ivanti

Cybersicherheitsbericht Zum Thema Remote-Work

2020

ÜBERSICHT

Secure Access-Lösungen halten Unternehmen am Laufen, indem sie sicheres Remote- Computing ermöglichen und Menschen und Geräte mit dem Rechenzentrum und Cloud- Anwendungen verbinden – selbst unter den unvorhersehbarsten Umständen.

Als sich die Auswirkungen des Coronavirus (COVID-19) verstärkten und zu einer Pandemie wurden, empfahl die Weltgesundheitsorganisation den Menschen, von zu Hause aus zu arbeiten und als Vorsichtsmaßnahme öffentliche Verkehrsmittel und Büroumgebungen zu meiden, um die Ausbreitung und das Risiko einer Infektion zu verringern.

Zu Beginn des Jahres 2020 begannen Regierungs- und Verwaltungsbeamte auf der ganzen Welt damit, den Bürgern zu raten und sie aufzufordern, zuhause zu bleiben und die Arbeit vor Ort einzustellen, sofern es sich nicht um wichtige Geschäfte handelt. Unternehmen leiteten sofortige Maßnahmen ein, um die Möglichkeiten des Home-Office (WFH – Work From Home) zu erweitern und zu erleichtern.

Abgesehen von den potenziellen Auswirkungen auf die Produktivität der Benutzer bedrohten diese Verlagerung des Arbeitsplatzes und der schnelle Bedarf an Remote- Arbeitskapazitäten die IT-Infrastruktur, die Geschäftskontinuität und die Informationssicherheit.

Der 2020 Remote Work From Home Report, der von Pulse Secure gesponsert und von Cybersecurity Insiders erstellt wurde, bietet eine detaillierte Perspektive auf die Umstellung von Mitarbeitern und Ressourcen in Unternehmen und zeigt die Herausforderungen, Bedenken, Strategien und erwarteten Ergebnisse der WFH-Cybersicherheit auf. Für die Umfrage, die im Mai 2020 durchgeführt wurde, wurden über 400 IT-Sicherheitsentscheider, Praktiker und Unternehmen unterschiedlicher Größe aus verschiedenen Branchen befragt. Die Umfrage ergab, dass 84 % der Unternehmen mit einer breiteren und dauerhaften Remote-Arbeit rechnen und fast ein Drittel plant, ihr Budget für sicheren Zugang in naher Zukunft zu erhöhen.

Zu den wichtigsten Ergebnissen gehören:

- Mehr als dreifache Steigerung der WFH-Benutzerkapazitäten mit über 75 % der Organisationen, die eine nahezu 100 %ige Abdeckung bieten
- 33 % der Unternehmen waren unzureichend auf den sicheren Fernzugriff im Notfall vorbereitet
- 54 % werden mehr Arbeitsabläufe und Anwendungen in die Cloud verlagern
- 38 % der Unternehmen erlebten Produktivitätssteigerungen und andere Vorteile
- 84 % erwarten breitere und dauerhafte WFH-Programme
- Mehr als die Hälfte erwartet in den nächsten zwölf Monaten (nach April 2020) eine Erhöhung des Budgets für sicheren Zugang
- 66 % erwarten erhöhte WFH-Sicherheitsbedrohungen und 63 % gehen davon aus, dass WFH Compliance-Risiken mit sich bringen könnte
- Malware, Phishing, unbefugter Benutzer- und Gerätezugriff sowie ungepatchte Systeme wurden als die höchsten WFH-Angriffsvektoren wahrgenommen
- Anti-Virus/Malware, Firewall, SSL VPN, Multi-Faktor-Authentifizierung und Backup waren die am häufigsten eingesetzten Lösungen zur Gewährleistung der WFHSicherheit/ Business Resiliency

Vielen Dank an Pulse Secure für die Unterstützung dieses wichtigen Forschungsprojekts.

Wir hoffen, dass Sie diesen Bericht informativ und hilfreich finden, um Ihre IT-Investitionen zu abzusichern, Geschäftskontinuität zu gewährleisten und Ihre Mitarbeiter zu schützen.

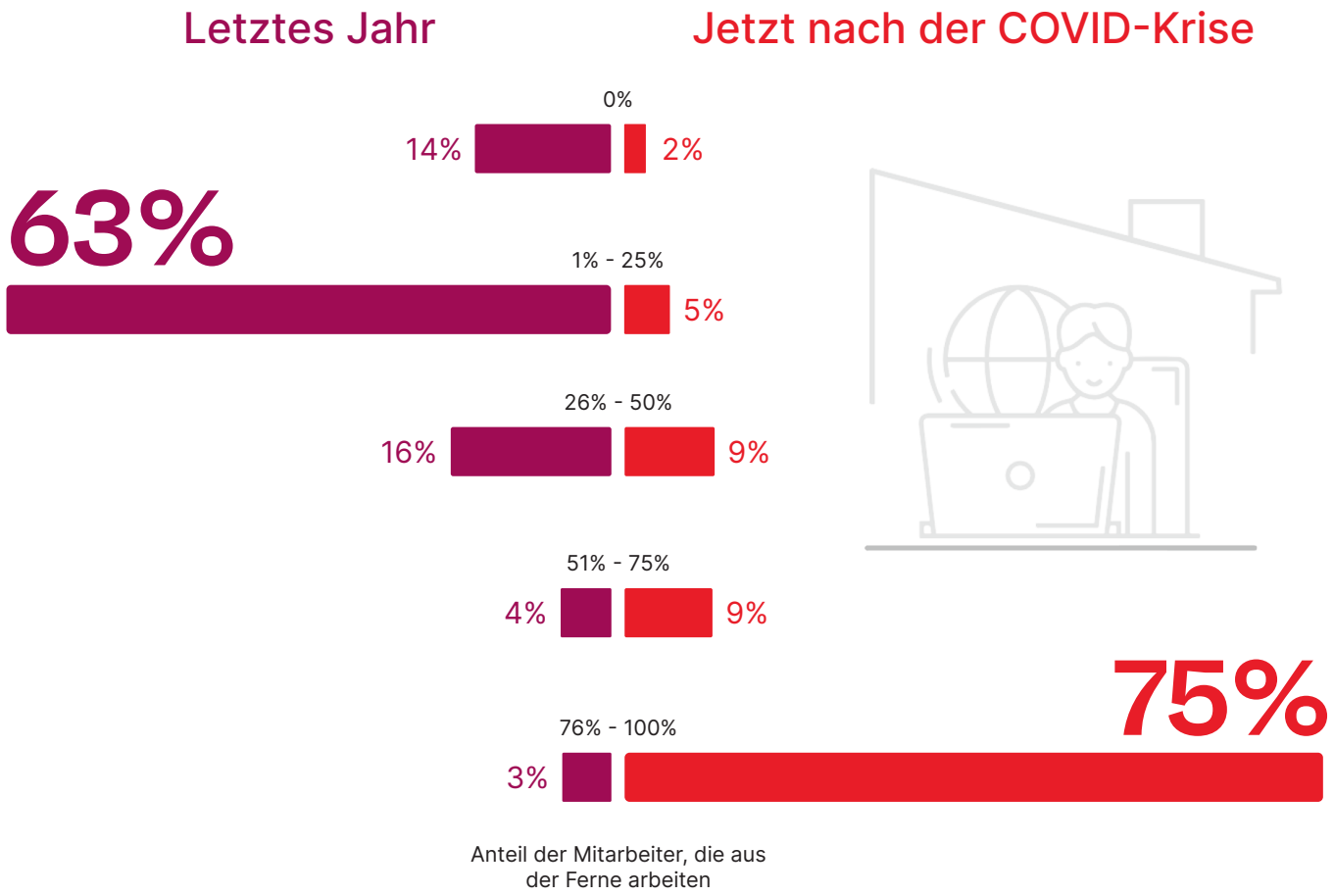
Danke!

Holger Schulze
CEO und Gründer
Cybersecurity Insiders

Explosive Zunahme Bei Remote-Arbeitskräften

Die Umfrage zeigt eine massive Verschiebung hin zu Remote- und Heimarbeitsplätzen aufgrund der COVID-19-Pandemie. Während eine Mehrheit von 63 % der Unternehmen vor der Krise bis zu einem Viertel der Mitarbeiter in Remote-/Heimarbeitsumgebungen arbeiten ließ, berichten satte drei Viertel derselben Unternehmen, dass nun über 75 % ihrer Belegschaft von zu Hause aus arbeiten.

Wie viel Prozent Ihrer Belegschaft hat LETZTES JAHR im Vergleich zu JETZT während der COVID-Krise per Fernzugriff/zu Hause gearbeitet?

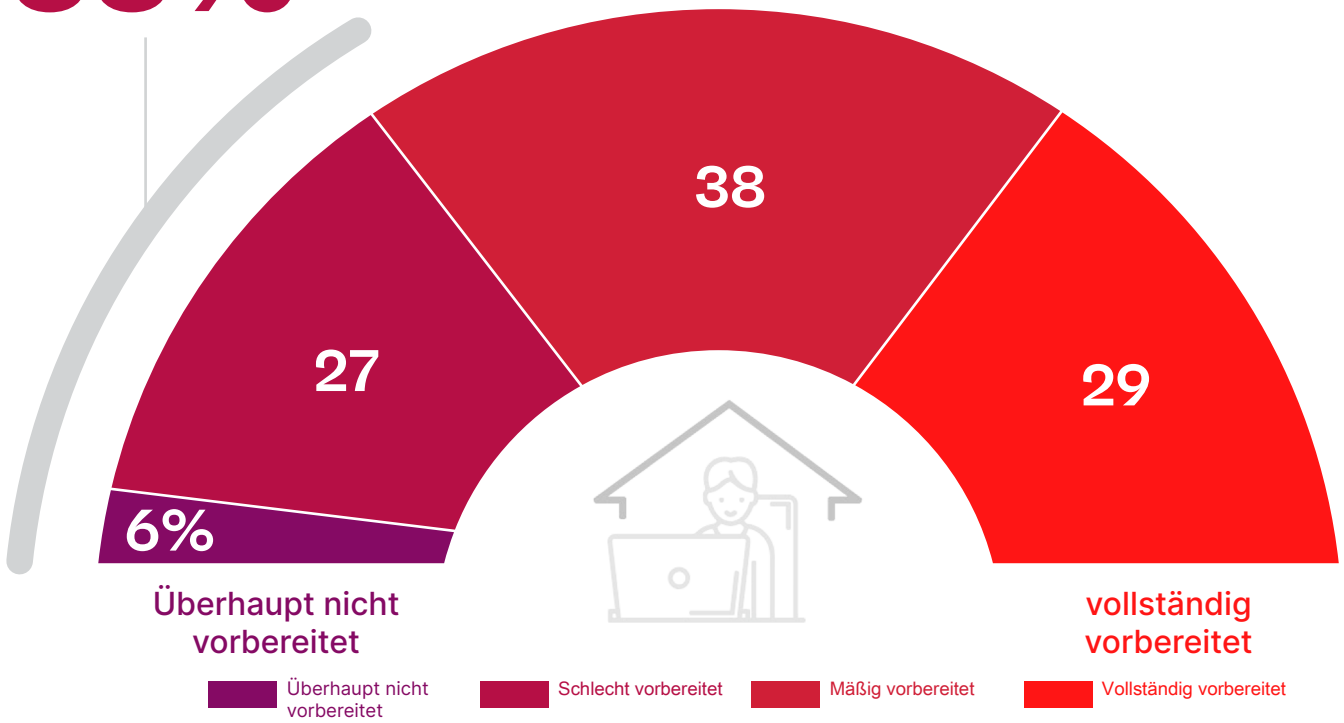


Bereitschaft Zur Fernarbeit

Ein Drittel der Unternehmen berichtet, dass sie nicht ausreichend auf den schnellen Wechsel von On-Premises- zu Remote-Arbeitsszenarien vorbereitet waren.

Wie gut war Ihr Unternehmen vor der COVID-19-Pandemie mit einem Unternehmenskontinuitäts/Notfall-Plan vorbereitet, der eine schnelle Umstellung von Mitarbeitern vor Ort auf Mitarbeiter an anderen Standorten vorsah?

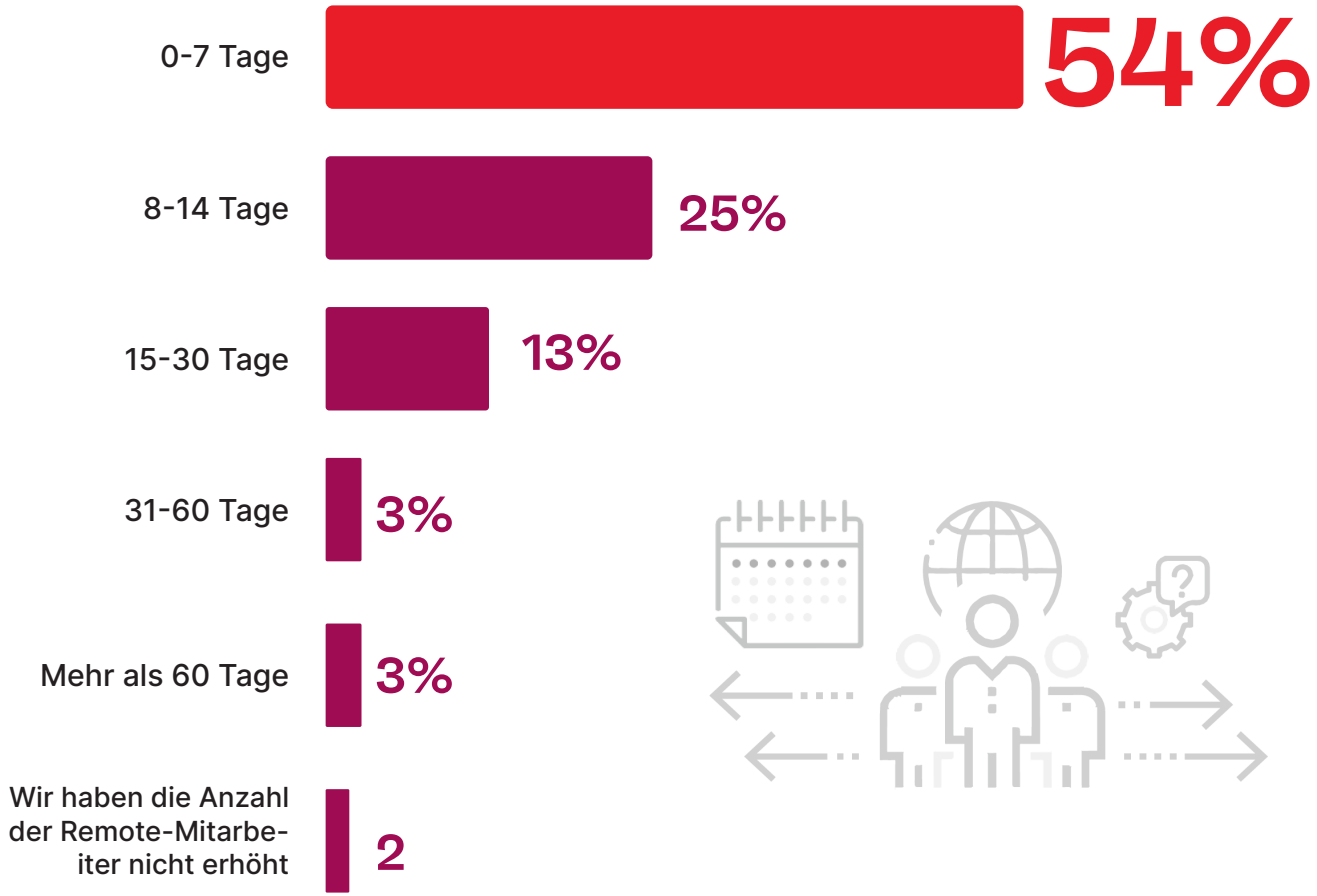
33% der Organisationen geben an, dass sie nicht ausreichend vorbereitet waren.



Tage Zur Erweiterung Der Remote-Kapazität

Eine Mehrheit der Unternehmen (54 %) gibt an, dass sie die Kapazitäten erfolgreich erweitert haben, um die erweiterte Belegschaft in sieben Tagen oder weniger vollständig zu unterstützen.

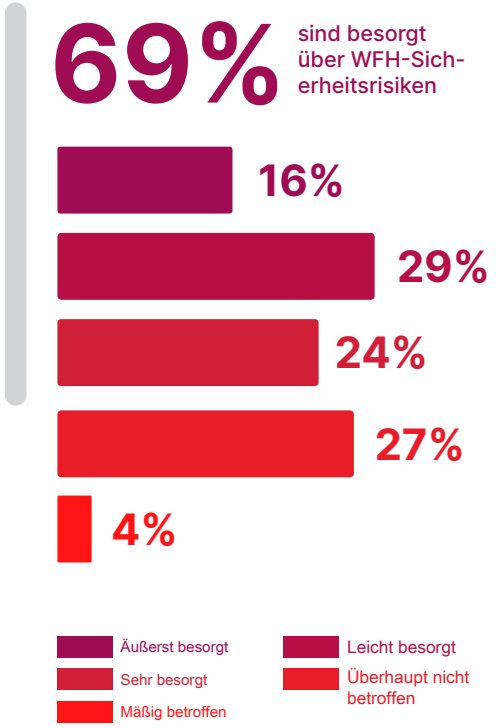
Wie viele Tage hat Ihr Unternehmen gebraucht, um die Kapazität zu erweitern, um die kürzlich erweiterte Remote-Belegschaft vollständig zu unterstützen?



Sicherheitsempfinden Im Home-Office

Während 79 % der Unternehmen glauben, dass sie angemessene Vorbereitungen für WFHSicherheit getroffen haben, sind zwei Drittel der Unternehmen in dieser Umfrage (69 %) besorgt über die Sicherheitsrisiken durch Benutzer, die von zu Hause aus arbeiten.

Wie besorgt sind Sie über die Sicherheitsrisiken, die durch Benutzer, die von zu Hause aus arbeiten, entstehen, und wie gut war Ihr Unternehmen aus der Sicherheitsperspektive auf die Umstellung auf Remote-Arbeit vorbereitet?



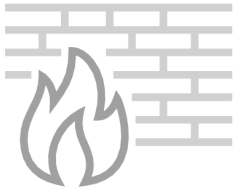
Vorhandene Sicherheitskontrollen

Die wichtigsten Sicherheitskontrollen zum Schutz von Remote-Arbeit/Home-Office sind Antiviren-/Antimalware-Lösungen (77 %), Firewalls (77 %), virtuelle private Netzwerke (66 %) und Multi-Faktor-Authentifizierung (66 %).

Welche Sicherheitskontrollen setzen Sie derzeit ein, um Remote Work-Home-Office-Szenarien abzusichern?

77%

Anti-Virus/
Anti-Malware



77%

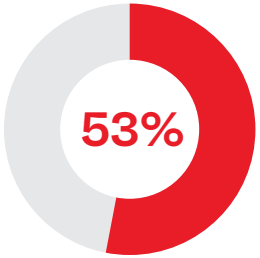
Firewalls

66%

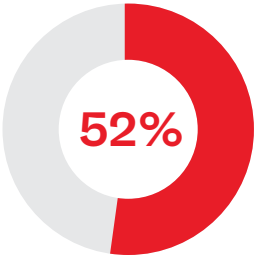
Virtuelles Privates Netzwerk
(VPN/SSL-VPN)

66%

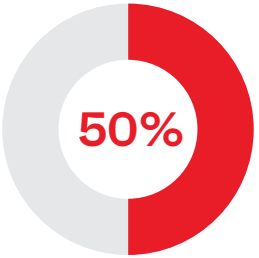
Multi-Faktor-Authentifizierung
(MFA)



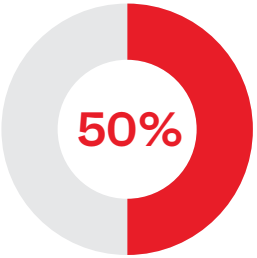
Sicherung und
Wiederherstellung



Passwortverwaltung



Datei-Verschlüsselung



Endpunkt-Sicherheit
(EDR)

Anti-Phishing 47 % | Single Sign-On 45 % | Endpoint Compliance 34 % | Mobile Device Management (MDM) 34 % | Web Application Firewall (WAF) 29 % | Virtual Desktop Infrastructure (VDI) 26 % | Load Balancing/Application Delivery Controller (ADC) 24 % | Web Proxy/Web Filtering 23 % | Cloud DLP 18 % | Cloud Access Security Brokers (CASB) 16 % | User and Entity Behavior Monitoring (UEBA) 11 % | Software-Defined Perimeter (SDP) 10 %

Zentrale Sicherheitsherausforderungen

Die Sensibilisierung der Benutzer steht an erster Stelle (59 %) auf der Liste der wichtigsten Sicherheitsherausforderungen, denen sich Unternehmen gegenübersehen, die ihre Remote- Arbeitskräfte aufstocken. Es folgen der Zugriff über private oder unsichere öffentliche Netzwerke (56 %) und die Verwendung persönlicher Geräte (43 %).

Was ist Ihrer Meinung nach die größte Sicherheitsherausforderung für Ihr Unternehmen in Bezug auf die Zunahme von Remote-Mitarbeitern?

59%

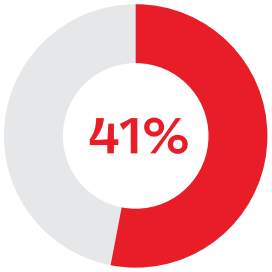
Benutzerbewusstsein und Schulung

56%

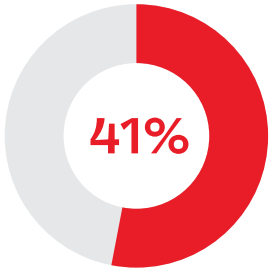
Sicherheit von privaten/öffentlichen WiFi-Netzwerken

43%

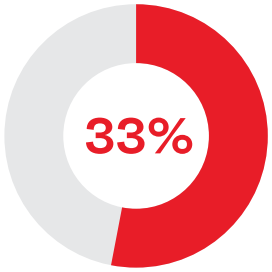
Verwendung von persönlichen Geräten/BYOD



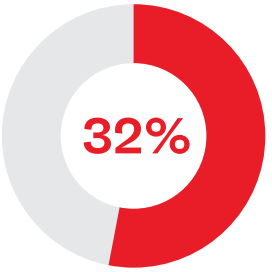
Sensible Daten verlassen den Perimeter



Erhöhte Sicherheitsrisiken



Fehlende Sichtbarkeit



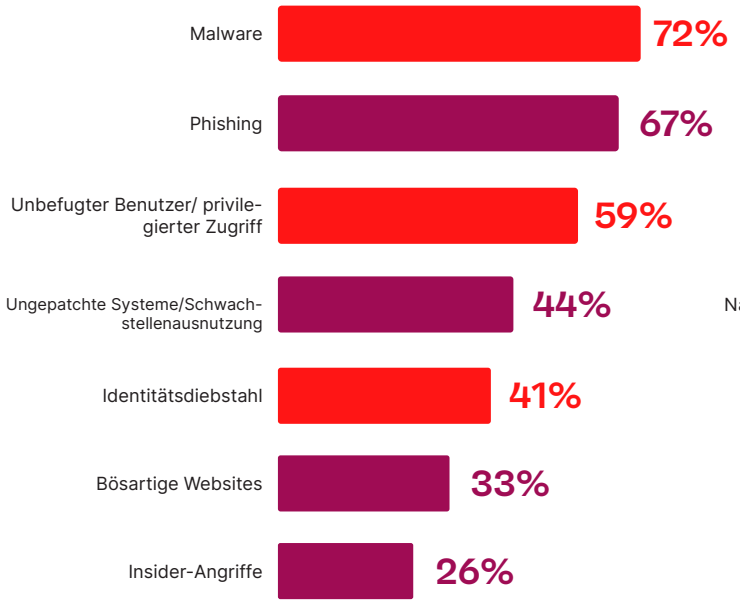
Zusätzliche Kosten für Sicherheitslösungen

Verfügbarkeit/Benutzererfahrung 30 % | Kapazitätserweiterung 24 % | Unerlaubte Nutzung

Verstärkte Angriffsvektoren

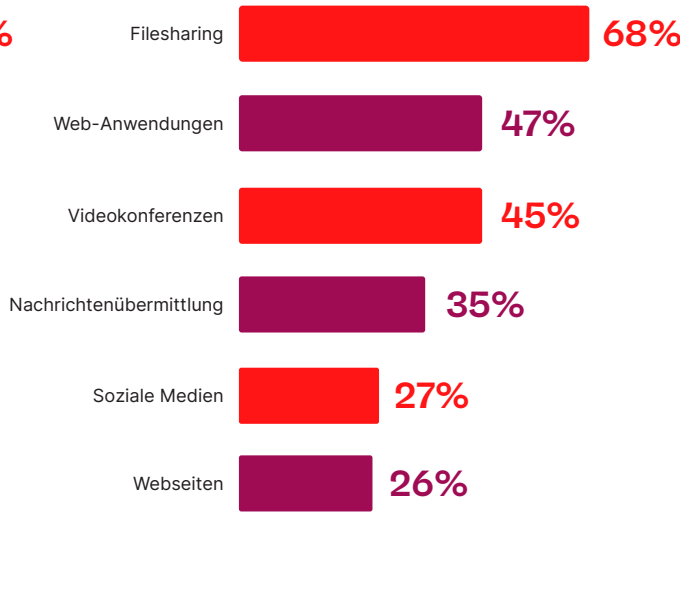
Malware, Phishing, unbefugter Benutzer-/Gerätezugriff und ungepatchte Systeme wurden als Top-Angriffsvektoren aufgrund von Mitarbeitern, die von zu Hause aus arbeiten, identifiziert. Unter den Anwendungen, die zur Produktivität und Zusammenarbeit beitragen, haben Unternehmen die größten Sicherheitsbedenken bei der gemeinsamen Nutzung von Dateien (68 %), Webanwendungen (47 %), Videokonferenzen (45 %) und Messaging (35 %).

Welche spezifischen Bedrohungsvektoren machen Ihnen bei Mitarbeitern, die von zu Hause aus arbeiten, die größten Sorgen?



Other 5%

Welche Arbeitsanwendungen, die von Remote-Mitarbeitern genutzt werden, bereiten Ihnen aus Sicht der Sicherheit die größten Sorgen?



Other 2%

Niveau Der Sicherheit Bei Fernarbeit

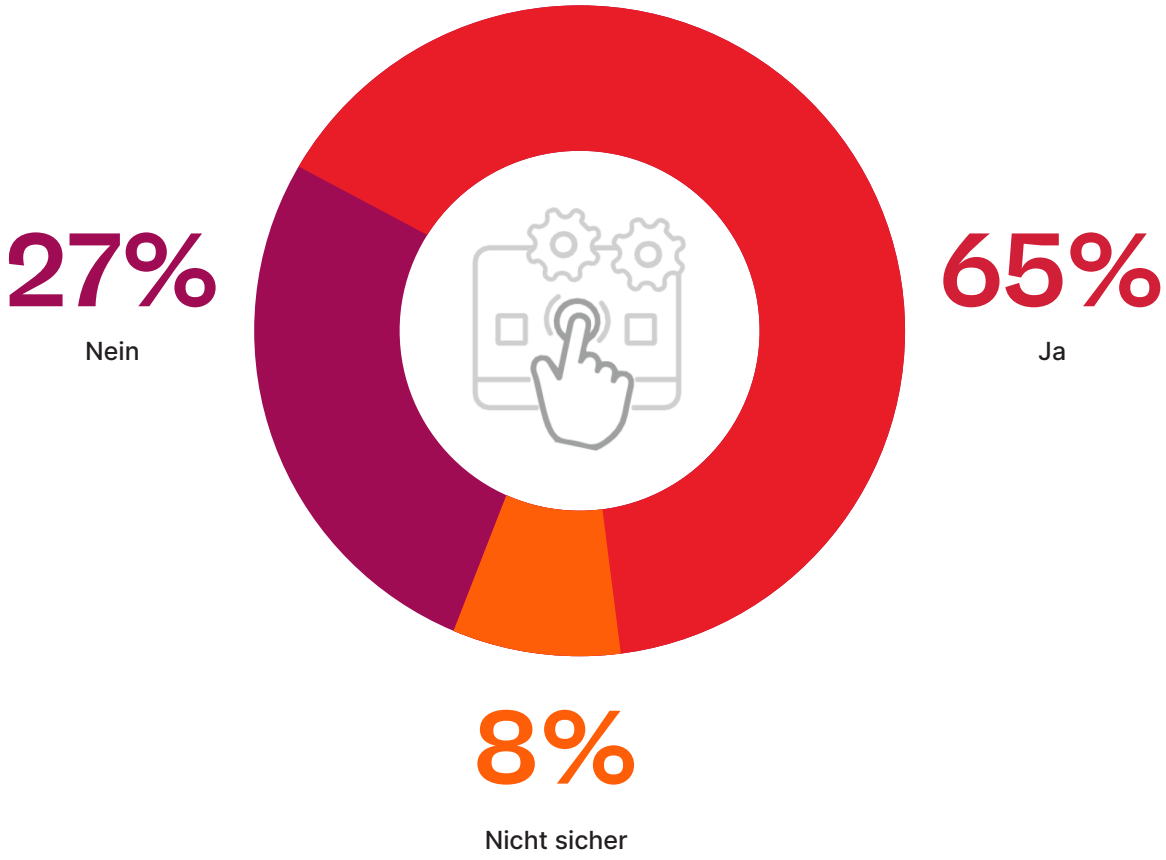
Eine Mehrheit von 78 % bestätigt, dass sie das gleiche Maß an Sicherheitskontrollen für alle Rollen durchsetzen, die aus der Ferne zugreifen.

Setzen Sie für alle Rollen im Unternehmen das gleiche Maß an Sicherheitskontrollen und Datenmanagement durch, wenn sie aus der Ferne zugreifen?

Zugriff Von Persönlichen Geräten

Fast drei Viertel der Unternehmen erlauben den Zugriff von persönlichen, nicht verwalteten Geräten, um Arbeit von zu Hause aus zu unterstützen, während mindestens 27 % dieses Szenario als erhebliches Sicherheitsrisiko ansehen.

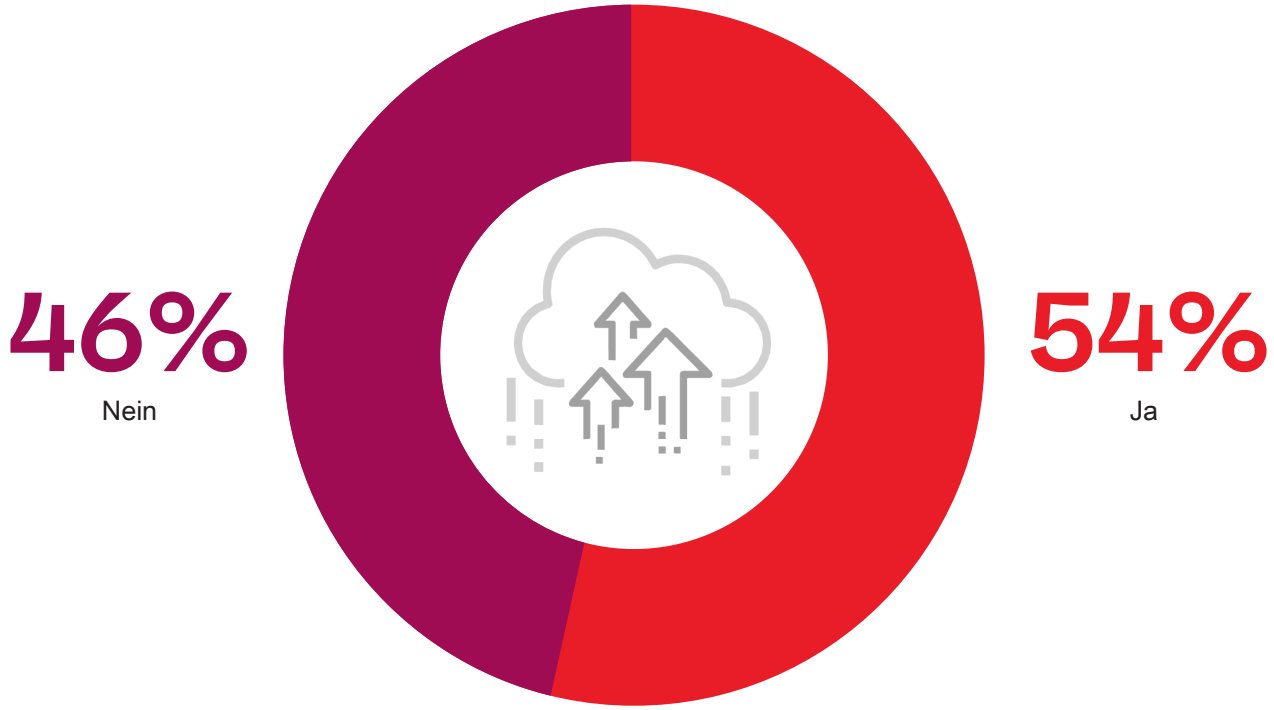
Können Mitarbeiter von persönlichen, nicht verwalteten Geräten aus auf verwaltete Anwendungen zugreifen?



Migration In Die Cloud

Eine Mehrheit von 54 % bestätigt, dass die COVID-Pandemie die Migration von Arbeitsabläufen auf cloudbasierte Apps beschleunigt hat.

Hat COVID die Migration weiterer Benutzer-Workflows oder Anwendungen auf Cloudbasierte Anwendungen beschleunigt?



Remote-Sicherheitsrisiko

Die größte Sorge der Unternehmen gilt dem Schutz sensibler Daten, insbesondere beim Zugriff über nicht verwaltete Endgeräte (46%), gefolgt von der zusätzlichen Gefährdung durch Malware (34%).

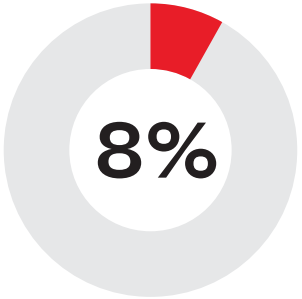
Welches ist das Hauptrisiko, das Sie befürchten, wenn sich Ihre Benutzer per Fernzugriff verbinden?

46%

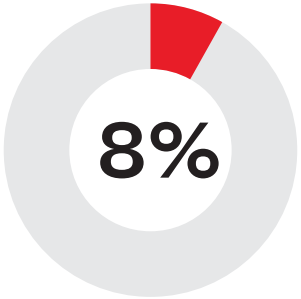
Schutz meiner Daten, insbesondere beim Zugriff durch nicht verwaltete Endpunkte

34%

Anfälligkeit für Malware, Phishing oder andere Exploits



Sicherstellung der Compliance meiner regulierten Anwender



Prüfung und Beaufsichtigung von Mitarbeitern, die von nicht verwalteten Ressourcen aus arbeiten

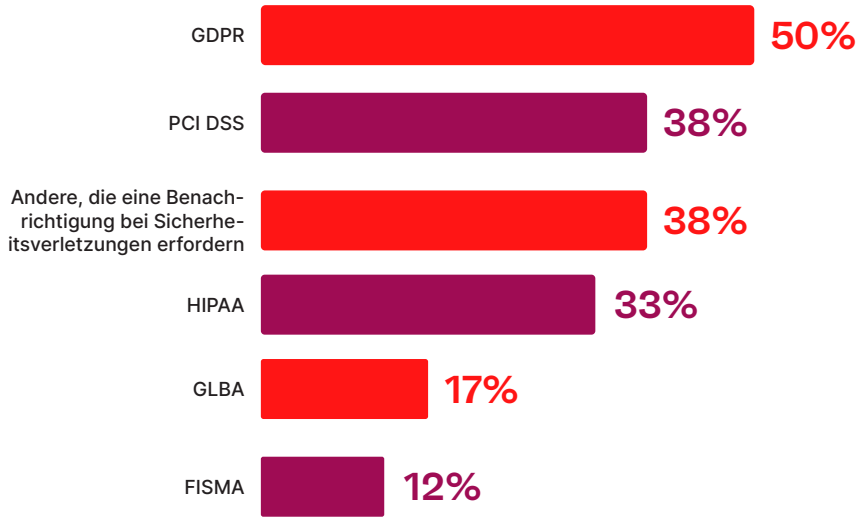
Other 4%

Compliance-Auswirkung

Zwei Drittel der Unternehmen sind der Meinung, dass Remote-Arbeitsumgebungen einen Einfluss auf ihre Compliance-Situation haben.

Könnte sich Remote-Arbeit auf die für Ihr Unternehmen geltenden Compliance-Vorschriften auswirken?

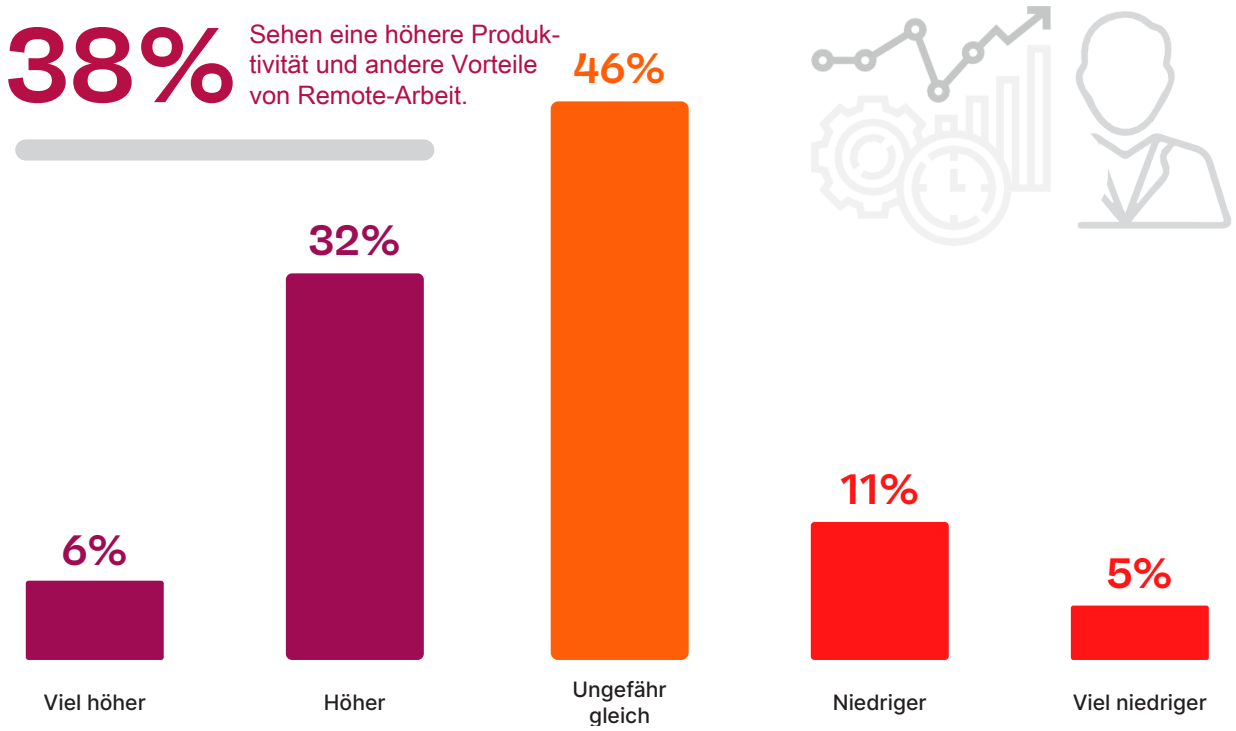
Wenn ja, welche?



Produktivitätseffekte

Achtunddreißig Prozent der Unternehmen gaben an, dass sie eine höhere Produktivität und andere Vorteile durch Remote-Arbeit. Nur 16 % sehen eine geringere Produktivität.

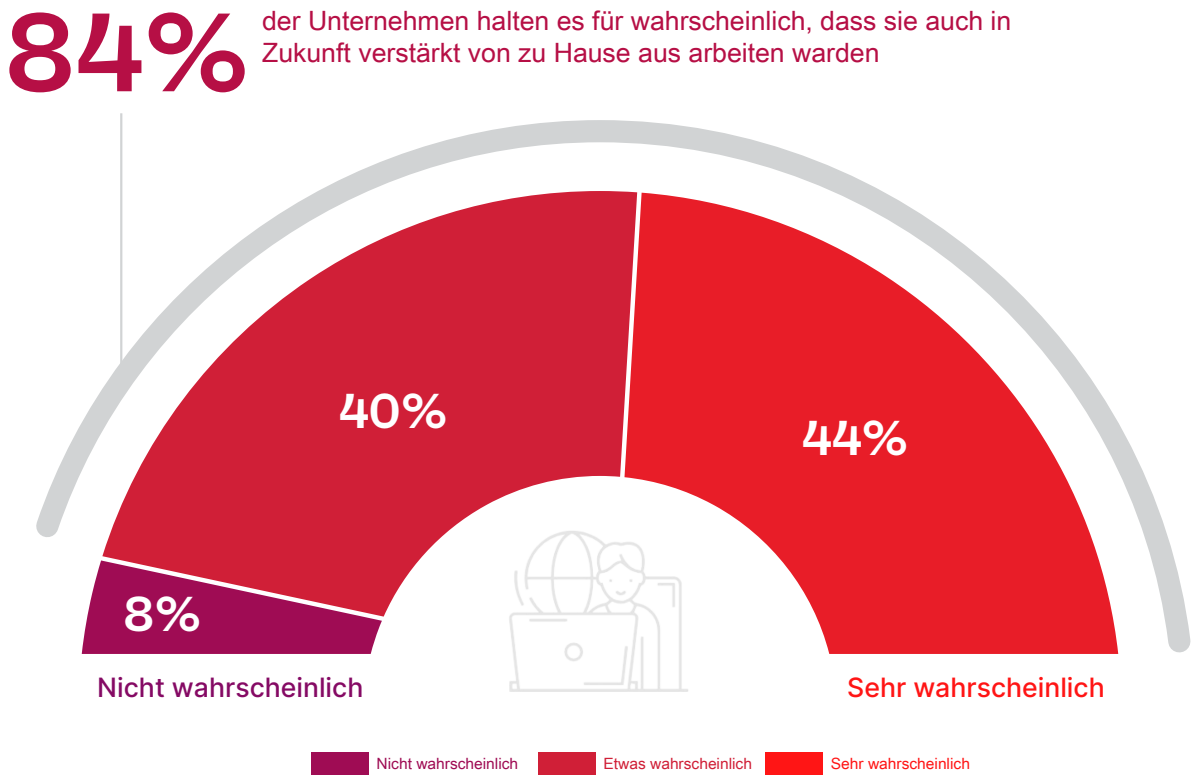
Sieht Ihr Unternehmen eine höhere Produktivität und andere Vorteile durch Remote- Arbeit?



Remote-Arbeit In Der Zukunft

Eine Mehrheit von 84 % der Unternehmen hält es für wahrscheinlich (44 % für sehr wahrscheinlich), dass sie auch in Zukunft vermehrt die Arbeit von zu Hause aus unterstützen werden, um die gesteigerte Produktivität und andere geschäftliche Vorteile zu nutzen.

Erwarten Sie, dass Sie auch in Zukunft vermehrt die Arbeit von zu Hause aus unterstützen werden (aufgrund der gesteigerten Produktivität und anderer geschäftlicher Vorteile)?

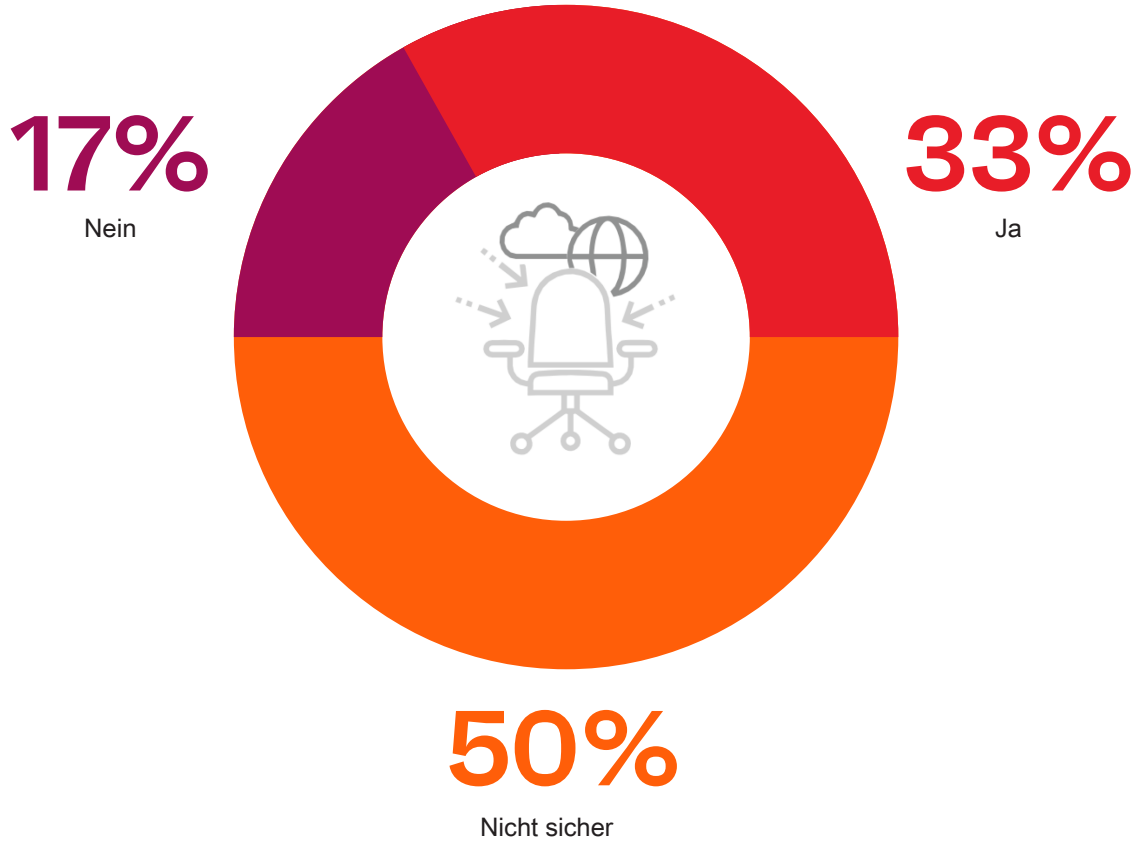


Not sure 8%

Fernarbeit Dauerhaft Machen

Ein Drittel der Unternehmen erwägt, einige Stellen nach Beendigung der COVID-Krise dauerhaft auszulagern.

Erwägt Ihre Organisation, einige Positionen (die früher vor Ort waren) nach dem Ende der COVID-Krise dauerhaft dezentral einzurichten?

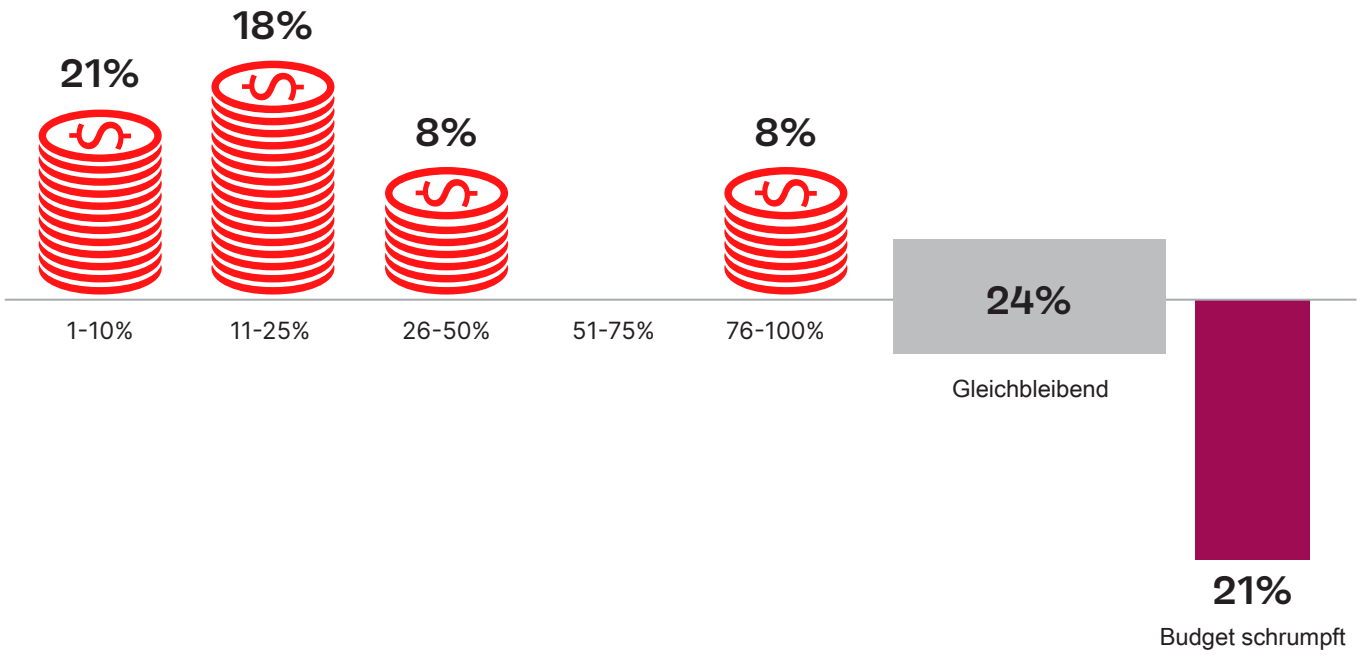


Budgetentwicklungen

Eine Mehrheit (55 %) der Unternehmen erwartet, dass die Budgets für die Sicherheit von Remote-Mitarbeitern in den nächsten 12 Monaten (nach April 2020) steigen werden. Für ein Viertel der Befragten werden diese Sicherheitsbudgets gleich bleiben und nur 21 % sehen die Budgets schrumpfen.

Wie wird sich Ihr Budget für Sicherheitskontrollen bei Remote-Arbeit in den nächsten 12 Monaten erhöhen?

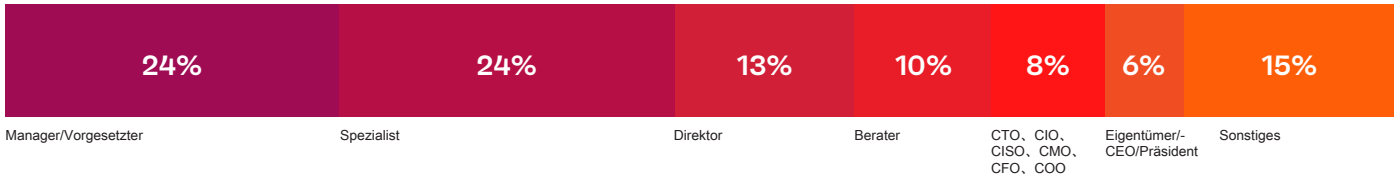
55% erwarten, dass die Budgets für die Sicherheit von Remote-Mitarbeitern in den nächsten 12 Monaten steigen werden.



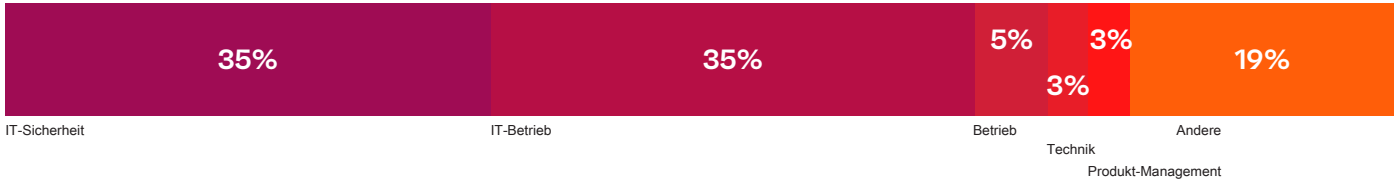
Methodik & Demographie

Dieser Bericht basiert auf den Ergebnissen einer umfassenden Online-Befragung von 413 IT und Cybersicherheitsexperten in den USA, die im Mai 2020 durchgeführt wurde, um die neuesten Trends, Herausforderungen, Lücken und Lösungspräferenzen bei der Einführung von Remote-Belegschaften in Unternehmen zu ermitteln. Die Befragten reichen von technischen Führungskräften bis hin zu IT-Sicherheitspraktikern und repräsentieren einen ausgewogenen Querschnitt von Unternehmen unterschiedlicher Größe und verschiedener Branchen.

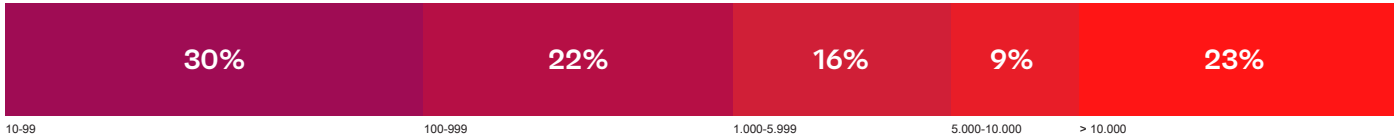
Karriere-ebene



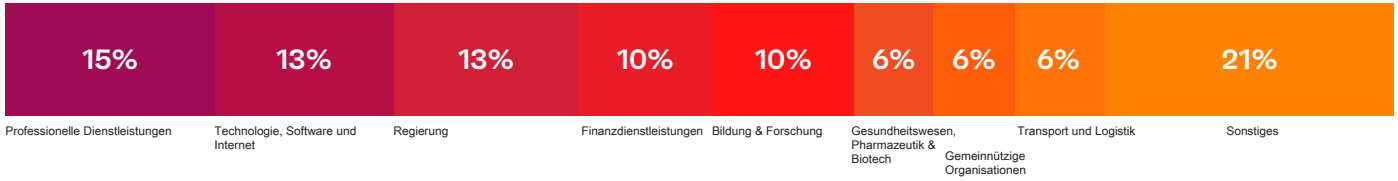
Abteilung



Firmengrösse



Branche



Pulse Secure
Acquired by Ivanti

Pulse Secure bietet einfache, umfassende softwaregesteuerte Secure Access-Lösungen für Menschen, Geräte, Dinge und Dienste, die die Transparenz, den Schutz und die Produktivität unserer Kunden verbessern. Unsere Suiten integrieren auf einzigartige Weise Cloud-, Mobil-, Anwendungs- und Netzwerkzugriff, um hybride IT in einer Zero-Trust-Welt zu ermöglichen. Mehr als 23.000 Unternehmen und Service Provider aus allen Branchen vertrauen auf Pulse Secure, um ihren mobilen Mitarbeitern den sicheren Zugriff auf Anwendungen und Informationen im Rechenzentrum und in der Cloud zu ermöglichen und gleichzeitig die Einhaltung von Unternehmensrichtlinien zu gewährleisten. Erfahren Sie mehr unter www.pulsesecure.net

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com