docusign | ENTRUST
SECURING A WORLD IN MOTION

Whitepaper

Die Zukunft der globalen Identitätsüberprüfung

Wie führende Unternehmen digitale Sicherheit mit Nutzererfahrung in Einklang bringen

Angesichts der wachsenden Bedrohung durch Identitätsbetrug suchen Unternehmen weltweit nach innovativen Wegen, um die Identität ihrer Kunden sicher zu überprüfen und zu authentifizieren. Lösungen zur Identitätsverifizierung (IDV) und Authentifizierung schaffen die notwendige Sicherheitsebene. Durch tiefere Einblicke in den Einsatz solcher Lösungen durch führende Unternehmen und ein besseres Verständnis der besonders anfälligen Bereiche der Customer Journey können sich Unternehmen gezielt vor steigenden Risiken schützen.

Docusign, das Unternehmen für Intelligent Agreement Management, und Onfido, ein Unternehmen von Entrust, haben diesen Bericht gemeinsam erstellt, um ein umfassendes Bild der globalen Bedrohung durch Identitätsbetrug zu zeichnen und die Rolle der Identitätsverifizierung (IDV) bei dessen Bekämpfung zu analysieren. Die Studie bietet nicht nur Einblicke, an welchen Stellen der Customer Journey Identitätsbetrug auftritt und wie Teams darauf reagieren, sondern beleuchtet auch die spezifischen Herausforderungen, mit denen Unternehmen in verschiedenen Regionen und Branchen konfrontiert sind.

Wichtige Erkenntnisse

1 **Fälle von Identitätsbetrug nehmen zu und kosten Unternehmen Zeit, Geld und Ressourcen.**

Ein erheblicher Teil der befragten Unternehmen büßt jährlich über 900.000 € durch Kosten ein, die direkt und indirekt im Zusammenhang mit Identitätsbetrug stehen – und diese Ausgaben werden voraussichtlich mit dem Fortschritt der künstlichen Intelligenz (KI) weiter steigen. Trotz dieser Herausforderungen zögern einige Unternehmen, Maßnahmen zur Betrugsprävention zu ergreifen, weil sie eine Beeinträchtigung der Kundenerfahrung fürchten. 66 % der befragten Unternehmen weltweit und 70 % der Unternehmen in Deutschland stimmen zu, dass Kundenerfahrung und Betrugsprävention konkurrierende Prioritäten darstellen. In der Praxis stellen jedoch viele Unternehmen fest, dass sich diese Ziele nicht ausschließen: Unternehmen, die eine Lösung zur Identitätsverifizierung nutzen, sind doppelt so zufrieden wie Unternehmen, die IDV nicht nutzen.

2 **Identitätsbetrug kann während der gesamten Customer Journey auftreten, am häufigsten jedoch, wenn sich Kunden anmelden oder eine Zahlung autorisieren.**

Neben Betrugsversuchen in verschiedenen Phasen der Customer Journey werden Unternehmen auch mit verschiedenen Betrugsarten konfrontiert. Die häufigsten Betrugsformen in allen Branchen stellen Identitätsdiebstahl, Kontoerstellung, digitale Dokumentenfälschung und Rückbuchungsbetrug dar. Besonders anfällig für Identitätsbetrug ist die Authentifizierungsmethode über Benutzername und Passwort. Eine detaillierte Analyse des organisatorischen Verhaltens zeigt, dass zwei Drittel der Unternehmen unterschiedliche Authentifizierungsstufen je nach Kundeninteraktion anwenden, basierend entweder auf dem Risikoprofil ihrer Kunden oder der Art der Interaktion.

3 **IDV bietet Unternehmen nicht nur eine starke Verteidigungslinie gegen Identitätsbetrug, sondern auch einen entscheidenden Wettbewerbsvorteil.**

Nutzer von IDV erkennen Identitätsbetrug früher in der Customer Journey und häufiger als Unternehmen, die keine IDV-Lösungen einsetzen. Durch die Prävention von Identitätsbetrug haben Unternehmen, die IDV verwenden, durchschnittlich ca. 7,4 Millionen € oder mehr eingespart. 63 % der Unternehmen, die stärker in IDV investiert haben als ihre Mitbewerber in der Branche, sind überzeugt, dass ihre Maßnahmen zur Betrugsprävention einen positiven Einfluss auf ihre Markenwahrnehmung hatten.

4 **Die Mehrheit der Unternehmen sieht in der Technologie den Schlüssel zur Bekämpfung und Minderung von Kundenbetrug.**

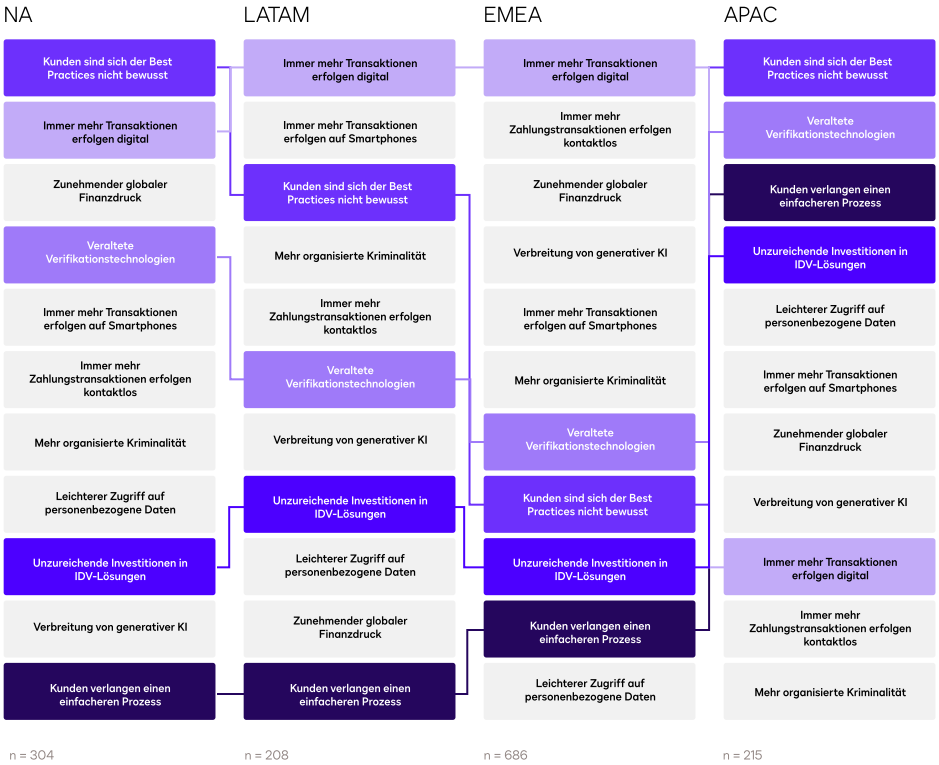
69 % der befragten deutschen Unternehmen sind der Ansicht, dass umfangreiche Investitionen in Technologielösungen der effektivste Weg sind, um das finanzielle Risiko von Identitätsbetrug zu verringern. IDV zählt dabei zu ihren wichtigsten Prioritäten und 74 % planen, in Zukunft noch mehr in IDV zu investieren.

Identitätsbetrug ist neben hohen Kosten und steigenden Kundenerwartungen eine zunehmende Sorge.

69 % der befragten Unternehmen weltweit sind sich einig, dass die Zahl der Versuche von Identitätsbetrug zunimmt. Obwohl viele Unternehmen mit dieser Herausforderung konfrontiert sind, variieren die Einschätzungen darüber, was diesen Anstieg verursacht, je nach Branche und Region. Zwei Gründe wurden in unseren Untersuchungen jedoch am häufigsten genannt:

- Heute werden immer mehr Transaktionen digital abgewickelt
- Kunden sind oft nicht mit den Best Practices zum Schutz ihrer Anmeldeinformationen und anderer sensibler Daten vertraut

Mangelndes Kundenbewusstsein für bewährte Sicherheitspraktiken und die Zunahme digitaler Transaktionen als Hauptursache für steigende Betrugsversuche



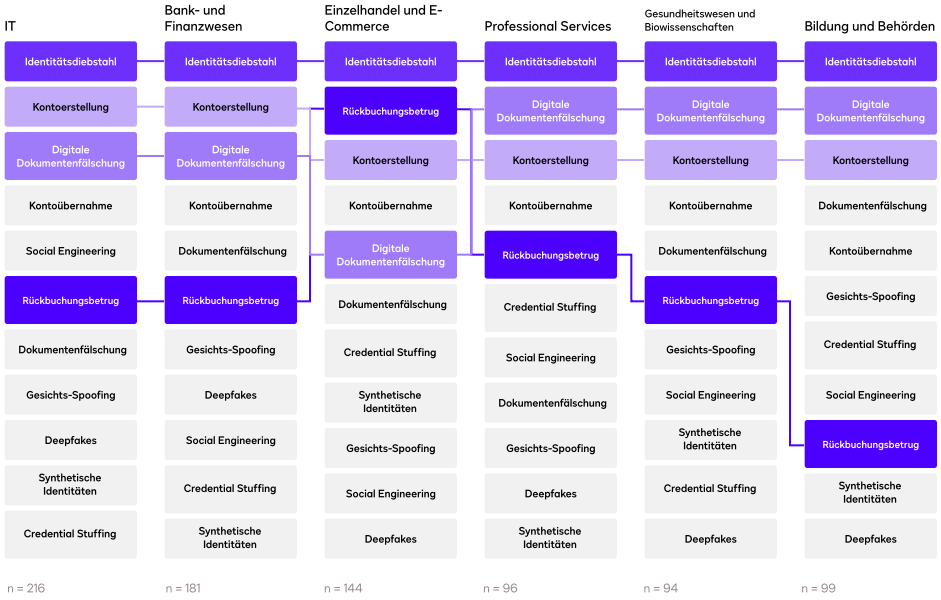
Was sind Ihrer Meinung nach die Hauptgründe für die Zunahme von Betrugsversuchen?

Obwohl nur wenige Unternehmen in dieser Umfrage KI als führenden Treiber von Betrug nannten, deuten andere Untersuchungen darauf hin, dass sie erheblich zur Veränderung der Sicherheitslandschaft beitragen könnte. Der 2025 Identity Fraud Report von Entrust zeigte, dass **digitale Dokumentenfälschungen,** die oft mit generativer KI erstellt werden, im vergangenen Jahr **um 244 % zugenommen haben.** Deepfakes wie diese Fälschungen machen mittlerweile 40 % des gesamten biometrischen Betrugs aus. Gleichzeitig sehen viele Unternehmen KI als ein entscheidendes Werkzeug im Kampf gegen Identitätsbetrug: 82 % der Befragten sind der Meinung, dass generative KI effektiver sein wird als ihre aktuellen Methoden, um das Betrugsrisiko für Kunden zu reduzieren.

Es zeigen sich auch klare Muster bei den verschiedenen Arten von Identitätsbetrug, die Unternehmen beobachten. Branchenübergreifend war Identitätsdiebstahl die am häufigsten genannte Form des Identitätsbetrugs, gefolgt von der Fälschung digitaler Dokumente sowie Betrug bei der Kontoerstellung und (in Deutschland) Kontoübernahmen. Der Einzelhandel und E-Commerce heben sich jedoch ab, da in diesen Sektoren auch Rückbuchungsbetrug – bei dem Kunden eine Abbuchung absichtlich anfechten, um eine Rückerstattung zu erhalten, während sie das Produkt oder die Dienstleistung behalten – unter den drei häufigsten Betrugsarten genannt wird. Dies ist auf die Rolle von Verbraucherkäufen in dieser Branche zurückzuführen.

Diese Erkenntnisse verdeutlichen, dass die meisten Versuche von Identitätsbetrügen in entscheidenden Momenten der Kundeninteraktion auftreten, sei es beim Erstellen eines Kontos, beim Zurücksetzen eines Passworts oder beim Eingeben von Zahlungsinformationen. Um diese kritischen Phasen der Customer Journey zu schützen, müssen Unternehmen Lösungen anbieten, die eine sichere Kontoeröffnung ermöglichen und die Identität der Kunden über den gesamten Lebenszyklus hinweg kontinuierlich überprüfen.

Identitätsdiebstahl, Kontoerstellung und -übernahme sowie digitale Dokumentenfälschungen sind in Deutschland die häufigsten Arten von Identitätsbetrug in verschiedenen Branchen



Welche Betrugsarten im Zusammenhang mit der Identitätsprüfung und Benutzerauthentifizierung treten in Ihrem Unternehmen am häufigsten im Rahmen des Kundentransaktionsprozesses auf?

Regionale Erkenntnisse

Prozentsatz der Unternehmen mit direkten Kosten von über 900.000 € durch Identitätsbetrug

Länder mit den höchsten Prozentsätzen

55 % **Deutschland**
65 % **Australien**

Länder mit den niedrigsten Prozentsätzen

27 % **Vereinigtes Königreich**
25 % **Brasilien**

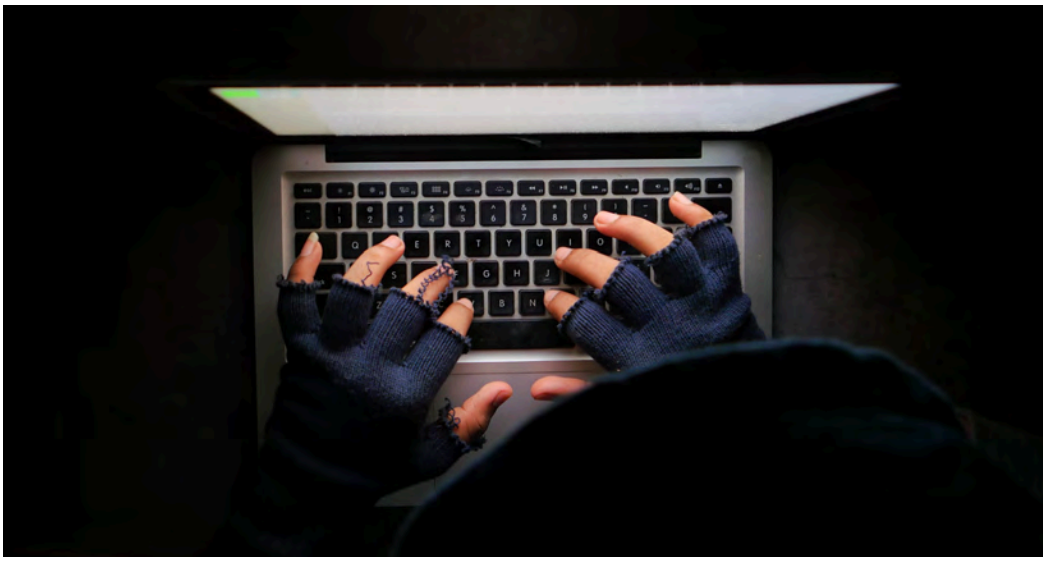
Prozentsatz der Unternehmen mit indirekten Kosten von über 900.000 € durch Identitätsbetrug

Länder mit den höchsten Prozentsätzen

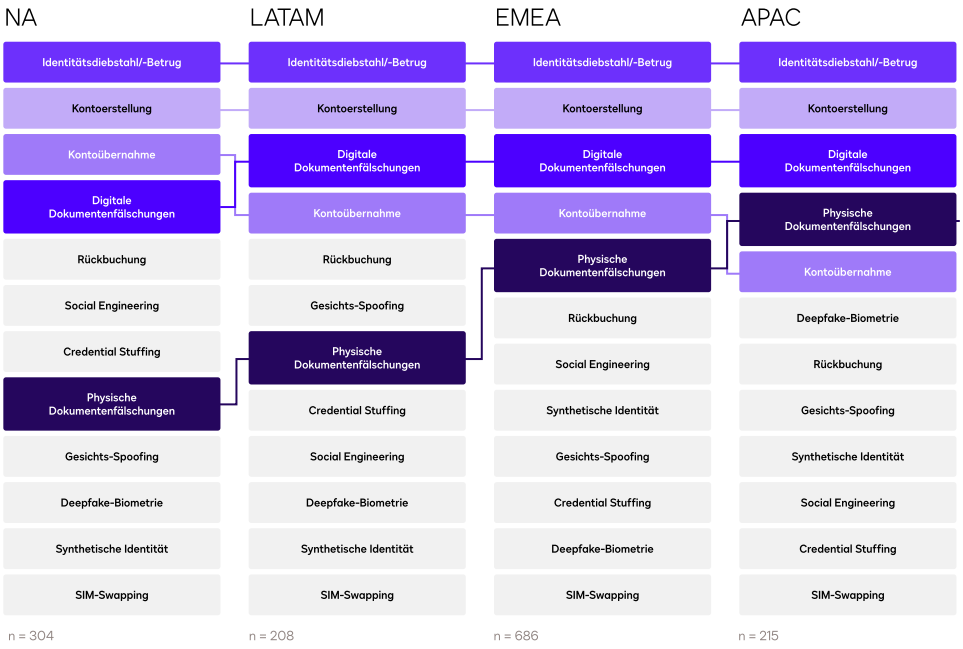
24 % **Brasilien**
29 % **Australien**

Länder mit den niedrigsten Prozentsätzen

6 % **Mexiko**



Identitätsdiebstahl, Kontoerstellung und digitale Dokumentenfälschungen sind die häufigsten Arten von Identitätsbetrug in allen Regionen



Welche Betrugsarten im Zusammenhang mit der Identitätsprüfung und Benutzerauthentifizierung treten in Ihrem Unternehmen am häufigsten im Rahmen des Kundentransaktionsprozesses auf? Bitte klicken Sie, um bis zu drei regelmäßig vorkommende Ereignisse nach deren Häufigkeit zu nennen.

Die Banken- und Finanzbranche meldete die höchsten direkten Kosten durch Identitätsbetrug. (51 % berichteten über jährliche direkte Kosten von über 900.000 €)

Die Branche der professionellen Dienstleistungen verzeichnete die höchsten indirekten Kosten durch Identitätsbetrug. (20 % berichteten über jährliche indirekte Kosten von über 900.000 €)

Identitätsbetrug kostet Organisationen durchschnittlich über 6 Millionen € pro Jahr

Viele Unternehmen sehen die mit Identitätsbetrug verbundenen Kosten lediglich als unvermeidlichen Preis für ihre Geschäftstätigkeit. Doch dieser Preis steigt täglich. Unternehmen sehen sich regelmäßig mit sechs- bis siebenstelligen Ausgaben konfrontiert, die sowohl direkte Kosten wie Rückbuchungen, Rückerstattungen und andere finanzielle Verluste umfassen, als auch indirekte Kosten, die durch den Einsatz wertvoller Mitarbeiterressourcen zur Erkennung und Behebung betrügerischer Transaktionen sowie zur Bewältigung von Schäden an Marke und Reputation entstehen. Unsere Untersuchungen haben Folgendes ergeben:

41 %

der Unternehmen weltweit und 57 % der Unternehmen in Deutschland haben jährlich direkte Kosten durch Identitätsbetrug von über 900.000 €.

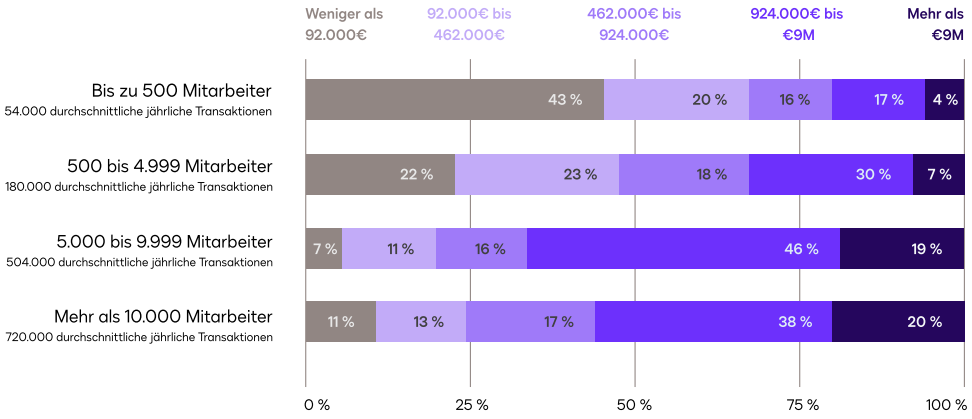
15 %

der Unternehmen weltweit und 18 % der Unternehmen in Deutschland haben jährlich indirekte Kosten durch Identitätsbetrug von über 900.000 €.

Größere Unternehmen, die eine erhebliche Anzahl an Kunden, Daten und Umsätzen verwalten, sind noch höheren Kosten durch Identitätsbetrug ausgesetzt. Besonders betroffen sind Unternehmen mit mehr als 5.000 Mitarbeitenden:

- **Die durchschnittlichen jährlichen direkten Kosten durch Identitätsbetrug belaufen sich auf ca. 12 Millionen €.** 28 % der Unternehmen verzeichnen jährliche indirekte Kosten durch Identitätsbetrug von über 900.000 €.
- Zudem steigen die finanziellen Belastungen mit der Unternehmensgröße erheblich. **So geben 20 % der befragten Unternehmen an, dass ihre direkten und indirekten Kosten durch Identitätsbetrug jährlich ca. 45 Millionen € oder mehr betragen.**

Große Unternehmen haben höhere direkte Kosten durch Identitätsbetrug



Wie hoch würden Sie die direkten finanziellen Kosten schätzen, die Ihrem Unternehmen pro Jahr durch Kundenbetrug entstehen? Unter direkten finanziellen Kosten verstehen wir den Geldbetrag, der durch Betrug verloren geht, unabhängig davon, ob er durch eine Versicherung gedeckt ist.

Auf Branchenebene sind Banken und Finanzen mit den höchsten direkten Kosten durch Identitätsbetrug konfrontiert. Dies liegt daran, dass Betrüger während des Kunden-Onboardings gefälschte Konten erstellen, die ihnen Zugang zu Finanzdienstleistungen ermöglichen, oder in einer späteren Phase des Kundenlebenszyklus Zugang zu legitimen Konten erhalten und diese leeren. In beiden Szenarien verliert das betroffene Unternehmen direkt Geld oder muss es dem legitimen Kunden zurückzahlen.

Die höchsten indirekten Kosten durch Identitätsbetrug entstehen in der Branche der professionellen Dienstleistungen. Identitätsbetrug wirkt sich mit größerer Wahrscheinlichkeit auf den Ruf solcher Unternehmen und das Vertrauen der Kunden aus, was zukünftige Einnahmen mindert und zu erheblichen indirekten Kosten führt.

66 %

der befragten Unternehmen weltweit sind der Meinung, dass Kundenerfahrung und Identitätsbetrugs-prävention konkurrierende Prioritäten sind.

45 %

der befragten Unternehmen weltweit räumen dem Kundenerlebnis Priorität gegenüber der Betrugsprävention ein.

58 %

der befragten Unternehmen weltweit sind besorgt, dass sie Kunden verärgern und die Abwanderungsrate erhöhen könnten, wenn sie die Prävention von Identitätsbetrug verstärken.

Das Bedürfnis von Kunden nach reibungslosen Erfahrungen wird immer lauter.

79 % der befragten Unternehmen sind sich einig, dass das Kundenerlebnis für ihren Erfolg sehr wichtig ist.

Unternehmen stehen unter Druck, einfache, angenehme und wettbewerbsfähige digitale Erlebnisse zu bieten, während sie gleichzeitig die Kundendaten schützen. Viele Kunden erwarten beispielsweise personalisierte Erlebnisse, für Mobilgeräte optimierte Transaktionen und Formulare, die bereits mit zu einem früheren Zeitpunkt gemachten Angaben ausgefüllt sind. Gleichzeitig gehen sie davon aus, dass ihre Daten bei solchen Interaktionen stets sicher bleiben. Viele Unternehmen haben Schwierigkeiten, diese Ziele miteinander in Einklang zu bringen.

Allerdings gibt es je nach Region, Branche und Generation unterschiedliche Ansätze für die Abwägung zwischen Identitätsbetrugsprävention und Kundenerfahrung. In der IT-Branche und im Bank- und Finanzwesen ist die Wahrscheinlichkeit größer, dass Kunden zum Schutz vertraulicher Daten bzw. hochwertiger Transaktionen strengen Authentifizierungsmaßnahmen unterzogen werden, selbst wenn diese Maßnahmen mehr Reibung verursachen.

Entscheidungsträger der Millennials und der Gen Z, die mit digitalen Identitätsüberprüfungen vertrauter sind, erwarten außergewöhnliche Benutzererfahrungen und Sicherheit bei digitalen Transaktionen und treiben dadurch technologische Innovationen voran.

Insgesamt sind Unternehmen, die IDV verwenden, doppelt so zufrieden wie Unternehmen, die es nicht verwenden, und finden ihre Methoden zur Betrugsprävention deutlich effektiver.

Wichtige Erkenntnis

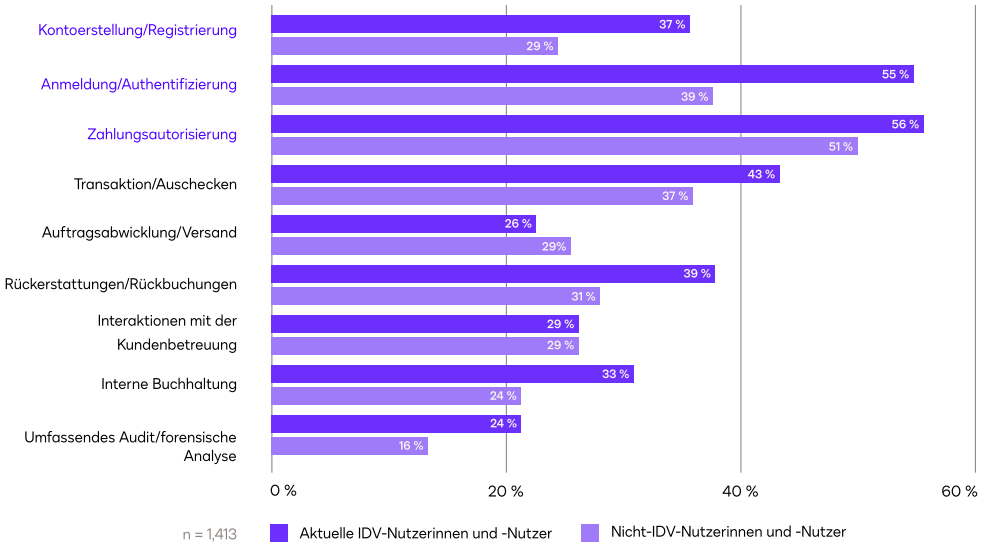
Die Bekämpfung der zunehmenden Versuche von Identitätsbetrug bei gleichzeitiger Bereitstellung eines reibungslosen Erlebnisses ist eine wachsende Herausforderung, aber IDV hilft Unternehmen, Identitätsbetrug zu reduzieren und gleichzeitig die Zufriedenheit zu steigern. Unternehmen, die Identitätsbetrug mit veralteten oder unzureichenden Technologien mindern möchten, werden Schwierigkeiten haben, sich gegen komplexe Techniken des Identitätsbetrugs zu verteidigen oder mit neuen Bedrohungen Schritt zu halten.

Identitätsbetrug tritt während der gesamten Customer Journey auf.

Identitätsbetrug tritt während der gesamten Customer Journey auf, aber Unternehmen **erkennen ihn am häufigsten in den frühen Phasen der Anmeldung und Zahlungsautorisierung.**

Unternehmen, die IDV verwenden, erkennen mit noch größerer Wahrscheinlichkeit Identitätsbetrugsversuche schon frühzeitig während Transaktionen und verbessern damit die Chancen, Schäden zu verhindern oder zu mindern.

IDV-Nutzer sind eher in der Lage, Betrug in frühen Phasen der Customer Journey zu entdecken



Zu welchem Zeitpunkt im Transaktionsprozess erfährt Ihr Unternehmen in der Regel, dass ein Betrugsversuch stattgefunden hat? Die unten aufgeführten Optionen sind in absteigender Reihenfolge von ersten Kundeninteraktionen bis zur Nachbearbeitung von Kundeninteraktionen aufgeführt.

Auf die Frage, welche Authentifizierungswerkzeuge am häufigsten mit Identitätsbetrug in Verbindung gebracht werden, nannten Unternehmen **die Authentifizierung mit Benutzernamen und Passwörtern als die schwächste Methode.** Dies könnte daran liegen, dass Benutzernamen und Passwörter leicht kompromittiert werden können, anfällig für Datenverletzungen sind und keine Multifaktor-Authentifizierung bieten. Im Jahr 2024 waren gestohlene Anmeldedaten wie Benutzernamen und Passwörter die häufigste Ursache für Datenlecks.[1]

1 "2024 Data Breach Investigations Report," Verizon Business.

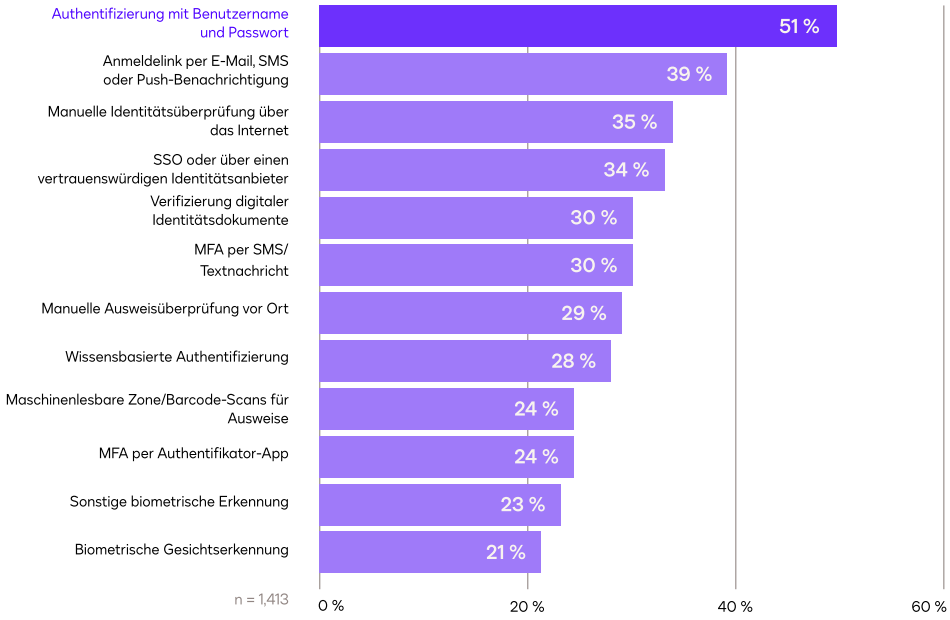
Unternehmen, die IDV einsetzen, erkennen Identitätsbetrugs-versuche im Durchschnitt in

20 %

mehr Phasen der Customer Journey als jene, die es nicht nutzen.

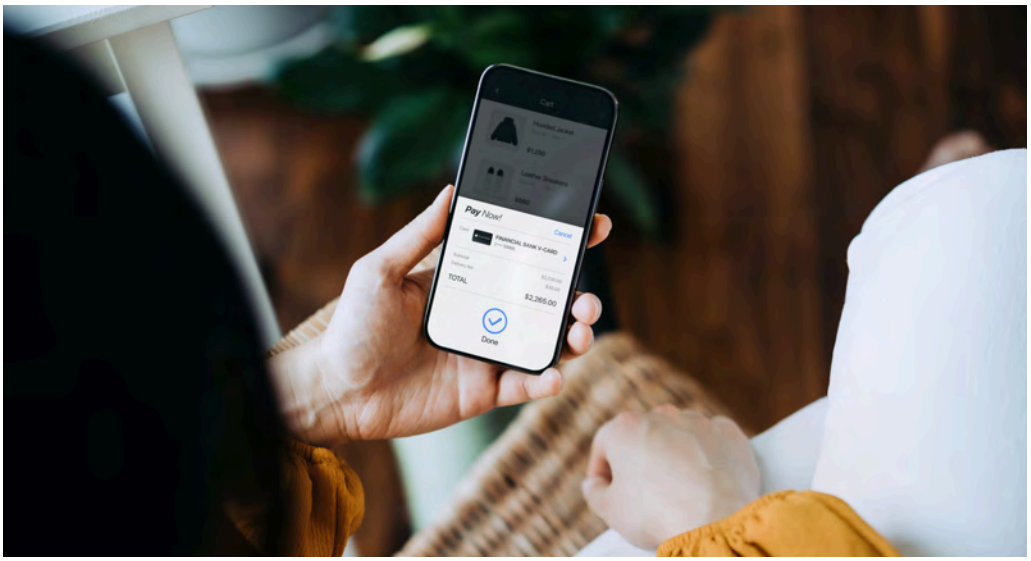
Identitätsbetrug tritt am häufigsten auf, wenn nur der Benutzername und das Passwort als Authentifizierungsmethode verwendet werden

Identitätsbetrug kommt mit dieser Technologie häufiger vor



Bitte geben Sie für jede Art der Benutzerauthentifizierung an, wie oft Sie Betrug im Vergleich zu anderen Authentifizierungstypen feststellen.

Die Umfrage ergab außerdem, dass in einem Unternehmen die Wahrscheinlichkeit der Erkennung von Betrug bei verschiedenen Authentifizierungsmethoden größer ist, je mehr digitale Transaktionen es abwickelt.



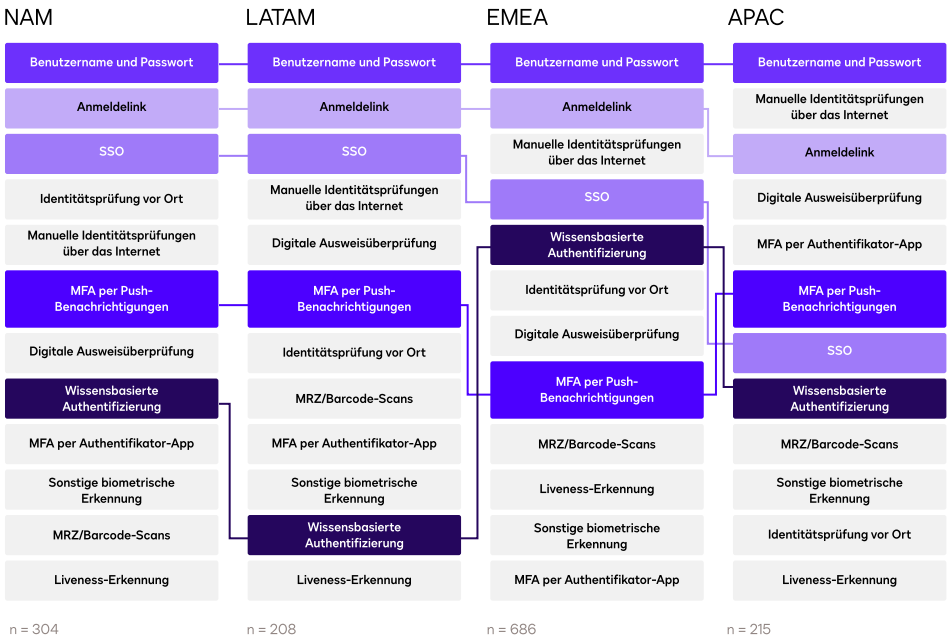
Zahlungsautorisierung und Anmeldung sind die häufigsten Phasen, in denen branchenübergreifend Betrug entdeckt wird

Zu welchen Zeitpunkten im Transaktionsprozess erfährt Ihr Unternehmen, dass ein Betrugsversuch stattgefunden hat?

Erkenntnisse zu verschiedenen Generationen

Unter den Entscheidungsträgern aus den Bereichen IT und Wirtschaft nutzen Führungskräfte der Millennials und Gen Z häufiger IDV als Babyboomer oder Gen X. Außerdem schätzen sie die Betrugsbekämpfung in ihrem Unternehmen eher als „sehr gut“ ein.

Benutzername und Passwort sind die Authentifizierungsmethode, die mit dem meisten Betrug in allen Regionen in Verbindung gebracht wird



Betrug kommt bei dieser Methode deutlich häufiger vor als im Durchschnitt.

Wichtigste Erkenntnis

Benutzername und Passwort sind die anfälligste Authentifizierungsmethode, aber selbst MFA reicht nicht aus, um vor immer komplexer werdenden Identitätsbetrugsversuchen zu schützen. Fortschrittliche Formen der IDV wie biometrische Authentifizierung und Dokumentenverifizierung sind unerlässlich, um Betrügern einen Schritt voraus zu bleiben.

Signifikante Investitionen in IDV führen zu greifbaren Ergebnissen.

Das durchschnittliche Unternehmen hat insgesamt mehr als ca.

7,3 Millionen €

durch die Betrugsprävention mit einer IDV-Lösung gespart.

Die Daten zeigen, dass IDV eine lohnende Investition ist. Durch die Implementierung einer IDV-Lösung sparten 52 % aller Unternehmen insgesamt über 900.000 € ein.

Aber die Bereitstellung einer IDV-Lösung ist nur der erste Schritt. Unternehmen, die die besten Ergebnisse vorweisen können, legen großen Wert auf ihre Sicherheit, indem sie erheblich mehr in IDV investieren als ihre Mitbewerber. Zusätzlich machen Unternehmen, die mehr investieren, ihre Unternehmen zu einem weniger attraktiven Ziel für Betrüger, was ihnen einen Wettbewerbsvorteil verschafft.

Unternehmen, die laut eigener Angabe erheblich mehr in IDV investieren als ihre Mitbewerber:

sparen mehr

1,5-mal

höhere Wahrscheinlichkeit, insgesamt über 900.000 € gespart zu haben als diejenigen, die etwas mehr investiert haben.

2,2-mal

höhere Wahrscheinlichkeit, insgesamt über 900.000 € gespart zu haben als diejenigen, die genauso viel oder weniger investiert haben.

reduzieren das Ausmaß von Identitätsbetrug

1,7-mal

höhere Wahrscheinlichkeit, ein erhebliches Aufkommen an Identitätsbetrug erfolgreich reduziert zu haben.

investieren weiterhin in IDV

2,8-mal

höhere Wahrscheinlichkeit, dass sie planen, mehr in IDV zu investieren.

erreichen größere interne Zufriedenheit und Kundenzufriedenheit

4-mal

höhere Wahrscheinlichkeit, mit den von ihnen verwendeten IDV-Lösungen sehr zufrieden zu sein.

1,6-mal

höhere Wahrscheinlichkeit eines positiven Einflusses auf ihre Marke.

sind wettbewerbsfähiger

2,7-mal

höhere Wahrscheinlichkeit, dass sie an einen Wettbewerbsvorteil glauben.

Die Daten deuten darauf hin, dass Kunden mehr Vertrauen in Unternehmen setzen, die alles tun, um ihre persönlichen Daten zu schützen.

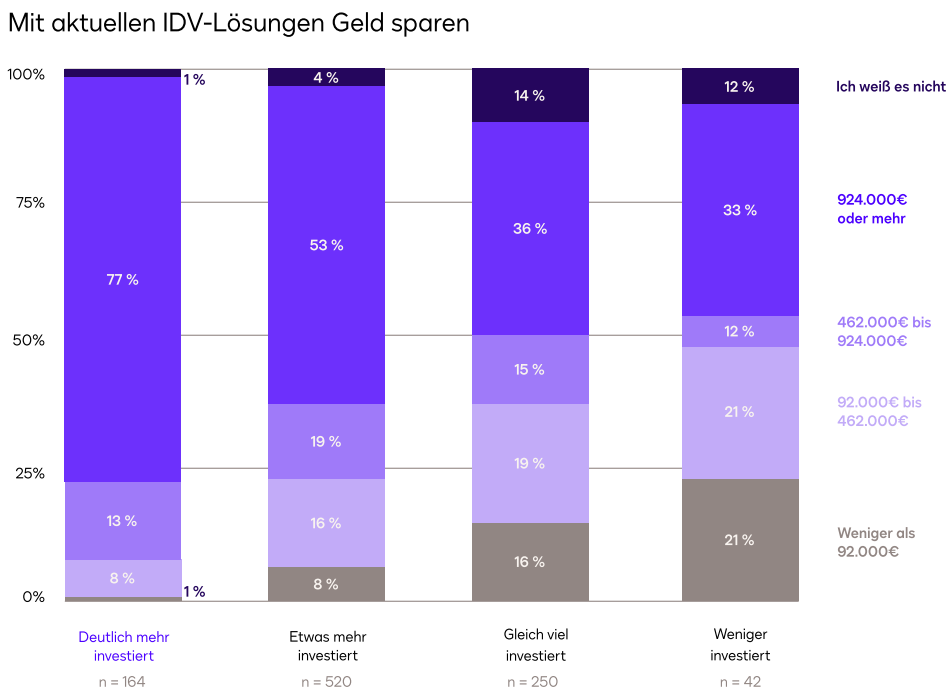
77 %

der Unternehmen, die deutlich mehr in Technologien zur Identitätsüberprüfung investiert haben als ihre Konkurrenten, haben

insgesamt über 900.000 € gespart,

im Vergleich zu 36 %, die die gleiche Summe wie ihre Konkurrenten investiert haben.

Unternehmen, die deutlich mehr als ihre Mitbewerber in IDV investierten, sparten mit größerer Wahrscheinlichkeit insgesamt 900.000 € oder mehr



Welchen Betrag hat Ihr Unternehmen schätzungsweise durch die Verhinderung von Kundenbetrug mithilfe Ihrer derzeitigen Lösungen zur Identitätsüberprüfung/ Benutzerauthentifizierung ungefähr eingespart?

Große Unternehmen investieren mehr in IDV und erzielen einen überproportional höheren Return on Investment (ROI).

Für Unternehmen, die in erheblichem Maße von Identitätsbetrug betroffen sind, führt eine Investition in IDV zu einem höheren ROI. Die Daten zeigen, dass große Unternehmen, die höhere Kosten durch Identitätsbetrug verzeichnen, zu erheblich höheren Investitionen in IDV-Lösungen neigen als ihre Mitbewerber und infolgedessen einen unverhältnismäßig höheren ROI erzielen.

78 %

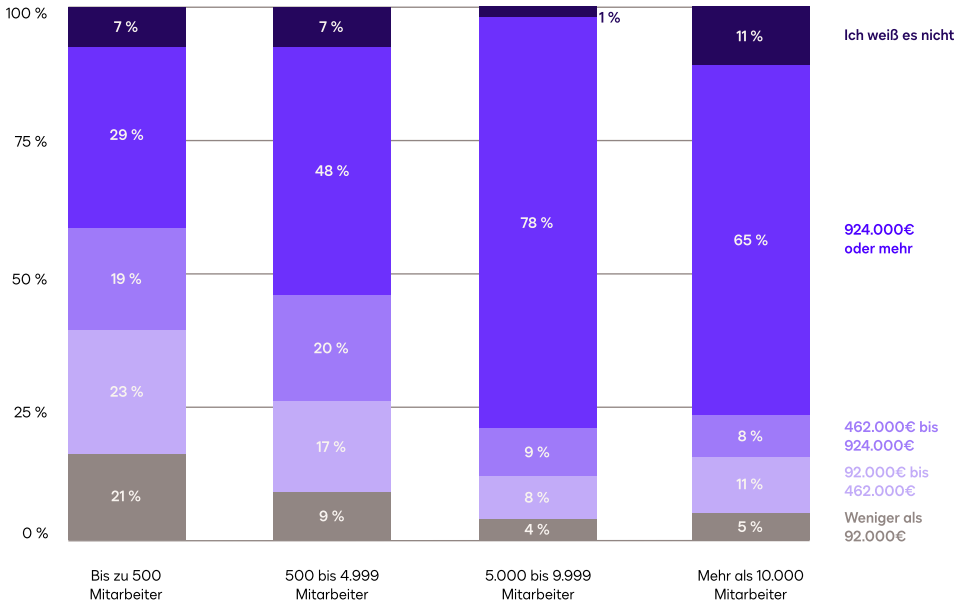
der Unternehmen mit 5.000 bis 9.999 Mitarbeitern haben insgesamt über 900.000 € mit IDV gespart.

65 %

der Unternehmen mit über 10 000 Mitarbeitern haben mit IDV insgesamt über 900.000 € gespart.

Große Unternehmen investieren erheblich mehr in IDV als ihre Branchenkollegen

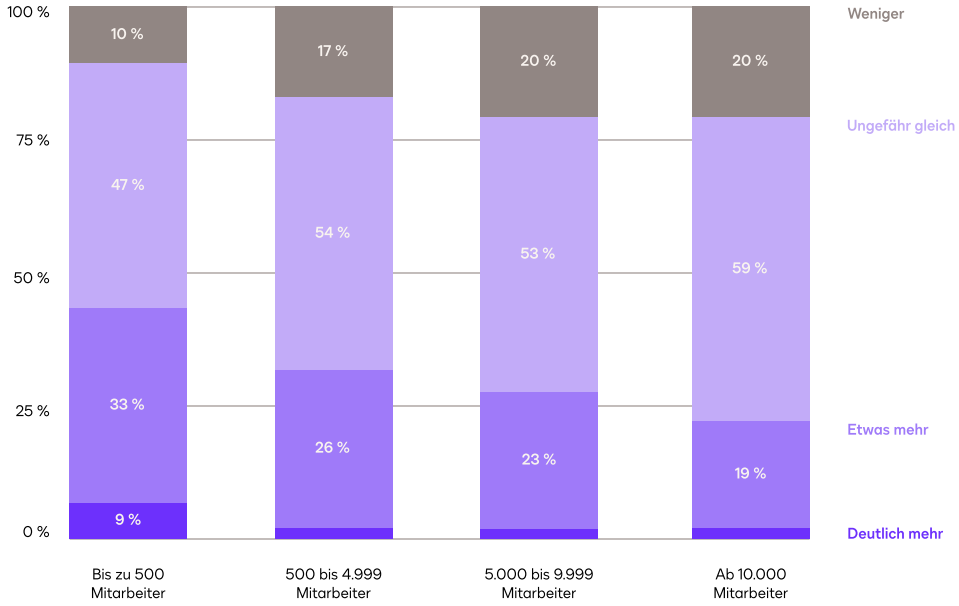
Mit aktuellen IDV-Lösungen Geld sparen



Welche der folgenden Optionen beschreibt die aktuellen Investitionen Ihres Unternehmens in Lösungen/Methoden zur Identitätsüberprüfung/Benutzerauthentifizierung am besten?

Große Unternehmen sparen mehr mit IDV-Lösungen

IDV-Investitionen im Vergleich zu Branchenkollegen



Welchen Betrag hat Ihr Unternehmen schätzungsweise durch die Verhinderung von Kundenbetrug mithilfe Ihrer derzeitigen Lösungen zur Identitätsüberprüfung/Benutzerauthentifizierung ungefähr eingespart?

Wichtige Erkenntnis

Unternehmen, die erheblich in IDV investieren, entsteht eine Reihe von Vorteilen, darunter größere Einsparungen, weniger Vorfälle von Identitätsbetrug, eine bessere Markenwahrnehmung, verbesserte Kundenerfahrungen und ein Wettbewerbsvorteil gegenüber Mitbewerbern.

Führende Unternehmen wenden sich der Technologie zu, um Betrug zu bekämpfen.

69 % der befragten Unternehmen in Deutschland stimmen zu, dass das finanzielle Risiko durch Identitätsbetrug am besten durch umfangreiche Investitionen in Technologie gemindert werden kann.

Es bestehen unterschiedliche Meinungen zur Zuversicht von Unternehmen, Identitätsbetrug bekämpfen zu können. 54 % der befragten Unternehmen in Deutschland glauben, dass sie Betrug eindämmen, aber niemals vollständig abschaffen können, während 38 % überzeugt sind, dass sie Betrug mit der richtigen Technologie vollständig abstellen können. Große Unternehmen mit über 10.000 Mitarbeitern fallen dabei eher in das Lager der Schadenseindämmer.

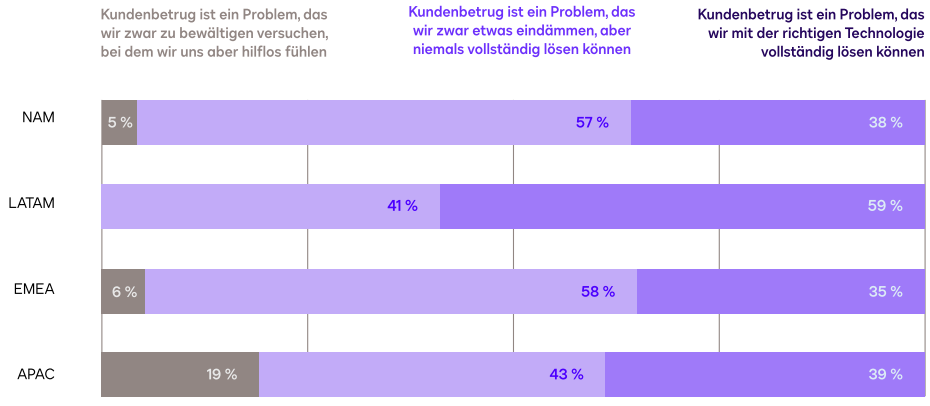
Obwohl die Wahrnehmungen des Problems selbst unterschiedlich ausfallen, sind sich die meisten Unternehmen über eine Lösung einig:

Diese 69 % zugunsten von Investitionen in Technologie übertreffen andere Ansätze von deutschen Unternehmen, wie Investitionen in Personal und Talente (22 %) und Investitionen in eine Versicherung gegen Wirtschaftskriminalität zur Abdeckung von Betrugskosten (9 %), reaktive Optionen, die darauf abzielen, Schäden zu beheben, anstatt ihre Unternehmen proaktiv vor Bedrohungen zu schützen.

Erkenntnisse zu verschiedenen Generationen

Führungskräfte, die zu den Millennials und der Gen Z gehören, sind eher als Babyboomer oder die Gen X der Meinung, dass Betrug mit der richtigen Technologie vollständig gelöst werden kann.

In Europa sind deutsche Unternehmen mit 38 % am optimistischsten, was die vollständige Lösung des Betrugsproblems angeht



Welcher der folgenden Aussagen stimmen Sie am ehesten zu?

Das verbreitetste IDV-Tool ist die Multi-Faktor-Authentifizierung.

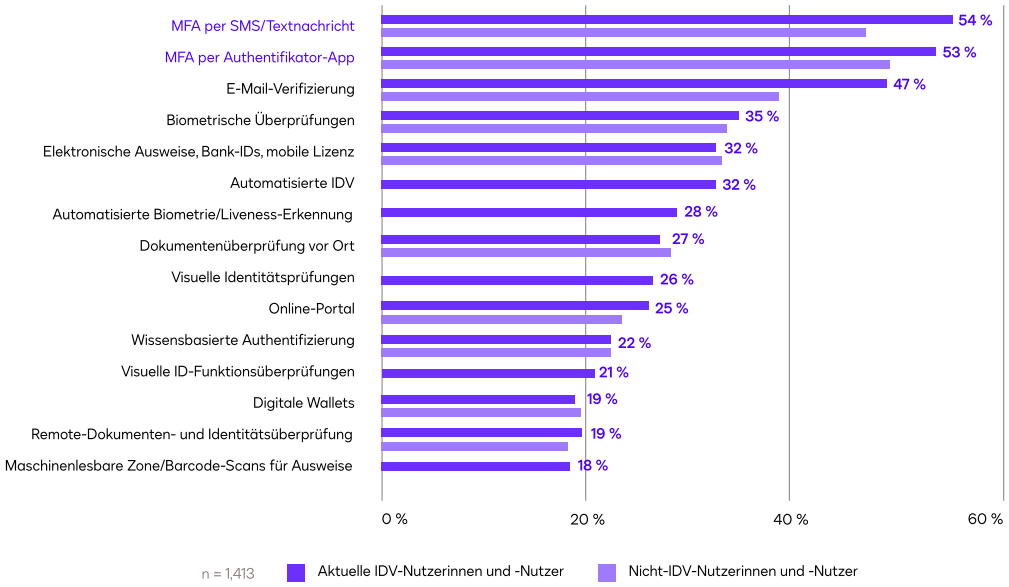
Unternehmen verwenden IDV-Tools an verschiedenen Berührungspunkten in der Customer Journey, aber die häufigste Phase ist die Authentifizierung mit Benutzername und Passwort – die Phase, in der Unternehmen die meisten Betrugsfälle melden.

Die Multi-Faktor-Authentifizierung (MFA) ist das am häufigsten von Unternehmen verwendete Werkzeug zur Überprüfung und Authentifizierung von Identitäten, sei es per SMS und Textnachricht oder mit einer Authentifizierungs-App.

Die Verbreitung von MFA ist gerechtfertigt: Sie ist eine der ältesten Methoden der digitalen Identifizierung und Kunden sind daran gewöhnt, was die Nutzung erleichtert und gleichzeitig eine wesentliche Sicherheitsebene bietet.

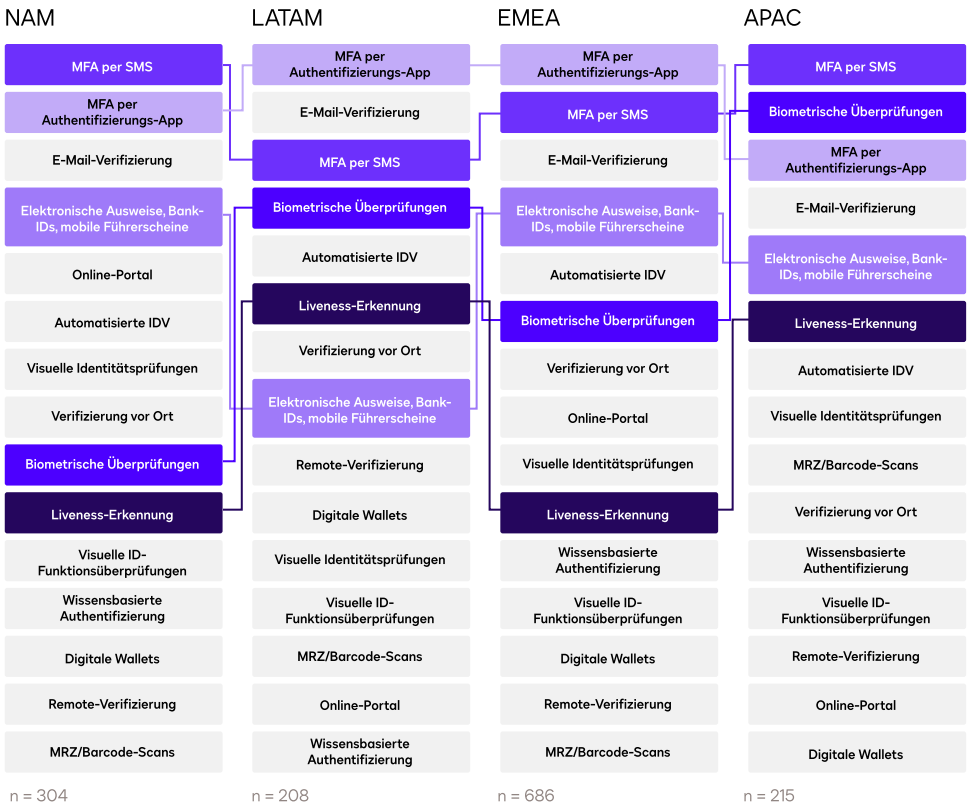
MFA ist das am häufigsten verwendete Tool zur Identitätsüberprüfung und Authentifizierung

Derzeit verwendete Arten von IDV und Nutzer-Authentifizierung



Welche der folgenden Arten der Identitätsüberprüfung/Nutzerauthentifizierung verwendet Ihr Unternehmen derzeit? Bitte wählen Sie alle zutreffenden aus.

In Europa werden biometrische Überprüfungen häufiger in Deutschland verwendet, während die E-Mail-Verifizierung häufiger in Großbritannien eingesetzt wird



Welche der folgenden Arten der Identitätsüberprüfung/Nutzerauthentifizierung verwendet Ihr Unternehmen derzeit?

Entscheidungsträger in Deutschland nutzen biometrische Werkzeuge häufiger als Entscheidungsträger in Großbritannien und Frankreich.

Erkenntnisse zu verschiedenen Generationen

Führungskräfte, die Millennials sind oder der Gen Z angehören, sind der Meinung, dass Biometrie ein wesentlicher Bestandteil der Online-Authentifizierung ist. Laut einer Untersuchung von IDEX Biometrics haben 47 % der Befragten in dieser Gruppe im letzten Monat biometrische Sicherheitsmethoden genutzt. Von diesen bevorzugen 52 % die biometrische Authentifizierung gegenüber anderen Methoden.

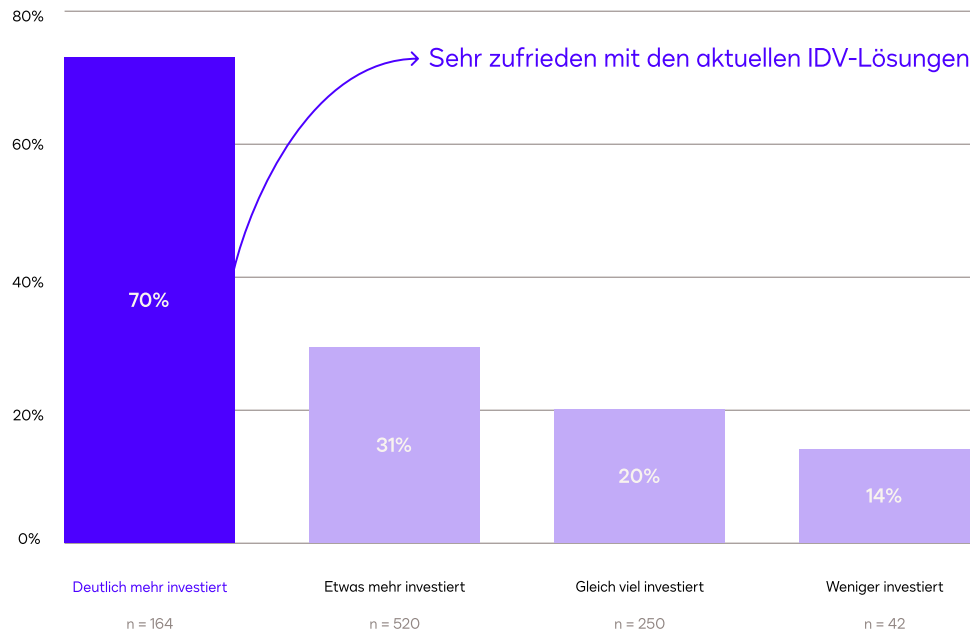
Global betrachtet sind das Bank- und Finanzwesen und die IT die Branchen, die am wahrscheinlichsten biometrische Prüfungen verwenden

Welche der folgenden Arten der Identitätsüberprüfung/Nutzerauthentifizierung verwendet Ihr Unternehmen derzeit?

Unternehmen, die mehr in IDV investieren, berichten über eine höhere Zufriedenheit mit IDV-Tools.

Während MFA das gebräuchlichste Tool ist, heben sich Unternehmen mit höheren Investitionen durch zusätzliche Maßnahmen hervor. Zum Beispiel sind Großinvestoren eher geneigt, ausgefeilte Werkzeuge wie biometrische Überprüfungen und visuelle ID-Funktionen am Anmeldepunkt einzusetzen. Dieser zusätzliche Aufwand steht in Verbindung mit einer höheren Kundenzufriedenheit hinsichtlich IDV-Lösungen.

Größere Investitionen in IDV im Vergleich zu Wettbewerbern sind mit höherer Zufriedenheit verbunden



Wie zufrieden ist Ihr Unternehmen mit der aktuell verwendeten Identitätsüberprüfung/ Nutzerauthentifizierung?

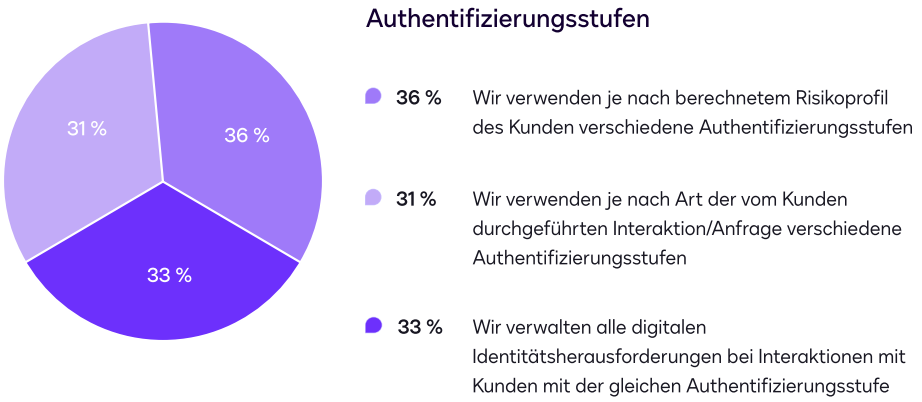
84 %

der Unternehmen in Deutschland sind bereit, Kunden einer intensiven Authentifizierung zu unterziehen, selbst wenn dies zu zusätzlicher Reibung führt.

Unternehmen nutzen verschiedene Methoden, um das passende Authentifizierungsniveau für jeden Kunden festzulegen.

Mehr als zwei von drei Unternehmen verwenden derzeit Authentifizierungsstufen in ihren Sicherheitsprozessen. Das heißt, ein Unternehmen kann zusätzliche Authentifizierungsmethoden für Kunden einführen, die aufgrund von Faktoren wie ihrer IP-Adresse, der Entfernung zum Absender oder ihrem Land als Hochrisikokunden eingestuft werden. Sie können auch zusätzliche Maßnahmen für bestimmte Arten von Kundeninteraktionen ergreifen, wie zum Beispiel bei der Eröffnung eines neuen Kontos oder beim Zugriff auf Finanzmittel.

Die Mehrheit der Unternehmen passt die Authentifizierungsstufen für jede Transaktion basierend auf dem Risikoprofil des Kunden oder der Art der Kundenanfrage an



Welche der folgenden Aussagen beschreibt am besten, wie Ihre Organisation Betrugsprävention handhabt?

Unternehmen ziehen eine Reihe von Kriterien heran, um die geeignete Authentifizierungsstufe für jede Kundeninteraktion zu bestimmen, und 58 % der Unternehmen in Deutschland sagen, dass die Wahl der geeigneten Stufe schwierig ist. Unternehmen beziehen sich am häufigsten auf interne Richtlinien und Kundenrisikoprofile, betrachten jedoch **den Transaktionswert und die Kosten-Nutzen-Analyse als die wichtigsten Kriterien** zur Risikobewertung.

Regionale Erkenntnisse

In Deutschland und Frankreich ist der prognostizierte Wert einer Transaktion das wichtigste Kriterium zur Bestimmung der Authentifizierungsstufen (25 bzw. 20 %)c, während dies in Großbritannien Kosten-Nutzen-Analysen sind (20 %).

Branchenerkenntnisse

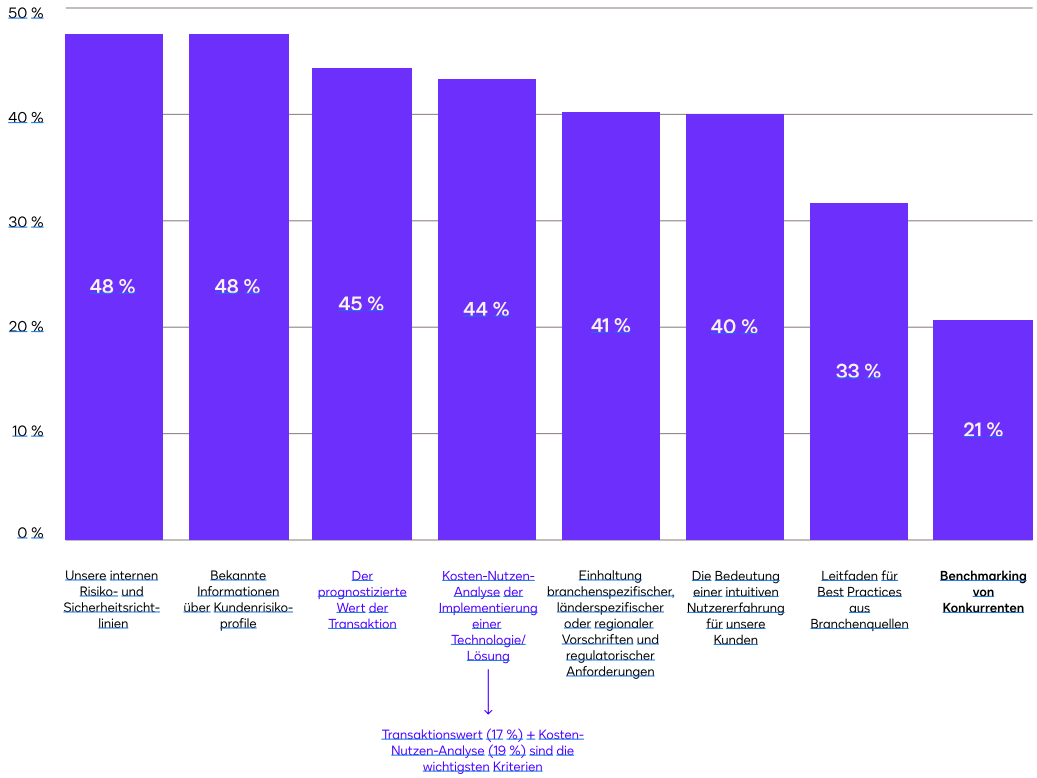
Global betrachtet sind regulatorische Anforderungen die verbreitetste Methode zur Bestimmung der Authentifizierungsstufen in der Gesundheitsbranche (29 %). Sie werden auch häufiger in der Immobilienbranche (25 %) und im Bank- und Finanzwesen (20 %) eingesetzt als in sonstigen Branchen.

Interne Richtlinien und der prognostizierte Wert der Transaktion sind in Deutschland die häufigsten Methoden zur Bestimmung der Authentifizierungsstufe

Der Wert der Transaktion und die Kosten-Nutzen-Analyse werden als am wichtigsten angesehen.

Wie entscheiden Sie sich für die richtige Stufe?

Die am häufigsten verwendete Methoden zur Bestimmung der Authentifizierungsstufe

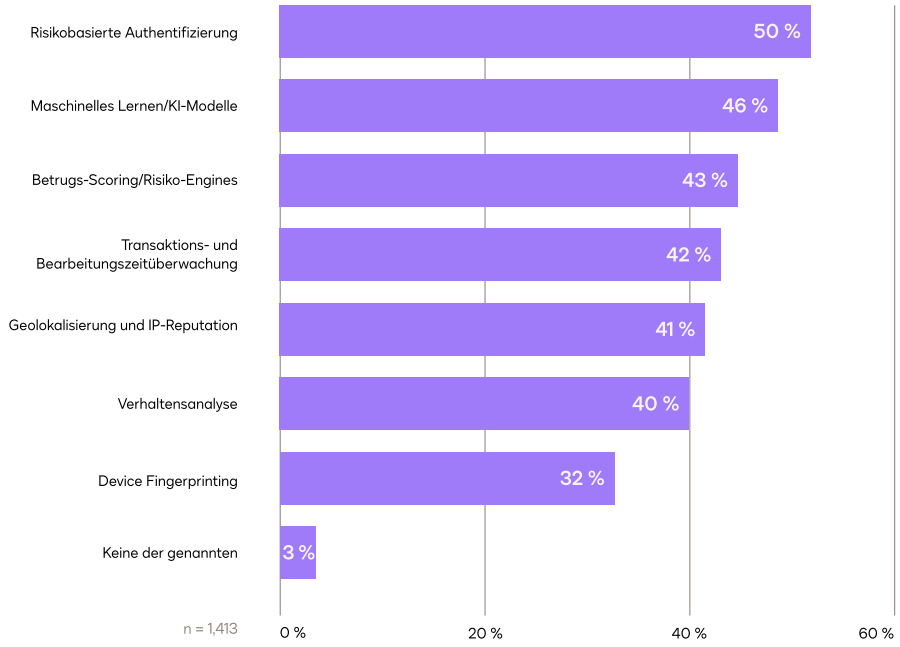


Worauf basiert die Entscheidung, welche Authentifizierungsstufe von Nutzern bei einer bestimmten Interaktion verlangt werden soll?

Zusätzlich zu einer Vielzahl von Methoden zur Bewertung des Kundenrisikos verwenden Unternehmen eine Reihe von Tools. Am verbreitetsten sind in Deutschland maschinelles Lernen/KI-Modelle, in Europa insgesamt hingegen sind es risikobasierte Authentifizierungstools, die den erforderlichen Grad der Identitätsüberprüfung für jede Interaktion automatisch basierend auf dem eingeschätzten Risiko eines Kunden anpassen. Ein Hochrisikokunde kann beispielsweise eine biometrische Überprüfung auslösen, während ein Niedrigrisikokunde möglicherweise nur MFA benötigt.

Maschinelles Lernen/KI-Modelle sind in Deutschland die verbreitetsten Tools zur Bewertung von Kundenrisiken

Werkzeuge zur Bewertung des Authentifizierungsrisikos



Welche der folgenden Optionen verwendet Ihr Unternehmen, um das Risiko im Zusammenhang mit einer bestimmten Interaktion zu bewerten?

73 %

der deutschen Unternehmen planen, künftig mehr in IDV-Lösungen zu investieren.

Unternehmen planen, kontinuierlich in IDV zu investieren

Während sich die Landschaft des Identitätsbetrugs weiterentwickelt und Unternehmen – unabhängig von Größe, Region oder Branche – weiterhin Strategien und Werkzeuge zur Risikobewertung und Betrugsprävention im Auge behalten, bleiben sie einer Überzeugung treu: Technologie ist der Schlüssel zur Bewältigung dieses wachsenden Problems.

Entscheidungsträger interessieren sich insbesondere dafür, welche Rolle die Biometrie und generative KI bei der Betrugsbekämpfung spielen werden. Im Vergleich zu den aktuellen Methoden zur Authentifizierung und Verifizierung von Nutzern:

80 %

der befragten Unternehmen in Deutschland glauben, dass die biometrische Authentifizierung das Risiko von Kundenbetrug wirksamer verringern wird.

82 %

der Befragten sind der Meinung, dass generative KI das Risiko von Kundenbetrug effektiver senken wird.

73 %

der Befragten sind davon überzeugt, dass eine risikobasierte Bewertung das Betrugsrisiko ihrer Kunden wirksamer senken kann.

Unter diesen drei Lösungen wird generative KI als die attraktivste für Kunden angesehen, aber viele Befragte befürchten dennoch eine ablehnende Kundeneinstellung. Während 47 % der deutschen Unternehmen der Meinung sind, dass ihre Kunden frustriert oder verärgert sein werden, wenn generative KI als Teil des IDV-Prozesses eingeführt wird, glauben 52 %, dass Betrug deutlich zunehmen wird, wenn sie dies nicht tun.

Fazit

Unternehmen auf der ganzen Welt sehen sich mit einer neuen Risikolandschaft konfrontiert. Der Aufstieg der generativen KI und die weit verbreitete Einführung digitaler Transaktionen, kombiniert mit dem mangelnden Bewusstsein der Kunden für bewährte Sicherheitspraktiken, haben dem Identitätsbetrug Tür und Tor geöffnet. Angesichts der zunehmenden Betrugsgefahr investieren weltweit führende Unternehmen zu ihrem Schutz in hochmoderne Tools wie Identitätsverifizierung.

Unsere Umfrage führte vor allem zu einer Erkenntnis: Technologie ist der Schlüssel, um Identitätsbetrug während der gesamten Customer Journey aufzudecken und gleichzeitig unnötige Ausgaben zu reduzieren.

Mit IDV können Unternehmen starke Abwehrmechanismen aufbauen, um ihren Ruf und ihre finanzielle Stabilität zu schützen. Selbst in finanziell angespannten Geschäftsumgebungen bringt eine Investition in IDV langfristige Vorteile in Form von Risikominderung und hohem ROI. Kunden wiederum haben die Gewissheit, dass ihre persönlichen Daten sicher sind, während sie gleichzeitig ein nahtloses digitales Erlebnis genießen.

Die Kosten durch Identitätsbetrug werden mit dem Fortschreiten der KI weiter steigen. Für Unternehmen, die ihre Kunden schützen, ihren Ruf verteidigen und junge Generationen ansprechen möchten, die stärker an den Einsatz von Tools zur digitalen Identitätsüberprüfung gewöhnt sind, war es noch nie so wichtig, proaktiv zu handeln und in Technologien zur Betrugsbekämpfung zu investieren.

Wichtige Empfehlungen

Überprüfen Sie Ihre Betrugsabwehrmaßnahmen.

Es gibt einen Grund, warum weltweit 74 % der Unternehmen mindestens einmal im Jahr neue Lösungen unter die Lupe nehmen: Betrüger lernen ständig dazu und wenden neue Techniken an. Unternehmen müssen ihre Abwehrmaßnahmen entsprechend aktualisieren. Der einfachste Weg ist dabei die kontinuierliche Suche nach und Zusammenarbeit mit Anbietern, die ihre eigenen Werkzeuge zur Abwehr der neuesten Taktiken und Herausforderungen regelmäßig weiterentwickeln.

Investieren Sie in KI-gestützte Technologie.

Laut der Mehrheit der befragten Entscheidungsträger ist die beste Möglichkeit, das finanzielle Risiko durch Identitätsbetrug zu mindern, eine umfangreiche Investition in Technologie. Anstatt wertvolle Ressourcen für reaktive Maßnahmen wie Versicherungen oder die Einstellung zusätzlicher Mitarbeiter aufzuwenden, bietet die Investition in KI-gestützte IDV-Lösungen Unternehmen den größten Vorteil im Kampf gegen Identitätsbetrug, insbesondere gegen hochentwickelte Bedrohungen wie generative KI.

Identifizieren Sie die anfälligsten Phasen in Ihrem Kundenlebenszyklus.

Laut unserer Umfrage sind Kontoerstellung, Anmeldung und Zahlungsautorisierung die Schritte der Customer Journey, die weltweit am stärksten von Identitätsbetrug betroffen sind. Sie können lohnende Bereiche sein, auf die Sie sich zunächst konzentrieren sollten. Wir empfehlen jedoch, mit einem qualifizierten Team zusammenzuarbeiten, um die Customer Journey abzustecken und herauszufinden, wo Ihr Unternehmen dem größten Risiko ausgesetzt ist.

Überwinden Sie den scheinbaren Gegensatz von Betrugsschutz und Benutzererfahrung.

Die erfahrensten Teilnehmer unserer Umfrage stellten fest, dass bessere Betrugsmaßnahmen keine Kompromisse bei der Benutzererfahrung bedeuten müssen. Im Gegenteil: IDV kann das Kundenerlebnis ergänzen und den Ruf der Marke verbessern. Um das beste IDV-Erlebnis zu bieten und eine reibungslose Implementierung zu gewährleisten, fördern Sie die Zusammenarbeit zwischen Ihren Risiko-, Produkt- und Wachstumsteams und priorisieren Sie benutzerfreundliche Produkte mit Automatisierung.

Berechnen Sie den ROI Ihrer Investitionen in die Betrugsbekämpfung.

Unternehmen, die deutlich mehr als ihre Mitbewerber in IDV investierten, erzielten tendenziell höhere Einsparungen als jene, die gleich viel investierten. Um sich eine ähnliche Rendite zu sichern, sollten Sie bei der Recherche nach neuer Technologie einige Faktoren berücksichtigen, darunter die erwartete Reduzierung der Betrugskosten, Einsparungen beim Personal durch Automatisierung, geringere Kosten für die Kundenakquise und Umsatzsteigerungen durch neue Kunden.

Erfüllen Sie die Erwartungen junger Verbraucher.

Entscheidungsträger der Millennials und der Gen Z in Unternehmen erkennen mit größerer Wahrscheinlichkeit den Wert von IDV-Tools zur Verbesserung der Markenwahrnehmung und -sicherheit. Bei ihren Kunden gibt es eine ähnliche Parallele: Verbraucher der Millennials und Gen Z bevorzugen innovative Technologien wie die biometrische Authentifizierung gegenüber anderen Methoden. Unternehmen können sicher sein, dass die Einführung fortschrittlicher Technologien ihnen den Respekt junger Kunden und Mitarbeiter einbringt und ihr Unternehmen auf Erfolgskurs bringt – jetzt und in Zukunft.

Erfahren Sie mehr über **Docusign Identify** und **Entrust**.

Anlage: Methodik

Der Bericht „Die Zukunft der globalen Identitätsüberprüfung“ basiert auf Daten, die im Rahmen einer quantitativen, globalen Online-Umfrage vom 6. November 2024 bis zum 4. Dezember 2024 erhoben wurden. Während der Datenerhebung hat unser Forschungsteam[2] mit Geschäfts- und IT-Entscheidungsträgern aus verschiedenen Branchen und Regionen zusammengearbeitet. Die in diesem Bericht befragten Entscheidungsträger arbeiten in Unternehmen mit 150 bis über 10.000 Mitarbeitern und stehen vor der Herausforderung, die Identität ihrer Kunden zu verifizieren.

Gesamt N=1.413

Zielgruppe	
Aktuelle IDV-Nutzerinnen und -Nutzer	N=976
Nutzerauthentifizierung / Digitale Nutzerinnen und Nutzer, aber keine IDV	N=309
Manuelle Authentifizierung / Keine IDV-Nutzerinnen und -Nutzer	N=128

Markt*	
Vereinigte Staaten und Kanada NAM	N=304
Vereinigtes Königreich EMEA	N=227
Deutschland EMEA	N=233
Frankreich EMEA	N=226
Mexiko LATAM	N=104
Brasilien LATAM	N=104
Australien APAC	N=102
Japan APAC	N=113

*Jeder Markt wurde in seiner Primärsprache befragt

Unternehmensgröße	
150–499	N=254
500–999	N=266
1.000–2.499	N=274
2.500–4.999	N=204
5.000–9.999	N=213
10.000+	N=202

Befragte Branchen

- Bankwesen
- Professionelle Dienstleistungen
- Bildung
- Finanzdienstleistungen
- Gesundheitswesen
- Versicherung
- IT-Dienstleistungen
- Biowissenschaften
- Pharmazeutika
- Einzelhandel und E-Commerce
- Bau- und Ingenieurwesen
- Fertigung
- Immobilienbranche
- Telekommunikation
- Energie und Versorgung

Befragte Rollen

- IT-Betrieb / IT-Abteilung
- IT-Sicherheit
- Einkauf und Lieferkettenmanagement
- Betrieb
- Kundenerlebnis
- Produktmanagement
- Risikomanagement / Compliance
- Betrugsanalyse
- Personalwesen
- Kundendienst
- Recht
- Vertrieb

2 Docusign und Onfido beauftragten das Marktforschungsunternehmen TL;DR Insights mit der Durchführung der Umfrage.

docusign | ENTRUST
SECURING A WORLD IN MOTION

Informationen zu Docusign

Docusign erweckt Verträge zum Leben. Mit mehr als einer Million Kunden und einer Milliarde Transaktionen in 180 Ländern ist die Lösung die weltweite Nummer 1 beim Versenden und Signieren von Dokumenten. Mit Intelligent Agreement Management erfasst Docusign den vollen Wert geschäftskritischer Daten in Dokumenten, um sie optimal zu nutzen. Bisher waren solche Daten von den geschäftskritischen Systemen abgekoppelt, was Unternehmen Zeit, Geld und Chancen kostete. Mit Docusign IAM bietet das führende Unternehmen für elektronische Signaturen und Contract Lifecycle Management (CLM) Lösungen, mit denen Unternehmen Verträge erstellen, abschließen und sie verwalten können.

Entrust ist ein innovativer Marktführer für identitätsorientierte Sicherheitslösungen und bietet eine integrierte Plattform mit skalierbaren, KI-gestützten Sicherheitsangeboten. Wir ermöglichen es Unternehmen, ihre Abläufe zu sichern, sich kompromisslos weiterzuentwickeln und ihre Interaktionen in einer vernetzten Welt zu schützen - damit sie ihr Geschäft mit Vertrauen transformieren können. Entrust unterstützt Kunden in über 150 Ländern und arbeitet mit einem globalen Partnernetzwerk zusammen. Die vertrauenswürdigsten Organisationen der Welt vertrauen uns.

Docusign Germany GmbH
Design Offices München
Highlight Towers
Mies-van-der-Rohe-Straße 6
80807 München, Deutschland
docusign.de

Weitere Informationen unte
emea@docusign.com
+49 800 724 17 48