



Workplace
Password
Malpractice
Report
2021

Exklusiver Studienbericht

Im Auftrag von Keeper Security

 **Pollfish**

© 2021 Keeper Security, Inc. | keeper.io/malpracticereport

Einleitung

Mangelnde Passworthygiene am Arbeitsplatz war schon vor COVID-19 eine Bedrohung für die Cybersicherheit von Unternehmen. Als dann die Pandemie Unternehmen weltweit dazu zwang, ihre Mitarbeitenden von heute auf morgen standortunabhängig einzusetzen und abzusichern, mussten diese aus der Ferne auf Unternehmensressourcen zugreifen, und zwar in Umgebungen außerhalb der Kontrolle ihrer Arbeitgeber und häufig mit ihren privaten Geräten.

Das Ponemon Institute veröffentlichte eine Studie zur internationalen Cybersicherheit im Zeitalter der Telearbeit: **Cybersecurity in the Remote Work Era: A Global Risk Report**, die von Keeper Security im Jahr 2020 in Auftrag gegeben wurde. In dieser Studie äußerten die Befragten ernste Bedenken in Bezug auf die Passwortsicherheit in ihren Unternehmen:

- 60 % der Befragten sagten aus, dass ihr Unternehmen in den vergangenen 12 Monaten einem Cyberangriff ausgesetzt war.
- Bei mehr als 50 % dieser Angriffe wurden Zugangsdaten entwendet.
- Der Diebstahl von IT-Ressourcen verursachte bei 25 % der Unternehmen Schäden von mehr als 5 Millionen US-Dollar.

Die Pandemie drängte Unternehmen dazu, in kürzester Zeit auf neue Technologien umzusteigen, um Mitarbeiter an entfernten Standorten miteinander zu vernetzen und die Zusammenarbeit zu ermöglichen. Von Zoom über Google Workspace bis hin zu Slack mussten Mitarbeiter noch mehr Online-Konten einrichten – und noch mehr Passwörter verwalten.

Keeper stellte sich die Frage, inwieweit sich die Passwortsicherheit verändert hat, seit die Unternehmen auf Remote-Arbeitsumgebungen umgestellt haben. Befolgen Beschäftigte auch an entfernten Standorten die Best Practices zum Schutz ihrer Passwörter, oder fallen sie der „Passwortmüdigkeit“ zum Opfer und setzen sich durch Fehlverhalten erheblichen Cybersicherheitsrisiken aus? Aufgrund dieser Überlegungen führte Keeper in Zusammenarbeit mit Pollfish die Studie zum Passwort-Fehlverhalten am Arbeitsplatz durch.

Während Ponemon seine Befragung in den Führungsetagen von Unternehmen durchführte, beschlossen wir, direkt an die Beschäftigten heranzutreten, und befragten 1.000 Vollzeitbeschäftigte in den Vereinigten Staaten zu ihren Passwortgewohnheiten. Die im Februar 2021 abgeschlossene Studie wandte sich ausschließlich an Personen, die Passwörter für die Anmeldung bei beruflich genutzten Online-Konten verwenden.

Im Anschluss sind die wichtigsten Ergebnisse der Befragung aufgeführt. Die ausführlichen Daten finden Sie ab Seite 6.

1. Erkenntnis: US-amerikanische Beschäftigte achten beim Organisieren und Speichern ihrer Anmeldedaten nicht auf Sicherheit.

Unsere Befragung ergab, dass Angestellte in den USA beim Organisieren und Speichern ihrer arbeitsbezogenen Passwörter nicht die bewährten Praktiken befolgen, was für ihre Arbeitgeber ein erhebliches Cybersicherheitsrisiko darstellt.

- Mehr als die Hälfte der Befragten (57 %) gab zu, Passwörter für beruflich genutzte Online-Konten auf Notizzettel zu schreiben, und zwei Drittel (67 %) gestanden, diese Zettel schon einmal verloren zu haben. Dies führt nicht nur dazu, dass sensible Firmendaten für jeden Bewohner oder Besucher der Wohnung einsehbar sind, sondern schadet auch der unternehmerischen Effizienz. Verlorene Notizzettel bedeuten verlorene Passwörter, wodurch Helpdesk-Tickets erstellt und Passwörter zurückgesetzt werden müssen.
- 62 % der Befragten schreiben ihre Anmeldedaten in ein Notizbuch, und die überwiegende Mehrheit (82 %) gab an, diese Notizbücher neben oder in der Nähe ihrer Arbeitsgeräte aufzubewahren, sodass jeder Bewohner oder Besucher der Wohnung darauf zugreifen kann.

Die Verwendung von Stift und Papier zum Notieren von Passwörtern ist in der Welt der Telearbeit noch problematischer geworden. Die meisten Beschäftigten (66 %) gaben an, dass sie im Home-Office arbeitsbezogene Passwörter eher aufschreiben als bei der Arbeit im Büro.

US-amerikanische Beschäftigte nutzen zwar digitale Lösungen zum Organisieren und Speichern von Passwörtern, die Praktiken im Hinblick auf die Passwortsicherheit sind jedoch mangelhaft.

- Fast die Hälfte der Befragten (49 %) speichert arbeitsbezogene Passwörter in einem Dokument in der Cloud.
- Knapp über die Hälfte (51 %) gab an, diese Passwörter in einer Datei auf ihrem PC hinterlegt zu haben.
- 55 % speichern arbeitsbezogene Passwörter auf ihrem Telefon.

Das Speichern von Passwörtern in unverschlüsselten Dateien ist extrem risikobehaftet. Ein Cyberkrimineller braucht also nur in den Cloud-Speicher, den Computer oder das mobile Gerät einzudringen, und schon hat er Zugriff auf alle Passwörter des Mitarbeiters.

2. Erkenntnis: US-amerikanische Beschäftigte erstellen schwache, einfach herauszufindende Passwörter.

Ein starkes Passwort besteht aus einer zufälligen Aneinanderreihung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Dennoch gaben viele Befragte zu, Passwörter zu verwenden, die personenbezogene Daten enthalten, die von Cyberkriminellen ohne Weiteres in den sozialen Netzwerken ausfindig gemacht werden können.

- Mehr als ein Drittel (37 %) der Befragten hat den Namen ihres Arbeitgebers in einem arbeitsbezogenen Passwort verwendet.

- Mehr als ein Drittel (34 %) hat den Namen oder das Geburtsdatum ihrer Lebensgefährtin bzw. ihres Lebensgefährten verwendet.
- Knapp ein Drittel (31 %) hat den Namen oder das Geburtsdatum eines ihrer Kinder verwendet.

Die Nutzung derselben Passwörter für privat und beruflich genutzte Konten ist für Unternehmen mittlerweile ein erhebliches Cybersicherheitsrisiko. 44 % der Befragten gaben zu, dieselben Passwörter für privat und beruflich genutzte Konten zu verwenden, und 53 % sagten aus, passwortgeschützte private Konten auch von ihren Arbeitsgeräten aus abzurufen.

3. Erkenntnis: US-amerikanische Beschäftigte teilen ihre arbeitsbezogenen Passwörter mit unbefugten Dritten.

Viele US-amerikanische Beschäftigte achten nicht sorgfältig darauf, mit wem sie ihre arbeitsbezogenen Passwörter teilen. Dies bringt Unternehmen in Gefahr, wenn diese Passwörter in die Hände von Personen mit mangelnder Aufmerksamkeit oder böswilligen Absichten gelangen.

- Im Laufe des vergangenen Jahres haben 14 % der Befragten ihre arbeitsbezogenen Passwörter mit ihrer Lebensgefährtin bzw. mit ihrem Lebensgefährten geteilt.
- 11 % der Befragten haben arbeitsbezogene Passwörter mit einem anderen Familienmitglied geteilt.

Selbst wenn keine Datenschutzverletzung vorliegt, könnte es dazu führen, dass die Compliance des Arbeitgebers nicht gegeben ist, und es könnten hohe Sanktionen verhängt werden, wenn sich herausstellt, dass Unbefugte Einblick in vorschriftsmäßig geschützte Daten genommen haben.

4. Erkenntnis: US-amerikanische Arbeitgeber leisten keinen Beitrag, um zu gewährleisten, dass Passwörter auf sicherem Wege und/oder nur mit befugten Personen geteilt werden.

Unserer Befragung zufolge ist es eine gängige Praxis, Passwörter am Arbeitsplatz mit anderen zu teilen.

- Fast die Hälfte der Befragten (46 %) verwies darauf, dass ihre Unternehmen Passwörter an mehrere Mitarbeitende zur gemeinsamen Nutzung von Konten freigibt.
- Mehr als ein Drittel (34 %) hat arbeitsbezogene Passwörter mit Kollegen desselben Teams geteilt.
- Knapp ein Drittel (32 %) hat arbeitsbezogene Passwörter mit ihren Vorgesetzten geteilt.
- 19 % haben ihre Passwörter mit ihrer Geschäftsleitung geteilt.

Am besten wäre es, jedem Benutzer ein eindeutiges Passwort für jedes beruflich genutzte Konto bzw. jede Anwendung zu geben, was in der Praxis mit Hilfe einer Enterprise Password Management-Plattform (EPM) umgesetzt werden kann. Der gemeinsamen Passwortnutzung am Arbeitsplatz ist nichts entgegenzusetzen, solange die Passwörter sicher und nur mit befugten Personen geteilt werden. Die Ergebnisse unserer Studie zeigen, dass viele US-amerikanische Arbeitgeber keine risikomindernden Strategien einsetzen, um die sichere Nutzung geteilter Passwörter zu gewährleisten.

- Die Mehrheit der Befragten (62 %) berichtet, dass sie arbeitsbezogene Passwörter per SMS oder E-Mail weitergeben. Dabei können diese von Cyberkriminellen auf dem Übertragungsweg abgefangen werden.
- Knapp ein Drittel der Befragten (32 %) gab zu, bereits auf ihr Online-Konto bei einem früheren Arbeitgeber zugegriffen zu haben, was darauf hindeutet, dass viele Arbeitgeber die Konten nicht sperren, wenn Mitarbeiter das Unternehmen verlassen.

Fazit

Durch die Einführung und Nutzung einer Passwortmanagement-Plattform, wie Keeper Enterprise, können Unternehmen die in dieser Studie aufgedeckten Passwort-Fehlpraktiken beseitigen. Die Zero Knowledge-Passwort-Verschlüsselung und das Zero Trust-Framework von Keeper ermöglichen eine effiziente Passwortverwaltung, die gesicherte Passwortfreigabe an mehrere Nutzer und andere nützliche Sicherheitsfunktionen. IT-Administratoren und Manager erhalten vollständige Transparenz und Kontrolle über die Passwortpraktiken aller Beschäftigten, einschließlich:

- Exklusives, proprietäres Zero Knowledge-Sicherheitsmodell und Zero Trust-Framework-System; alle Daten sind bei der Übertragung und im Ruhezustand verschlüsselt und können weder von Mitarbeitern von Keeper Security noch von Außenstehenden eingesehen werden.
- Schnelle Einrichtung auf allen Geräten, ohne dass zuvor in teure Ausrüstung investiert werden muss, und ohne Installationskosten.
- Personalisiertes Onboarding, 24/7-Support und Training durch Support-Fachpersonal.
- Unterstützung von RBAC, 2FA, Auditing, Event-Reporting und zahlreichen Compliance-Standards, darunter HIPAA, DPA, FINRA und GDPR.
- Bereitstellung von gesicherten gemeinsamen Ordnern, Unterordnern und Passwörtern für Teams.
- Single Sign-On-Authentifizierung (SAML 2.0)
- Aktivierung des Offline-Zugriffs auf den Datentresor (Vault), wenn SSO nicht verfügbar ist.
- Dynamische Bereitstellung von Vaults über SCIM.
- Konfiguration für Hochverfügbarkeit (High Availability, HA).
- Erweiterte Zwei-Faktor-/Multi-Faktor-Authentifizierung
- Synchronisierung mit Active Directory und LDP
- Bereitstellung von SCIM und Azure AD
- Entwickler-APIs für Passwortrotation und Backend-Integration

Ergebnisse der Studie

NUR EINE ANTWORT MÖGLICH

SF1. Sind Sie gegenwärtig Vollzeit beschäftigt?

#	Antworten	Antworten (%)	Zähler
A1	Ja	100,00%	1000
A2	Nein	0,00%	0

NUR EINE ANTWORT MÖGLICH

SF2. Verwenden Sie gegenwärtig Passwörter, um sich bei beruflichen Online-Konten anzumelden?

#	Antworten	Antworten (%)	Zähler
A1	Ja	100,00%	1000
A2	Nein	0,00%	0

NUR EINE ANTWORT MÖGLICH

F1. Haben Sie derzeit Notizzettel, auf denen arbeitsbezogene Online-Passwörter stehen?

#	Antworten	Antworten (%)	Zähler
A1	Ja	57,30%	573
A2	Nein	42,70%	427

NUR EINE ANTWORT MÖGLICH

Q2. Wenn ja, ist Ihnen schon einmal ein Notizzettel verloren gegangen?

#	Antworten	Antworten (%)	Zähler
A1	Ja	66,55%	382
A2	Nein	33,45%	192

NUR EINE ANTWORT MÖGLICH

F3. Schreiben Sie sich arbeitsbezogene Online-Passwörter häufiger auf, wenn Sie von zu Hause aus arbeiten?

#	Antworten	Antworten (%)	Zähler
A1	Ja	66,00%	660
A2	Nein	34,00%	340

NUR EINE ANTWORT MÖGLICH

F4. Bewahren Sie Ihre Anmeldedaten und Passwörter gegenwärtig in einem Notizbuch auf?

#	Antworten	Antworten (%)	Zähler
A1	Ja	62,10%	621
A2	Nein	37,90%	379

NUR EINE ANTWORT MÖGLICH

F5. Wenn ja, befindet sich dieses Notizbuch neben Ihrem Arbeitsgerät oder in nächster Umgebung?

#	Antworten	Antworten (%)	Zähler
A1	Ja	81,79%	512
A2	Nein	18,21%	114

NUR EINE ANTWORT MÖGLICH

F6. Speichern Sie gegenwärtig arbeitsbezogene Passwörter in einem Dokument in der Cloud?

#	Antworten	Antworten (%)	Zähler
A1	Ja	48,90%	489
A2	Nein	51,10%	511

NUR EINE ANTWORT MÖGLICH

F7. Speichern Sie gegenwärtig arbeitsbezogene Passwörter in einem Dokument auf Ihrem PC/Desktop?

#	Antworten	Antworten (%)	Zähler
A1	Ja	50,60%	506
A2	Nein	49,40%	494

NUR EINE ANTWORT MÖGLICH

F8. Speichern Sie gegenwärtig arbeitsbezogene Passwörter in Ihrem Telefon?

#	Antworten	Antworten (%)	Zähler
A1	Ja	54,70%	547
A2	Nein	45,30%	453

NUR EINE ANTWORT MÖGLICH

F9. Haben Sie arbeitsbezogene Passwörter schon einmal per SMS oder E-Mail versendet?

#	Antworten	Antworten (%)	Zähler
A1	Ja	38,10%	381
A2	Nein	61,90%	619

MEHRERE ANTWORTEN MÖGLICH

F10. Mit wem haben Sie im vergangenen Jahr Ihre arbeitsbezogenen Passwörter gemeinsam genutzt (bitte alles Zutreffende auswählen)?

Ⓞ Der Prozentwert (Befragte) berechnet sich aus der Anzahl der Antworten, geteilt durch die Gesamtzahl der Befragten.

Der Prozentwert (Antworten) berechnet sich aus der Anzahl der Antworten, geteilt durch die Gesamtzahl der erfassten Antworten.

#	Antworten	Befragte (%)	Antworten (%)	Zähler
A1	Kollegen im selben Team	34,40%	18,86%	344
A2	Kollegen in anderen Abteilungen	13,10%	7,18%	131
A3	Vorgesetzte	31,70%	17,38%	317
A4	Geschäftsleitung	18,50%	10,14%	185
A5	Ehemalige Kollegen	6,90%	3,78%	69
A6	Lebensgefährte/in oder Ehepartner/in	14,40%	7,89%	144
A7	Kind	7,90%	4,33%	79
A8	Anderes Familienmitglied	10,60%	5,81%	106
A9	Freund/in, mit der/dem ich nicht arbeite	4,70%	2,58%	47
A10	Keine der genannten Optionen	37,60%	20,61%	376
A11	Sonstiges	2,60%	1,43%	26

NUR EINE ANTWORT MÖGLICH

F11. Haben Sie sich schon einmal bei einem Online-Konto Ihres früheren Arbeitgebers angemeldet, nachdem Sie das Unternehmen verlassen hatten?

#	Antworten	Antworten (%)	Zähler
A1	Ja	32,40%	324
A2	Nein	67,60%	676

NUR EINE ANTWORT MÖGLICH

F12. Haben Sie beim Erstellen eines neuen Passworts für ein berufliches Konto den Namen Ihres Unternehmens verwendet?

#	Antworten	Antworten (%)	Zähler
A1	Ja	36,70%	367
A2	Nein	63,30%	633

NUR EINE ANTWORT MÖGLICH

F13. Gibt Ihr Unternehmen Passwörter für Konten frei, die von mehreren Mitarbeitenden genutzt werden?

#	Antworten	Antworten (%)	Zähler
A1	Ja	46,10%	461
A2	Nein	53,90%	539

NUR EINE ANTWORT MÖGLICH

F14. Enthalten Ihre arbeitsbezogenen Passwörter, die von mehreren Mitarbeitern verwendet werden, den Namen des Unternehmens?

#	Antworten	Antworten (%)	Zähler
A1	Ja	33,80%	338
A2	Nein	47,20%	472
A3	Das trifft auf mich nicht zu	19,00%	190

NUR EINE ANTWORT MÖGLICH

F15. Verwenden Sie gegenwärtig dasselbe Passwort für privat und beruflich genutzte Konten?

#	Antworten	Antworten (%)	Zähler
A1	Ja	43,70%	437
A2	Nein	56,30%	563

NUR EINE ANTWORT MÖGLICH

F16. Enthält eines Ihrer arbeitsbezogenen Passwörter den Namen oder das Geburtsdatum Ihrer Lebensgefährtin oder Ihres Lebensgefährten?

#	Antworten	Antworten (%)	Zähler
A1	Ja	34,20%	342
A2	Nein	65,80%	658

NUR EINE ANTWORT MÖGLICH

F17. Enthält eines Ihrer arbeitsbezogenen Passwörter den Namen oder das Geburtsdatum Ihres Kindes?

#	Antworten	Antworten (%)	Zähler
A1	Ja	31,40%	314
A2	Nein	52,00%	520
A3	Ich habe keine Kinder	16,60%	166

NUR EINE ANTWORT MÖGLICH

F18. Haben sich Ihre Kinder schon einmal bei Ihren beruflichen Konten oder Programmen angemeldet oder darauf zugegriffen?

#	Antworten	Antworten (%)	Zähler
A1	Ja	20,60%	206
A2	Nein	59,40%	594
A3	Ich habe keine Kinder	20,00%	200

NUR EINE ANTWORT MÖGLICH

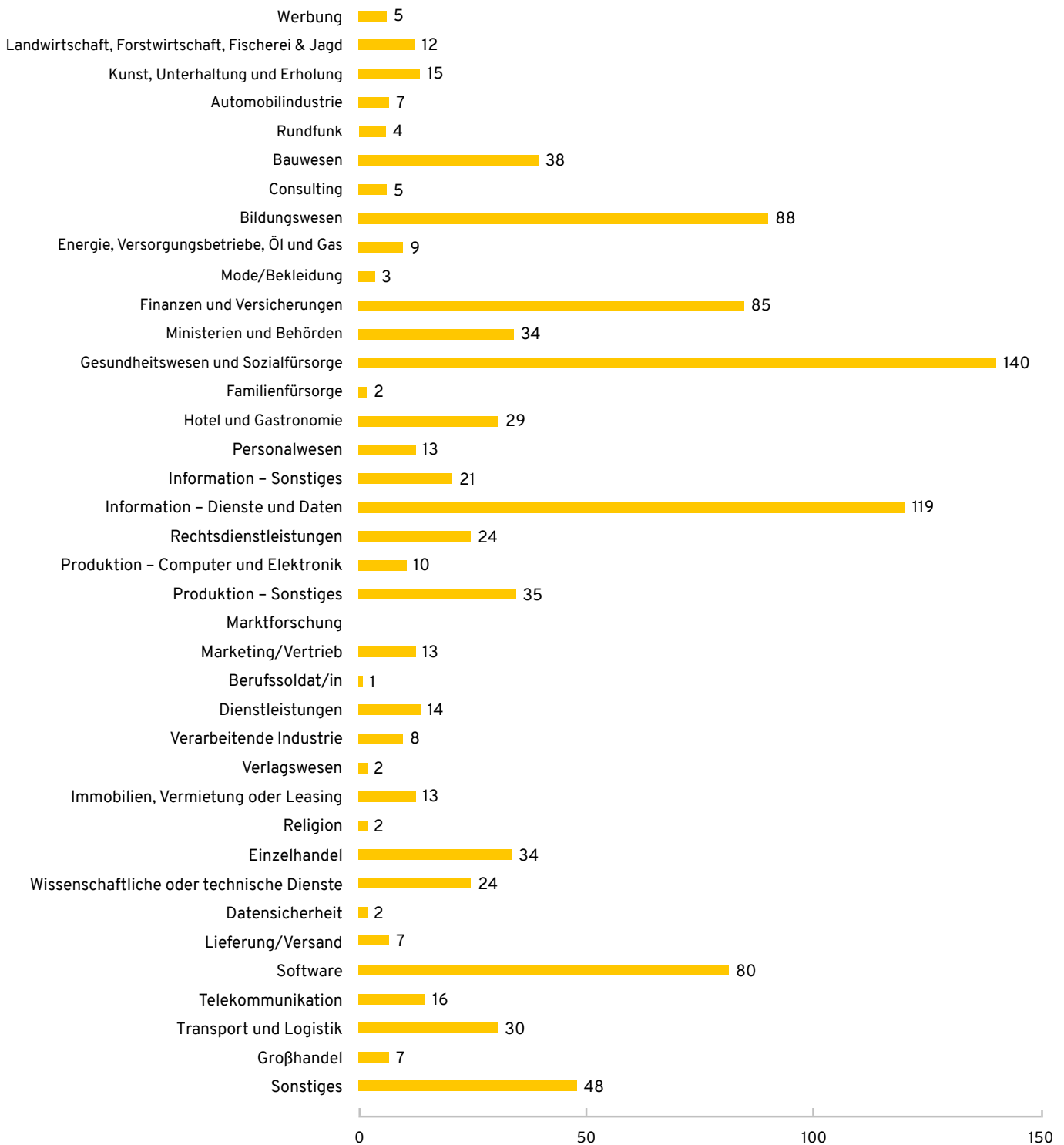
F19. Haben Sie passwortgeschützte private Konten auf Ihrem Arbeitsgerät gespeichert?

#	Antworten	Antworten (%)	Zähler
A1	Ja	53,35%	534
A2	Nein	46,65%	467

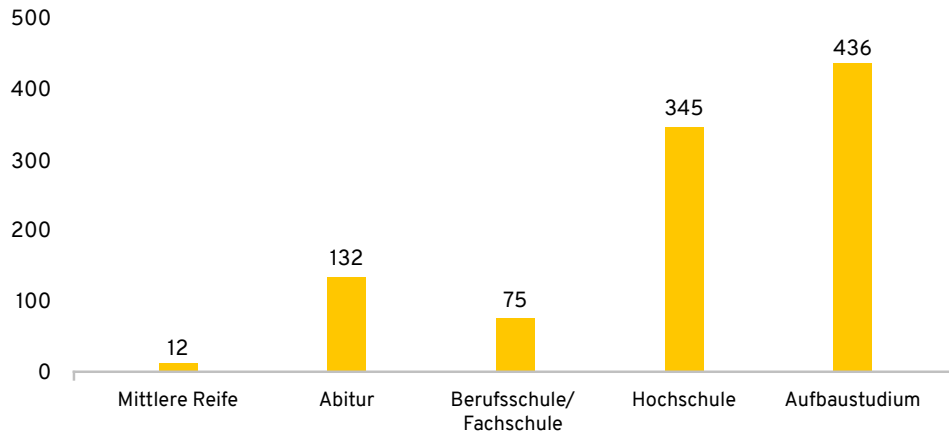
Demografische Daten der Studienteilnehmer

Anzahl der Befragten: 1000

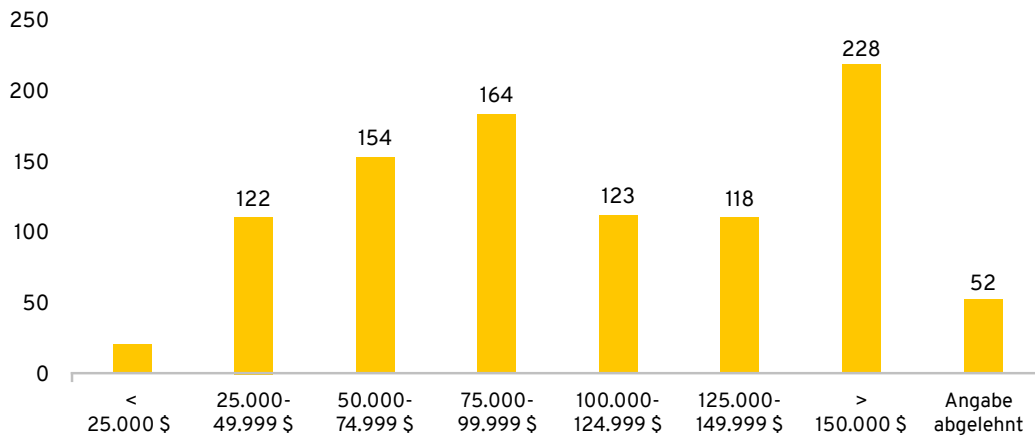
Branche



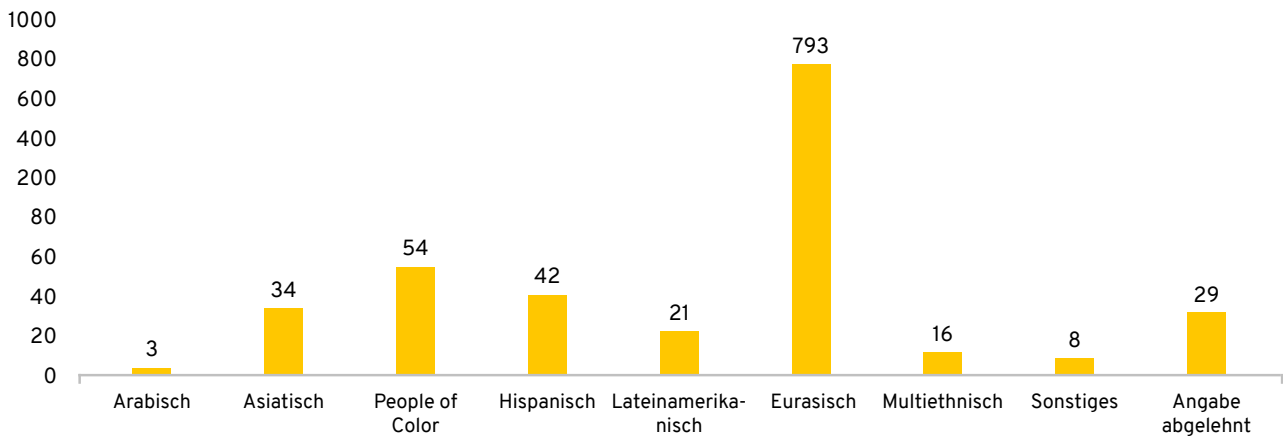
Bildungsgrad



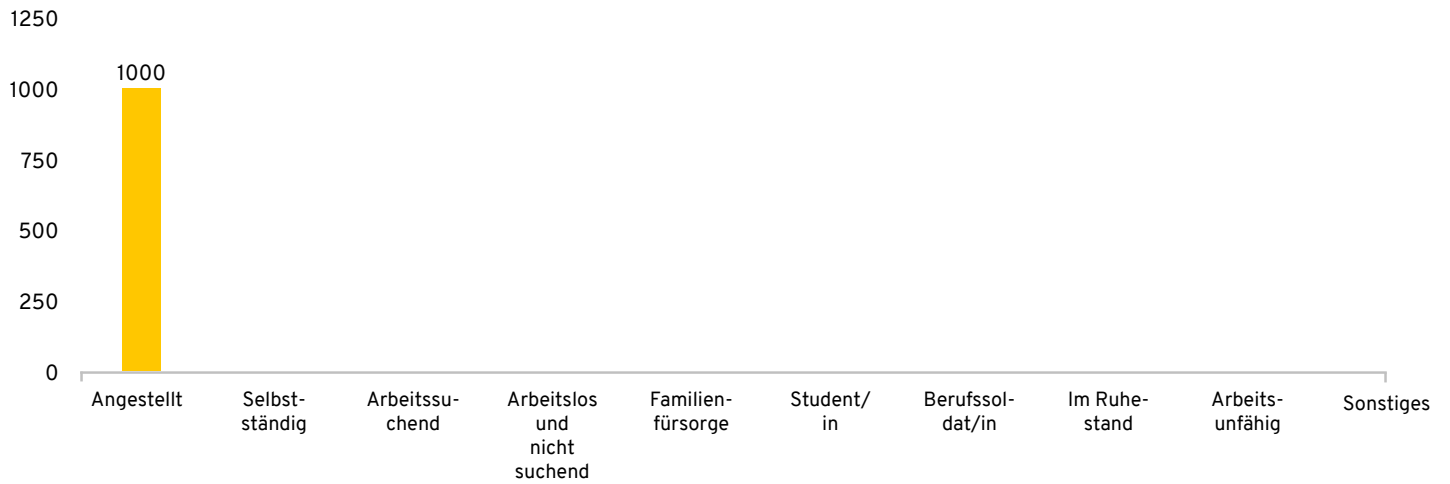
Einkommen



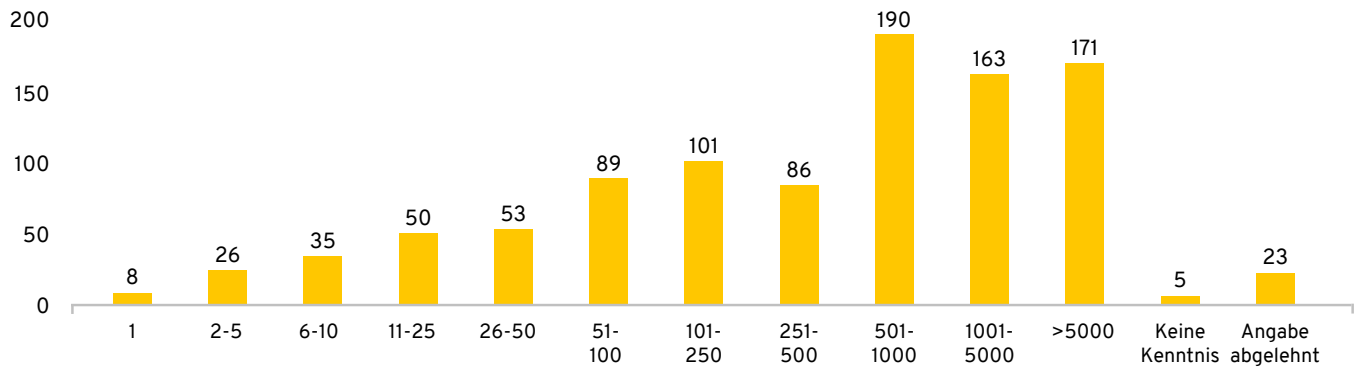
Ethnische Zugehörigkeit



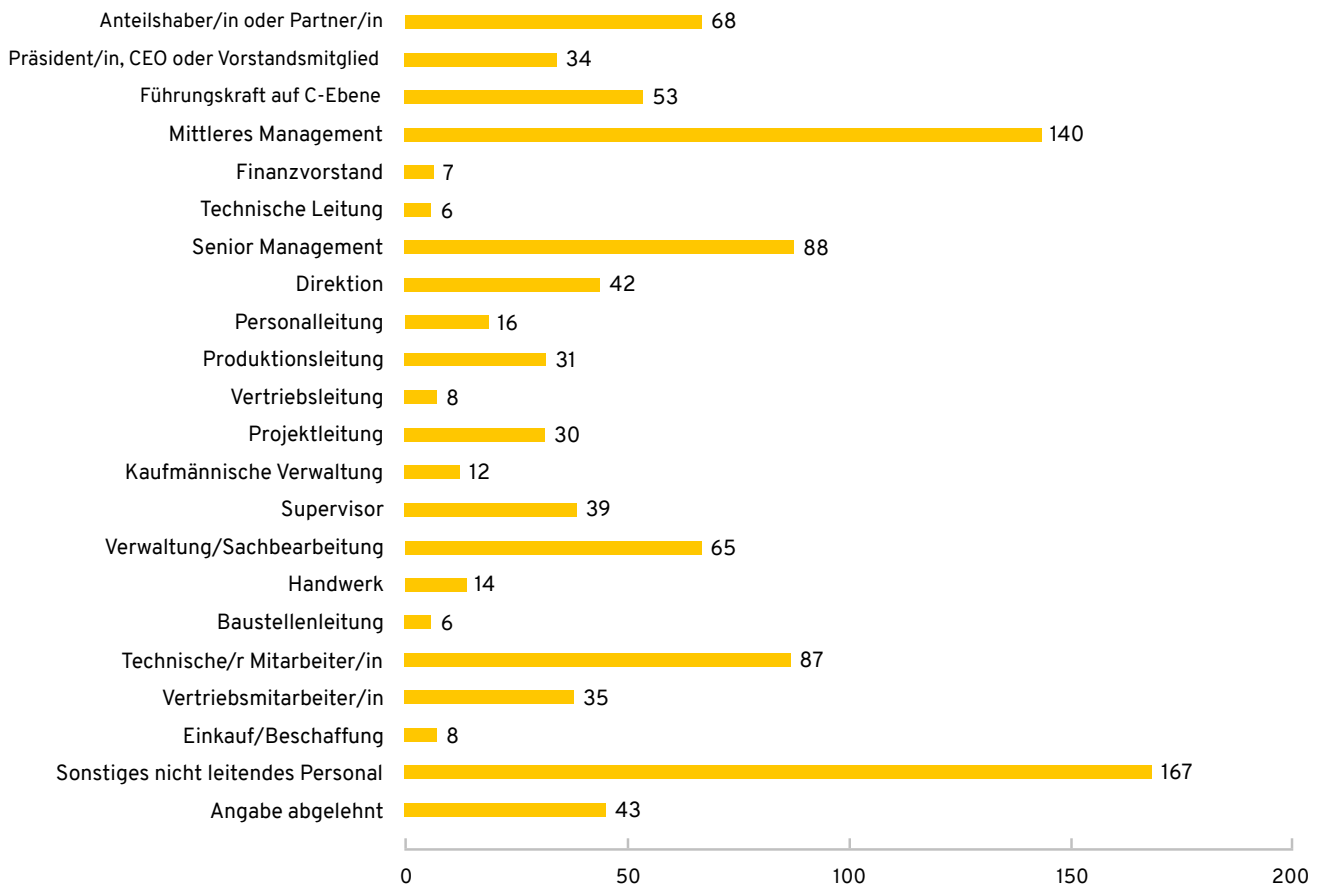
Beschäftigungsstatus



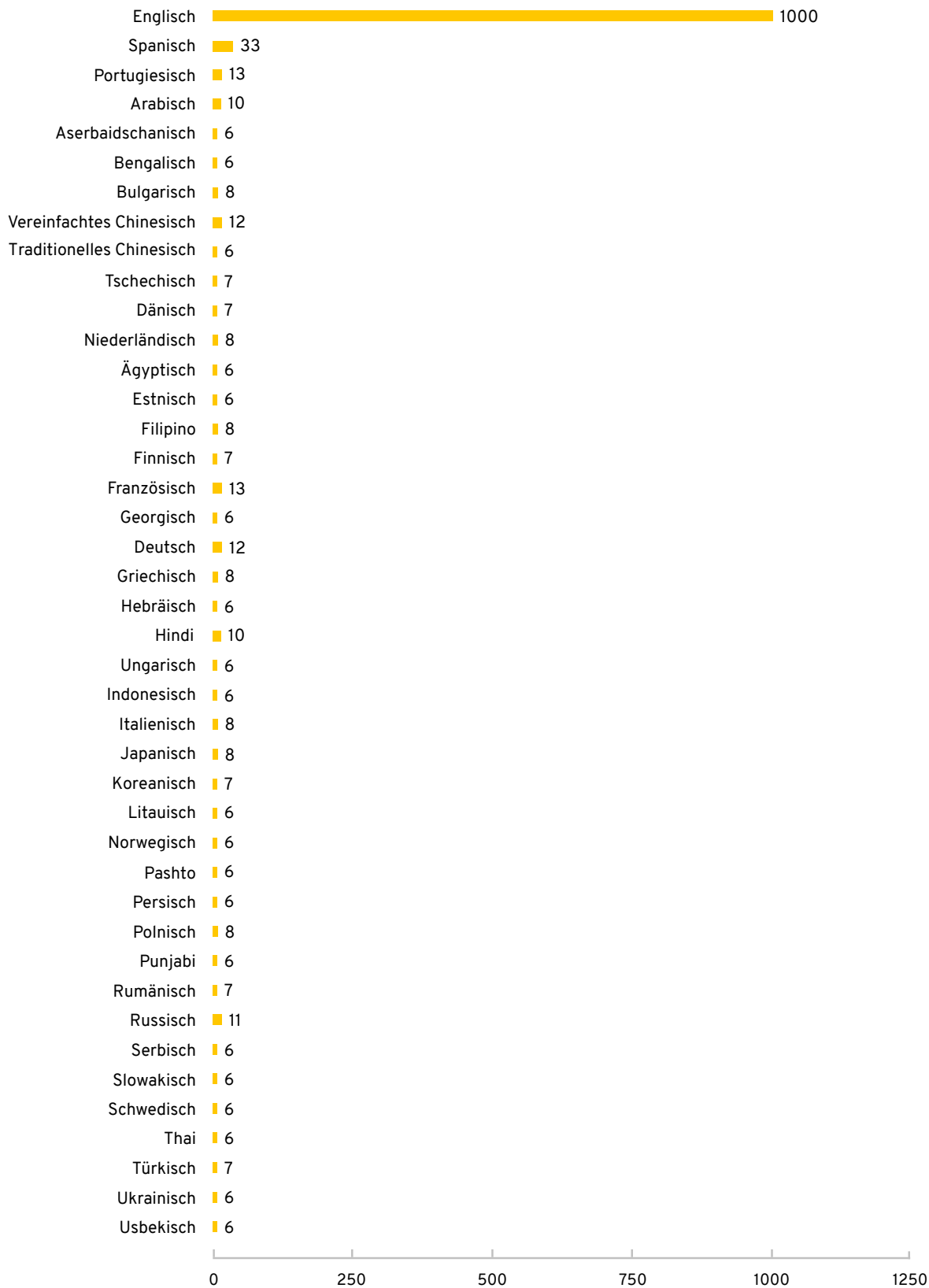
Beschäftigtenzahl



Funktion im Unternehmen



Gesprochene Sprachen



Bewertungen und Auszeichnungen

Keeper wurde vom PC Magazine als „Best Password Manager of the Year & Editors' Choice“ und von PCWorld zwei Jahre in Folge als „Editors' Choice“ ausgezeichnet und erhielt vier G2-Awards für die beste Software und vier InfoSec-Awards für das beste Produkt im Bereich der Passwortverwaltung für KMU und das beste Produkt für KMU-Cybersicherheit. Keeper ist nach SOC-2 und ISO 27001 zertifiziert und für die Nutzung durch die US-Bundesregierung über das System for Award Management (SAM) gelistet.



Gartner Peer Insights
4,9 von 5 Sternen



Spiceworks
5 von 5 Sternen





Editors' Choice
4,5 von 5 Sternen







2020 Enterprise Leader
4,7 von 5 Sternen



-  **Publisher's Choice für Cybersicherheit und Passwortverwaltung**
-  **Cutting Edge Chief Executive des Jahres**



-  **Bestes Produkt im Bereich der Passwortverwaltung**
-  **Bestes Produkt für KMU-Cybersicherheit**
-  **Publisher's Choice für Chief Executive des Jahres**
-  **Innovativster CTO des Jahres**



Bester Passwort-Manager des Jahres
Editors' Choice 2019 und 2020



Editors' Choice 2018 und 2019



Für den Download der Studie zum Passwort-Fehlverhalten am Arbeitsplatz, einer Infografik oder sonstiger Informationen besuchen Sie unseren Ressourcen-Hub. Mehr Informationen zu Keeper Security oder darüber, wie Sie Ihr Unternehmen vor passwortbezogenen Datendiebstählen schützen können, finden Sie unter keepersecurity.com.

Methodik

Keeper Security beauftragte Pollfish mit der Durchführung dieser Befragung unter 1.000 Vollzeitbeschäftigten in den USA. Erfasst wurden nur Personen, die Passwörter verwenden, um sich bei beruflich genutzten Online-Konten anzumelden. Die Studie wurde im Februar 2021 abgeschlossen.

Über Keeper Security, Inc.

Keeper Security, Inc. (Keeper) ist eine anerkannte und patentierte Cybersicherheitsplattform zur Vermeidung passwortbezogener Datenverletzungen und Cyberbedrohungen. Millionen von Menschen und Tausende von Unternehmen weltweit vertrauen auf die Zero Knowledge-Sicherheits- und Verschlüsselungssoftware von Keeper, um das Risiko von Cyberdiebstahl zu mindern, die Mitarbeiterproduktivität zu steigern und Compliance-Standards zu erfüllen. 2020 wurde Keeper von PCMag drittmalig zum besten Passwortmanager des Jahres & Editors' Choice gekürt. Keeper erhielt auch von PCWorld den Editors' Choice-Award und wurde von G2 bereits viermal für die beste Software und von InfoSec für das beste Produkt im Bereich Passwortmanagement für KMU-Cybersicherheit ausgezeichnet. Keeper ist nach SOC-2 und ISO 27001 zertifiziert und für die Nutzung durch die US-Bundesregierung über das System for Award Management (SAM) gelistet.