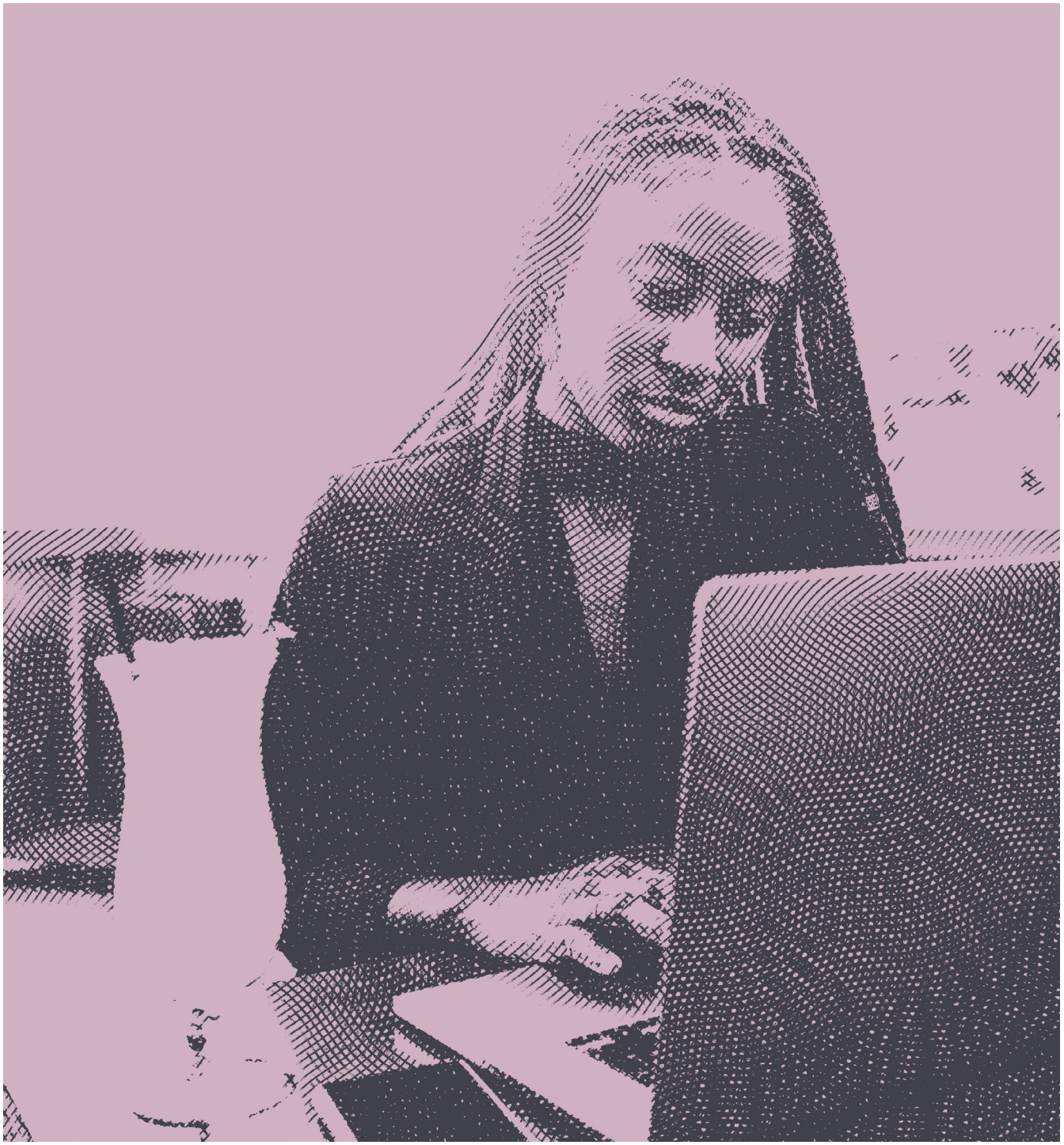
Der Okta Digital Trust Index

Vertrauen in einer Welt des schnellen Wandels



okta

Inhalt

> Trust is a confident relationship with the unknown.
>
> Rachel Botsman, Trust Fellow an der Saïd Business School der Universität Oxford

Einleitung

Vertrauen baut auf Sicherheit

2020 ist das Thema Vertrauen noch stärker in den Fokus gerückt: Beinahe über Nacht wurde das Vertrauen in Regierungen und Institutionen für viele Menschen zu einem zentralen Anliegen. Die Ereignisse des vergangenen Jahres haben zudem die Bedeutung des Kundenvertrauens für den Umsatz und Erfolg von Marken und Unternehmen inmitten einer schweren wirtschaftlichen Rezession verdeutlicht. Und sie haben nicht zuletzt viele Organisationen dazu gezwungen, Vorbehalte abzubauen, ihren Mitarbeitern auch im Homeoffice zu vertrauen und sich auf digitale Kanäle zu verlassen, um mit Kunden zu kommunizieren und Produkte und Dienstleistungen bereitzustellen.

All dies geschieht vor dem Hintergrund wachsender Sicherheitsbedenken, als Reaktion auf ein nie dagewesenes Maß an Datenschutzverletzungen und Cyberbedrohungen, strengeren Datenschutzbestimmungen, opportunistischen Social-Engineering-Betrügereien und steigenden Erwartungen der Verbraucher an Datenschutz.

Kriminelle haben sich die instabile soziale und wirtschaftliche Lage sowie die allgemeine Unsicherheit zu Nutze gemacht. Laut einer **Einschätzung von INTERPOL** haben Phishing-Angriffe im Zuge der Pandemie um 59 % zugenommen, ebenso wie Malware, Ransomware, bösartige Domains und Fake News.

Aus Unternehmensperspektive baut Sicherheit auf Vertrauen auf: Um Sicherheit effektiv zu gewährleisten, müssen Unternehmen zunächst wissen, welchen Mitarbeitern, Partnern und Kunden außerhalb des traditionellen Perimeters sie vertrauen können, um ihnen Zugriff auf sensible Daten und Systeme zu geben. Aber auch andersherum wird ein Schuh daraus: Vertrauen beginnt mit Sicherheit. Mit anderen Worten: Der beste Weg, das Vertrauen der Stakeholder zu gewinnen, ist der Einsatz effektiver Sicherheitslösungen und -richtlinien als Basis von Cybersicherheit.

Und es ist zudem der schnellste Weg, die Produktivität zu steigern und Loyalität und Engagement aufzubauen – nicht nur bei Mitarbeitenden, sondern auch bei Kundinnen und Kunden.

Um mehr über den Zusammenhang von Sicherheit und Vertrauen zu erfahren, hat Okta eine Umfrage unter über 13.000 Büroangestellten, darunter mehr als 2.000 in Deutschland, in Auftrag gegeben, um folgende Fragen zu beantworten:

Wie viel unseres Vertrauens wird im digitalen Raum aufgebaut, gepflegt, aber auch zerstört?

Wie groß ist unser Vertrauen jenseits von menschlichen Beziehungen, wenn wir nur digital kommunizieren?

Werden von Unternehmen, Marken und staatlichen Organisationen ausreichend Maßnahmen ergriffen, um Vertrauen aufzubauen?

Welche externen Einflüsse verändern unser Vertrauen in Bezug auf digitale Kanäle?

Methodik:

Alle Zahlen, sofern nicht anders angegeben, stammen von YouGov Plc. Der Gesamtumfang der Stichprobe betrug 13.163 Büroangestellte aus Deutschland, Frankreich, Italien, Japan, den Niederlanden, Spanien, Schweden, den USA und dem Vereinigten Königreich. Der Umfang der Stichprobe in Deutschland betrug 2042 Büroangestellte. Die Umfrage wurde vom 26. November – 10. Dezember 2020 online durchgeführt.

Der folgende Okta Digital Trust Index untersucht das Kundenvertrauen in digitale Kanäle in einer zunehmend von der Pandemie geprägten Welt. Des Weiteren gibt der Report Anregungen, wie Einzelpersonen, Unternehmen sowie staatliche und öffentliche Organisationen ein starkes und nachhaltiges digitales Vertrauen aufbauen und vermitteln können.

> Vertrauen kommt zu Fuß und geht im Ferrari.
>
> Mark Carney, Gouverneur der kanadischen Zentralbank

Teil Eins

Welche Faktoren sind wichtig für das Kundenvertrauen?

Im Jahr 2020, mit der unvermeidlichen Verlagerung zum Homeoffice, wurden aus vielen Büroangestellten digital-affine Konsumenten, die online mehr Zeit verbrachten und mehr Geld ausgaben. Das **Institut für Handelsforschung Köln**[1] prognostiziert für den deutschen Onlinehandel 2020 ein Umsatzvolumen zwischen 80 und 88 Mrd. Euro, was mindestens einer Verdoppelung des Wachstums im Vergleich zum Vorjahr entspräche.

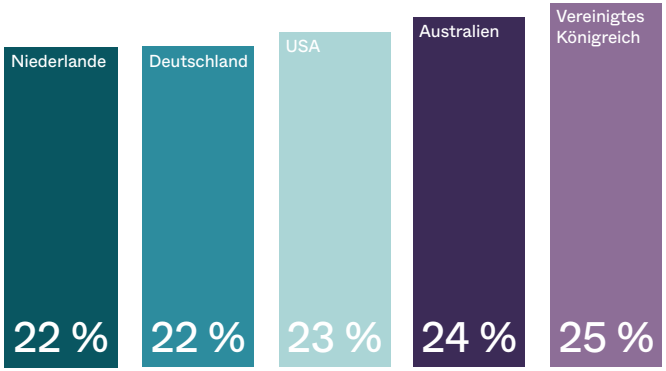
2021 wird ein Jahr des Übergangs, in dem sich neue Online-Praktiken als Norm etablieren werden. Marken stehen vor der Herausforderung, mit ihren Stakeholdern neue Ansätze für die Vertrauensbildung und Kundenbindung zu entwickeln.

Vertrauen ist heute schwerer aufzubauen und gleichzeitig leichter zu verlieren. Obwohl Verbraucher hohe ethische Werte bei Investoren und Vorständen zunehmend schätzen, hat die Umfrage gezeigt, dass es für Kundinnen und Kunden noch wichtiger ist, dass digitale Marken[1] zunächst die richtigen Grundlagen schaffen. 30 % der Befragten in Deutschland gaben an, dass sie einer digitalen Marke am ehesten aufgrund der Zuverlässigkeit des Services vertrauen, z. B. wenn die Ware pünktlich und in gutem Zustand ankommt.

30 % der Befragten in Deutschland gaben an, dass sie einer Marke am ehesten aufgrund der Zuverlässigkeit des Service vertrauen, z. B. wenn die Ware pünktlich und in gutem Zustand ankommt.

Auch die Sicherheit ist für Kunden entscheidend: Knapp ein Viertel (22 %) gab an, dass sichere Login-Optionen wie Multi-Faktor-Authentifizierung (MFA) und andere Maßnahmen ihr Vertrauen stärken.

Dieses Sicherheitsbedürfnis ließ sich auch bei den Befragten in Dieses Sicherheitsbedürfnis ließ sich auch bei den Befragten in den Niederlanden (22 %), den USA (23 %), in Australien (24 %) und im Vereinigten Königreich (25 %) beobachten.



Anteil der Befragten, die angaben, dass sichere Login-Optionen wie Multi-Faktor-Authentifizierung (MFA) das Vertrauen in eine Marke stärken.

[1] Als digitale Marke gilt im Kontext der Studie jede Marke, die über eine Online-Präsenz verfügt, d. h. durch Websites, Apps, soziale Medien, Videos o.ä.

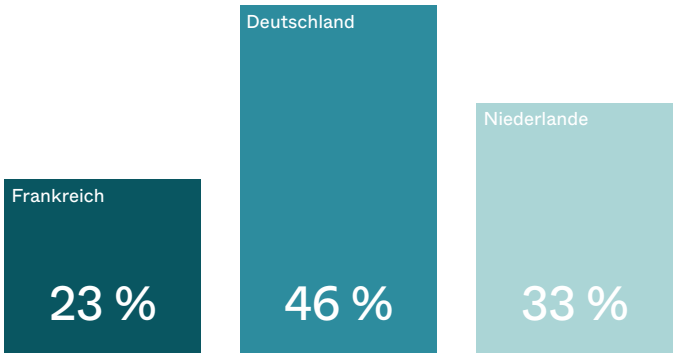
Datenschutz ist entscheidend

Für 6 % der in Deutschland Befragten gehören ethische Werte zu den wichtigsten vertrauensbildenden Faktoren. Werte – insbesondere in Bezug auf die „Datenethik“ – spielen für Verbraucher eine große Rolle bei der Entscheidung, welche Marken sie nutzen und kaufen.

Die beiden weltweit am häufigsten genannten Attribute, die das Kundenvertrauen schädigen, waren:

Vorsätzlicher Missbrauch oder Verkauf persönlicher Daten	38 %
Datenschutzverletzungen	14 %

Beide Aspekte sind für digitale Marken jedoch nicht nur ethische Fragen, sondern würden bei Verstoß auch die DSGVO-Regulierer in Deutschland und der EU auf den Plan rufen.



Anteil der Befragten, die den Missbrauch oder Verkauf persönlicher Daten als Grund für den Verlust ihres Vertrauen in ein Unternehmen angaben.

Um dem Unmut der Kunden und einem Reputations- und finanziellen Schaden zu entgehen, benötigen Unternehmen geeignete Datenschutzmaßnahmen, beginnend mit einem Best-Practice-Identitätsmanagement.

Der vorsätzliche Missbrauch oder Verkauf von Daten wurde in allen Märkten als DER Grund für Vertrauensverlust gegenüber einer Marke genannt, wobei die Befragten in Deutschland und dem Vereinigten Königreich den Ländervergleich mit 46 % und 47 % anführen.

Die zweitgrößte Sorge für die Befragten in Deutschland (11 %) und in Ländern wie Australien (16 %), den USA (15 %) und den Niederlanden (13 %) stellten Datenschutzverletzungen dar. In Frankreich (23 %), Spanien (21 %) und Schweden (16 %) waren Unannehmlichkeiten oder Fehler bei der Bestellung der zweitwichtigste Faktor für den Vertrauensbruch. Letzteres verdeutlicht, dass neben der Datenethik auch ein nahtloser Kundenservice von großer Bedeutung ist.

45 %	Einstellung der Nutzung der Dienste
43 %	Löschung des Nutzerkontos
39 %	Änderung der Benutzereinstellungen

Reaktionen der Befragten in Deutschland auf eine Datenschutzverletzung oder einen Datenmissbrauch bei einem Unternehmen, dessen Dienste sie genutzt haben.

Wenn das Vertrauen beschädigt ist

Vertrauen ist in der heutigen hart umkämpften Geschäftswelt von entscheidender Bedeutung für den nachhaltigen Erfolg digitaler Marken.

79 % der Befragten in Deutschland gaben an, dass sie wahrscheinlich nicht bei einem Unternehmen kaufen würden, dem sie nicht vertrauen.

51 % gaben an, ernsthafte Vorbehalte zu haben, auf einer Website einzukaufen, von der sie zuvor noch nie gehört haben.

Ist das Vertrauen der Stakeholder gewonnen, gilt es für Unternehmen alles daran zu setzen, dieses Vertrauen zu pflegen und auszubauen. Effektive Cybersicherheit ist dabei ein wichtiger Faktor.

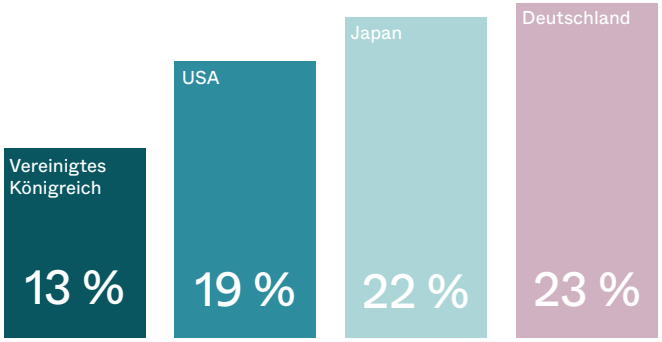
29 % der Büroangestellten in Deutschland gaben an, schon einmal das Vertrauen in ein Unternehmen aufgrund einer Datenpanne oder Ähnlichem verloren zu haben; in den USA waren es sogar 56 %, in Australien 40 %.

Nach diesem Vorfall haben 45 % der Befragten in Deutschland die Nutzung der Dienste des Unternehmens dauerhaft eingestellt und 43 % ihr Konto bei dem Unternehmen gelöscht. 39 % änderten Benutzereinstellungen wie Passwörter und E-Mail-Adressen, was die Bedeutung sicherer Log-ins für die Vertrauensbildung und -pflege unterstreicht.

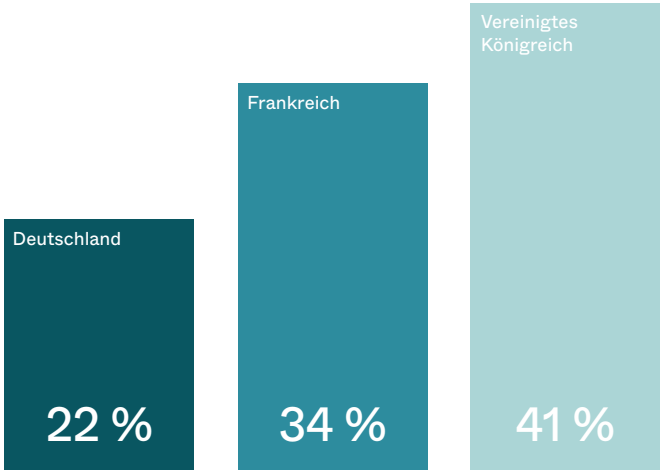
> Wenn das Vertrauen in eine digitale Marke fehlt oder verletzt wird, entscheiden sich Kunden gegen die Nutzung von Produkten und Services, indem sie das Angebot von vornherein nicht wahrnehmen oder es bei einem Vertrauensbruch für eine bestimmte Zeit oder für immer einschränken oder einstellen. Das verdeutlicht die Wichtigkeit von Vertrauen für die Kundenbindung und die strategische Bedeutung für den Erfolg digitaler Plattformen, Angebote und Geschäftsmodelle. Von einem starken „Digital Trust“ profitieren alle Seiten: Einerseits können Unternehmen ihre Produkte und Services unter der verantwortungsvollen Nutzung der User-Daten adäquat platzieren, andererseits haben Kunden und Kundinnen das gute Gefühl einer sicheren und zuverlässigen Nutzung des Angebots.
>
> Sven Kniest, Regional Vice President, Central and Eastern Europa, Okta

Handlungsbedarf in Sachen Vertrauen

In Sachen Vertrauen gibt es noch viel Arbeit zu tun: 23 % der Befragten in Deutschland gaben an, dass sie keinem digitalen Kanal den sicheren Umgang mit ihren Daten zutrauen, ähnlich wie die Befragten in Japan (22%) und den USA (19%). Außerdem hat die Umfrage gezeigt, dass Kommunikations-Apps, die üblicherweise für die Arbeit verwendet werden (17 %), in Deutschland mehr Vertrauen genießen als private (7 %).



Prozentualer Anteil der Befragten, die keinem digitalen Kanal den sicheren Umgang mit ihren Daten zutrauen.



Anteil der Befragten, die Websites der Regierung von allen digitalen Kanälen am vertrauenswürdigsten einstufen.

Am vertrauenswürdigsten von allen digitalen Kanälen wurden in Deutschland die Websites des Regierung eingestuft (22 %). Mit Ausnahme von Japan (12 %), war das Vertrauen in diese Internetauftritte in allen anderen Ländern sogar noch größer, darunter Australien (41 %) und das Vereinigte Königreich (41 %), die Niederlande (37 %) und Frankreich (34 %). Trotz anfänglicher Bedenken über den Umgang mit COVID-19 und persönlichen Daten der Bürger gab es bisher keine größeren Verstöße, und die kontinuierliche Überprüfung scheint zu verbesserten Standards der Datensicherheit zu führen.

> Es ist sehr gut, dass die Menschen den Webseiten der Regierung im Umgang mit ihren Daten mehr vertrauen als allen anderen digitalen Kanälen. Es ist wichtig, dass staatliche Organisationen Cybersicherheitsmaßnahmen priorisieren und die Sicherheit der Daten ihrer Bürger gewährleisten.“
>
> Sven Kniest, Regional Vice President, Central and Eastern Europa, Okta

Teil Zwei

Wie die Pandemie das Nutzerverhalten verändert hat

49 % der Befragten in Deutschland gab an, dass sie aktuell „hauptsächlich“ oder „gelegentlich“ von zu Hause arbeiten. Diese Mitarbeitenden werden auch nach der Krise mehr Flexibilität in Sachen Remote Work und Homeoffice fordern.

Aktuell sind viele der isoliert zu Hause Arbeitenden steigenden Cyberbedrohungen ausgesetzt. Diese zielen darauf ab, sowohl Firmen-Logins als auch persönliche Identitätsdaten zu stehlen.

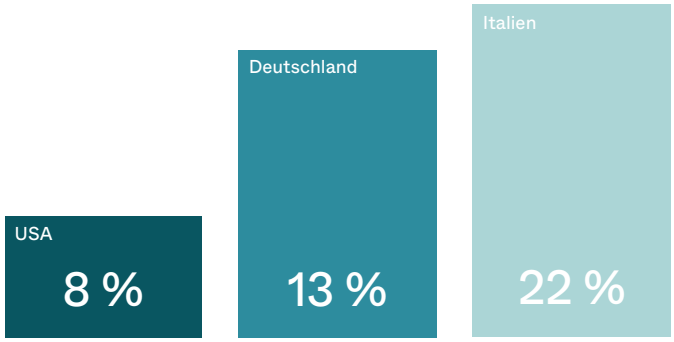
Phishing hat sich im Jahr 2020 zu einem bevorzugten Angriffsmuster vieler Cyberkrimineller entwickelt. Sie nutzten Falschinformationen zu COVID-19-Impfstoffen oder gefälschte Updates von vertrauenswürdigen Institutionen wie der WHO und köderten die Empfänger so, auf entsprechende Links und Anhänge zu klicken. Bereits im **April gab Google** an, täglich 18 Millionen Malware- und Phishing-E-Mails im Zusammenhang mit COVID-19 zu blockieren.

Da überrascht es wenig, dass 31 % der in Deutschland befragten Büroangestellten angaben, vorsichtiger geworden seien, wenn es um die Übermittlung ihrer persönlichen Informationen gehe, während nur 3 % erklärten, nun weniger vorsichtig zu sein.

Die Arbeit in den eigenen vier Wänden hat die Befragten in Deutschland außerdem misstrauischer gegenüber Phishing-E-Mails (36 %), Datenschutzverletzungen (33 %) und sogar KI-generierten „Deepfakes“ (29 %) zur Verbreitung von Falschinformationen gemacht.

23 % der Befragten gaben an, Identitätsdiebstahl in Zukunft als größte Bedrohung zu sehen - nachvollziehbar angesichts der steigenden Zahl von Phishing-Attacken.

Malware (17 %) und Passwortdiebstahl (13 %) komplettieren die drei größten wahrgenommenen Bedrohungen.



Prozentsatz der Befragten, die Passwortdiebstahl als Bedrohung wahrnehmen

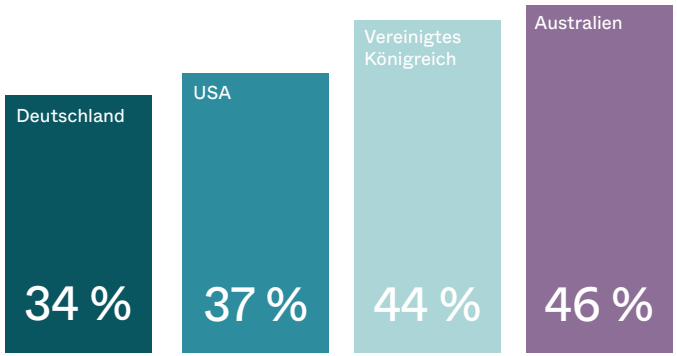
Von einem Diebstahl von Passwörtern fühlten sich 13 % der Befragten in Deutschland bedroht. Noch stärker war dies in Italien (22 %) und Spanien (19 %) zu beobachten, was die Notwendigkeit der Umstellung auf passwortlose Authentifizierung verdeutlicht.

Außerdem ist zu bedenken, dass Angestellte nicht nur durch Angriffe auf die eigene Person und eigene Geräte, sondern auch durch Mitbewohner, die sich online riskant verhalten, Cyberbedrohungen ausgesetzt sein können.

> Die Bedrohungssituation ist bei Remote Work und Homeoffice aus mehreren Gründen verschärft. Personen teilen sich Geräte, Heimnetzwerke und physische Räume. Das erhöht das Risiko und gefährdet die Vertraulichkeit von digitalen Inhalten und Telefongesprächen.
>
> „Kollegen“ reichen aktuell von engen Familienmitgliedern bis hin zu wenig vertrauten Mitbewohnern – während gleichzeitig die Möglichkeit entfällt, sich an andere Mitarbeiter oder und den IT-Helpdesk wenden zu können. Hinzu kommt, dass das tagtägliche Jonglieren von beruflichen und privaten Verpflichtungen Sicherheitsbedenken und vormals eingeübte Verhaltensregeln beeinträchtigen können.
>
> Ben King, CSO EMEA, Okta

Zeit für Transparenz

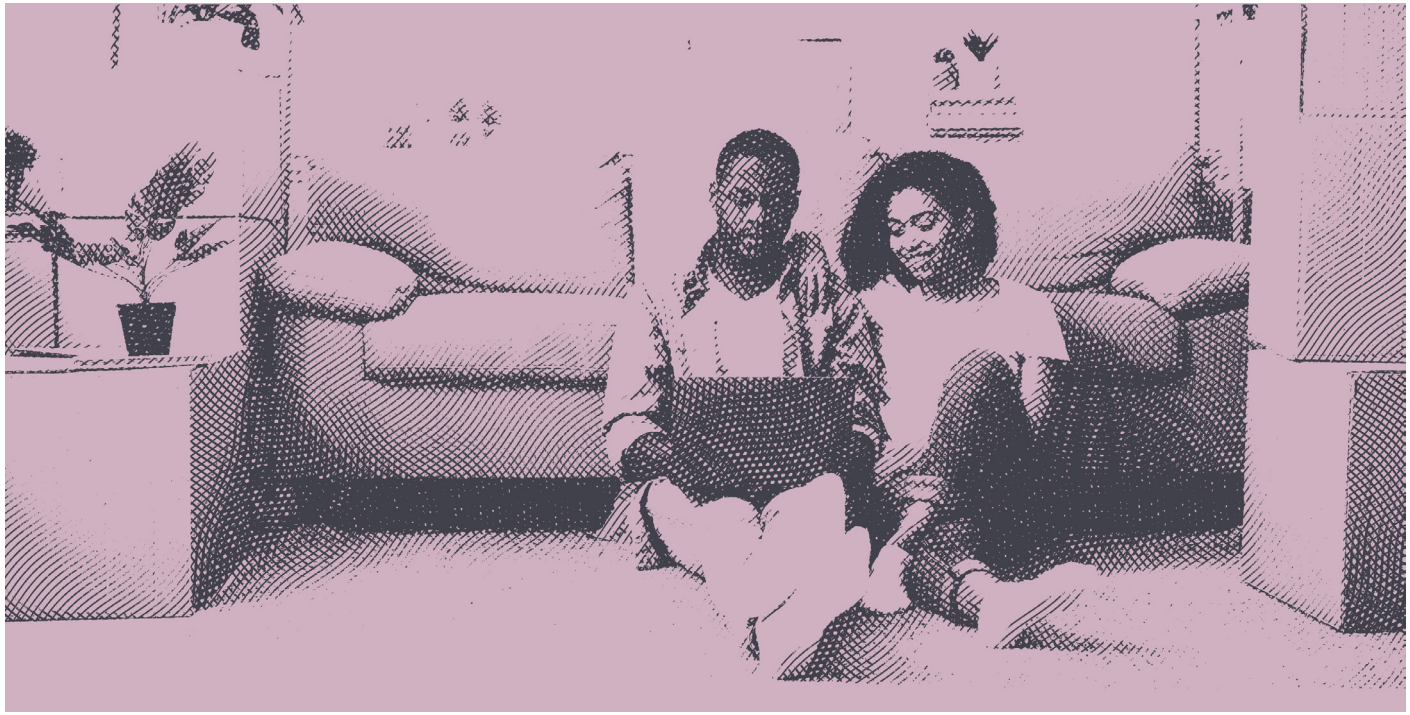
Als Hauptgrund für ihre erhöhte Vorsicht im Internet während der Pandemie nannten die Befragten in Deutschland die Medienberichterstattung zu Onlinebedrohungen (34 %), genau wie die Büroangestellten in den USA (37 %), im Vereinigten Königreich (44 %) und in Australien (46 %).



Anteil der Befragten, die ihre erhöhte Vorsicht während der Pandemie auf die Medienberichterstattung zu Cyberbedrohungen zurückführen.

Es ist sehr erfreulich, dass Journalisten ihren Teil zur Aufklärung der Öffentlichkeit beitragen. Gleichzeitig ergibt sich hier eine Chance für digitale Marken, ihrerseits das Bewusstsein für Security-Themen bei Kundinnen und Kunden zu verbessern. Werden solche Initiativen zudem mit Sicherheitslösungen wie MFA kombiniert, können Unternehmen mehr Sicherheit bieten, Vertrauen auf- und ausbauen und nachhaltig den Umsatz steigern und sich vom Mitbewerb differenzieren.

Auch in ihrer Rolle als Arbeitgeber können Unternehmen einen Beitrag leisten. Durch eine verstärkte Sensibilisierung, Updates der vorhandenen und für Onlinebedrohungen anfälligen Technik und das Aufzeigen der Wirksamkeit von Sicherheitsmaßnahmen wie Endpoint-Anti-Malware können sie ihren Mitarbeitern das Vertrauen vermitteln, in ihren eigenen vier Wänden genauso gut geschützt zu sein, wie im Büro. Davon profitieren nicht nur indirekt die digitalen Marken von Drittanbietern, sondern auch das eigene Unternehmen: Der Ausbau des Mitarbeitervertrauens in die im Homeoffice genutzten Tools trägt zu einer höheren Produktivität bei.

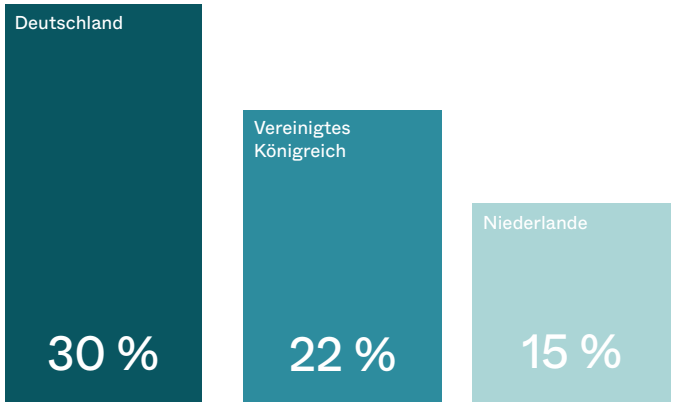


Teil Drei

Wie reagieren die Unternehmen?

Eine Vielzahl von Unternehmen haben Schritte unternommen, um den zunehmenden Cyberbedrohungen, die sich gegen ihre Mitarbeitenden im Homeoffice richten, Einhalt zu gebieten. Neue Sicherheitsanwendungen und -technologien wie MFA (26 %) waren in Deutschland die beliebteste Maßnahme, gefolgt von verbesserten Schulungen für Angestellte (23 %). Beides sind wichtige Maßnahmen zur Stärkung des Vertrauens der Mitarbeitenden und eine Investition in nachhaltigen Unternehmenserfolg.

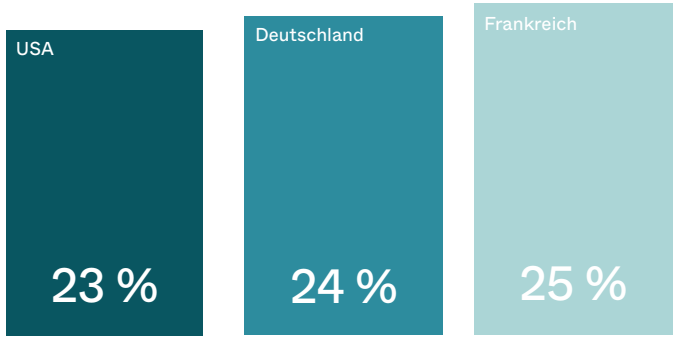
Besorgniserregend ist jedoch die Tatsache, dass 30 % der Befragten in Deutschland angaben, ihr Arbeitgeber habe bisher nichts gegen den pandemiebedingten Anstieg der Online-Bedrohungen unternommen. Das ist der höchste Wert im europäischen Vergleich. In Italien lag er bei 25 %, in Frankreich und im Vereinigten Königreich bei 22 % und in den Niederlanden bei 15 %. Die Umfrage hat weiterhin branchenspezifische Unterschiede gezeigt: Dabei haben in Deutschland insbesondere Befragte aus dem Bildungssektor (38 %), der Immobilienbranche (36 %) und dem Gesundheitswesen (37 %) angegeben, ihr Arbeitgeber habe keine Maßnahmen zur Bekämpfung der Cyberbedrohungen ergriffen.



Anteil der Befragten, die angaben, dass ihr Arbeitnehmer bisher keine Maßnahmen gegen den pandemiebedingten Anstieg von Online-Bedrohungen unternommen hat.

Darüber hinaus gab knapp ein Viertel aller deutschen befragten Büroangestellten (24 %) an, nicht zu wissen, ob ihr Arbeitgeber proaktive Sicherheitsmaßnahmen durchgeführt habe, ähnlich wie in den USA (23 %) und in Frankreich (25 %). In Schweden lag der Wert sogar bei 40 %.

Dies weist auf einen Mangel an Transparenz und Kommunikation zwischen Führungskräften, IT-Verantwortlichen und Mitarbeitern hin. Auch die besten Cybersicherheitssysteme können nur dann einen positiven Effekt auf das Vertrauen der Mitarbeiter haben, wenn diese über deren Einsatz informiert sind.



Anteil der Befragten, die angaben, nicht zu wissen, ob ihr Arbeitgeber proaktiv Sicherheitsmaßnahmen ergriffen hat.

> Cyberangreifer lernen immer neue Methoden – und die Mitarbeitenden sind sich dessen bewusst. Viele werden immer misstrauischer gegenüber Phishing, Datenschutzverletzungen und neuen Risiken wie Deepfake-Betrug. Unternehmen müssen daher sicherstellen, dass sie in diesem Spiel immer mindestens einen Schritt voraus sind und neue Bedrohungen mit neuen Ansätzen bekämpfen.
>
> Sven Kniest, Regional Vice President, Central and Eastern Europa, Okta

IT-Führungskräfte sollten nahtlose, risikobasierte Identitätsmanagementlösungen einsetzen und so die vertrauensbasierte Security im Jahr 2021 vorantreiben, um die Produktivität der Mitarbeiter zu steigern und Cyberrisiken zu minimieren. Darüber hinaus sollten sie neuen Technologien und Sicherheitsrichtlinien transparenter gestalten und kommunizieren.

Teil Vier

Fazit und Empfehlungen

IDC definiert [digitales] Vertrauen[2] als eine „Aufwertung der Sicherheitsdiskussion, die Attribute wie Risiko, Compliance, Datenschutz und Geschäftsethik einbezieht".

Angesichts der wachsenden Angriffsfläche für Cyberangriffe und der neuen Kanäle für die Kundenkommunikation und Unterstützung von Mitarbeitenden können IT- und Unternehmensleitende dieses Konzept nicht länger ignorieren. Richtig angegangen, kann digitales Vertrauen nicht nur potenzielle Schäden minimieren, sondern trägt auch entscheidend zur Steigerung des Umsatzes und des Wertes der Organisationen bei.

Im Unternehmen beginnt dies mit einem Zero-Trust-Ansatz. Dieser konzentriert sich auf die Identität der Anwender und hat risikobasierte Zugriffsrichtlinien sowie kontinuierliche, adaptive Authentifizierung und einen reibungslosen Zugriff auf Anwendungen und Daten zum Ziel.

Die Pandemie hat die Notwendigkeit eines solchen Ansatzes noch einmal verdeutlicht: Mit der steigenden Zahl an Cyberattacken, die darauf zielen in Unternehmensnetzwerke einzudringen, müssen Unternehmen sicher sein, dass Remote-User wirklich die sind, die sie vorgeben zu sein. Genauso wichtig ist es, das Vertrauen der Mitarbeitenden zu fördern, damit diese produktiver arbeiten können.

Das Thema Vertrauen schließt auch Kunden und Kundinnen ein. Digitale Unternehmen müssen deren Vertrauen pflegen und sich als verantwortungsvolle Manager von Kundendaten präsentieren.

Dies fördert die Kundenbindung und den Unternehmenserfolg – besonders wenn Daten- und Identitätsdiebe während der Pandemie ihre Aktivitäten intensivieren. Auch im Kundenkontext beginnt Vertrauen mit Sicherheit. Identität ist hier die zentrale Säule. Digitale Marken sollten ihren Kunden die richtigen Werkzeuge an die Hand geben, um sich nahtlos und sicher zu authentifizieren.

[2] IDC Perspective, 2020, Future of Trust: Defining Trust, April 2020, #US46185920

Zusammenfassung der wichtigsten Empfehlungen

Führungskräfte und IT-Verantwortliche müssen ihre implementierten Cybersecurity-Maßnahmen und -Richtlinien transparent mit ihren Mitarbeitern kommunizieren, um Vertrauen und Akzeptanz zu fördern.

Neue Sicherheitstools wie MFA und Biometrie zur passwortlosen Authentifizierung sind entscheidend für den Schutz vor Identitätsdiebstahl bei Kunden und für die Sicherung des Remote-Zugriffs für Mitarbeiter.

Interne Schulungen zum Thema Phishing und zu bewährten Sicherheitspraktiken helfen, die Risiken bei Remote Work und im Homeoffice zu minimieren.

Aktualisierungen der Sicherheitsstrategie stellen sicher, dass diese auf die sich ständig verändernde Bedrohungslandschaft, das regulatorische Risikoumfeld und die Haltung gegenüber dem Thema Vertrauen abgestimmt ist.

Das Aufzeigen und Veranschaulichen der Effektivität von Sicherheitsmaßnahmen gibt Remote-Mitarbeitenden das Vertrauen, zu Hause genauso gut geschützt zu sein wie im Büro.

Es ist wichtig, dass staatliche Organisationen Cybersicherheits- und Datenschutzmaßnahmen priorisieren, um die Daten und Identitäten der Bürger während der Pandemie zu schützen.

Datenethik ist ein wichtiges Anliegen von Kundinnen und Kunden. Daher sollten Unternehmen sich nicht nur an gesetzliche Richtlinien halten, sondern jeglichen Missbrauch verhindern und das Risiko von Datenschutzverletzungen minimieren.

Teil Fünf

Absicherung des Unternehmens mit Okta

Identität ist die Grundlage für den Aufbau vertrauensbasierter, sicherer Organisationen. Mit der Okta Identity Cloud können Verantwortliche weltweit die besten digitalen Erfahrungen für ihre Mitarbeitenden, Partner, Kunden und Kundinnen schaffen.

Sichern Sie Ihre Mitarbeitenden – egal von wo sie arbeiten – mit den **Workforce Identity-Lösungen** von Okta. Erhalten Sie die passenden Tools zur Absicherung und Automatisierung von Cloud Journeys und vollen Support für hybride Umgebungen.

Nutzen Sie die **Customer-Identity-Lösungen** von Okta, um sichere, nahtlose Kundenerlebnisse zu schaffen, von denen Entwickler und Nutzer gleichermaßen profitieren.

Über Okta

Okta ist der führende unabhängige Anbieter von Identitätslösungen für Unternehmen. Die Okta Identity Cloud ermöglicht es Unternehmen, die richtigen Personen zum richtigen Zeitpunkt sicher mit den richtigen Technologien zu verbinden. Mit über 6.500 vorgefertigten Integrationen zu Anwendungen und Infrastrukturanbietern können Okta-Kunden die besten Technologien für ihr Unternehmen einfach und sicher nutzen. Mehr als 9.400 Unternehmen, darunter Adobe, FreeNow, Hannover Rück, KWS Saat, Merz Pharma, Siemens und Zürich Versicherung vertrauen auf Okta, um die Identität ihrer Mitarbeiter und Kunden zu schützen.

www.okta.com/de

okta