yubico

EXKLUSIVE FORSCHUNG | 2024

Umfrage zum globalen Status der Authentifizierung

Ein ganzheitlicher Ansatz zur Bekämpfung von Cyberbedrohungen am Arbeitsplatz und zuhause

Zusammenfassung

Cybersicherheitsverletzungen und Phishing betreffen nicht nur IT-Abteilungen und technisch versierte Personen. Auch für die breite Öffentlichkeit bringen derartige Bedrohungen signifikante Risiken mit sich, insbesondere im Zeitalter von künstlicher Intelligenz (KI). Cyberangriffe und Online-Betrugsmaschen werden immer raffinierter. Folglich müssen auch Einzelpersonen wachsamer denn je sein – und zwar sowohl im privaten Umfeld als auch am Arbeitsplatz.

> 20,000
Antworten

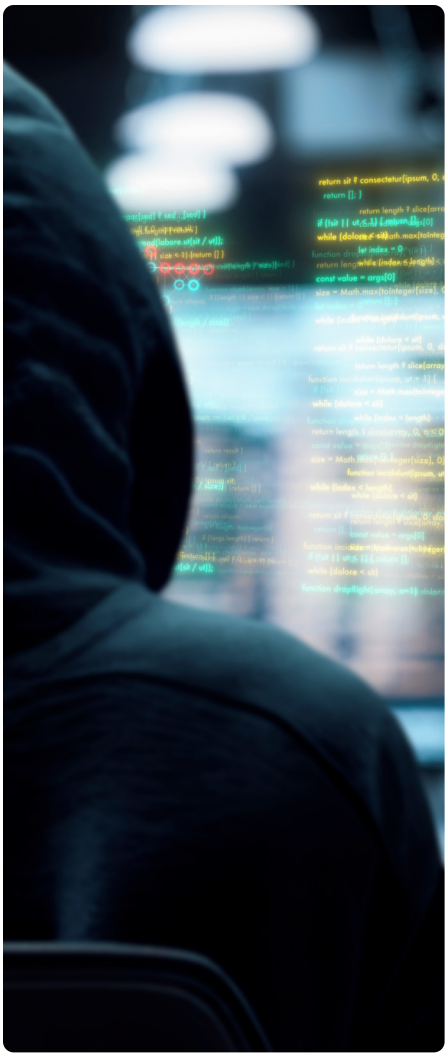
Organisationen mit
1 bis mehr als 2.000
Angestellten

10
Länder

Obwohl die Zahl der Cyberbedrohungen zunimmt, betrachten viele Menschen das Thema Sicherheit nicht aus einer ganzheitlichen Perspektive. Unternehmen sind oft bemüht, strenge Sicherheitsprotokolle am Arbeitsplatz einzuführen. Unsere Ergebnisse zeigen allerdings, dass die Angestellten zuhause weniger strikt auf die Cybersicherheit achten. Diese Kluft zwischen Arbeitsplatz und Privatleben birgt nicht nur ein Risiko für personenbezogene Daten von Einzelpersonen, sondern schafft auch potenzielle Schwachstellen für die Unternehmen, in denen diese Personen tätig sind.

In einer von Yubico in Auftrag gegebenen globalen Umfrage mit Teilnehmenden aus Australien, Frankreich, Deutschland, Indien, Japan, Polen, Singapur, Schweden, dem Vereinigten Königreich und den Vereinigten Staaten sollten die globalen Auswirkungen von unsicheren Praktiken im Cyberspace sowohl im privaten als auch im beruflichen Kontext untersucht werden. Unsere Untersuchungen zum aktuellen Stand der Cybersicherheit im Privatleben und auch am Arbeitsplatz bringen alarmierende Trends zum Vorschein, beispielsweise eine weit verbreitete Nachlässigkeit bei der Nutzung von Multi-Faktor-Authentifizierung (MFA) und eine größtenteils reaktive Vorgehensweise im Hinblick auf Cyberbedrohungen. Mit unserer breit angelegten Umfrage, die in mehreren Ländern durchgeführt wurde, haben wir die Risiken durch unzulängliche Sicherheitspraktiken untersucht und uns angesehen, welche Auswirkungen sie auf die Sicherheit von Einzelpersonen und Unternehmen haben.

Unsere Ergebnisse unterstreichen dabei, wie notwendig eine ganzheitliche Cybersicherheitsstrategie ist, die sowohl das private als auch das berufliche Umfeld berücksichtigt. Zu derartigen Strategien gehören die Einführung stärkerer Authentifizierungsmethoden, um für Resistenz gegenüber Phishing-Angriffen zu sorgen, die Förderung einer Bewusstseinskultur für das Thema Sicherheit durch konsistente Schulung der Mitarbeitenden und vieles mehr. Um auf breiter Front konsistent gegen Cyberbedrohungen vorgehen zu können, bedarf es letztlich eines konzertierten Versuchs, die Kluft zwischen der empfundenen und der tatsächlichen Sicherheit zu schließen. Indem wir fortschrittliche Sicherheitsmaßnahmen zu einem festen Bestandteil aller Bereiche unseres digitalen Lebens machen, können wir uns selbst, unsere Daten und auch unsere Unternehmen besser schützen.



Beste Voraussetzungen: KI verändert Vorgehensweise bei Hacker-Angriffen

Schon seit Jahren nutzen Hacker neue Technologien, um ihre Phishing-Angriffe effektiver und schneller zu gestalten. Das Aufkommen von KI hat jedoch dafür gesorgt, dass es mittlerweile zu einer beispiellosen Herausforderung geworden ist, Cybersicherheit zu gewährleisten. KI bietet die Möglichkeit, große Datenmengen zu analysieren, aus Mustern zu lernen und raffinierte Phishing-Angriffe zu generieren. Somit kann sie die Cybersicherheitslandschaft potenziell deutlich stärker in Aufruhr versetzen.

Im Mai 2024 veröffentlichte das FBI eine Erklärung, um die Öffentlichkeit vor den erhöhten Risiken im Zusammenhang mit KI-basierten Cybersicherheitsbedrohungen zu warnen. Zu den Bedrohungen zählen beispielsweise auch Techniken, mit denen Sprach- und Videoaufnahmen so geklont werden, dass der Eindruck entsteht, es handle sich um echte Aufnahmen von vertrauenswürdigen Personen wie etwa Familienmitgliedern oder Mitarbeitenden.

Was ist Phishing?

Phishing ist eine gängige Taktik, die Hacker für den Zugriff auf vertrauliche Informationen verwenden, und trägt zu über **80 %** aller Sicherheitsverstöße bei. Bei diesen Angriffen werden Personen dazu verleitet, personenbezogene Daten offenzulegen, indem die Hacker sich in E-Mails, in den sozialen Medien, in Textnachrichten oder auf gefälschten Websites als natürliche Personen ausgeben.

Das Augenmerk der Angreifenden liegt bei Phishing-Angriffen in vielen Fällen auf Passwörtern, da diese für Hacker leider nach wie vor das gängigste Mittel sind, um sich Zugang zu fremden Konten zu verschaffen. Passwörter sind zwar schon seit langer Zeit das Mittel der Wahl, um die eigene Identität im Netz zu verifizieren – allerdings sind sie von Natur aus unsicher. In der Regel wählen Benutzer bei dieser Authentifizierungsart komplexe Zeichenfolgen, die sie sich merken und dann jedes Mal, wenn sie auf ein System oder eine Anwendung zugreifen wollen, korrekt eingeben müssen. Diese Methode hat sich jedoch in vielerlei Hinsicht als mit Schwachstellen behaftet erwiesen.

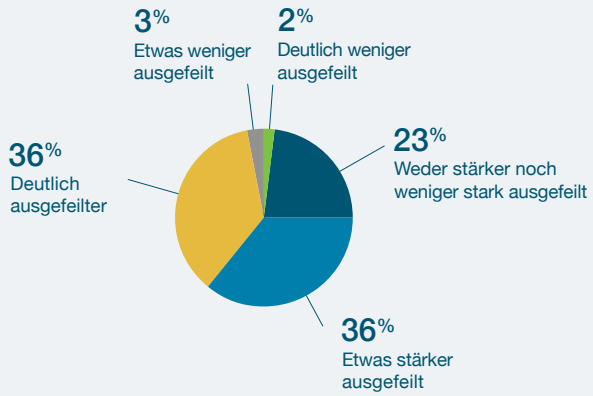
Der Grund dafür ist, dass Menschen dazu neigen, dasselbe Passwort gleich für mehrere Konten zu verwenden bzw. Passwörter zu wählen, die leicht zu erraten sind. So können Hacker mit nur einer Anmeldung gleich mehrere Konten knacken. Hinzu kommt, dass Personen aufgrund der raffinierten Phishing-Angriffe der heutigen Zeit leicht dazu verleitet werden können, ihre Passwörter preiszugeben. So können Hacker beispielsweise eine Fake-Website erstellen, die täuschend echt aussieht.

58% der Befragten *****

sind **besorgt** darüber, dass KI die Sicherheit ihrer persönlichen bzw. geschäftlichen Konten gefährden könnte

KI und Cybersicherheitsbedrohungen: Ergebnisse der Umfrage

Denken Sie, dass Online-Betrugsversuche und Phishing-Versuche durch den Einsatz von künstlicher Intelligenz (KI) ausgefeilter oder weniger ausgefeilt geworden sind?



Wenig überraschend ergab unsere Umfrage, dass die befragten Personen große Angst vor den Cybersicherheitsgefahren haben, die KI mit sich bringt:

- **72 %** der Befragten glauben, dass Online-Betrugsversuche und Phishing-Angriffe durch den Einsatz von KI ausgefeilter geworden sind.
- **66 %** der Befragten sind der Ansicht, dass diese Angriffe aufgrund von KI inzwischen erfolgreicher sind.
- **58 %** der Befragten machen sich Gedanken darüber, dass KI die Sicherheit ihrer persönlichen bzw. geschäftlichen Konten beeinträchtigen könnte.

Die wachsende Bedrohung durch KI unterstreicht, wie dringend ein besser integrierter Ansatz für die Cybersicherheit vonnöten ist – also ein Ansatz, der auch die immer wichtigere Rolle der neuen Technologie bei Online-Betrugsmaschen berücksichtigt. Es reicht nicht mehr aus, sich auf veraltete Sicherheitspraktiken zu verlassen. Die Tools und Techniken, die wir zum Schutz unserer Daten verwenden, müssen sich im Einklang mit den Bedrohungen, denen wir ausgesetzt sind, weiterentwickeln.

Fast die Hälfte (49%) der Befragten

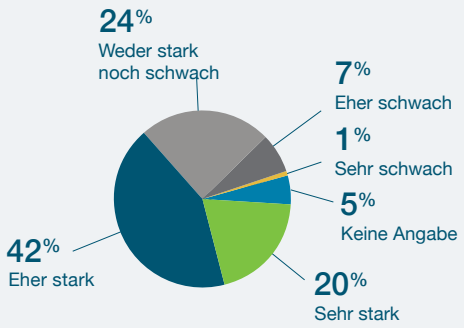
macht sich größere Sorgen um die Sicherheit ihrer **eigenen personenbezogenen** Daten als um die Sicherheit der Daten ihrer Unternehmen.

Phishing-resistente Multi-Faktor-Authentifizierung (MFA)

MFA ist ein wichtiges Tool im Kampf gegen Phishing-Angriffe. Allerdings **sind nicht alle MFA-Methoden gleich**. Phishing-resistente MFA wie zum Beispiel **Hardware-Sicherheitsschlüssel bieten ein höheres Maß an Schutz**, da zur Authentifizierung ein physisches Gerät erforderlich ist. Das macht es für Angreifer deutlich schwieriger, sich Zugriff auf Ihre Konten zu verschaffen.

Persönliche Cybersicherheit: Zuversicht vs. Realität

Wie stark oder schwach sind Ihrer Meinung nach die Cybersicherheitsmaßnahmen, die Sie zum Schutz Ihrer personenbezogenen Daten getroffen haben?

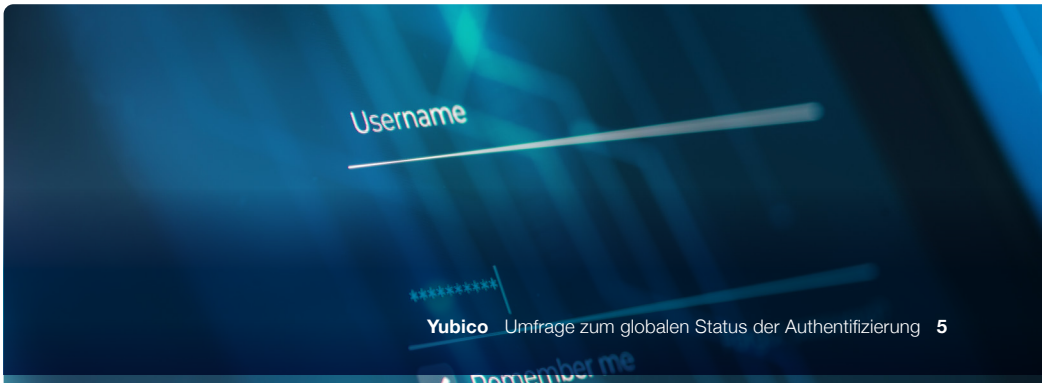


Eine beträchtliche Anzahl der Teilnehmenden unserer Umfrage ist eigenen Angaben zufolge zuversichtlich, was die eigenen Praktiken für die persönliche Cybersicherheit angeht, und räumt dieser persönlichen Cybersicherheit im Vergleich zur Sicherheit im beruflichen Kontext laut eigenen Aussagen sogar eine höhere Priorität ein.

- **63 %** der Befragten geben an, dass sie starke oder sehr starke Cybersicherheitsmaßnahmen zum Schutz ihrer persönlichen Daten implementiert haben.
- Fast die Hälfte (**49 %**) der Befragten macht sich mehr Gedanken über die Sicherheit ihrer personenbezogenen Daten als über die Sicherheit der Daten ihrer Unternehmen.

Doch auch wenn sich viele Personen zuversichtlich in Bezug auf ihre persönlichen Cybersicherheitsmaßnahmen zeigen, ist diese Zuversicht möglicherweise nicht angebracht. Denn wenn man sich die tatsächlichen Praktiken und Erfahrungen einmal genauer ansieht, wird klar, dass viele Personen gar nicht so gut geschützt sind, wie sie glauben:

- **70 %** der Befragten wurden in den vergangenen zwölf Monaten im Privatleben Opfer von Cyberangriffen.
- Viele Befragte reagieren eher reaktiv als proaktiv auf Cyberbedrohungen in ihrem privaten und beruflichen Umfeld (**45 %** bzw. **44 %**).
- **39 %** sind der Meinung, dass die einfache Verwendung eines Benutzernamens und Passworts der sicherste Weg ist, um Konten und Informationen zu schützen. Zudem verwenden **58 %** der Befragten lediglich einen Benutzernamen und ein Passwort, um sich bei ihren persönlichen Konten anzumelden.



70% der Befragten

wurden in den letzten zwölf Monaten **im Privatleben** Opfer von Cyberangriffen

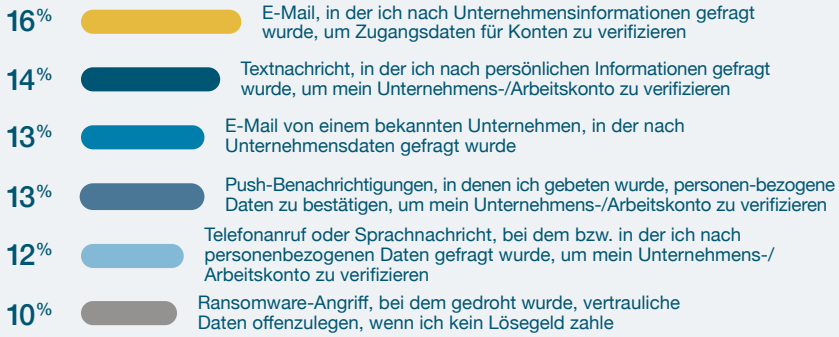
60% der Befragten

wurden in den letzten zwölf Monaten **am Arbeitsplatz** Opfer von Cyberangriffen

Dominoeffekt: Auswirkungen der persönlichen Cybersicherheit auf den Arbeitsplatz

Welchen Arten von Cyberangriffen am Arbeitsplatz waren Sie in den letzten zwölf Monaten ausgesetzt?*

Die sechs häufigsten Antworten



* Mehrere Antworten zulässig.

Die Lücken in den Vorgehensweisen bei der persönlichen Cybersicherheit stellen nicht nur für Einzelpersonen ein Risiko dar, sondern lassen auch Schwachstellen für die Unternehmen entstehen, bei denen diese Personen tätig sind. Da immer mehr Mitarbeitende remote arbeiten oder persönliche Geräte für arbeitsbezogene Aufgaben verwenden, verschwimmt die Grenze zwischen der Cybersicherheit im persönlichen und im beruflichen Kontext immer mehr. Diese Verflechtung kann Cyberkriminellen ungewollt Türen öffnen, um sich über kompromittierte persönliche Konten Zugriff auf Unternehmensnetzwerke zu verschaffen.

Unsere Umfrage ergab, dass **50 %** der Befragten in den letzten zwölf Monaten Opfer von Cyberangriffen wurden. Diese Statistik hebt hervor, wie stark vernetzt der Bereich Cybersicherheit heutzutage ist.

> „Wenn Einzelpersonen nicht für einen ausreichenden Schutz ihrer persönlichen Konten sorgen, entsteht dadurch auch ein Risiko für ihren Arbeitsplatz. Deshalb ist es für Unternehmen entscheidend, bei der Cybersicherheit einen ganzheitlichen Ansatz zu verfolgen, der sowohl den Schutz von beruflichen Umgebungen als auch die Sicherheit im privaten Umfeld berücksichtigt.“
>
> **Derek Hanson** | VP Standards and Alliances | Yubico

Lösungen für ein einheitliches Vorgehen bei der Cybersicherheit

Angesichts dessen, wie stark moderne Cybersicherheitsbedrohungen miteinander verflochten sind, ist klar, dass sowohl Einzelpersonen als auch Unternehmen bei der Sicherheit auf einen stärker integrierten Ansatz setzen müssen. Das bedeutet, dass nicht nur am Arbeitsplatz starke Maßnahmen implementiert werden müssen, sondern vielmehr die Mitarbeitenden auch dazu angehalten und befähigt werden sollten, in ihrem Privatleben bessere Praktiken anzuwenden. Wir empfehlen dabei unter anderem die folgenden Sicherheitsmaßnahmen:

LÖSUNG NR. 1: Kluft zwischen Arbeitsplatz und Privatleben schließen

Um eine wirklich sichere Umgebung zu schaffen, müssen sowohl Unternehmen als auch Mitarbeitende verstehen, dass das Thema Cybersicherheit nicht bloß am Arbeitsplatz eine Rolle spielt. Ein umfassender Ansatz für die Cybersicherheit muss konsistente und proaktive Maßnahmen zum Schutz aller Aspekte des digitalen Lebens umfassen.

Aus diesem Grund sollten Unternehmen Ressourcen bereitstellen, die über den Arbeitsplatz hinausgehen und Mitarbeitenden dabei helfen, auch ihre persönlichen Geräte und Konten zu schützen. Beispielsweise können Schwachstellen deutlich reduziert werden, indem sowohl für berufliche als auch für private Konten zur Verwendung von Phishing-resistenter MFA und anderen fortschrittlichen Sicherheitsmaßnahmen aufgerufen wird.

LÖSUNG NR. 2: Mitarbeitende schulen und sensibilisieren

Sie haben angegeben, dass Sie in den letzten zwölf Monaten am Arbeitsplatz Opfer eines Cyberangriffs wurden. Welche neuen Sicherheitstechnologien oder -richtlinien hat Ihr Unternehmen infolgedessen implementiert?*

Die zwölf häufigsten Antworten

* Mehrere Antworten zulässig.

40% der Befragten

berichteten, dass sie **am Arbeitsplatz** nicht zum Thema Cybersicherheit geschult wurden

47% der Befragten

gaben an, dass sich ihre persönlichen Gewohnheiten in Bezug auf die digitale Sicherheit basierend auf dem, was sie **am Arbeitsplatz** zum Schutz ihrer Konten gelernt haben bzw. umsetzen, geändert haben

Weiterbildungen und umfassende Schulungen stellen für Unternehmen eine effektive Möglichkeit dar, um ihre Cybersicherheitspraktiken zu verbessern. Unsere Umfrage ergab jedoch, dass nicht alle Mitarbeitenden angemessen geschult werden und dass selbst jene, die entsprechende Schulungen durchlaufen, die Praktiken nicht immer auf ihre Privatleben übertragen. Die Statistiken dazu sehen wie folgt aus:

- **40 %** der Befragten gaben an, dass sie am Arbeitsplatz keine Schulung zum Thema Cybersicherheit erhalten haben.
- **47 %** der Befragten äußerten sich dahingehend, dass sich ihre persönlichen Gewohnheiten in Bezug auf die digitale Sicherheit basierend auf dem, was sie am Arbeitsplatz zum Schutz ihrer Konten gelernt haben bzw. umsetzen, geändert haben.

Diese Daten zeigen, dass Schulungen zwar effektiv sein können, jedoch nicht alle Mitarbeitenden erreichen, und dass im Hinblick auf die Durch- und Fortführung von Schulungen Verbesserungspotenzial besteht. Darüber hinaus müssen Cybersicherheitsschulungen auf allen Ebenen des Unternehmens einheitlich durchgeführt werden – angefangen bei den Mitarbeitenden der untersten Ebene bis hin zu Führungskräften. Insbesondere Mitarbeitende, die in der Hierarchie weiter unten stehen, sollten hier nicht außer Acht gelassen werden.

Zudem sollten Unternehmen ihre Mitarbeitenden regelmäßig über die neuesten Cybersicherheitsbedrohungen informieren. Das gilt insbesondere für Bedrohungen im Zusammenhang mit KI-gestützten Angriffen. Die Bedeutung von MFA sollte klar kommuniziert werden, um sicherzustellen, dass die Mitarbeitenden verstehen, wie sie diese Methode sowohl für berufliche als auch für private Konten implementieren sollten.

An dieser Stelle sei auch angemerkt, dass fast ein Viertel (**23 %**) der Mitarbeitenden, die am Arbeitsplatz Opfer eines Cyberangriffs waren, berichteten, dass ihre Arbeitgeber infolgedessen obligatorische Sicherheitsschulungen eingeführt haben. Dies ist zwar eine angemessene Reaktion, um Cyberbedrohungen einzudämmen – allerdings sollten Mitarbeitende als vorbeugende Maßnahme regelmäßig zu verschiedenen Zeitpunkten im Jahr an die „Best Practices“ erinnert werden.

58% der Befragten

verwenden **Benutzername und Passwort**

34% der Befragten

verlassen sich auf **SMS-basierte** Authentifizierung

22% der Befragten

verwenden **eine App** zur Authentifizierung per Mobilgerät

54% der Arbeitskonten

verwenden **Benutzername und Passwort**

21% der Arbeitskonten

verlassen sich auf **SMS-basierte** Authentifizierung

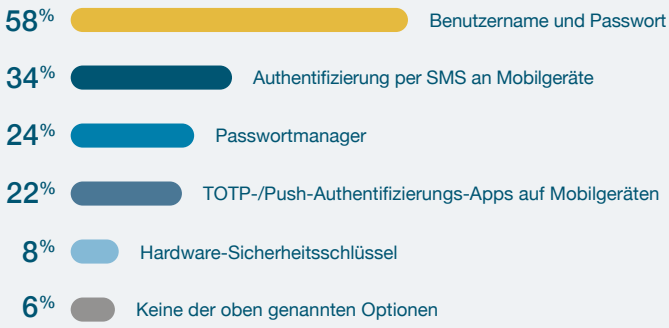
21% der Arbeitskonten

verwenden **eine App** zur Authentifizierung per Mobilgerät

LÖSUNG NR. 3: Authentifizierungsmethoden für einen sicheren Zugriff am Arbeitsplatz und zu Hause

Wie erfolgt die Authentifizierung/Anmeldung bei Ihren persönlichen Konten?*

Die sechs häufigsten Antworten



* Mehrere Antworten zulässig.

Die Multi-Faktor-Authentifizierung ist einer der wichtigsten Aspekte für die Cybersicherheit. Unsere Umfrage hat jedoch gezeigt, dass viele Menschen nach wie vor veraltete Methoden nutzen, um ihre Konten zu sichern – sowohl am Arbeitsplatz als auch im Privatleben.

- Bei privaten Konten nutzen **58 %** der Befragten Benutzername und Passwort, **34 %** der Befragten verlassen sich auf die SMS-basierte Authentifizierung und **22 %** verwenden eine App zur Authentifizierung per Mobilgerät.
- Bei geschäftlichen Konten verwenden **54 %** Benutzername und Passwort, **21 %** verlassen sich auf die Authentifizierung per SMS an ein Mobilgerät und **21 %** nutzen eine Authentifizierung per Mobilgerät.

Diese Ergebnisse deuten darauf hin, dass zwar die Mehrheit der Befragten eine Form der Authentifizierung per Mobilgerät entweder mittels SMS-Nachricht oder mittels Authentifizierungs-Apps nutzt, einige Mitarbeitende jedoch keine Authentifizierung per Mobilgerät verwenden möchten. Dafür gibt es zahlreiche Gründe. Vielleicht möchten sie keine persönlichen Geräte für den Job verwenden oder Administratoren Zugriff auf ihre Geräte geben. Möglicherweise gibt es aber auch Vorgaben seitens einer Gewerkschaft oder Compliance-Anforderungen. Es kann auch sein, dass einige Mitarbeitende nicht einmal in der Lage sind, ein Smartphone zu verwenden. Wenn die Alternativlösung in solchen Fällen dann Benutzernamen und Passwörter sind, macht dies das Unternehmen noch anfälliger für Phishing-Angriffe und Kontoübernahmen.

Die passwortlose Multi-Faktor-Authentifizierung (MFA) bietet eine sichere und benutzerfreundliche Lösung, um gegen derartige Bedrohungen vorzugehen. Da hier keine Passwörter erforderlich sind, wird die Identität bei dieser Methode über alternative Faktoren wie Biometrie oder Hardware-Sicherheitsschlüssel verifiziert. Dadurch wird das Risiko eines unbefugten Zugriffs deutlich reduziert, da es keine Passwörter gibt, die Hacker stehlen oder erraten könnten

Passkeys, oder genauer gesagt Hardware-Sicherheitsschlüssel mit gerätegebundenen Passkeys, sind die Zukunft der Authentifizierung. Hardware-Sicherheitsschlüssel sind eine handfeste Passkey-Lösung und bieten ein Höchstmaß an Schutz vor Phishing-Angriffen, da sie im Vergleich zu Passwörtern weniger anfällig für Diebstähle oder Kompromittierungen sind. Darüber hinaus wird auch die User Experience durch die passwortlose Authentifizierung vereinfacht, da Benutzer sich keine komplexen Passwörter mehr merken müssen. Das führt zu einer höheren Zufriedenheit und Produktivität, vor allem in Unternehmen.

Argumente für Passkeys

> Passkeys sind nicht nur extrem sicher, sondern steigern die Benutzerfreundlichkeit zudem signifikant. Da sich Benutzer keine komplexen Passwörter mehr merken müssen, erfolgt der Anmeldeprozess reibungsloser und es gibt weniger Frust durch vergessene Passwörter.
>
> Dadurch kann die Zufriedenheit und Produktivität der Benutzer steigen, und zwar vor allem in Unternehmen, in denen Mitarbeitende oft mit vielen Konten und Passwörtern arbeiten müssen.
>
> Wenn wir uns die aktuellen Optionen bei Passkeys ansehen, bieten gerätegebundene Sicherheitsschlüssel das höchste Maß an Phishing-Resistenz und erfüllen auch die striktesten Sicherheitsstandards."
>
> **Derek Hanson** | VP Standards and Alliances | Yubico

Was sind Ihrer Meinung nach die sichersten Authentifizierungsmethoden?*

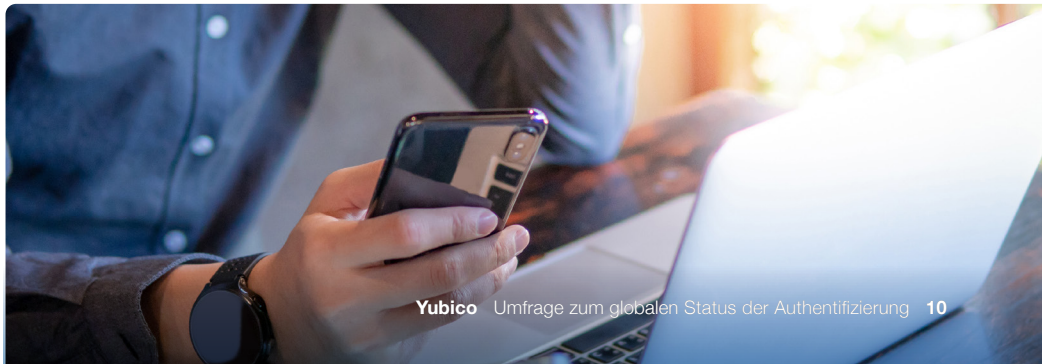
Die fünf häufigsten Antworten

* Multiple answers allowed

Passkeys werden immer beliebter und auch immer häufiger implementiert. Hier ist ein regelrechter Boom zu beobachten, was darauf zurückzuführen ist, dass sie eine breite Unterstützung durch die weltweit größten Technologieunternehmen – die insgesamt betrachtet auch die am weitesten verbreiteten Identitätsprovider sind – erfahren. Das führt dazu, dass Millionen von Benutzern nun beginnen, auf diese Authentifizierungsmethode umzusteigen. Dennoch gibt es nach wie vor viel Aufklärungsbedarf sowohl bei Verbrauchern als auch bei Unternehmen, denn **39 %** der Befragten sind der Meinung, dass Benutzername und Passwort die sicherste Option darstellen. Aus diesem Grund sollten Arbeitgeber ihre Mitarbeitenden dabei unterstützen, mehr über Passkeys – und insbesondere über gerätegebundene Passkeys – zu erfahren, und sie auch dazu schulen, warum Passkeys ein wichtiges Element einer gesunden Vorgehensweise beim Thema Cybersicherheit sind.

Passkeys sind eine neue Authentifizierungsmethode, bei der kryptografische Sicherheits-„Schlüssel" erstellt und dann in der Cloud oder lokal auf dem Gerät des Benutzers gespeichert werden. Diese Methode hat den Vorteil gegenüber Passwörtern, dass Benutzer hier keine langen Zeichenfolgen im Kopf behalten bzw. manuell eingeben müssen, die leicht vergessen, gestohlen oder abgefangen werden können.

Passkeys auf einem Hardware-Sicherheitsschlüssel bieten ein noch höheres Maß an Sicherheit, da sie gerätegebunden (also auf physischer Hardware gespeichert) sind und nicht kopiert werden können oder an einen bestimmten Anbieter gebunden sind. Andere Arten von Passkeys wiederum können synchronisiert werden, was bedeutet, dass sie in der Cloud gespeichert werden. Diese Passkeys sind an eine bestimmte Plattform gebunden und können auf verschiedene Geräte kopiert werden. Es ist wichtig, sich diesen Unterschied bewusst zu machen, da sich Einzelpersonen und Unternehmen weiterhin mit der Einführung von Passkeys auseinandersetzen. Dabei müssen sie herausfinden, was angesichts ihrer jeweiligen Bedrohungen die sicherste Option für den jeweiligen Anwendungsfall ist.



Fazit

Die Ergebnisse dieser Umfrage zeigen, wie wichtig es ist, bei der Cybersicherheit einen stärker integrierten und proaktiven Ansatz zu verfolgen. Die KI entwickelt sich immer weiter und Cyberbedrohungen werden immer ausgeklügelter. Angesichts dessen müssen Einzelpersonen und Organisationen Hand in Hand arbeiten, um auf breiter Front einheitlich gegen diese Risiken vorzugehen.

Unsere Untersuchungen haben aufgedeckt, dass Cyberbedrohungen – und insbesondere jene mit KI-Unterstützung – immer komplexer werden. Folglich bedarf es eines fortschrittlicheren und ganzheitlichen Ansatzes für Cybersicherheit. Offensichtlich gibt es eine erhebliche Kluft zwischen wahrgenommener und tatsächlicher Sicherheit, und zwar sowohl im persönlichen als auch im beruflichen Kontext. Viele Menschen schätzen den Grad ihres Schutzes besser ein, als er tatsächlich ist. Dadurch entstehen Schwachstellen, die Cyberkriminelle ausnutzen können.

Eine einheitliche Cybersicherheitsstrategie, die die Kluft zwischen persönlicher und beruflicher Sicherheit überwindet, ist von entscheidender Bedeutung. Dazu gehört es, Mitarbeitende zu Best Practices zu schulen und zur Nutzung von sichereren Authentifizierungsmethoden wie Hardware-Sicherheitsschlüsseln und Passkeys aufzufordern. Außerdem muss gewährleistet werden, dass Schulungen und Sicherheitsprotokolle konsistent auf allen Ebenen und von allen Mitarbeitenden einer Organisation umgesetzt werden, damit Benutzer Phishing-resistent werden.

Die Cybersicherheitslandschaft befindet sich in einem stetigen Wandel und wird zunehmend gefährlicher. Auf unserem weiteren Weg wird die Einführung von aufkommenden Technologien wie Hardware-Sicherheitsschlüsseln und Passkeys dabei zweifellos eine entscheidende Rolle spielen, wenn es darum geht, unsere digitalen Identitäten und auch die Systeme und Dienste, auf die wir jeden Tag angewiesen sind, zu schützen.

yubico

Über Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO), Erfinder des YubiKey, bietet den Goldstandard für eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA), die Kontoübernahmen vorbeugt und sichere Anmeldungen einfach und für alle möglich macht. Seit seiner Gründung im Jahr 2007 hat das Unternehmen federführend an der Festlegung globaler Standards für den sicheren Zugriff auf Computer, Mobilgeräte, Server, Browser und Internetkonten mitgewirkt. Yubico hat wesentlich zur Entwicklung der offenen Authentifizierungsstandards FIDO2, WebAuthn und FIDO Universal 2nd Factor (U2F) beigetragen. Das Unternehmen ist ein Pionier bei der Bereitstellung einer hardwarebasierten passwortlosen Authentifizierung in Form von hochsicheren Passkeys für Kunden in über 160 Ländern.

Die Lösungen von Yubico ermöglichen eine passwortlose Anmeldung mit der sichersten Form der Passkey-Technologie. YubiKeys funktionieren out-of-the-box mit Hunderten von Verbraucher- und Unternehmensanwendungen und -diensten und vereinen hohe Sicherheit mit Schnelligkeit und Benutzerfreundlichkeit.

Im Rahmen seiner Mission, das Internet für alle sicherer zu machen, spendet Yubico über die gemeinnützige Initiative Secure it Forward YubiKeys an Organisationen, die besonders gefährdete Personen unterstützen. Yubico hat seinen Hauptsitz in Stockholm und Santa Clara, Kalifornien. Für weitere Informationen über Yubico besuchen Sie uns bitte unter www.yubico.com.

Methodik

Diese Umfrage wurde von Talker Research zwischen dem 22. Juli und dem 12. August 2024 durchgeführt. Teilgenommen haben jeweils 2.000 angestellte Erwachsene aus den folgenden Ländern: Vereinigte Staaten, Vereinigtes Königreich, Australien, Indien, Japan, Polen, Singapur, Frankreich, Deutschland und Schweden. Ziel der Umfrage war es, Einblicke in und Auffassungen zu Cybersicherheitspraktiken im persönlichen und beruflichen Kontext zu erhalten, vor allem angesichts aufkommender Bedrohungen.