit 78 % in der LATAM-Region und 85 % sowie 91 % in Nordamerika bzw. APAC.)

Das passt auch zum relativ niedrigen Prozentsatz (nur 15 %) der VerbraucherInnen in EMEA, deren Vertrauen in die Unternehmen, mit denen sie zu tun haben, in den letzten Jahren gestiegen ist. Dieser Wert light unter dem in APAC (19 %), LATAM (24 %) und Nordamerika (31 %).

DIGITALES VERTRAUEN IST EXTREM WICHTIG, NACH REGION



EINBLICKE VON KENNERN IN SACHEN DIGITALES VERTRAUEN

Im letzten Abschnitt haben wir gelesen, dass die Umsetzung des digitalen Vertrauens in den Unternehmen recht gut läuft. Wir wollten wissen, ob das allgemein gilt, oder ob bestimmte Unternehmen besser oder schlechter dastehen als der Durchschnitt.

Wir haben deshalb auf die Antworten der metrikbasierten Fragen ein Punktsystem angewendet:

Bewertungsschlüssel

- Sehr schlecht -2
- Eher schlecht -1
- Weder schlecht noch gut 0
- Eher gut +1
- Sehr gut +2

Wir vergaben drei einzelne Bewertungen und errechneten pro befragtem Unternehmen eine Gesamtpunktzahl. Die Ergebnisse haben wir in drei Ränge eingeteilt:

Unternehmensränge für digitales Vertrauen

- Oberster Rang (oberstes Drittel der Punktzahlen unter allen Befragten)
- Mittlerer Rang (mittleres Drittel)
- Unterster Rang (unterstes Drittel)

Nun traten dramatische Unterschiede zwischen den besten Unternehmen im obersten Rang und den schlechtesten im untersten Rang zutage.

Wie viel besser?

Selbstverständlich steht das obere Drittel bei den Metriken des digitalen Vertrauens am besten da; schließlich haben wir die Antworten ja so sortiert. Interessant ist jedoch, um wie viel das obere Drittel besser ist als das untere. So geben zum Beispiel dreimal so viele Unternehmen im obersten Rang eine gute Performance und Verfügbarkeit ihrer eCommerce-Website an, und 2,9-mal so viele stufen sich als gut bei der Prävention von Phishing und anderen E-Mail-basierten Angriffen ein. Im oberen Drittel sind die Ergebnisse zwischen 10 % und 300 % besser in allen Metriken:

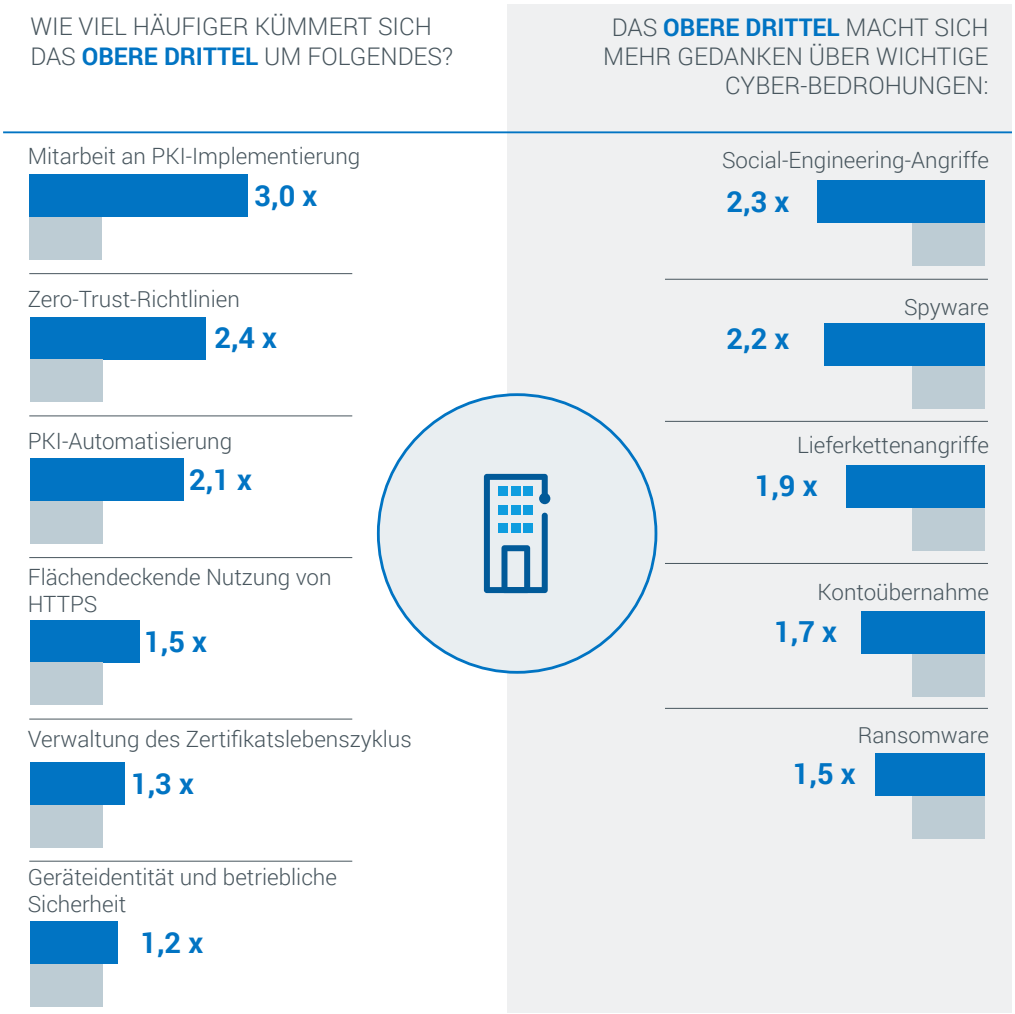
OBERES DRITTEL: HIER VERTRAUEN KUNDEN UNTERNEHMEN DEUTLICH HÄUFIGER ALS IM **UNTEREN DRITTEL**.

DIE BESTEN UNTERNEHMEN SIND **VIEL BESSER** ALS DIE SCHLECHTESTEN

Warum ist das obere Drittel so viel besser?

Es gibt einige markante Unterschiede zwischen dem oberen und dem unteren Drittel, die diese großen Varianzen beim digitalen Vertrauen ausmachen:

- Einstellung: Im oberen Drittel geht man mit vier- bis viereinhalbmal so hoher Wahrscheinlichkeit davon aus, dass KundInnen nach einem Vertrauensverlust abwandern würden. Auch die Einstellung, dass digitales Vertrauen die Marke, den Umsatz und die Marge beeinflusst, findet sich häufiger. Außerdem geben diese Firmen 5,6-mal häufiger an, den Partner wechseln zu wollen, wenn das Vertrauen verloren geht.
- Früher begonnen: Im oberen Drittel sind die Initiativen für das digitale Vertrauen bereits weiter gediehen und werden erheblich eher abgeschlossen sein als im unteren Drittel.
- Cyber-Bedrohungen ernster genommen: Im oberen Drittel werden Cyber-Bedrohungen sehr viel ernster genommen. In Unternehmen dieses Ranges ist man mit 1,5-mal bis 2,3-mal höherer Wahrscheinlichkeit besorgt über Cyber-Bedrohungen.
- Mehr Bemühungen um gängige Cyber-Sicherheitsmaßnahmen: Im obersten Drittel werden wichtige Cyber-Sicherheitsmaßnahmen mit bis zu dreimal höherer Wahrscheinlichkeit ernst genommen.



Wo gehört das digitale Vertrauen hin?

Die Entscheidung, wo im Unternehmen das digitale Vertrauen seinen Sitz haben sollte, ist von großer Bedeutung. Zwischen dem oberen und dem unteren Drittel in der Rangfolge der befragten Unternehmen gibt es hier klare Unterschiede.

Für die überwältigende Mehrheit im oberen Drittel ist das digitale Vertrauen in der IT-Organisation Sache des CIO; im unteren Drittel dagegen ist man der Meinung, sie gehöre in die Hände der operativen Sicherheits-Teams.

Wir wollen hier weder die Sicherheits-Teams noch ihre entscheidende Rolle herabsetzen. Vielmehr sehen wir die aktive Beteiligung der CIOs im oberen Drittel als Anerkennung der wichtigen Rolle des digitalen Vertrauens für den Erfolg eines technologiegestützten Unternehmens. Zudem spiegelt sie den strategischen Ansatz dieser Unternehmen für das digitale Vertrauen wider.

DIE EINSCHÄTZUNG VON DIGICERT

Als weltweit führender Anbieter digitaler Vertrauenslösungen, mit deren Hilfe Unternehmen und Einzelpersonen digitalen Interaktionen in dem Wissen vertrauen können, dass ihre digitale Infrastruktur und ihre Anbindung an eine Welt voller Online-Transaktionen sicher und geschützt sind, war DigiCert bereits früh ein Pionier im Bereich digitales Vertrauen. Unser Rat an Unternehmen, die es den Vorreitern im erfolgreichen oberen Drittel nachtun möchten, besteht aus fünf Punkten:

Machen Sie digitales Vertrauen zum strategischen Muss. Das ist ein Merkmal, das Unternehmen im oberen Dritte auszeichnet. Hier gilt als erwiesen, dass digitales Vertrauen sich auf wichtige Geschäftsergebnisse wie das Markenimage, die Kundenbindung, den Umsatz und die Margen auswirkt.

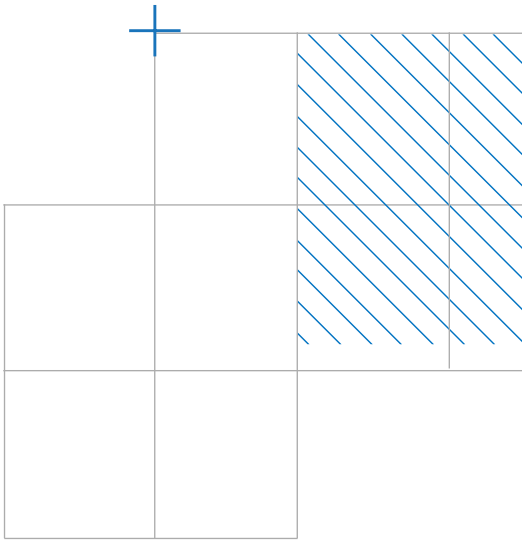
Richten Sie für Ihre Unternehmens-technologie ein Digital Trust Office ein, dessen Führungsperson Entscheidungsbefugnis erhält.

Verinnerlichen Sie, dass Ihre Benutzer – einschließlich Ihrer KundInnen – immer mehr Wert auf digitales Vertrauen legen und dass Ihr geschäftlicher Erfolg und Ihre Reputation direkt von Ihrer Fähigkeit abhängen, ein hohes Niveau an digitalem Vertrauen zu erzielen.

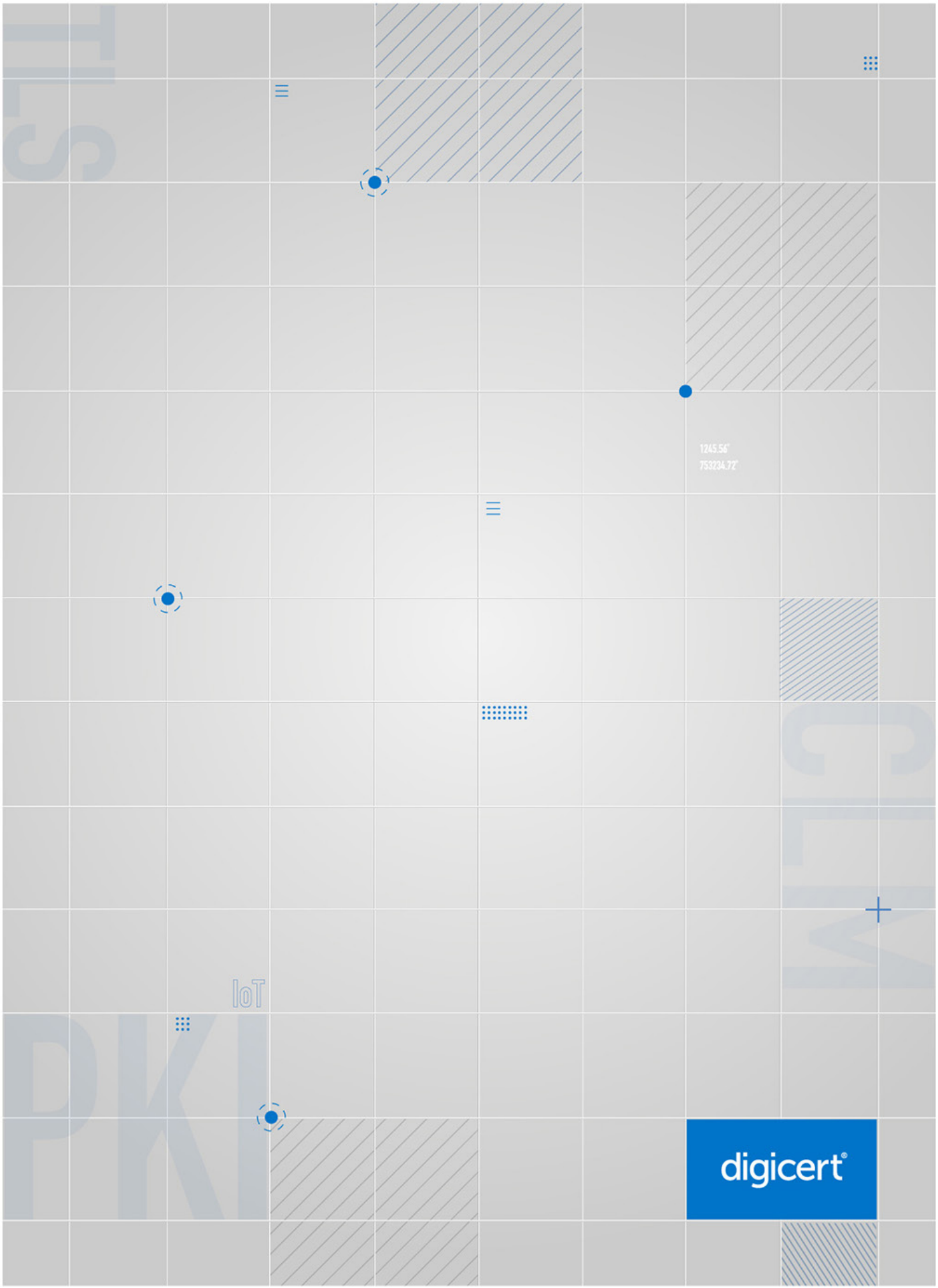
Holen Sie sich Sachverstand für digitales Vertrauen ins Haus. Eine der von den Befragten genannten Herausforderungen war der unzureichende Wissensstand in der Belegschaft. Achten Sie darauf, dass Ihre künftigen Partner ein umfassendes Portfolio in allen Unterbereichen des digitalen Vertrauens mitbringen und Lösungen für ein einheitliches Vertrauensmanagement in Ihrem gesamten Unternehmen bieten können.

Denken Sie immer daran, dass digitales Vertrauen ein wichtiges Thema für Ihre Kundschaft ist. Kommunizieren Sie offen mit ihnen darüber und berichten Sie dabei nicht nur über Ihr Engagement zum Thema, sondern auch über Ihre Fortschritte.

Das wird auch durch eine bemerkenswerte Studie von Bain & Company[5] bestätigt, derzufolge eine Verbesserung der Kundenbindungsrate um fünf Prozent den Profit um 25 % bis 95 % steigert. Angesichts der hohen Wahrscheinlichkeit, mit der KundInnen bei Vertrauensverlust abwandern, sollte eine Maximierung des digitalen Vertrauens eigentlich zwingend sein.



[5] „Prescription for Cutting Costs", Bain & Company


TLS
1245.56
753234.72
IoT
PKI
digicert®