

2026

Global State of Authentication Survey

Wahrnehmung vs. Realität:
Lücken in der
Authentifizierungssicherheit

yubico



okta

Inhalt

Executive Summary	1
Die Adoptionslücke	3
Hohe Vertrautheit mit moderner Authentifizierung	4
Gefangen im Onboarding-Standard	5
Der Überlauf von Zuhause zur Arbeit	6
Optimismus-Bias und die nicht-menschliche Bedrohung	7
Was es kostet: Die Welle des KI-Phishings	8
Das Ende des „offensichtlichen“ Phishings	9
Deepfakes und hohe Erfolgsquoten	10
Erkennen Sie den Bot? (Spoiler: Die Expertinnen und Experten konnten es nicht)	11
Die agentische Zukunft: Nicht-menschliche Identitäten absichern	12
Die Pflicht zur Verifizierung	13
Delegation überholt Sicherheitskontrollen	14
Die Notwendigkeit von Human-in-the-Loop	15
Regionale Analyse	16
Eine neue Sicherheitsarchitektur schaffen	18
Fazit	20
Unternehmensprofile und Methodik	22

Executive Summary

Seit Jahren beruhen Sicherheitsstrategien in Unternehmen auf einer grundlegenden Annahme: Wenn wir Menschen schulen, folgt die Sicherheit von selbst. Cybersecurity-Verantwortliche wissen genau, was nötig ist, um Organisationen und Einzelpersonen zu schützen: die Einführung von Multi-Faktor-Authentifizierung (MFA) und die Vorbereitung auf KI-gestützte Bedrohungen, die bestehende Sicherheitslücken weiter vergrößern könnten.

Dennoch wird Sicherheitswissen allzu oft nicht in die Praxis umgesetzt, und Organisationen bleiben angreifbar. Zwischen Wissen und Handeln klafft eine hartnäckige Lücke.

Die Ergebnisse dieses Reports deuten darauf hin, dass diese Lücke nicht auf mangelnde Bildung zurückgeht, sondern struktureller Natur ist: Sowohl im Beruf als auch privat ziehen Reibungsverluste beim Login und Authentifizierungsmüdigkeit selbst die versiertesten Fachleute immer wieder auf den Weg des geringsten Widerstands. Verstärkt wird dies möglicherweise durch die Sorge, aus privaten Konten ausgesperrt zu werden - Einzelne greifen dann womöglich wieder auf einfache Passwörter und vertraute SMS-basierte MFA zurück. Um unsichere Standards wie Benutzernamen und Passwörter zu überwinden, muss man anerkennen, dass auch hochqualifizierte Expertinnen und Experten menschlichen Verhaltensverzerrungen und operativen blinden Flecken unterliegen. Die Chance liegt nicht darin, den Menschen zu verändern, sondern die zugrunde liegende Infrastruktur: Organisationen müssen veraltete Standards abschaffen und sie in allen Systemen durch reibungslose, phishing-resistente Authentifizierung ersetzen.

In den vergangenen Jahren haben wir Berufstätige weltweit befragt, um herauszufinden, inwieweit sie kluge Cybersecurity-Praktiken in ihren Alltag integrieren. In diesem Jahr hat Yubico einen neuen Ansatz gewählt und gemeinsam mit Okta fast 2.000 Cybersecurity- und IT-Fachleute in neun Ländern befragt. Diese Menschen leben hauptberuflich in der Welt der IT-Sicherheit. Sie entwerfen Richtlinien, verwalten Zugriffe und wissen besser als jeder andere, wie leicht herkömmliche Passwörter einem Angriff zum Opfer fallen.

Nahezu

2,000

Technologie- Und
Sicherheitsfachleute

9

Länder

Mehr als Passwörter und Awareness

Unsere Ergebnisse zeigen für Organisationen eine große Chance, ihre Cybersecurity-Praktiken durch eine neue Sicherheitsarchitektur zu modernisieren. Während Fachwissen und Bewusstsein für sichere Authentifizierungsmethoden auf einem Allzeithoch sind, verlassen sich selbst Sicherheitsprofis nach wie vor auf veraltete, passwortbasierte Abläufe, die beim Onboarding eingeführt wurden. Und solange Unternehmen beim Onboarding Passwörter ausgeben, werden Mitarbeitende sie auch weiterhin nutzen.

Beim Thema Phishing setzen zukunftsorientierte Sicherheitsteams nicht darauf, dass Mitarbeitende subtile Auffälligkeiten einer gefälschten Webseite per Sichtprüfung erkennen. Sie wissen: Phishing-resistente Authentifizierung ist der ultimative Schutz, denn sie nimmt den Menschen vollständig aus der Sicherheitsentscheidung heraus. Moderne Authentifizierungsmethoden sichern stattdessen genau im Moment des Zugriffs ab – durch einen kryptografischen Austausch signierter Nonces und eine Domain-Verifizierung. So schlägt die Authentifizierung automatisch fehl und der Angriff wird vollständig gestoppt, selbst wenn ein Mitarbeitender auf einen Phishing-Köder hereinfällt.

Das Fazit: Nicht das Sicherheitsbewusstsein ist der Engpass auf dem Weg zum sicheren Unternehmen. Der Engpass sind operative Reibungsverluste und veraltete Standardpraktiken, die Identität nicht vor, während und nach der Authentifizierung berücksichtigen. Um diese Lücke zu schließen, müssen wir über Schulungen hinausgehen und hardwaregestützte, phishing-resistente Authentifizierung für jede Identität verbindlich durchsetzen – für menschliche wie maschinelle.



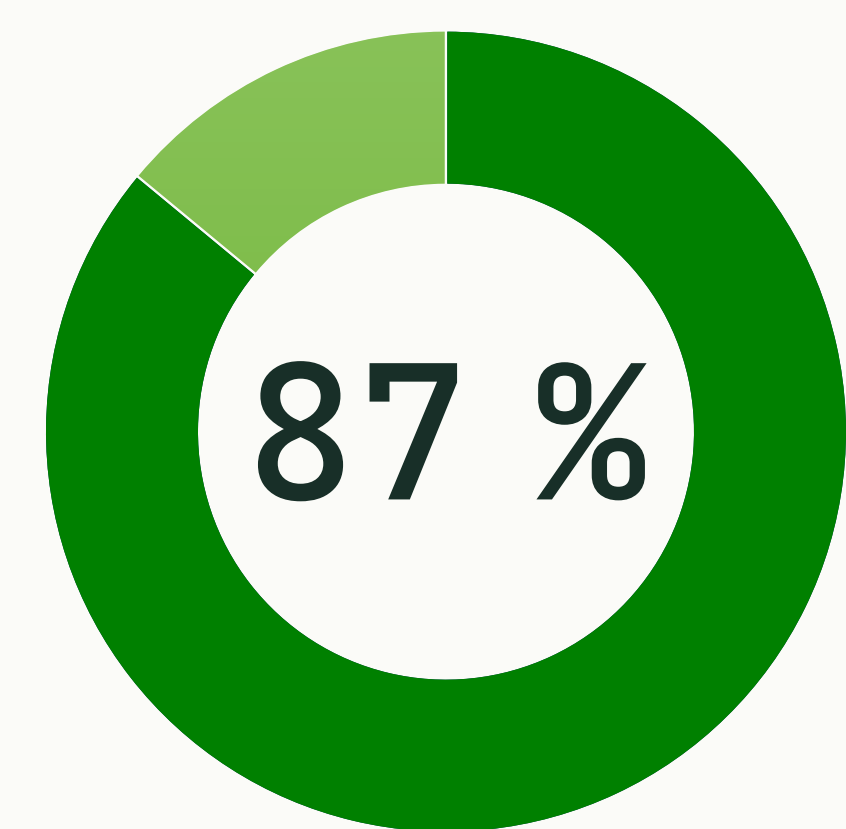
Die Adoptionslücke



Hohe Vertrautheit mit moderner Authentifizierung

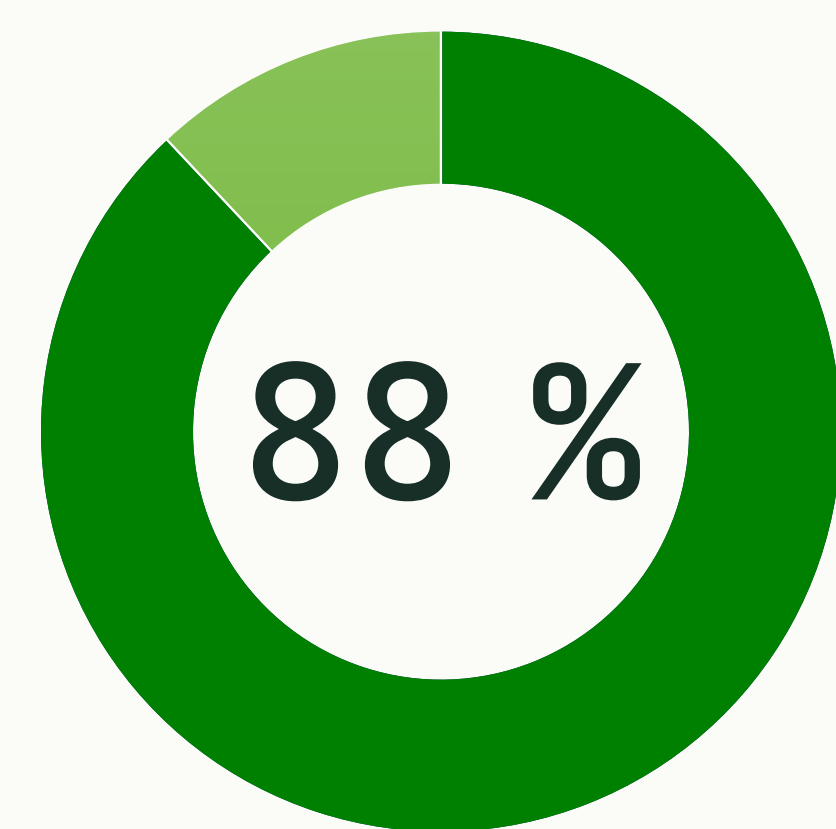
Sicherheitsteams in Unternehmen verfügen über tiefes Fachwissen. Bei der Bewertung von Zugangskontrollen stufen sie gerätegebundene, hardwaregestützte Passkeys als am sichersten ein (**31%**), vor mobilen Authenticator-Apps (29%) und synchronisierten Passkeys (**27%**).

Ihre Vertrautheit ist unbestreitbar: **87%** sind mit Passkeys vertraut, **82%** haben von ihrem Arbeitgeber eine Sicherheitsschulung erhalten, und nur **3%** haben noch nie einen Passkey verwendet. Auf dem Papier sind diese Fachleute Expertinnen und Experten darin, zu erkennen, welche Tools der Goldstandard zum Schutz von Unternehmen, Mitarbeitenden und Kunden vor Cyberbedrohungen sind.



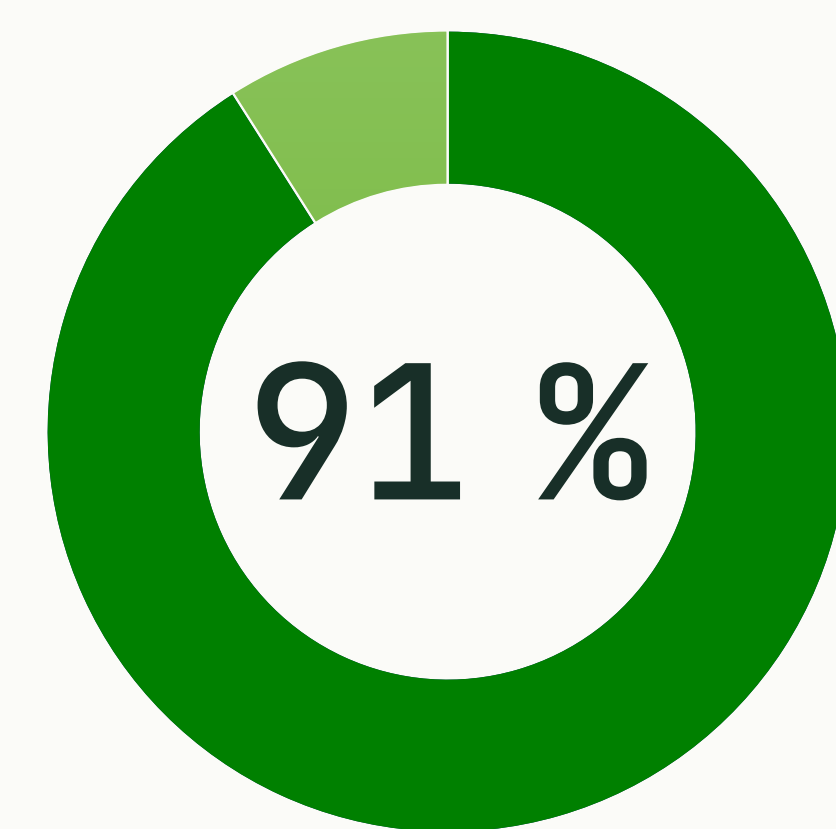
Hohes Bewusstsein:

87% der Sicherheitsexperten sind mit Passkeys vertraut, und **31%** erkennen gerätegebundene, hardwaregestützte Passkeys ausdrücklich als die sicherste verfügbare Anmeldeoption an.



Proaktive Sicherheitskultur:

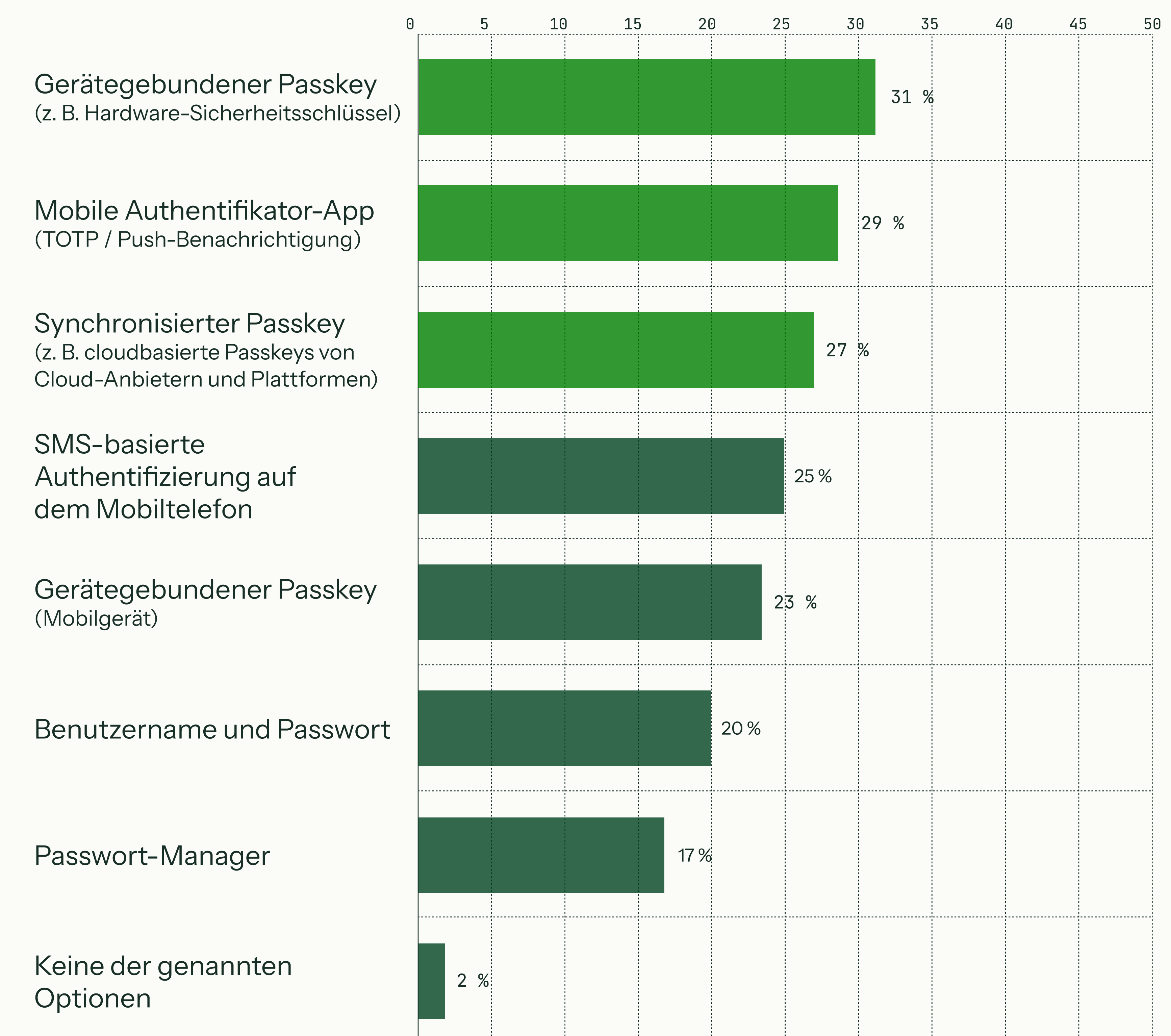
88% der Führungskräfte im Sicherheitsbereich äußern Vertrauen in das aktuelle Sicherheitsniveau ihrer Organisation, was auf erhebliche Investitionen in Tools, Infrastruktur und Schulung der Teams zurückzuführen ist.



Bereit für das KI-Zeitalter:

91% der Führungskräfte erkennen die Bedeutung der Authentifizierung von KI-Agenten und beweisen damit eine zukunftsorientierte Bereitschaft für nicht-menschliche Identitäten.

Welche Authentifizierungsmethoden sind Ihrer Meinung nach am sichersten?



Gefangen im Onboarding-Standard

Trotz ihrer Expertise gleichen ihre täglichen Gewohnheiten denen nicht-technischer Mitarbeitender. Benutzername und Passwort sind nach wie vor die häufigste Methode, mit der sich Sicherheitsprofis bei beruflichen Konten anmelden (**43 %**), während hardwaregestützte Passkeys in der tatsächlichen täglichen Nutzung mit **25 %** zu den Schlusslichtern zählen.

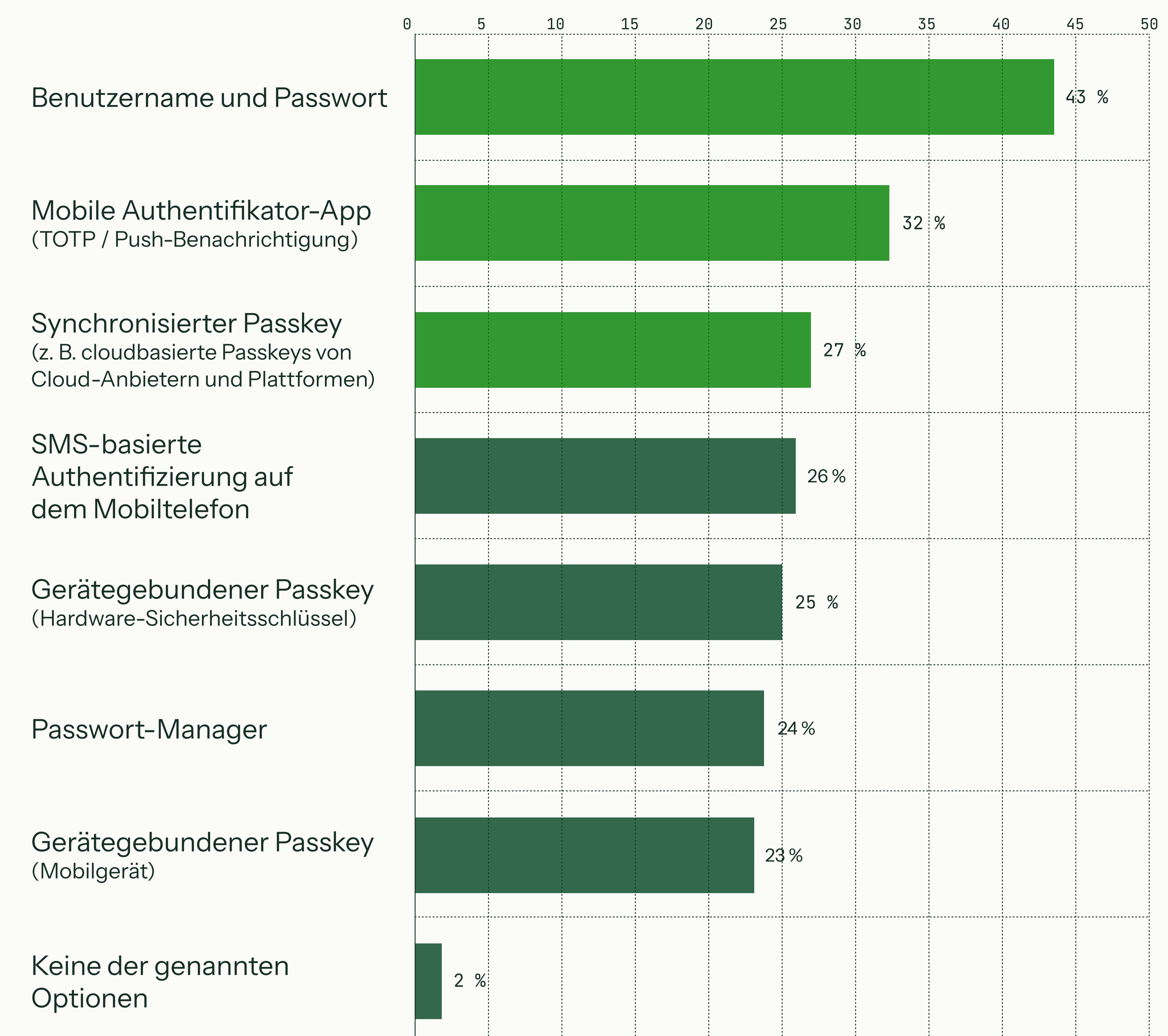
Die Umfrage zeigt, dass langjährige Gewohnheiten am Arbeitsplatz häufig auf Standardvorgaben vom ersten Arbeitstag zurückgehen. Mehr als die Hälfte der Befragten (**52 %**) erhielt zum Stellenantritt klassische Zugangsdaten aus Benutzername und Passwort – und damit veraltete Login-Gewohnheiten, die sich langfristig halten.

Operative Brüche verstärken das Risiko:

- **76 %** der Organisationen nutzen für verschiedene interne Anwendungen uneinheitliche Authentifizierungsmethoden.
- **45 %** setzen über diese fragmentierten Systeme hinweg auf Benutzername und Passwort als primäre Zugangsdaten.
- **23 %** schreiben MFA nicht für alle Unternehmensanwendungen und -dienste vor.

Der Kontext dieser Standards unterscheidet sich zwischen Arbeit und Zuhause. Im beruflichen Umfeld steht hinter Onboarding-Vorgaben und möglichen Aussperrungen ein IT-Helpdesk, der den Zugang wiederherstellt. Zu Hause sind Einzelne bei ihrer Sicherheit auf sich allein gestellt.

Wie authentifizieren/melden Sie sich bei Ihren Arbeitskonten an?

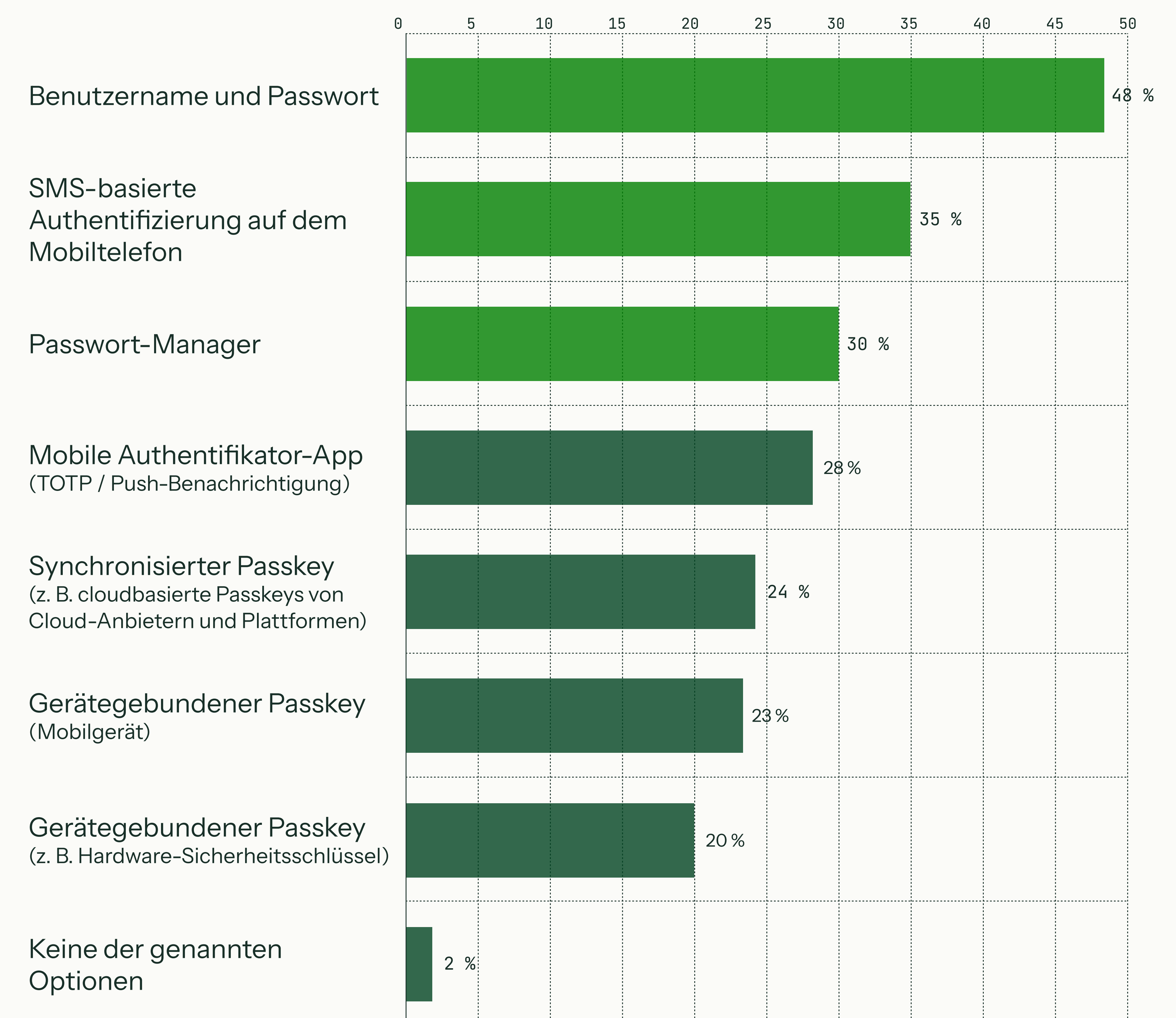


Wie private Gewohnheiten auf den Job abfärben

Da wir Menschen dazu neigen, den einfachsten Weg zu wählen, erfordert es sowohl im Beruf als auch privat gezielte Anstrengung, Authentifizierungsstandards zu überwinden – ebenso wie die Authentifizierungsmüdigkeit, die durch ständige Sicherheitsabfragen entstehen kann. Es überrascht daher vielleicht nicht, dass sich auch im Privatleben **48 %** der Cybersecurity-Profis in erster Linie auf Benutzernamen und Passwörter verlassen, gefolgt von SMS-basierter Verifizierung (**35 %**). Nur **20 %** nutzen hardwaregestützte Passkeys für private Konten.

Da **28 %** ihr privates E-Mail-Konto nicht mit MFA schützen, finden Angreifer einen einfachen Einstiegspunkt. Ein ungeschütztes Postfach, das mit einem Mobilfunkanbieter verknüpft ist (**38 %**), wird zum Ausgangspunkt für SIM-Swap-Angriffe. Liefert es die für einen SIM-Swap nötigen Daten, können Angreifer telefonbasierte Wiederherstellungscodes kapern und direkt auf verknüpfte Unternehmenszugangsdaten übergreifen – und so sowohl die persönliche Identität als auch Unternehmenszugänge gefährden.

Wie authentifizieren/melden Sie sich bei Ihren privaten Konten an?



Optimismus-Bias und die nicht-menschliche Bedrohung

Trotz dieser Schwachstellen bezeichnen **88 %** der Befragten ihr Unternehmen als „sicher“ (**34 %** sogar als „sehr sicher“).

In der Verhaltenspsychologie wird dies als Optimismus-Bias bezeichnet: die Überzeugung, dass Fachwissen eine Person oder Institution vor negativen Folgen schützt. Sicherheitsverantwortliche bewerten ihre eigene Sicherheitslage großzügig und gehen davon aus, dass Wettbewerber stärker gefährdet sind.

Wenn Unternehmen autonome KI-Software-Agenten in ihre täglichen Abläufe integrieren, werden passwortgeschützte Konten bald von nicht-menschlichen Helfern genutzt. Eine Organisation, die keine starke Authentifizierung für ihre menschlichen Mitarbeitenden durchsetzt, kann autonome Agenten nicht sicher steuern.

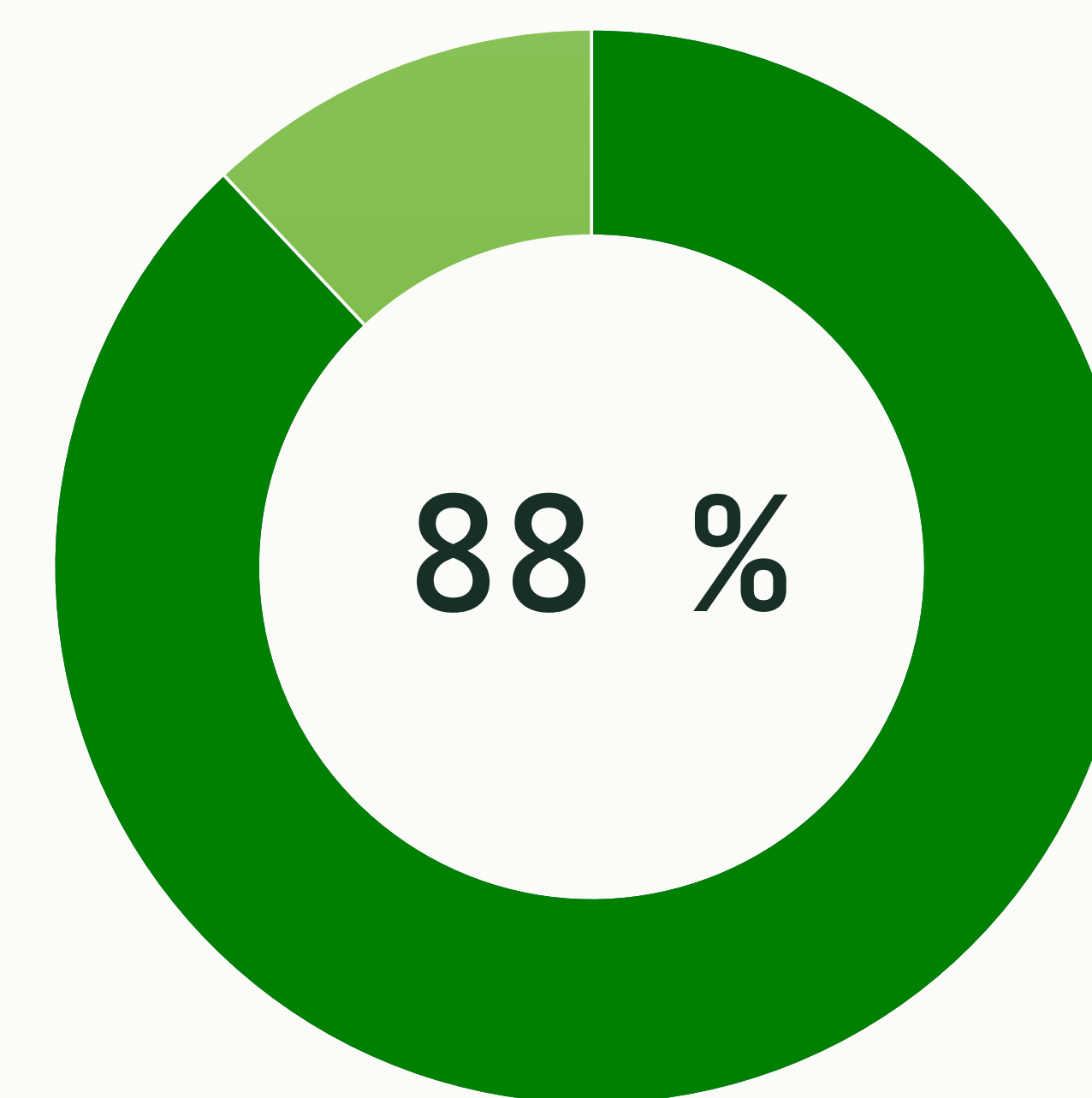
Die cybersicherheit in unternehmen hat eine kritische umsetzungslücke. Sicherheitsverantwortliche wissen, dass hardwaregestützte passkeys - insbesondere hardware-sicherheitsschlüssel - den höchsten schutz bieten, und doch verlässt sich fast die hälfte täglich auf einfache benutzernamen und passwörter. Die herausforderung ist nicht fehlende expertise, sondern die reibungsverluste zu überwinden, die der akzeptanz bei den nutzern im weg stehen.



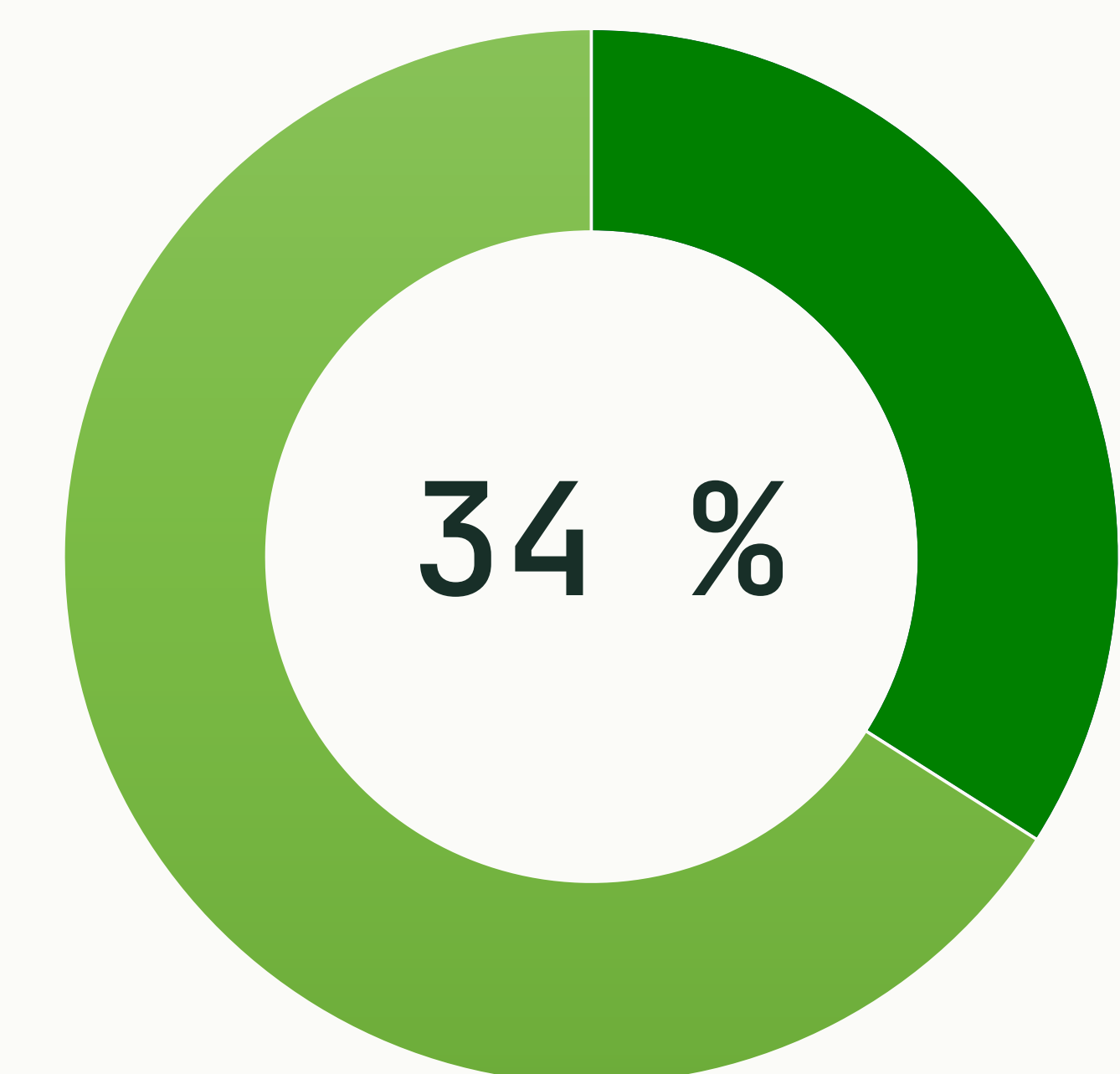
Poupak Enbom,
Chief Market and Growth Officer bei Yubico



Operative Diskrepanzen vergrößern das Risiko



88 % der Befragten beschreiben ihr Unternehmen als „sicher“



34 % geben „sehr sicher“ an

Was es kostet: Die Welle des KI-Phishings



Das Ende des „offensichtlichen“ Phishings

Da generative KI die digitale Kommunikation beschleunigt und individueller macht, haben KI-gestützte Phishing-Versuche branchenweit zwangsläufig zugenommen. **70 %** der Befragten stellten im vergangenen Jahr einen Anstieg von Phishing in ihrer Organisation fest, **55 %** wurden direkt Ziel personalisierter Angriffe. **22 %** haben sogar innerhalb der letzten Woche gezielte Nachrichten erhalten.

Statt sich auf herkömmliche Merkmale einer Phishing-Webseite wie Tippfehler oder holprige Formulierungen zu verlassen, erkennen zukunftsorientierte Sicherheitsteams: Der ultimative Schutz ist phishing-resistente Authentifizierung, nicht die menschliche Sichtprüfung. Mit anderen Worten: Menschen sollten nicht dafür verantwortlich sein, KI-basierte Bedrohungen zu erkennen und zu stoppen. Die innovativsten Methoden sichern stattdessen im Moment der Authentifizierung ab – durch Domain-Verifizierung und kryptografische Sicherheit. So kann die Authentifizierungstechnologie den Login erkennen und blockieren, selbst wenn ein Nutzer auf einen Phishing-Versuch hereinfällt und den Angriff gar nicht bemerkt.



Deepfakes und hohe Erfolgsquoten

Da moderne Angriffe die herkömmlichen kognitiven Filter umgehen, sind die Quoten erfolgreicher Erstangriffe sprunghaft gestiegen. 44 % der Befragten geben an, dass ihre Organisation in den vergangenen zwölf Monaten mindestens einen erfolgreichen KI-gestützten Angriff erlitten hat.

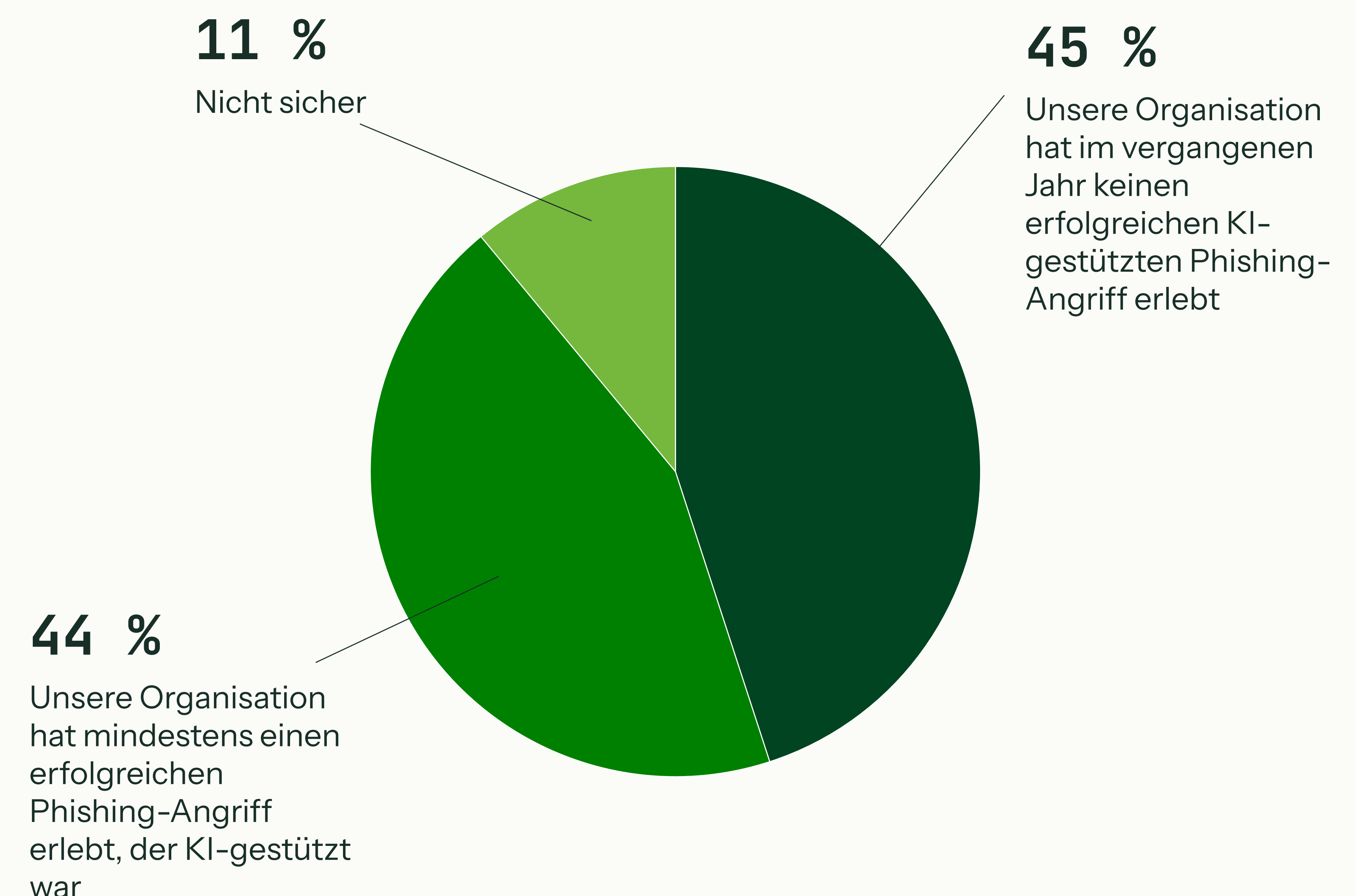
Stimmenklonung und synthetische Medien ermöglichen es Angreifern heute, sich mit minimalem Ausgangsmaterial als vertraute Kolleginnen und Kollegen auszugeben:

- 43 % berichteten von verdächtigen Video-, Sprachnachrichten- oder Telefon-Imitationen, die sich gegen Führungskräfte oder Kunden richteten.
- 29 % waren direkt Ziel von Deepfake-Kommunikation.

Oktas Report „AI Agents at Work 2026“ beschreibt einen zweiten Weg in dieselben Organisationen. Mehr als die Hälfte der Befragten (52 %) gab an, bei der Arbeit nicht genehmigte KI-Tools zu nutzen, fast ein Viertel davon regelmäßig. Unter denjenigen, die nicht genehmigte Tools verwenden, wurden am häufigsten interne Nachrichten und E-Mails (54 %), HR-bezogene Informationen (45 %) sowie vertrauliche Unternehmensdokumente einschließlich Finanzdaten und Verträgen (39 %) geteilt.



Welche der folgenden Aussagen trifft auf den Erfolg KI-gestützter Phishing-Angriffe in Ihrer Organisation im vergangenen Jahr zu?



Erkennen Sie den Bot? (Spoiler: Die Expertinnen und Experten konnten es nicht)

Organisationen haben sich lange auf ihre Mitarbeitenden als „menschliche Firewall“ verlassen, um Auffälligkeiten zu erkennen. Um diese Verteidigungslinie zu testen, haben wir Sicherheitsverantwortlichen zwei Nachrichten vorgelegt – eine von einem Menschen geschrieben, eine von KI generiert – und sie gebeten, die Quelle zu bestimmen.

Die Ergebnisse zeigen, dass **menschliche Erkennung keine tragfähige Sicherheitskontrolle mehr ist:**

- Nur **36 %** der Sicherheitsfachleute erkannten eine von einem Menschen geschriebene Frage korrekt, **54 %** hielten die Nachricht für KI-generiert, und **10 %** waren unsicher.
- **39 %** der Befragten erkannten zudem die KI-generierte Frage nicht.

Von Menschen verfasste E-Mail

Hallo [NAME],

unser Mitarbeiterhandbuch wurde im Hinblick auf Änderungen für 2027 aktualisiert. Es wurden mehrere neue Abschnitte hinzugefügt. Bitte lesen Sie das aktualisierte Dokument vollständig durch und bestätigen Sie den Erhalt bis zum 1. November 2026.

Erforderliche Maßnahme – Fällig bis 1. November 2026

Bitte melden Sie sich im Firmen-Intranet an und rufen Sie unter ‚Aufgaben‘ die entsprechende Aufforderung auf. Das Handbuch sowie alle weiteren Richtlinien finden Sie auf unserer Startseite.

Vielen Dank im Voraus für Ihre Mitwirkung, damit unser Unternehmen weiterhin alle Vorgaben einhält.

Herzliche Grüße
Ihr HR-Team

Von KI verfasste E-Mail

Hallo [NAME],

während wir nach vorne blicken und für die Zukunft planen, haben wir unser Mitarbeiterhandbuch für 2027 auf den neuesten Stand gebracht. Wir haben einige wichtige neue Abschnitte hinzugefügt, um sicherzustellen, dass unsere Richtlinien Sie und unser wachsendes Team weiterhin bestmöglich unterstützen.

Aufsichtsbedingt bitten wir alle, das aktualisierte Dokument kurz durchzusehen und den Erhalt rasch zu bestätigen.

Was wir bis zum 1. November 2026 von Ihnen benötigen:

1. Melden Sie sich im Firmen-Intranet an.
2. Überprüfen Sie Ihre „Aufgaben“-Liste auf der Startseite.
3. Werfen Sie einen Blick in das aktualisierte Handbuch und klicken Sie auf die Bestätigung, dass Sie es erhalten haben.

(Denken Sie daran: Sie finden das Handbuch sowie alle anderen Unternehmensrichtlinien jederzeit direkt auf der Intranet-Startseite angepinnt, falls Sie etwas nachschlagen möchten.)

Vielen Dank, dass Sie sich ein paar Minuten Zeit nehmen, um uns dabei zu helfen, dass alles reibungslos und richtlinienkonform abläuft!

Herzliche Grüße
Ihr HR-Team

Die agentische Zukunft: Nicht- menschliche Identitäten absichern



Die Pflicht zur Verifizierung

Da sich autonome KI-Agenten von passiven Assistenten zu aktiven operativen Werkzeugen entwickeln, hat die Verifizierung maschineller Identitäten oberste Priorität erlangt. 91 % der Befragten halten es für unerlässlich, die Identität und Authentizität von KI-Agenten zu verifizieren, 57 % stufen dies als kritisch ein.

Oktas Report „Businesses at Work 2026“ zeigt: 74 % der Organisationen berichten von einer weitverbreiteten oder moderaten Nutzung nicht-menschlicher Identitäten, 90 % fehlt eine umfassende Strategie zu deren Steuerung, und nur 32 % steuern KI-Agenten mit derselben Sorgfalt wie menschliche Identitäten.



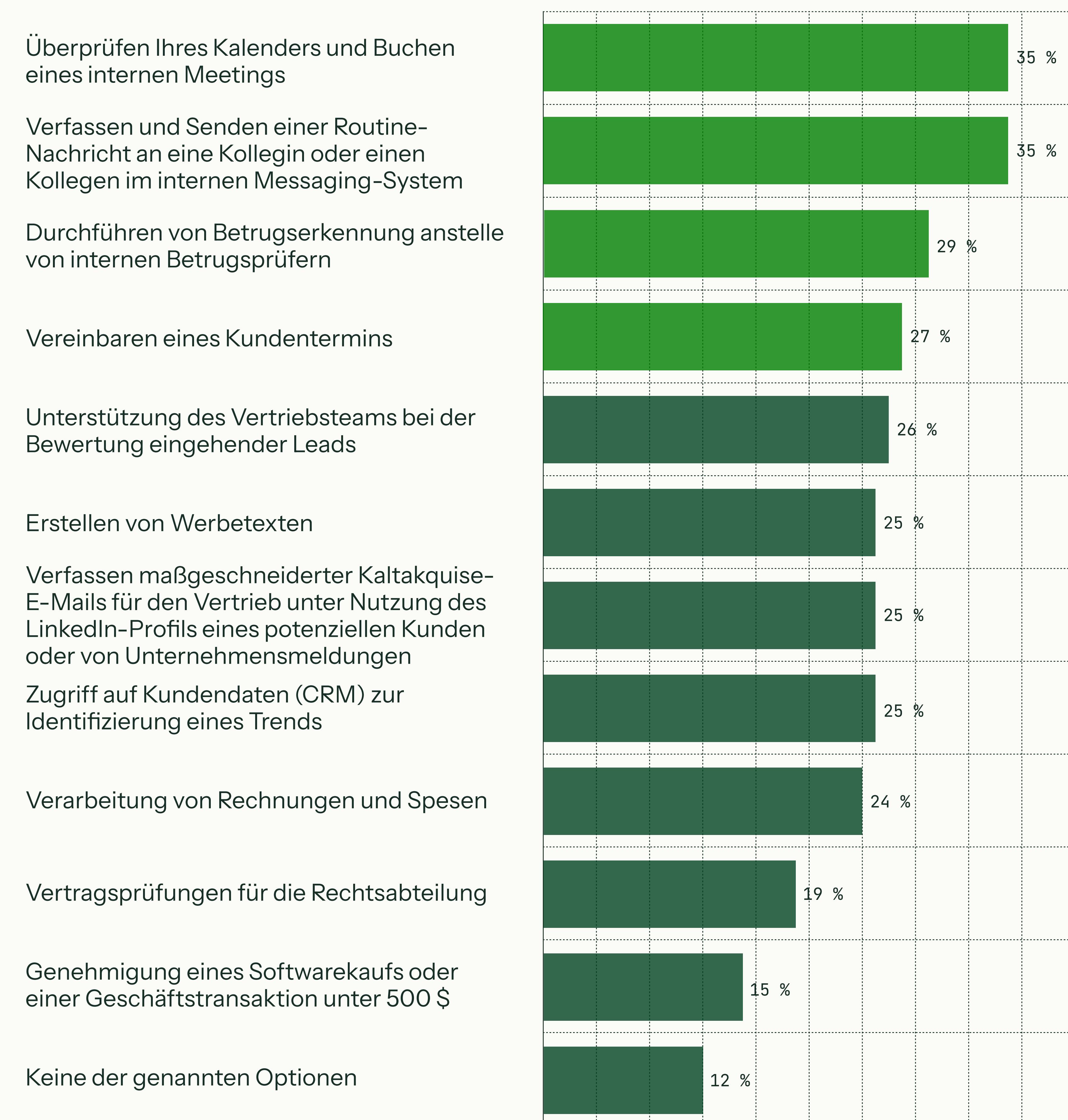
Delegation überholt Sicherheitskontrollen

Die Delegation von Aufgaben an KI-Agenten beschleunigt sich, und Sicherheitsverantwortliche übergeben operative Aufgaben zunehmend bereitwillig an KI.

1. Terminplanung und Kalenderverwaltung (35 %)
2. Entwurf interner Kommunikation (35 %)
3. Automatisierte Betrugserkennung (29 %)
4. Meetings mit Kunden (27 %)

Bei KI-delegierter Kommunikation zeigen sich deutliche Generationsunterschiede: **68 % der Gen-Z-Fachleute** fühlen sich wohl dabei, einem KI-Agenten zu erlauben, in ihrem Namen mit Kunden oder Kollegen zu kommunizieren – gegenüber nur **27 % der Babyboomer**.

Bei welchen Aufgaben (falls vorhanden) wären Sie bereit, diese an einen KI-Agenten auszulagern, damit er sie in Ihrem Namen automatisiert?



Die Notwendigkeit von Human-in-the-Loop

Auch wenn das Vertrauen in KI-Delegation unterschiedlich ausgeprägt ist, steht eines fest: Human-in-the-Loop bleibt entscheidend. **91 % bestehen auf einem „Human-in-the-Loop“-Freigabeschritt**, bevor ein Agent in ihrem Namen Aktionen ausführt.

Während Agent-zu-Agent-Workflows eine autonome Ausführung benötigen, um zu skalieren, kann menschliche Verifizierung als Sicherheitsprüfung für kritische Abläufe dienen – etwa bevor ein Agent Berechtigungen ausweitert oder Finanztransaktionen ausführt.

“Während Sicherheitsverantwortliche und jüngere Generationen operative Aufgaben bereitwillig an KI übergeben – von der Terminplanung (35 %) bis zur Kundeninteraktion (bis zu 68 % bei der Gen Z) –, ziehen überwältigende 91 % bei der Ausführung eine klare Grenze und bestehen darauf, dass ein Mensch die finale Freigabe erteilt.



Poupak Enbom,
Chief Market and Growth Officer bei Yubico



Regionale Analyse

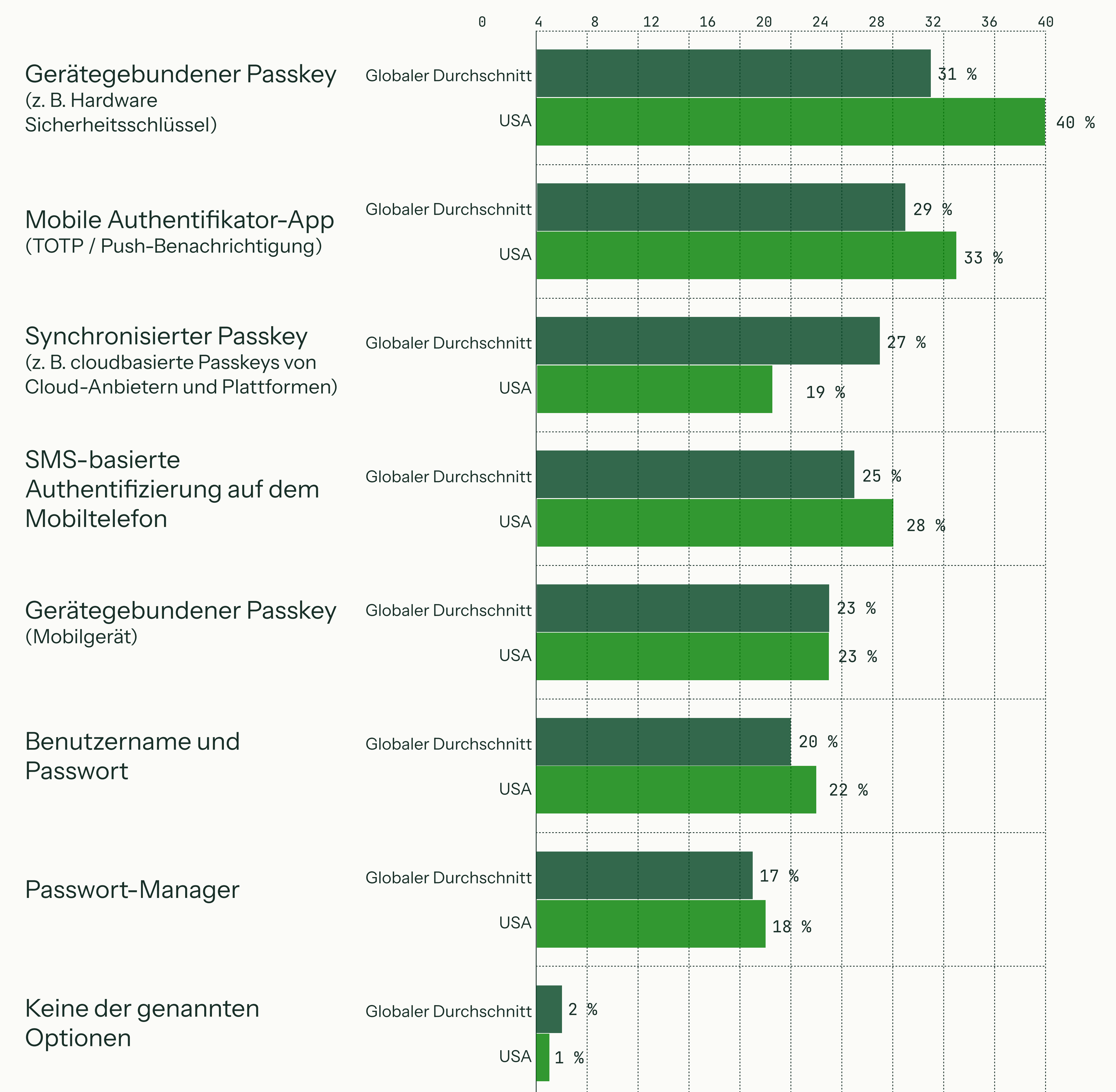


Die Adoptionslücke in den USA

Kein Markt veranschaulicht die Lücke zwischen Bewusstsein und Praxis deutlicher als die Vereinigten Staaten: Sie haben das höchste technische Bewusstsein, das geringste Vertrauen in das System und das langsamste Tempo operativer Veränderung.

- **Hohes Bewusstsein:** **40 %** der US-Sicherheitsverantwortlichen nennen hardwaregestützte Passkeys als sicherste Zugangsmethode (gegenüber **23 %** in Großbritannien), und **48 %** der Passkey-Nutzenden haben persönliche Erfahrung mit hardwaregestützten Schlüsseln (gegenüber 28 % in Singapur).
- **Hohe Abhängigkeit von veralteten Zugangsdaten:** Gleichzeitig führen die USA alle Märkte bei der Passwortabhängigkeit an – **50 %** nutzen Benutzername und Passwort bei der Arbeit, **56 %** zu Hause.
- **Geringeres Vertrauen:** Nur **58 %** der US-Befragten glauben, dass die Unternehmen, die ihre personenbezogenen Daten verarbeiten, genug für deren Schutz tun (gegenüber **82 %** in Indien).

Was sind die sichersten Authentifizierungsmethoden?



Eine neue Sicherheits architektur schaffen



Eliminierung des Zugangsdaten-Risikos: Ein Drei-Phasen-Schutzplan mit Hardware

Ein sichereres Unternehmen aufzubauen, erfordert die Erkenntnis, dass Awareness-Schulungen kein architektonisches Problem lösen können. Trotz hoher Sicherheitskompetenz werden Organisationen durch operative Reibungsverluste, vermeintliche Einführungskosten und veraltete Onboarding-Standards ausgebremst, die hochsichere MFA als optionalen Luxus statt als grundlegende Anforderung behandeln.

Um Risiken durch Zugangsdaten im KI-Zeitalter zu beseitigen, müssen Sicherheitsarchitekturen phishing-resistente, hardwaregestützte Passkeys und andere gerätegebundene kryptografische Authentifikatoren in drei klar abgegrenzten Phasen durchsetzen.

- **Vor der Authentifizierung:** Prüfungen von Gerätezustand und Sicherheitsstatus vorschreiben, um die Konformität des Endgeräts zu verifizieren, bevor eine Zugriffssitzung aufgebaut wird. Neuen Mitarbeitenden im Rahmen des Onboardings phishing-resistente Authentifikatoren aushändigen, damit hochsichere MFA ab dem ersten Login-Versuch gewährleistet ist.
- **Während der Authentifizierung:** Phishing-resistente Authentifizierung in den Sign-on-Richtlinien der Anwendungen durchsetzen, um KI-Phishing-Versuche bei der Anmeldung konsequent und automatisch abzuwehren.
- **Nach der Authentifizierung:** Kontext und Risiko kontinuierlich bewerten, um kompromittierte Sitzungen zu erkennen. Einen Nachweis menschlicher Anwesenheit verlangen – entweder durch eine physische Hardware-Interaktion wie das Berühren eines Schlüssels oder durch biometrische Authentifizierung –, um autonome KI-Workflows per Human-in-the-Loop freizugeben.



Fazit



Vom Bewusstsein zur Durchsetzung

Die Ergebnisse der Studie „2026 Global State of Authentication“ zeigen, dass Sicherheitsbewusstsein allein nicht ausreicht, um Unternehmen zu schützen. Die Chance besteht darin, ein systemisches Muster zu durchbrechen: Innerhalb und außerhalb des Arbeitsplatzes drängen Standardvorgaben und eingebaute Reibungsverluste selbst kluge, hochqualifizierte Fachleute auf den Weg des geringsten Widerstands. Echte Sicherheit darf nicht von menschlicher Wachsamkeit gegenüber immer raffinierteren KI-Bedrohungen abhängen. Sie erfordert eine Neuausrichtung der Unternehmensarchitektur, bei der die kluge Wahl zum automatischen Standard wird.

Sicherheitsverantwortliche wissen bereits, was funktioniert. Es ist an der Zeit, dass Unternehmensrichtlinien und Infrastruktur dieses Wissen widerspiegeln.



Unternehmensprofile Und Methodik

Über Yubico

Yubico (Nasdaq Stockholm: YUBICO) ist ein globaler Cybersecurity-Pionier und Erfinder des YubiKey, des Goldstandards für phishing-resistente, hardwaregestützte Authentifizierung. Seit Yubico 2007 an der Entwicklung globaler Passkey-Standards mitgewirkt hat, verhindert das Unternehmen Kontoübernahmen für Unternehmen, Behörden und Privatpersonen in mehr als 160 Ländern. Zu unserer globalen Präsenz gehören Hauptsitze in Stockholm (Schweden), im Silicon Valley (Kalifornien) und in Singapur. Mehr unter www.yubico.com.

Über Okta

Okta, Inc. ist The World's Identity Company™. Wir sichern KI-, maschinelle und menschliche Identitäten, damit alle jede Technologie sicher nutzen können. Unsere Lösungen für Mitarbeitende und Kunden befähigen Unternehmen und Entwickler, ihre KI-Agenten, Nutzer, Mitarbeitenden und Partner zu schützen und dabei Sicherheit, Effizienz und Innovation voranzutreiben. Warum die führenden Marken der Welt Okta bei Authentifizierung, Autorisierung und mehr vertrauen, erfahren Sie auf okta.com.

Methodik

Talker Research führte eine quantitative Online-Umfrage unter 1.890 Technologie- und Sicherheitsfachleuten in neun Märkten durch: USA, Großbritannien, Australien, Indien, Japan, Singapur, Frankreich, Deutschland und Schweden.

Die Befragten hatten Positionen in den Bereichen Cybersecurity, IT, Produktmanagement, Software-Engineering und Hardware-Engineering in Unternehmen mit mindestens 500 Mitarbeitenden inne. Die Umfrage wurde von Yubico und Okta in Auftrag gegeben und zwischen dem 2. und 16. Juli 2026 durchgeführt.

Ergebnisse können variieren: Fallstudien, Kundenstimmen und Leistungskennzahlen geben die spezifischen operativen Ergebnisse der vorgestellten Organisationen unter ihren jeweiligen Konfigurationen, Netzwerkumgebungen und Implementierungsparametern wieder. ©2026 Okta, Inc. und/oder verbundene Unternehmen

Diese Materialien dienen ausschließlich allgemeinen Informationszwecken und stellen keine Rechts-, Datenschutz-, Sicherheits-, Compliance- oder Unternehmensberatung dar.