Globale Umfrage zum Stand der Authentifizierung 2025

Wahrnehmung Vs. Realität: Lücken In Der Authentifizierungssicherheit

Erkenntnisse von Yubico

yubico

Table of Contents

Einleitung

Cybersicherheitsbedrohungen stellen für Unternehmen jeder Größe eine Gefahr dar, die sich ständig weiterentwickelt. Dennoch reagieren viele Organisationen nur langsam auf neue und aufkommende Risiken. Tatsächlich glauben viele Mitarbeiter und Unternehmen, dass ältere Sicherheitsprotokolle heute noch genauso wirksam sind wie noch vor Monaten oder sogar Jahren. Leider entspricht diese Wahrnehmung nicht der Realität.

Zunehmende Bedrohungen durch Angriffe mit künstlicher Intelligenz (KI) in Verbindung mit veralteten Cybersicherheitsrichtlinien und risikoreichen Gewohnheiten der Mitarbeiter machen unzählige Organisationen anfällig für Sicherheitsverletzungen. Die Umfrage untersuchte die Gewohnheiten in Bezug auf die Cyberrsicherheit sowohl am Arbeitsplatz als auch im Privatleben. Außerdem wurden die Gefahren schwacher Sicherheitspraktiken untersucht und die wachsenden Bedenken hinsichtlich neuer Technologien wie KI und deren Auswirkungen auf die Sicherheit von Organisationen und Einzelpersonen bewertet.

Zusammenfassung

Yubico gab eine weltweite Umfrage in Auftrag, die mit 18.000 berufstätigen Erwachsenen aus Australien, Indien, Japan, Frankreich, Deutschland, Singapur, Schweden, dem Vereinigten Königreich und den Vereinigten Staaten durchgeführt wurde. Sie deckte grundlegende Mängel in der Unternehmenssicherheit auf, die auf eine Diskrepanz zwischen der Wahrnehmung der Mitarbeiter hinsichtlich der Sicherheit ihrer Unternehmen und der realen Anfälligkeit für moderne Cyberbedrohungen zurückzuführen sind.

Fast die Hälfte der Befragten hat noch nie eine Cybersicherheitsschulung erhalten und verwendet nach wie vor veraltete Authentifizierungsmethoden. Diese galten zwar einst als sicher, sind heute jedoch durch ausgeklügelte Angriffe wie moderne Phishing-Attacken leicht zu umgehen. Passwörter, SMS-basierte Verifizierung und sogar grundlegende Multi-Faktor-Authentifizierung (MFA) sind zunehmend anfällig und stellen Schwachstellen dar, die Cyberkriminelle ausnutzen können.

Vielleicht noch aussagekräftiger ist, dass persönliche Sicherheitsgewohnheiten auch die Schutzprotokolle von Unternehmen untergraben: 50 Prozent der Mitarbeiter nutzen private Konten auf Arbeitsgeräten und umgekehrt. Darüber hinaus setzt fast ein Drittel der Befragten außerhalb der Arbeit keinerlei MFA ein, was Hackern die Möglichkeit eröffnet, persönliche Informationen für Angriffe auf Unternehmen zu nutzen.

Das rasante Wachstum und die zunehmende Nutzung von KI durch Kriminelle haben die Entwicklung neuer Bedrohungen dramatisch beschleunigt. Unsere Ergebnisse zeigen, dass sich die Befragten dieser neuen Realität bewusst sind: 76 Prozent der Befragten sind besorgt, dass ihre Konten nun einem viel höheren Risiko von Angriffen ausgesetzt sind – ein deutlicher Anstieg gegenüber den 58 Prozent, die dies in einem ähnlichen Bericht aus dem Jahr 2024 angaben.

18.000+

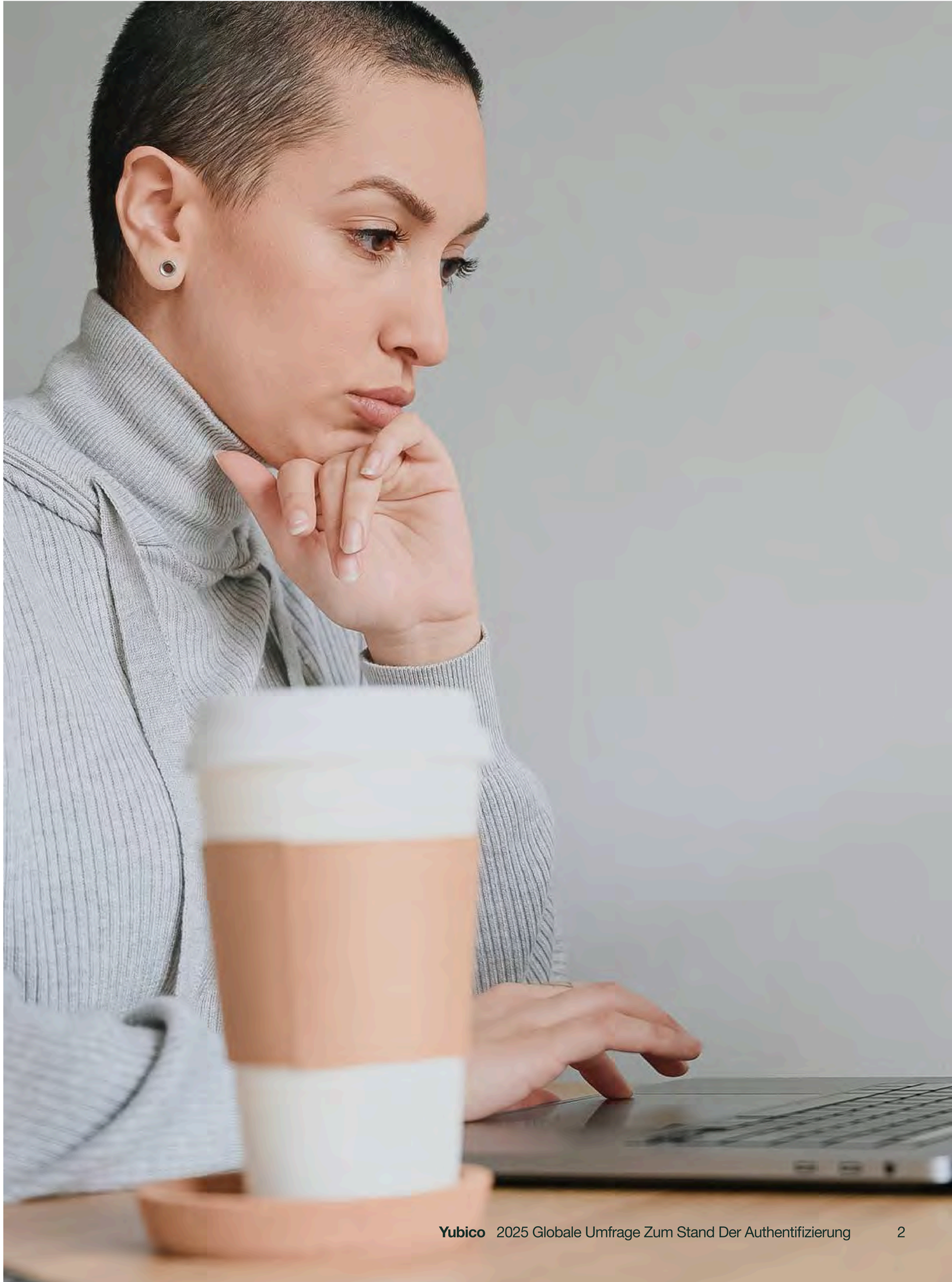
Reaktionen

9

Länder

I.

Die neue Cyber-Landschaft



Ein globaler Weckruf für die Cybersicherheit

Unsere Untersuchung hat ergeben, dass 4 von 10 (40 Prozent) Mitarbeitern noch nie eine Schulung zum Thema Cybersicherheit erhalten haben. Darüber hinaus warten 44 Prozent der Unternehmen länger als 3–5 Monate, bevor sie ihre Richtlinien zur Cybersicherheit aktualisieren.

Diese beiden Statistiken deuten darauf hin, dass fast die Hälfte der Mitarbeiter nie mit den Sicherheitsrichtlinien ihres Unternehmens vertraut gemacht wurde. Darüber hinaus arbeitet etwa die Hälfte derjenigen, die eine Cybersicherheitsschulung erhalten haben, mit veralteten Informationen.

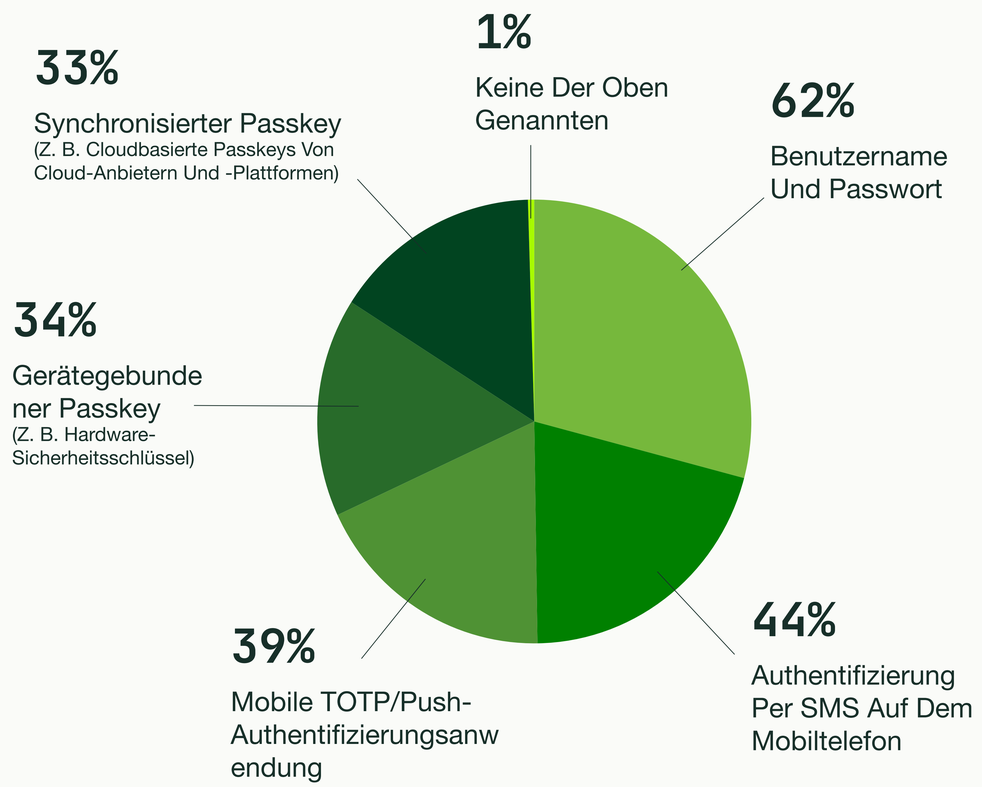
Angesichts der ständigen Entwicklung neuer Angriffstechniken und der Zunahme von KI-basierten Bedrohungen führen inkonsistente Cybersicherheitsschulungen zu einer ständigen Gefährdung von Unternehmen und Mitarbeitern.

Uneinheitliche Authentifizierung

Das Risikoprofil moderner Unternehmenssysteme wird durch die uneinheitliche Verwendung von Authentifizierungsverfahren zusätzlich erschwert. Unternehmen, die ihren Mitarbeitern mehrere Arten der Authentifizierung für Apps und Dienste zur Verfügung stellen, schaffen eine schwächere Abwehr gegen potenzielle Schwachstellen.

Noch aufschlussreicher ist vielleicht, dass 62 Prozent der Unternehmen nach wie vor hauptsächlich auf Benutzernamen und Passwörter als Anmeldedaten setzen - trotz zahlreicher Belege dafür, dass diese veraltete Methode zunehmend anfällig ist. Weitere 44 Prozent der Unternehmen verwenden SMS-basierte Einmalpasswörter (OTPs), die anfällig für SIM-Swapping-Angriffe und Social Engineering sind, das dank KI mittlerweile immer ausgefeilter wird.

Welche Formen der Authentifizierung verwendet Ihr Unternehmen für die verschiedenen Anwendungen/Programme, die im Unternehmen eingesetzt werden?



Wahrnehmung vs. Realität

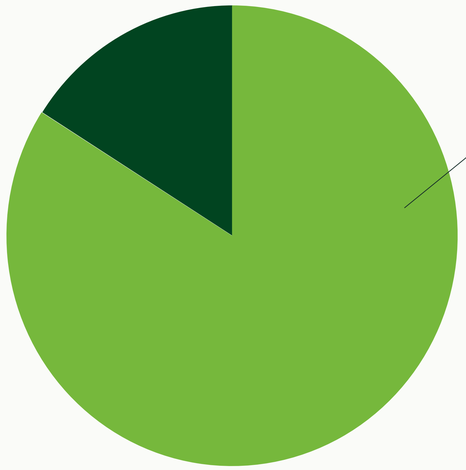
Unsere Ergebnisse zeigen, dass Mitarbeiter die Risiken für ihre sicheren Anmeldedaten durchweg unterschätzen und dieSysteme, die diese schützen sollen, überschätzen.

Als sicherste Methode gaben in unserer Studie 41 Prozent der Befragten dieSMS-Authentifizierung an, 33 Prozent wählten zeitkritische OTPs über spezielle mobile Apps. Diese Methoden sind zwar besser als gar keine, bieten aber dennoch Angriffsfläche für Bedrohungen, die von Social Engineering über SIM-Swapping bis hin zum Diebstahl mobiler Geräte reichen.
Überraschenderweise glauben immer noch mehr als ein Viertel (26 Prozent) der Befragten, dass Passwörter am sichersten sind - obwohl diese sehr anfällig für Phishing-Angriffe sind.

Gerätegebundene Passkeys, wie sie beispielsweise auf Hardware-Sicherheitsschlüsseln zu finden sind, wurden nur von 30 Prozent der Befragten als die sicherste Methode angesehen, obwohl sie gegen eine Vielzahl von Angriffsarten hochwirksam sind. Diese falschen Vorstellungen beeinflussen individuelleEntscheidungen und übergreifende Richtlinien und erhöhen so die Anfälligkeit des gesamten Unternehmens.

Trotz dieser Schwachstellen glauben 84 Prozent der Befragten, deren Unternehmen je nach Rolle unterschiedliche Sicherheitsmaßnahmen anwenden, immer noch, dass die Cybersicherheit ihres Unternehmens ausreicht. Dies zeugt von einem falschen Vertrauen: alle Ebenen eines Unternehmens müssen einheitlich behandelt werden, damit Cybersicherheitstools wirksam sind.

Trotz Der Schwachstellen Glauben 84 Prozent Der Befragten, Deren Unternehmen Unterschiedliche Sicherheitsmaßnahmen Je Nach Rolle Und Anforderungen Einsetzen, Dass Ihr Unternehmens Angemessen Abgesichert Ist. Dies Deutet Auf Eine Übermäßige Zuversicht Hin.



84%

sind immer noch der Meinung, dass die Cybersicherheit ihres Unternehmens so sicher ist, wie sie sein muss

Was Ist Die Sicherste Methode Zur Authentifizierung?

Hardware-Sicherheitsschlüssel gelten allgemein als die sicherste Form der Authentifizierung. Die kleinen physischen Geräte müssen sich in Ihrem Besitz befinden, um Ihre Identität zu überprüfen – wodurch sie Phishing-Angriffe und Identitätsdiebstahl äußerst wirksam verhindern. Gerätegebundene Passkeys, die auf einem Hardware-Sicherheitsschlüssel gespeichert sind, gelten als „Goldstandard“ in der Authentifizierung.

Persönliche Gewohnheiten gefährden die Unternehmenssicherheit

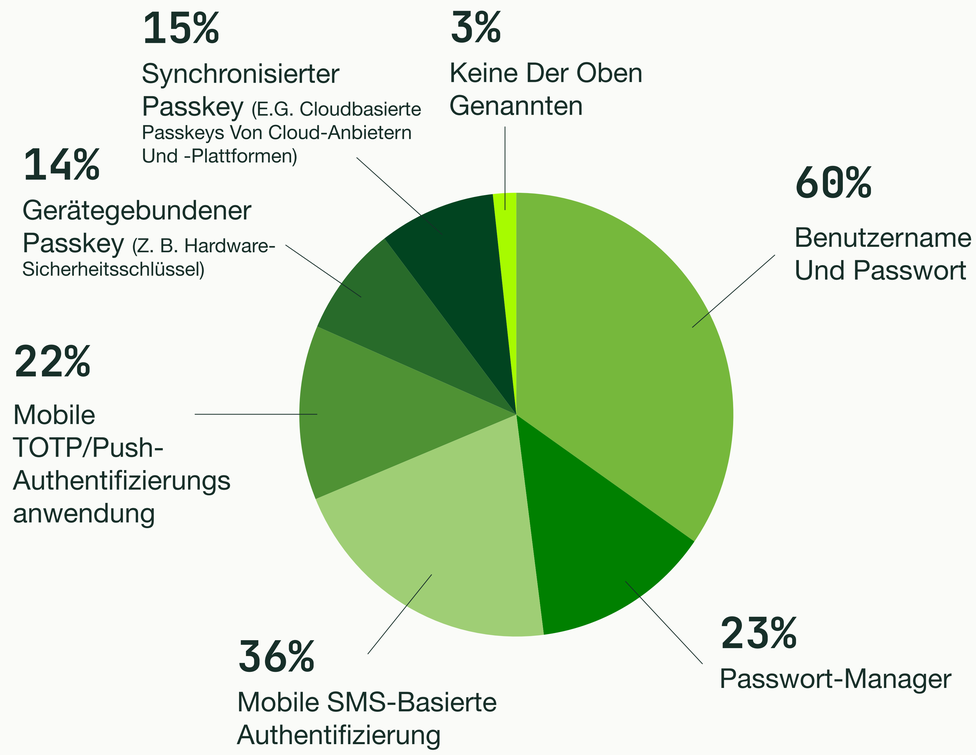
Die Grenze zwischen Privat- und Berufsleben verschwimmt zunehmend, und die Gewohnheiten von Arbeitnehmern zu Hause können schnell zu Sicherheitsrisiken für Arbeitgeber führen. Unsere Ergebnisse zeigen eine starke Überschneidung zwischen der privaten und beruflichen Nutzung von Geräten: 40 Prozent der Mitarbeiter nutzen ihre Arbeitsgeräte, um private E-Mail-Konten zu überprüfen, und 40 Prozent greifen von ihren privaten Geräten aus auf ihre Arbeits-E-Mails zu. Diese erlaubt es Angreifern, in berufliche Konten einzudringen, ohne direkt ein Unternehmensziel anzugreifen.

Angesichts der Tatsache, dass 29 Prozent der Befragten keine MFA-Optionen für ihre privaten E-Mail-Konten nutzen, entstehen zwangsläufig Schwachstellen. Diese können von Kriminellen ausgenutzt werden, um auf berufliche Systeme zuzugreifen, gezielte Phishing-Angriffe gegen Kollegen durchzuführen und persönliche Informationen für Social-Engineering-Zwecke zu sammeln.

Es überrascht nicht, dass die persönlichen Authentifizierungsmethoden den in Unternehmen beobachteten Trends sehr ähnlich sind: Die gängigsten Methoden zur Sicherung persönlicher Konten sind Passwörter (60 Prozent) und SMS (36 Prozent). Nur 14 Prozent der Personen verwenden gerätegebundene Passkeys für persönliche Konten.

> Mitarbeiter nutzen private Geräte für die Arbeit und Arbeitsgeräte für private Aktivitäten, wodurch ein privater Vorfall zu einer potenziellen Schwachstelle für das Unternehmen wird. Persönliche und berufliche Cybersicherheit sollten Hand in Hand gehen und sich gegenseitig ergänzen.“
>
> **Ronnie Manning, Chief Brand Advocate, Yubico**

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



KI hat Cyberangriffe verstärk

KI ermöglicht es den Nutzern, in kürzerer Zeit mehr zu erledigen. Während sie am Arbeitsplatz positive Eigenschaften wie Produktivität und Wachstum mit sich bringt, hat sie auch die Bedrohungslandschaft verändert. Die Hürden für die Durchführung ausgeklügelter Angriffe sind jetzt deutlich niedriger, und KI-gestützte Tools bieten selbst ungeschulten Angreifern die Möglichkeit, erheblichen Schaden anzurichten.

Die Fähigkeit der KI, Cyberkriminalität zu fördern, geht über automatisierte Tools oder Bots hinaus.Sie ermöglicht es Angreifern, äußerst überzeugende Phishing-E-Mails zu verfassen, diese an einzelne Ziele anzupassen und ihre Erfolgschancen damit drastisch zu erhöhen. Hacker ohne Programmiererfahrung können gefälschte Websites erstellen, die den Originalen nahezu identisch sind. Dank Deepfake-Video- und Audiodateien können Mitarbeiter getäuscht werden - und all das schnell und in großem Umfang.

Die gute Nachricht ist, dass die Zunahme von Online-Betrug und Phishing im Zusammenhang mit KI kein Geheimnis mehr ist. 78 Prozent der Befragten gaben an, dass sie sich der neuen Gefahren bewusst sind, und 70 Prozent glauben, dass diese Art von Angriffen erfolgreicher sind. Diese Zahlen stimmen mit den Beobachtungen zu globalen Cyberbedrohungen überein und deuten darauf hin, dass die meisten Menschen die sich schnell verändernde Bedrohungslage erkennen, obwohl ihre Unternehmen keine Maßnahmen ergreifen.

Erfreulicherweise äußerten 76 Prozent der Befragten Bedenken hinsichtlich der Auswirkungen von KI auf die Sicherheit ihrer privaten oder beruflichen Konten. Dies ist ein Anstieg von 18 Prozent gegenüber dem vorherigen Umfragezeitraum: 2024 stellten Talker und Yubico in ihrer Umfrage fest, dass nur 58 Prozent der Befragten ähnliche Bedenken hatten, was auf ein schnell wachsendes Bewusstsein für die Risiken durch KI hindeutet.

> KI schreibt die Regeln der Cyberkriminalität neu und erleichtert es Kriminellen, ausgeklügelte und gezielte Angriffe zu starten. Unternehmen, die grundlegende Authentifizierungsmethoden wie Passwörter und SMS verwenden, werden ins Hintertreffen geraten. Es ist klar, dass es für Unternehmen jetzt an der Zeit ist, sich zu modernisieren und Sicherheitsmethoden einzuführen, die sich gegen die heutigen Bedrohungen bewährt haben.“
>
> **Ronnie Manning, Chief Brand Advocate, Yubico**

Verschwommene Grenzen zwischen menschlicher und KI-Kommunikation

Eine der größten Gefahren, die KI im Bereich der Cybersicherheit darstellt, ist ihre beeindruckende Fähigkeit, menschliche Kommunikationsmuster nachzuahmen. Dies macht eine der effizientesten Methoden zum Filtern von Phishing-Angriffen zunichte: das Erkennen verdächtiger oder ungewöhnlicher Texte.

34 Prozent der Befragten, die bereits Opfer eines Phishing-Angriffs wurden, gaben an, dass sie auf den Trick hereingefallen sind, weil er scheinbar von einer vertrauenswürdigen Quelle stammte. Angesichts der Fähigkeit der KI, auf ihr Gegenüber einzugehen und aus riesigen Datenmengen zu schöpfen, wird diese Art der Bedrohung zunehmen und erfolgreicher werden.

Unsere Daten zeigen, dass die meisten Befragten auch Schwierigkeiten haben, zwischen von Menschen und von KI generierten Inhalten zu unterscheiden. Bei der Vorlage von Beispielnachrichten identifizierten nur 30 Prozent der Befragten eine von Menschen verfasste Nachricht korrekt, während 70 Prozent sie fälschlicherweise der KI zuordneten oder sich nicht sicher waren. Umgekehrt identifizierten 54 Prozent der Befragten eine von KI generierte Nachricht entweder falsch oder gar nicht, während nur 46 Prozent sie korrekt als KI kennzeichneten.

Diese Ergebnisse waren jedoch nicht in allen Altersgruppen einheitlich. Jüngere Generationen konnten menschliche Texte besseridentifizieren. Diesdeutet darauf hin, dass Personen, die mit dieser Art von Technologie aufgewachsen sind, den Unterschied eher intuitiv erkennen.

E-Mail von Menschen

Hallo [NAME],

um die Sicherheit unseres Netzwerks zu gewährleisten, bitten wir alle Benutzer, ihre Anmeldedaten für unser Projektmanagementsystem alle 90 Tage zurückzusetzen. Ihre Anmeldung läuft bald ab. Bitte verwenden Sie den unten stehenden Link, um Ihre Anmeldedaten zurückzusetzen. Bei Problemen wenden Sie sich bitte an uns.

https://link/example.com

Vielen Dank,
[NAME]
Unternehmensadministrator

KI-E-Mail

Hallo [NAME],

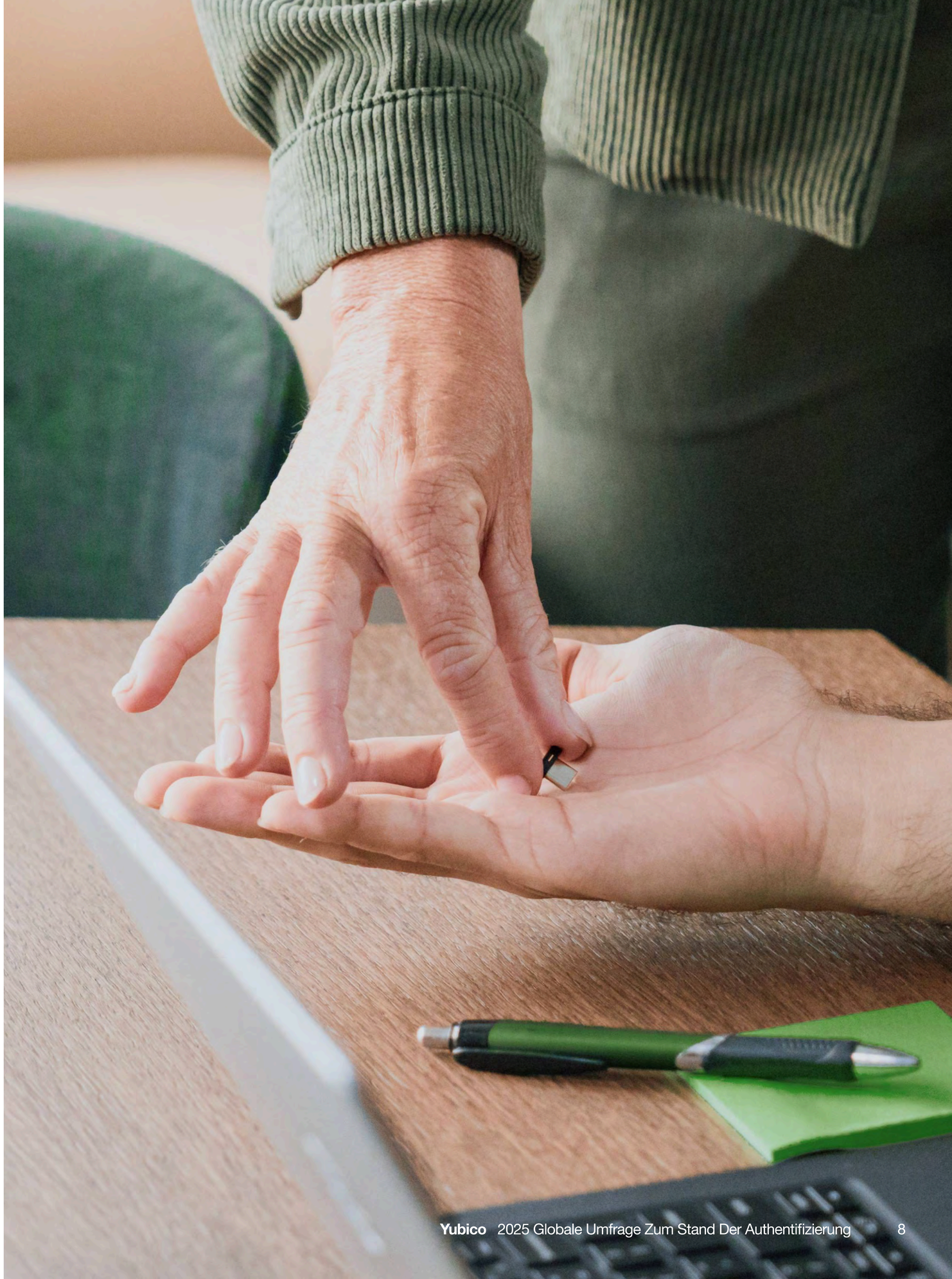
nur eine kurze Info: Ihr Login für das Projektmanagementsystem des Unternehmens ist abgelaufen (wir setzen es alle 90 Tage zurück). Aus Sicherheitsgründen bitten wir Sie, ein neues Login einzurichten. Klicken Sie dazu auf den folgenden Link: https://link/example.com

Wenden Sie sich bei Problemen an uns.

Mit freundlichen Grüßen,
[NAME]
Unternehmensadministrator

II.

Lösungen: Der Weg zum Aufbau von Cyber-Resilienz



Wissen ist die erste Verteidigungslinie

Eine effektive Cybersicherheit erfordert einen mehrgleisigen Ansatz. Technologie allein ist wirkungslos, wenn den Mitarbeitern das Wissen fehlt, das sie benötigen, um sich selbst und ihr Unternehmen zu schützen. Unsere Ergebnisse deuten auf erhebliche Lücken in der allgemeinen Cybersicherheitsausbildung hin, die angegangen werden müssen, um modernen Bedrohungen standhalten zu können.

Ein eindrucksvolles Beispiel dafür, wie Fehlvorstellungen Sicherheitsbemühungen zunichte machen können, ist die mangelnde Akzeptanz von MFA. Befragte, die MFA für ihre persönlichen Konten vermeiden, geben als Gründe dafür an, dass sie damit nicht vertraut sind (40 Prozent), es für zu komplex halten (24 Prozent), keine Zeit haben (22 Prozent) und von hohen Kosten ausgehen (9 Prozent).

In ähnlicher Weise scheint die wiederkehrende mangelnde Akzeptanz von Passkeys eher auf Wissenslücken als auf technische Hürden zurückzuführen zu sein. Von den Befragten, die keine Passkeys verwenden, gaben 45 Prozent an, noch nie davon gehört zu haben. Weitere 12 Prozent gaben an, dass sie für die von ihnen genutzten Websites und Dienste keine Option darstellen, und 11 Prozent befürchteten, dass sie zu kompliziert sind. Dies deutet darauf hin, dass Aufklärung und das Engagement der Unternehmen erforderlich sind, um die Authentifizierungssicherheit zu verbessern.

Wirksame Aufklärungsstrategien

Die Stärkung der Cybersicherheit in Unternehmen erfordert einen praxisorientierten Ansatz, der Schulungsprogramme, technische Anleitungen und eine regelmäßige Überprüfung der Sicherheitsgewohnheiten umfasst. Es ist wichtig, falsche Vorstellungen über die vermeintliche Komplexität der Cybersicherheit zu beseitigen und die verfügbaren Tools einfachenund verständlich zu präsentieren. Moderne Sicherheitslösungen sind auf allgemeine Nutzer zugeschnitten und bieten im Vergleich zu veralteten Passwörtern einen optimierten Ansatz.

Schulungsprogramme müssen die Bedeutung der beruflichen und persönlichen Cybersicherheit hervorheben und den Mitarbeitern ein tiefes Verständnis dafür vermitteln, wie sich persönliche Gewohnheiten auf die Sicherheit am Arbeitsplatz auswirken können. Regelmäßige Schulungen sind in der sich schnell verändernden Bedrohungslandschaft von heute unerlässlich.Unternehmen sollten deshalb kontinuierlich Schulungen zu neuen Risiken anbieten, einschließlich Bewertungen, um den Wissensstand sicherzustellen.

> Unternehmen müssen ihre Mitarbeiter schulen und mit dem Mythos aufräumen, dass Cybersicherheit nur etwas für technisch versierte Personen ist. Mit dem richtigen Wissen und den richtigen Tools kann und sollte jeder einzelne Mitarbeiter im Unternehmen zu einem sicheren Cybersicherheits-Ökosystem beitragen.“
>
> **Yubico Spokesperson**

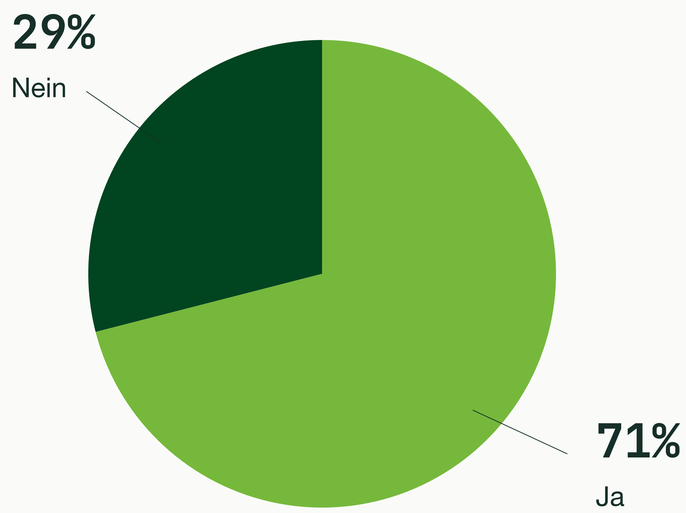
Die Lücke bei der Einführung von MFA schließen

Unsere Daten zeigen eine positive Entwicklung für MFA, was auf eine gewisse Offenheit und Akzeptanz bei Menschen und Organisationen hindeutet. Da jüngere Generationen wie die Generation Z (71 Prozent) und die Millennials (68 Prozent) eine höhere Nutzungsrate für ihre persönlichen Konten aufweisen, ist es wahrscheinlich, dass die Akzeptanz von MFA weiterhin organisch wachsen wird. Unternehmen sollten sich jedoch nicht auf dieser natürliche Entwicklung ausruhen, sondern stattdessen proaktiv an einer breiten Akzeptanz arbeiten.

Globale Unterschiede in den Akzeptanzraten liefern zusätzliche Einblicke in effektive Implementierungsstrategien. Insgesamt geben 82 Prozent der Befragten an, dass sie mit MFA-Passkeys vertraut sind, wobei die USA bei der Verwendung von gerätegebundenen Passkeys an zweiter Stelle (33 Prozent) hinter Indien (39 Prozent) bei der liegen.Australien und Singapur führen bei der MFA-Akzeptanz (beide 78 Prozent) speziell für persönliche Konten an, was verdeutlicht, was mit angemessener Cybersicherheitsaufklärung und -unterstützung erreicht werden kann.

Für Unternehmen ist es unerlässlich, als ersten Schritt daran zu arbeiten, Hindernisse für die Einführung von MFA zu beseitigen. Unternehmen sollten benutzerfreundliche Tools, leicht verständliche Anleitungen sowie kontinuierlichen Support und Fehlerbehebung bereitstellen. Das Ziel sollte sein, MFA-Optionen bequem und optimiert zu gestalten, anstatt nur ihre Verwendung vorzuschreiben.

Haben Sie die Multi-Faktor-Authentifizierung (MFA) für Ihre persönliche E-Mail aktiviert?



Hier Ist Die Deutsche Übersetzung?

Unter denjenigen, die keine MFA nutzen, sind die häufigsten Gründe mangelnde Vertrautheit (40 %), das Gefühl, nicht über das nötige technische Wissen zu verfügen (24 %), die Annahme, es sei zu zeitaufwändig (22 %) und der Glaube, es sei zu teuer (9 %)

Argumente für Hardware-Sicherheitsschlüssel

In der modernen Bedrohungslandschaft mit KI-gestützten Phishing-Angriffen und leistungsstarken Social-Engineering-Techniken bieten Hardware-Sicherheitsschlüssel mit Passkeys einen robusten Schutz. Sie ermöglichen eine Phishing-resistente Authentifizierung, die den physischen Besitz des Schlüssels sowie die Interaktion des Benutzers erfordert.

Da sie sowohl den Besitz des Schlüssels als auch diemenschliche Anwesenheit verlangen, bieten Hardware-Sicherheitsschlüssel einen starken Schutz, selbst gegen die ausgefeiltesten KI-gestützten Phishing-Angriffe. Während Passwörter gehackt und aus der Ferne verwendet werden können und SMS-Nachrichten abgefangen werden können, sind Hardware-Sicherheitsschlüssel gegen diese Angriffsvektoren resistent.

Deshalb sind gerätegebundene Passkeys wie Hardware-Sicherheitsschlüssel heute der Goldstandard. Cloud-basierte synchronisierte Passkeys bieten zwar ein höheres Maß an Sicherheit als reine Passwörter, sind aber dennoch potenziell anfällig für Kompromittierungen, wenn ein Angreifer in den Cloud-Dienst oder das individuelle Konto des Benutzers eindringt. Gerätegebundene Passkeys, die kryptografische Schlüssel lokal speichern, sind diesen Risiken nicht ausgesetzt.

Obwohl sie das derzeit wirksamste Mittel gegen Phishing sind, verwenden nur 17 Prozent der Unternehmen gerätegebundene Passkeys für ihre Mitarbeiter, was darauf hindeutet, dass es bei den Unternehmen noch erheblichen Verbesserungsbedarf gibt. Auch hier gibt die Unterscheidung zwischen den Generationen Anlass zur Hoffnung auf eine zunehmende Verbreitung: Mit 20 Prozent bei den Millennials und 19 Prozent bei der Generation Z weisen diese Altersgruppen die höchsten Nutzungsraten in Unternehmen auf.

Wie bei der Einführung jeder neuen Technologie erfordert auch die Implementierung von Hardware-Sicherheitsschlüsseln Planung und Benutzerunterstützung, aber die Vorteile überwiegen bei weitem sowohl die Anfangsinvestition als auch die möglicherweise erforderlichen Schulungen. Der erfolgreiche Einsatz von Hardware-Sicherheitsschlüsseln führt in der Regel zu einem erheblichen ROI, einem drastischen Rückgang von Kontovorfällen, einem geringeren Bedarf an technischem Support und einer Verbesserung des Vertrauens und der Sicherheit der Benutzer insgesamt.

Hier Ist Die Deutsche Übersetzung

Generationelle Trends lassen auf eine erhöhte Akzeptanz hoffen, wobei Millennials (20 %) und Gen Z (19 %) bei der Nutzung von MFA in Unternehmensumgebungen führend sind.

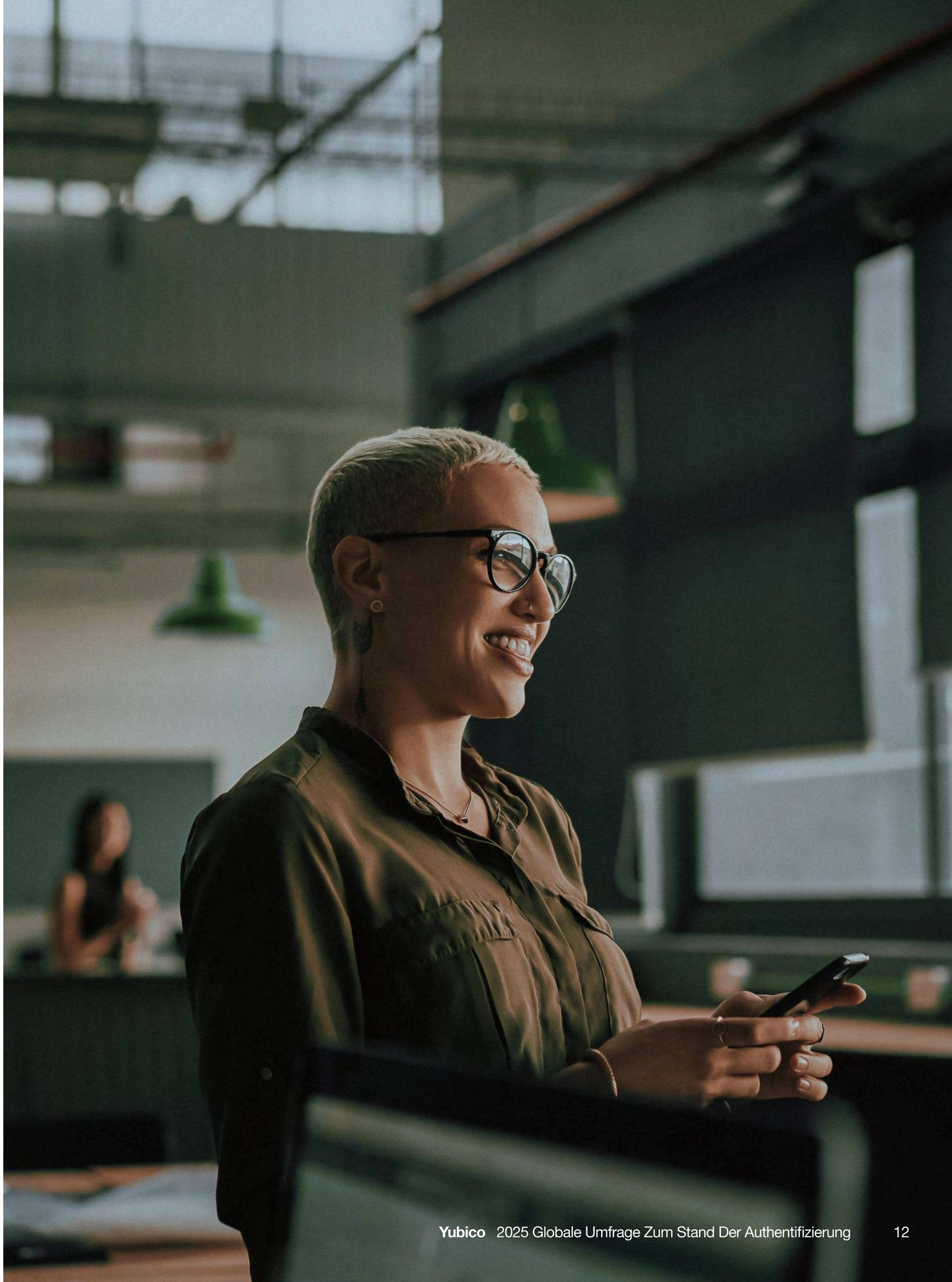
Fazit

Die heutige Cybersicherheitslandschaft ist schnelllebiger und mit mehr Bedrohungen behaftet als je zuvor. KI-gestützte Angriffe und grundlegende MFA-Verfahren können viele Unternehmen gefährlich exponieren. Das Vertrauen auf schwache Authentifizierungsmethoden, uneinheitliche Mitarbeiterschulungen und fragmentierte Sicherheitsrichtlinien hat zu einer Kluft geführt zwischen dem, was Unternehmen für ihren Schutz halten, und dem, was tatsächlich funktioniert.

Bewährte Lösungen gibt es bereits. Gerätegebundene Passkeys, wie Hardware-Sicherheitsschlüssel, sind effektiv und können in großem Umfang eingesetzt werden. Die Hindernisse für die Einführung liegen weniger in der Technologie als vielmehr in der Denkweise der Unternehmen, was bedeutet, dass Veränderungen sowohl möglich als auch in greifbarer Nähe sind.

Generationelle Trends geben Anlass zu Optimismus für die Zukunft, da jüngere Mitarbeiter fortschrittliche Sicherheitsoptionen schneller annehmen und gegenüber KI-generierten Inhalten eine größere Skepsis an den Tag legen. Da diese Digital Natives sich für Führungspositionen positionieren, gehen wir davon aus, dass sie die breite Einführung fortschrittlicher Sicherheitsprotokolle in Unternehmen vorantreiben werden.

Der Weg in die Zukunft ist für Unternehmen klar: Sie müssen integrierte Ansätze mit bewährten Technologien nutzen, die echten Schutz vor Cyberangriffen bieten. Durch entschlossenes Handeln können Unternehmen heute die Lücke zwischen Erwartung und Realität schließen und eine Zukunft schaffen, in der Sicherheit eine gemeinsame Stärke und keine anhaltende Schwachstelle ist.



Über Yubico:

Yubico (Nasdaq Stockholm: YUBICO) ist ein modernes Cybersicherheitsunternehmen, das sich zum Ziel gesetzt hat, das Internet für alle sicherer zu machen. Als Erfinder des YubiKey haben wir den Goldstandard für moderne, phishing-resistente, hardwarebasierte Authentifizierung gesetzt, die Kontoübernahmen verhindert und die sichere Anmeldung vereinfacht.

Seit 2007 haben wir globale Authentifizierungsstandards mitgestaltet, FIDO2, WebAuthn und FIDO U2F mitentwickelt und den ursprünglichen Passkey eingeführt. Heute schützt unsere Passkey-Technologie Menschen und Organisationen in über 160 Ländern und verändert die Art und Weise, wie digitale Identitäten geschützt werden, von der Registrierung bis zur Kontowiederherstellung.

YubiKeys genießen das Vertrauen der weltweit sicherheitsbewusstesten Marken, Regierungen und Institutionen und funktionieren sofort mit Hunderten von Apps und Diensten. Sie bieten schnellen, passwortlosen Zugriff ohne Reibungsverluste oder Kompromisse.

Wir sind davon überzeugt, dass starke Sicherheit niemals unerreichbar sein sollte. Im Rahmen unserer philanthropischen Initiative „Secure it Forward“ spenden wir YubiKeys an gemeinnützige Organisationen, die gefährdete Gemeinschaften unterstützen.

Yubico hat seinen Hauptsitz in Stockholm, Schweden, und Santa Clara, Kalifornien, und ist stolz darauf, als eines der 100 einflussreichsten Unternehmen des TIME Magazine und als eines der innovativsten Unternehmen des Fast Company Magazine ausgezeichnet worden zu sein. Weitere Informationen finden Sie unter www.yubico.com.

Methodik

Talker Research befragte 18.000 erwerbstätige Erwachsene, davon jeweils 2.000 in den folgenden Ländern: Vereinigte Staaten, Vereinigtes Königreich, Australien, Indien, Japan, Singapur, Frankreich, Deutschland und Schweden. Die Umfrage wurde von Yubico in Auftrag gegeben und zwischen dem 15. und 27. August 2025 online durchgeführt.