Bericht zur Zukunft der sicheren Remote-Arbeit

cisco SECURE

INHALT

ZUSAMMENFASSUNG

Die COVID-19-Pandemie hat dazu geführt, dass Unternehmen weltweit mit beispielloser Geschwindigkeit und Skalierung auf eine Remote-Arbeitsumgebung umsteigen. Was einst für Mitarbeiter und Unternehmen „nice to have“ war, wurde fast über Nacht zum „must have“. Unternehmen auf der ganzen Welt verlagerten ihre gesamte Belegschaft auf Remote-Arbeitsmodelle. Im Zuge der Umstellung mussten Unternehmen ihren Cybersicherheitsansatz, ihre Lösungen und Richtlinien anpassen und weiterentwickeln, damit ihre Mitarbeiter remote arbeiten, sicher auf Unternehmensressourcen zugreifen und die Business Continuity gewährleisten können.

In einem Jahr voller Unsicherheiten hat sich ein bedeutender Trend entwickelt: die flexible und hybride Zukunft der Arbeit. Nachdem Mitarbeiter über einen längeren Zeitraum remote gearbeitet haben, erwarten sie jetzt, dass sie auch nach COVID von überall, zu jeder Zeit und auf jedem Gerät flexibel arbeiten können, selbst wenn mittlerweile ein Teil der Arbeit wieder im Büro stattfindet.

Daher müssen Unternehmen ihren Cybersicherheitsstatus neu bewerten, insbesondere da Führungskräfte im Moment die Widerstandsfähigkeit ihrer Unternehmen steigern möchten. Sicherheit kann die Brücke zur Business Resiliency sein, da sie Unternehmen eine flexible und sichere Anpassung sowie den Schutz gegenwärtiger und zukünftiger Unternehmensressourcen ermöglicht. Hierfür müssen Netzwerk- und Collaboration-Lösungen flexibel, benutzerfreundlich, effektiv und sicher sein, unabhängig davon, ob sie über lokale Rechenzentren oder in der Cloud bereitgestellt werden, und über alle Benutzergeräte – ob geschäftlich oder privat – hinweg.

Wir wollten verstehen, wie gut Unternehmen weltweit darauf vorbereitet sind, ihren Geschäftsbetrieb zu schützen, während sie aufgrund der Pandemie gezwungen waren, ihre gesamte Belegschaft auf Remote-Arbeit umzustellen. Noch wichtiger war uns, Einblicke in den heutigen Stand der Unternehmen im Hinblick auf die steigenden Bedrohungen und Warnungen im Bereich der Cybersicherheit zu gewinnen, in die Herausforderungen, denen sie sich bei diesem plötzlichen Übergang gegenübersehen, und in die Art und Weise, wie sie ihre Cybersicherheitsansätze anpassen, um sich besser auf die hybride und flexible Arbeitsumgebung vorzubereiten – denn dieser Umgebung gehört die Zukunft. Zu diesem Zweck haben wir eine globale Umfrage in 21 Märkten in Nord- und Südamerika (AMER), im Asien-Pazifik-Raum, in Japan und China (APJC) sowie in Europa durchgeführt. Dabei haben wir über 3.000 IT-Entscheidungsträger von kleinen und großen Unternehmen befragt.

Die Studie mit dem Titel „Die Zukunft der sicheren Remote-Arbeit“ zielt darauf ab, die Herausforderungen zu verstehen, mit denen Unternehmen beim Wechsel zu Remote-Arbeit konfrontiert waren. , und gleichzeitig den Zustand ihrer Cybersicherheitsbereitschaft sowie die Veränderungen ihrer Prioritäten, Richtlinien und Investitionen bei der Vorbereitung auf eine hybride Arbeitsumgebung, die auch in Zukunft Bestand haben dürfte, aufzudecken.

Die Ergebnisse sind aufschlussreich.

HIGHLIGHTS AUS EUROPA

HIGHLIGHTS AUS EUROPA

Regionale Zusammenfassung

In der Studie wurden mehr als 600 Teilnehmer aus vier europäischen Ländern befragt: aus Frankreich, Deutschland, Italien und dem Vereinigten Königreich. Basierend auf den Angaben der Befragten hatte COVID-19 überall in Europa ähnliche Auswirkungen, und Remote-Arbeit dürfte dort künftig einen festen Platz im Beschäftigungsmix einnehmen. 34 % der Unternehmen glauben, dass ***mehr als die Hälfte*** ihrer Mitarbeiter auch nach der Pandemie remote weiterarbeiten werden.

Im Gegensatz zu ihren Pendants in anderen Regionen scheinen Unternehmen in Europa besser darauf vorbereitet zu sein, den plötzlichen Übergang zu einer Remote-Belegschaft zu unterstützen. Während 45 % angaben, ***sehr gut vorbereitet*** zu sein (verglichen mit 40 % weltweit und 39 % in APJC und AMER), antworteten 50 %, dass sie ***etwas vorbereitet*** waren (verglichen mit 53 % weltweit), und 6 % sagten, sie seien ***nicht vorbereitet*** (genauso viele wie in AMER und im globalen Durchschnitt).

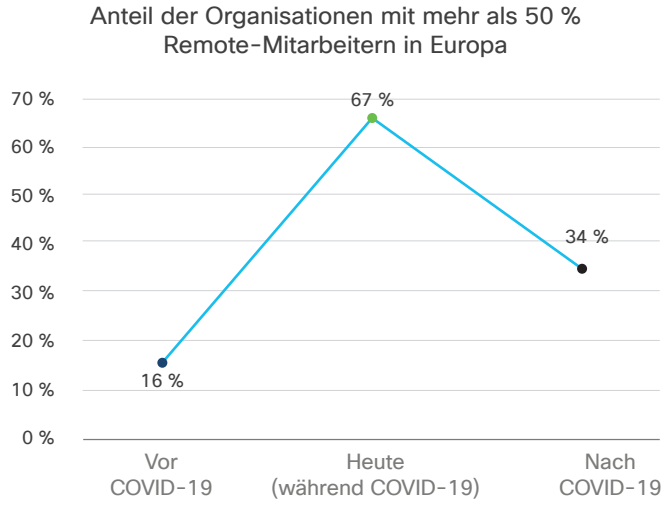
Während nur 37 % der Befragten in Europa einen Anstieg von ***25 % oder mehr*** bei Cyberbedrohungen oder -warnungen verzeichneten, was unter dem weltweiten Durchschnitt von 61 % liegt, wussten besorgniserregende 17 % der Befragten in Europa nicht, ob es überhaupt eine Zunahme oder einen Rückgang der Cyberbedrohungen oder -warnungen gab. Dies ist deutlich mehr als der Durchschnitt in AMER (5 %) und APJC (6 %).

	Global	APJC	AMER	Europa
Zunahme von Cyberwarnungen oder -angriffen (25 % oder mehr)	61 %	69 %	64 %	37 %
Weiß nicht	8 %	6 %	5 %	17 %

Etwas mehr als die Hälfte (52 %) der Unternehmen in Europa gab an, dass die COVID-19-Situation zu einem Anstieg zukünftiger Investitionen in die Cybersicherheit führen wird. Damit ist Europa die Region mit dem ***geringsten Anteil der Unternehmen, die einen Anstieg der Investitionen in die Cybersicherheit in den drei Regionen erwarten,*** verglichen mit dem globalen Durchschnitt von 66 %. 37 % geben an, dass sich die Investitionen ihres Unternehmens nicht verändern werden. Dies ist der höchste Wert im Vergleich zu den Durchschnittswerten von AMER (23 %) und APJC (17 %).

Wichtigste Ergebnisse

Die Umstellung auf eine hybride Arbeitsumgebung geht in Europa weiter, allerdings auf unterschiedlichem Niveau.



Europa hatte vor der Pandemie den niedrigsten Anteil an Remote-Mitarbeitern. Nur 16 % der Unternehmen gaben an, dass mehr als die Hälfte ihrer Belegschaft an Remote-Standorten tätig war – etwas weniger als der weltweite Durchschnitt (19 %). Nach dem Ausbruch der Pandemie stieg der Anteil der Unternehmen, bei denen ***mehr als der Hälfte*** der Belegschaft remote arbeitet, auf 67 % und lag damit über dem weltweiten Durchschnitt von 62 %. 34 % der europäischen Unternehmen gehen davon aus, dass nach COVID-19 mehr als die Hälfte ihrer Mitarbeiter weiterhin remote arbeiten werden, doppelt so viele wie vor dem Ausbruch.

- Während sich in Frankreich und Italien der Anteil der Unternehmen, bei denen ***mehr als die Hälfte*** der Belegschaft remote arbeiten, auf dem Höhepunkt der Pandemie mehr als vervierfacht hat (64 % in Frankreich und 65 % in Italien gegenüber jeweils 15 % vor der Pandemie), verzeichnete das Vereinigte Königreich den höchsten Anstieg der Remote-Mitarbeiter weltweit: Dort arbeiteten während der Pandemie in 85 % der Unternehmen ***mehr als die Hälfte*** der Mitarbeiter remote – zuvor waren es nur 18 %. Dies ist wahrscheinlich auf die strengen Lockdown-Maßnahmen des Landes auf dem Höhepunkt des Ausbruchs zurückzuführen.
- Den Daten zufolge erwarten mehr Unternehmen im Vereinigten Königreich (50 %), dass ***mehr als die Hälfte*** ihrer Mitarbeiter auch nach COVID-19 weiterhin remote arbeiten werden – die größte Zunahme der Remote-Arbeit in allen weltweit befragten Ländern und deutlich über dem globalen Durchschnitt von 37 %.
- Unternehmen in Frankreich (32 %), Deutschland (24 %) und Italien (33 %) rechnen für die Zeit nach der Pandemie ebenfalls mit mehr Remote-Mitarbeitern als vor COVID-19, doch diese Zahlen sind niedriger als der globale Durchschnitt.

32 %
Frankreich

24 %
Deutschland

33 %
Italien

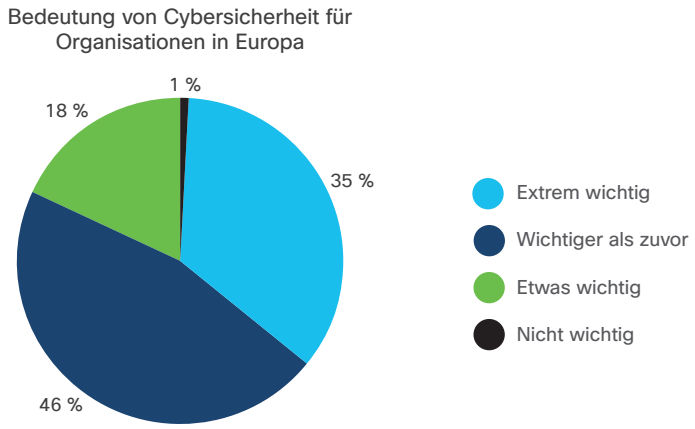
Im Vereinigten Königreich war der Anteil an Unternehmen, die zu Beginn von COVID-19 angaben, auf einen beschleunigten Übergang zu einer Remote-Arbeitsumgebung ***sehr gut vorbereitet*** zu sein, mit 59 % weltweit am zweithöchsten nach Vietnam (67 %). Dagegen verzeichneten Frankreich mit 9 % und Italien mit 8 % den europaweit höchsten Anteil an Unternehmen, die auf den Übergang ***nicht vorbereitet*** waren – beide Werte liegen über dem weltweiten Durchschnitt.

Vorbereitung der Cybersicherheit auf den Remote-Betrieb	Frankreich	Deutschland	Italien	Vereinigtes Königreich
Sehr gut vorbereitet	43 %	41 %	35 %	59 %
Etwas vorbereitet	47 %	55 %	57 %	39 %
Nicht vorbereitet	9 %	4 %	8 %	2 %

Vorbereitung der Cybersicherheit auf den Remote-Betrieb nach Land

Cybersicherheit ist wichtig, aber nicht wichtig genug

In einer Zeit, in der Unternehmen durch den plötzlichen und massiven Übergang zu Remote-Arbeit vor Herausforderungen stehen, war der Anteil der Unternehmen, die angaben, dass Cybersicherheit ***wichtiger sei als zuvor***, in Europa mit 46 % am höchsten. Der Durchschnittswert in APJC und weltweit lag hier bei 41 %, in AMER betrug er 38 %. Gleichwohl lag hier Anteil der Unternehmen, die anerkannten, dass Cybersicherheit ***extrem wichtig*** ist, mit nur 35 % weltweit am niedrigsten.



Bedeutung von Cybersicherheit	Global	APJC	AMER	Europa
Extrem wichtig	44 %	44 %	50 %	35 %
Wichtiger als zuvor	41 %	41 %	38 %	46 %
Etwas wichtig	15 %	15 %	11 %	18 %
Nicht wichtig	1 %	1 %	1 %	1 %

Bedeutung der Cybersicherheit für Unternehmen – regional im Vergleich zum weltweiten Durchschnitt

- Ein detaillierterer Blick zeigt, dass die Bedeutung der Cybersicherheit innerhalb Europas sehr unterschiedlich wahrgenommen wird. 46 % der Unternehmen im Vereinigten Königreich gaben an, dass die Cybersicherheit ***extrem wichtig*** sei. Dieser Wert liegt 2 Prozentpunkte über dem weltweiten Durchschnitt von 44 %. In den übrigen europäischen Ländern, in denen die Befragung durchgeführt wurde (Frankreich, Deutschland und Italien), gaben mehr Unternehmen an, dass Cybersicherheit ***wichtiger ist als zuvor***.

- Europa ist auch die Region, in der die meisten Unternehmen angaben, dass die Cybersicherheit nur ***etwas wichtig*** sei – der Wert lag hier bei 18 % und damit über dem weltweiten Durchschnitt von 15 %.

Bedeutung von Cybersicherheit	Frankreich	Deutschland	Italien	Vereinigtes Königreich
Extrem wichtig	34 %	32 %	28 %	46 %
Wichtiger als zuvor	44 %	47 %	57 %	35 %
Etwas wichtig	20 %	19 %	15 %	17 %
Nicht wichtig	2 %	1 %	–	1 %

Bedeutung der Cybersicherheit für Unternehmen nach Land

Unternehmen in Europa erlebten seit Beginn der Pandemie die geringste Zunahme von Cyberbedrohungen oder -warnungen, aber viele sind sich nicht ganz sicher

Wie bereits erwähnt, verzeichneten die meisten europäischen Unternehmen im Vergleich zu ihren Pendants in AMER und APJC einen geringeren Anstieg von Cyberbedrohungen oder -warnungen. Allerdings war hier auch der Anteil der Unternehmen, die sich bezüglich der Zunahme oder Abnahme von Cyberbedrohungen oder -warnungen nicht sicher sind, am größten.

Beispielsweise kam es bei der Hälfte der Unternehmen in Frankreich (48 %) während der Pandemie zu einem Anstieg von ***25 % oder mehr*** bei den Cyberbedrohungen oder -warnungen. Dies ist der höchste Wert, der unter den vier befragten europäischen Ländern beobachtet wurde, und auch höher als der regionale Durchschnitt (37 %).

Auf der anderen Seite verzeichneten zwar nur 24 % der Unternehmen im Vereinigten Königreich einen Anstieg der Cyberbedrohungen oder -warnungen um ***25 % oder mehr***, aber dort war der Anteil von Unternehmen, die ***nicht wissen***, ob es einen Anstieg oder Rückgang gab, europaweit am höchsten (27 %). Dies ist deutlich mehr als der Durchschnitt weltweit (8 %) und europaweit (17 %).

Zunahme von Cyberbedrohungen oder -warnungen	Frankreich	Deutschland	Italien	Vereinigtes Königreich
25 % oder mehr	48 %	31 %	43 %	24 %
Weiß nicht	12 %	14 %	14 %	27 %

Zunahme von Cyberbedrohungen oder -warnungen nach Land

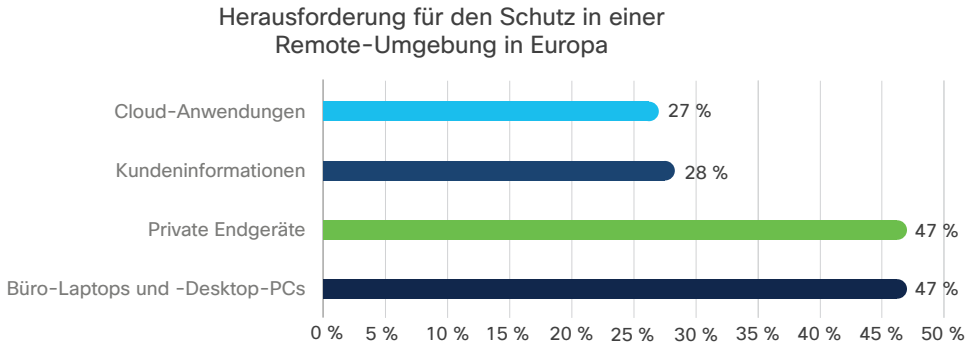
Die Herausforderungen im Bereich der Cybersicherheit sind nach wie vor erheblich

Da immer mehr Benutzer sich auch weiterhin remote verbinden, verzeichnen die Unternehmen in der EU vermehrt Herausforderungen im Zusammenhang mit der Cybersicherheit. Sicherer Zugriff wurde als die **größte Herausforderung für die Cybersicherheit** genannt, mit der der größte Anteil der Unternehmen (57 %) konfrontiert war. Weitere Bedenken betrafen den Datenschutz (41 %), der Auswirkungen auf die allgemeine Sicherheitslage hat, und die Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien (39 %).

Endpunktsicherheit ist eine wichtige Maßnahme

Mitarbeiter, die Unternehmensgeräte mit nach Hause nehmen, wurden von fast der Hälfte (47 %) der europäischen Unternehmen als Achillesferse identifiziert. Bedrohungen in Bezug auf Endpunktsicherheit umgehen herkömmliche Cybersicherheitsmaßnahmen, die nicht für den Remote-Einsatz eingerichtet wurden. Dies entspricht dem globalen Trend, dass jeder zweite Befragte angab, dass Büro-Laptops/-Desktop-PCs (56 %) und private Geräte (54 %) eine der größten Herausforderungen beim Schutz einer Remote-Umgebung darstellen.

Europäische Unternehmen empfanden auch den Schutz von Kundeninformationen (28 %) und Cloud-Anwendungen (27 %) in Remote-Arbeitsumgebungen als Herausforderung. Diese Zahlen lagen jedoch beide deutlich unter dem weltweiten Durchschnitt (jeweils 46 %).



- Das Vereinigte Königreich ist das einzige Land in der Region, in dem ein größerer Anteil von Unternehmen den Schutz von Bürogeräten als größere Herausforderung empfand (46 %) als den von privaten Geräten (39 %).

- In Deutschland war der Anteil der Unternehmen, die den Schutz von privaten Geräten bzw. Büro-Laptops/-Desktop-PCs in einer Remote-Arbeitsumgebung als Herausforderung betrachten, jeweils gleich hoch (55 %) – der einzige Markt in der Region mit Gleichstand. Dieser Wert lag 8 Prozentpunkte höher als der regionale Durchschnitt von 47 %.

Unterstützung für Remote-Mitarbeiter mit den richtigen technologischen Prioritäten

Während Unternehmen dazu übergingen, den Großteil ihrer Meetings nicht mehr persönlich abzuhalten, sondern ihre gesamte Kommunikation fast über Nacht zu virtualisieren, liegt Europa in Bezug auf die sichere Remote-Vernetzung von Mitarbeitern auf demselben Niveau wie der Rest der Welt. Im Einklang mit globalen Trends stuften mehr als die Hälfte (55 %) der Unternehmen, die diese Lösungen einführten, Cybersicherheitsmaßnahmen als wichtigste Priorität ein, vor Collaboration-Tools (von 48 % als Top-Priorität bezeichnet) und Professional Services (für 25 % der wichtigste Punkt).

- In Europa selbst haben alle Länder außer Deutschland Cybersicherheitsmaßnahmen als höchste Priorität eingestuft.

Am weitesten verbreitet	vs.	Höchste Priorität
Collaboration-Tools 76 %	1	Cybersicherheitsmaßnahmen 55 %
Cybersicherheitsmaßnahmen 65 %	2	Collaboration-Tools 48 %
Cloud-basierte Dokumentfreigabe 56 %	3	Professional Services 25 %

Am weitesten verbreitete IT-Lösungen vs. Priorität bei der Unterstützung von Remote-Arbeit in europäischen Unternehmen

- Während die Region insgesamt Professional Services auf dem dritten Platz einstufte, lag in drei der vier in Europa befragten Länder (alle außer Frankreich) Cloud Sharing auf dem dritten Platz.

Frankreich	Deutschland	Italien	Vereinigtes Königreich
Cybersicherheits-maßnahmen (51 %)	Collaboration-Tools (54 %)	Cybersicherheits-maßnahmen (58 %)	Cybersicherheits-maßnahmen (63 %)
Collaboration-Tools (50 %)	Cybersicherheits-maßnahmen (46 %)	Collaboration-Tools (44 %)	Collaboration-Tools (43 %)
Professional Services (31 %)	Cloud-basierte Dokumentfreigabe (31 %)	Cloud-basierte Dokumentfreigabe (21 %)	Cloud-basierte Dokumentfreigabe (23 %)

Von Unternehmen in Europa als am wichtigsten eingestufte IT-Lösungen

Rückbesinnung auf Cybersicherheitsrichtlinien

Während Unternehmen weiterhin darauf hinarbeiten, ihre Remote-Mitarbeiter zu schützen, war die Mehrheit der Meinung, dass ihre Cybersicherheitsrichtlinien sofort aktualisiert werden müssen, um diese massive Verschiebung zu unterstützen. 93 % der Unternehmen in Europa meldeten Änderungen an ihren Cybersicherheitsrichtlinien – der niedrigste Anteil unter allen drei Regionen und auch weniger als der weltweite Durchschnitt (96 %). Die wichtigste richtlinienbezogene Änderung, die vorgenommen wurde, war die **Erhöhung der VPN-Kapazität** (64 %), die über dem weltweiten Durchschnitt von 59 % lag. Weitere wichtige richtlinienbezogene Änderungen waren die **Implementierung der Multi-Faktor-Authentifizierung** (38 % in Europa vs. 53 % weltweit), die **Ausweitung von Webkontrollen und Richtlinien zur akzeptablen Nutzung** (34 % in Europa vs. 55 % weltweit) und der **Endpunktschutz** (34 %). in Europa vs. 48 % weltweit).

- Interessanterweise gab ein höherer Anteil der Unternehmen in Frankreich und Deutschland mit 37 % bzw. 40 % an, dass ihre dritte Änderung von Cybersicherheitsrichtlinien den Endpunktschutz betrifft.

Frankreich	Deutschland	Italien	Vereinigtes Königreich
Erhöhte VPN-Kapazität (63 %)	Erhöhte VPN-Kapazität (64 %)	Erhöhte VPN-Kapazität (66 %)	Erhöhte VPN-Kapazität (65 %)
Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung (40 %)	Implementierung von Multi-Faktor-Authentifizierung (44 %)	Implementierung von Multi-Faktor-Authentifizierung (40 %)	Implementierung von Multi-Faktor-Authentifizierung (35 %)
Endpunktschutz (37 %)	Endpunktschutz (40 %)	Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung (39 %)	Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung (29 %)

Die wichtigsten richtlinienbezogenen Änderungen nach Land

Einfachheit und Aufklärung sind der Schlüssel zur Stärkung von Protokollen

Während die Pandemie Unternehmen zwang, ihre Digitalisierung und Remote-Arbeitspläne zu beschleunigen, änderten und entwickelten viele Mitarbeiter ihre Arbeitsgewohnheiten in Echtzeit, und viele arbeiteten zum ersten Mal remote. Schulungen zum Sicherheitsbewusstsein wurden wichtiger denn je, da böswillige Akteure diese potenzielle Wissenslücken erkannten und immer neue Wege fanden, um die Unbedarftheit der Mitarbeiter auszunutzen.

54 % der europäischen Unternehmen (gegenüber 59 % weltweit) gaben an, dass die mangelnde Sensibilisierung und Aufklärung der Mitarbeiter die ***größte Herausforderung bei der Stärkung der Cybersicherheitsprotokolle*** für Remote-Arbeit war, gefolgt von zu vielen zu verwaltenden Tools und Lösungen (43 % vs. 50 % weltweit). Nur 22 % der europäischen Unternehmen gaben an, Probleme mit der Bereitstellung inkonsistenter Schnittstellen zu haben (gegenüber 35 % weltweit). Während der europäische Durchschnitt niedriger ist als der weltweite und auch der Durchschnittswert in allen anderen Regionen, zeigen die Ergebnisse, dass es Gelegenheiten für Weiterbildung und bessere Sicherheitsmaßnahmen gibt, die einfach und benutzerfreundlich sind und gut zusammenarbeiten.

Global	APJC	AMER	Europa
Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter (59 %)	Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter (61 %)	Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter (58 %)	Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter (54 %)
Zu viele zu verwaltende Tools/ Lösungen (50 %)	Zu viele zu verwaltende Tools/ Lösungen (53 %)	Zu viele zu verwaltende Tools/ Lösungen (49 %)	Zu viele zu verwaltende Tools/ Lösungen (43 %)
Inkonsistente Schnittstellen (35 %)	Inkonsistente Schnittstellen (40 %)	Inkonsistente Schnittstellen (33 %)	Inkonsistente Schnittstellen (22 %)

Die 3 größten Herausforderungen bei der Stärkung von Cybersicherheitsprotokollen nach Region

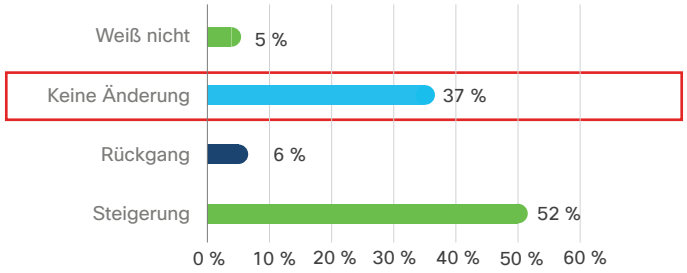
- Deutschland steht dem Trend entgegen: Hier gaben viele Unternehmen an, dass sie mit zu vielen Tools und Lösungen als Hauptherausforderung zu kämpfen haben, und zwar 55 % und damit mehr als der regionale Durchschnitt (43 %).

Ein wohlüberlegter, aber proaktiver Ansatz zur Steigerung der Investitionen in die Cybersicherheit

Mehr als die Hälfte (52 %) der Unternehmen in Europa gab an, dass die COVID-19-Situation zu einem Anstieg zukünftiger Investitionen in die Cybersicherheit führen wird. Dies ist ein Schritt in die richtige Richtung, auch wenn die Region den niedrigsten Anteil an Unternehmen verzeichnet, die solche Investitionen fördern möchten. Folglich gaben 37 % der europäischen Unternehmen an, dass es ***keine Änderung*** der Investitionen ihrer Unternehmen in die Cybersicherheit geben wird – der höchste Wert in allen Regionen.

- Mehr als die Hälfte der Unternehmen in Frankreich (56 %), Italien (52 %) und Deutschland (56 %) gaben an, dass sie nach der Pandemie ihre Ausgaben für Cybersicherheit erhöhen werden.
- Im Vereinigten Königreich dagegen lag der Anteil der Befragten, die angaben, ihre zukünftigen Investitionen in Cybersicherheit nicht verändern zu wollen, mit 49 % weltweit am höchsten. Außerdem lag dort der Anteil der Unternehmen, die einen Anstieg ihrer Investitionen in Cybersicherheit vermeldeten, mit 44 % weltweit am niedrigsten.

Änderungen bei den Investitionen in die Cybersicherheit in Europa nach COVID-19



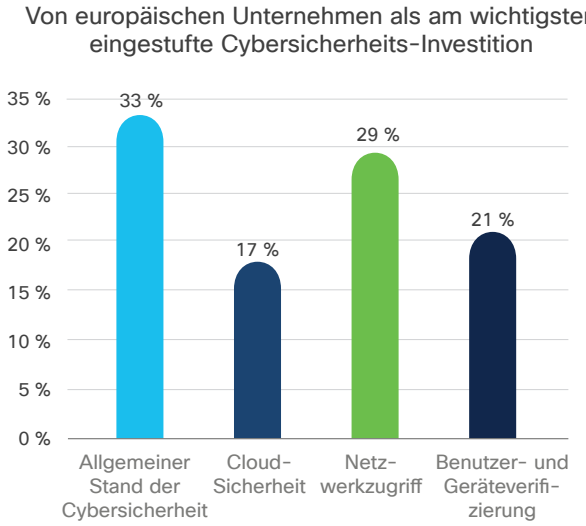
Veränderungen in der Cybersicherheit Investitionen aufgrund von COVID-19	Global	APJC	AMER	Europa
Steigerung	66 %	70 %	68 %	52 %
Rückgang	9 %	11 %	7 %	6 %
Keine Änderung	22 %	17 %	23 %	37 %
Weiß nicht	3 %	2 %	2 %	5 %

Änderungen bei den Investitionen in die Cybersicherheit – regionale vs. globale Durchschnittswerte

Die Pandemie treibt Unternehmen dazu an, ihre Cybersicherheits-Strategie neu zu überdenken

Was die Rangordnung der Cybersicherheits-Investitionen angeht, hat der allgemeine Stand der Cybersicherheit den höchsten Stellenwert (33 % nannten dies als wichtigsten Faktor).

In Italien (32 %) und im Vereinigten Königreich (48 %) nimmt dies die höchste Priorität ein. Weitere von europäischen Unternehmen gemeldete vorrangige Investitionen sind der Netzwerkzugriff (für 29 % am wichtigsten) und die Benutzer- und Geräteverifizierung (für 21 % am wichtigsten). Dies deutet darauf hin, dass Unternehmen in Europa ihre Cybersicherheits-Strategie auf einen ganzheitlichen Zero-Trust-Ansatz ausrichten, um eine hybride Zukunft der Arbeit infolge der Pandemie sicher zu unterstützen.



Frankreich	Deutschland	Italien	Vereinigtes Königreich
Netzwerkzugriff (33 %)	Netzwerkzugriff (32 %)	Allgemeiner Stand der Cybersicherheit (32 %)	Allgemeiner Stand der Cybersicherheit (48 %)
Allgemeiner Stand der Cybersicherheit (25 %)	Allgemeiner Stand der Cybersicherheit (28 %)	Netzwerkzugriff (32 %)	Benutzer- und Geräteverifizierung (20 %)
Benutzer- und Geräteverifizierung (22 %)	Benutzer- und Geräteverifizierung (22 %)	Benutzer- und Geräteverifizierung (21 %)	Netzwerkzugriff (17 %)
Cloud-Sicherheit (20 %)	Cloud-Sicherheit (18 %)	Cloud-Sicherheit (15 %)	Cloud-Sicherheit (15 %)

Prioritäten bei Cybersicherheits-Investitionen (Platz 1) nach Land

LÄNDERDETAILS: EUROPA

Frankreich

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Die Bedeutung von Cybersicherheit in einer hybriden Zukunft der Arbeit			
Anteil der Unternehmen, in denen ***mehr als die Hälfte*** der Belegschaft remote arbeitet	• Vor COVID-19: 15 % • Während COVID-19: 64 % • Nach COVID-19: 32 %	• Vor COVID-19: 16 % • Während COVID-19: 67 % • Nach COVID-19: 34 %	• Vor COVID-19: 19 % • Während COVID-19: 62 % • Nach COVID-19: 37 %
Bedeutung von Cybersicherheit für Unternehmen	• Extrem wichtig: 34 % • Wichtiger als zuvor: 44 % • Etwas wichtig: 20 %	• Extrem wichtig: 35 % • Wichtiger als zuvor: 46 % • Etwas wichtig: 18 %	• Extrem wichtig: 44 % • Wichtiger als zuvor: 41 % • Etwas wichtig: 15 %
Schutz durch Widerstandsfähigkeit: Angehen von Bedrohungen und Herausforderungen im Bereich Cybersicherheit			
Ausmaß der Zunahme von Cyberbedrohungen und -warnungen	• Zunahme um 25 % oder mehr: 48 % • Weiß nicht: 12 %	• Zunahme um 25 % oder mehr: 37 % • Weiß nicht: 17 %	• Zunahme um 25 % oder mehr: 61 % • Weiß nicht: 8 %
Die drei größten Herausforderungen im Bereich Cybersicherheit	• Sicherer Zugriff: 52 % • Datenschutz: 40 % • Schutz vor Malware: 36 %	• Sicherer Zugriff: 57 % • Datenschutz: 41 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 39 %	• Sicherer Zugriff: 62 % • Datenschutz: 55 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 50 %
Herausforderung für den Schutz in einer Remote-Umgebung	• Private Endgeräte: 49 % • Dienstliche Laptops/ Desktop-PCs: 44 % • Cloud-Anwendungen: 26 % • Kundendaten: 25 %	• Private Endgeräte: 47 % • Dienstliche Laptops/ Desktop-PCs: 47 % • Kundendaten: 28 % • Cloud-Anwendungen: 27 %	• Dienstliche Laptops/ Desktop-PCs: 56 % • Private Endgeräte: 54 % • Kundeninformationen UND Cloud-Anwendungen: 46 %
Vorbereitung auf den Übergang zu einer Remote-Arbeitsumgebung zu Beginn von COVID-19	• Sehr gut vorbereitet: 43 % • Etwas vorbereitet: 47 % • Nicht vorbereitet: 9 %	• Sehr gut vorbereitet: 45 % • Etwas vorbereitet: 50 % • Nicht vorbereitet: 6 %	• Sehr gut vorbereitet: 40 % • Etwas vorbereitet: 53 % • Nicht vorbereitet: 6 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Priorisierung von Cybersicherheit für Gegenwart und Zukunft			
Die 3 wichtigsten IT-Lösungen zur Ermöglichung von Remote-Arbeit	• Collaboration-Tools: 73 % • Cybersicherheits-maßnahmen: 66 % • Cloud-basierte Dokumentfreigabe: 53 %	• Collaboration-Tools: 76 % • Cybersicherheits-maßnahmen: 65 % • Cloud-basierte Dokumentfreigabe: 56 %	• Collaboration-Tools: 73 % • Cybersicherheits-maßnahmen: 68 % • Cloud-basierte Dokumentfreigabe: 63 %
Eingesetzte IT-Lösungen nach Wichtigkeit geordnet (% der Unternehmen, die die Lösung als wichtigste eingestuft haben)	• Cybersicherheits-maßnahmen: 51 % • Collaboration-Tools: 50 % • Professional Services: 31 %	• Cybersicherheits-maßnahmen: 55 % • Collaboration-Tools: 48 % • Professional Services: 25 %	• Cybersicherheits-maßnahmen: 52 % • Collaboration-Tools: 41 % • Professional Services: 27 %
Die drei wichtigsten Änderungen von Cybersicher-heitsrichtlinien zur Unterstützung von Remote-Arbeit	• Erhöhte VPN-Kapazität: 63 % • Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 40 % • Endpunktschutz: 37 %	• Erhöhte VPN-Kapazität: 64 % • Implementierung von Multi-Faktor-Authentifizierung: 38 % • Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 34 %	• Erhöhte VPN-Kapazität: 59 % • Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 55 % • Implementierung von Multi-Faktor-Authentifizierung: 53 %
Anteil der permanenten Änderungen an Cybersicher-heitsrichtlinien	• 30 % oder weniger: 53 % • Mehr als 30 %: 45 %	• 30 % oder weniger: 45 % • Mehr als 30 %: 48 %	• 30 % oder weniger: 50 % • Mehr als 30 %: 45 %
Die 3 größten Herausforderungen bei der Durchsetzung von Cybersicher-heitsprotokollen	• Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 50 % • Zu viele zu verwaltende Tools/Lösungen: 46 % • Inkonsistente Schnittstellen: 27 %	• Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 54 % • Zu viele zu verwaltende Tools/Lösungen: 43 % • Inkonsistente Schnittstellen: 22 %	• Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 59 % • Zu viele zu verwaltende Tools/Lösungen: 50 % • Inkonsistente Schnittstellen: 35 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Investitionen in Cybersicherheit nehmen zu			
Änderung der zukünftigen Investitionen von Unternehmen in die Cybersicherheit aufgrund von COVID-19	• Zunahme: 56 % • Rückgang: 9 % • Keine Änderung: 29 %	• Zunahme: 52 % • Rückgang: 6 % • Keine Änderung: 37 %	• Zunahme: 66 % • Rückgang: 9 % • Keine Änderung: 22 %
Anteil des Anstiegs künftiger Investitionen in die Cybersicherheit	• 30 % oder weniger: 63 % • Mehr als 30 %: 27 %	• 30 % oder weniger: 65 % Mehr als 30 %: 23 %	• 30 % oder weniger: 59 % • Mehr als 30 %: 36 %
Cybersicherheits-Investitionen nach Wichtigkeit geordnet (% der Unternehmen, die die Investition als wichtigste eingestuft haben)	• Netzwerkzugriff: 33 % • Allgemeiner Stand der Cybersicherheit: 25 % • Benutzer- und Geräteverifizierung: 22 % • Cloud-Sicherheit: 20 %	• Allgemeiner Stand der Cybersicherheit: 33 % • Netzwerkzugriff: 29 % • Benutzer- und Geräteverifizierung: 21 % • Cloud-Sicherheit: 17 %	• Allgemeiner Stand der Cybersicherheit: 34 % • Netzwerkzugriff: 24 % • Cloud-Sicherheit: 22 % • Benutzer- und Geräteverifizierung: 20 %

Deutschland

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Die Bedeutung von Cybersicherheit in einer hybriden Zukunft der Arbeit			
Anteil der Unternehmen, in denen ***mehr als die Hälfte*** der Belegschaft remote arbeitet	• Vor COVID-19: 15 % • Während COVID-19: 53 % • Nach COVID-19: 24 %	• Vor COVID-19: 16 % • Während COVID-19: 67 % • Nach COVID-19: 34 %	• Vor COVID-19: 19 % • Während COVID-19: 62 % • Nach COVID-19: 37 %
Bedeutung von Cybersicherheit für Unternehmen	• Extrem wichtig: 32 % • Wichtiger als zuvor: 47 % • Etwas wichtig: 19 %	• Extrem wichtig: 35 % • Wichtiger als zuvor: 46 % • Etwas wichtig: 18 %	• Extrem wichtig: 44 % • Wichtiger als zuvor: 41 % • Etwas wichtig: 15 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Schutz durch Widerstandsfähigkeit: Angehen von Bedrohungen und Herausforderungen im Bereich Cybersicherheit			
Ausmaß der Zunahme von Cyberbedrohungen und -warnungen	• Zunahme um 25 % oder mehr: 31 % • Weiß nicht: 14 %	• Zunahme um 25 % oder mehr: 37 % • Weiß nicht: 17 %	• Zunahme um 25 % oder mehr: 61 % • Weiß nicht: 8 %
Die drei größten Herausforderungen im Bereich Cybersicherheit	• Sicherer Zugriff: 64 % • Datenschutz: 54 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 43 %	• Sicherer Zugriff: 57 % • Datenschutz: 41 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 39 %	• Sicherer Zugriff: 62 % • Datenschutz: 55 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 50 %
Herausforderung für den Schutz in einer Remote-Umgebung	• Private Endgeräte UND dienstliche Laptops/ Desktop-PCs: 55 % (GLEICHSTAND) • Cloud-Anwendungen: 42 % • Kundendaten: 31 %	• Private Endgeräte: 47 % • Dienstliche Laptops/ Desktop-PCs: 47 % • Kundendaten: 28 % • Cloud-Anwendungen: 27 %	• Dienstliche Laptops/ Desktop-PCs: 56 % • Private Endgeräte: 54 % • Kundeninformationen UND Cloud-Anwendungen: 46 % (GLEICHSTAND)
Vorbereitung auf den Übergang zu einer Remote-Arbeitsumgebung zu Beginn von COVID-19	• Sehr gut vorbereitet: 41 % • Etwas vorbereitet: 55 % • Nicht vorbereitet: 4 %	• Sehr gut vorbereitet: 45 % • Etwas vorbereitet: 50 % • Nicht vorbereitet: 6 %	• Sehr gut vorbereitet: 40 % • Etwas vorbereitet: 53 % • Nicht vorbereitet: 6 %
Priorisierung von Cybersicherheit für Gegenwart und Zukunft			
Die 3 wichtigsten IT-Lösungen zur Ermöglichung von Remote-Arbeit	• Collaboration-Tools: 72 % • Cybersicherheits-maßnahmen: 62 % • Cloud-basierte Dokumentfreigabe: 53 %	• Collaboration-Tools: 76 % • Cybersicherheits-maßnahmen: 65 % • Cloud-basierte Dokumentfreigabe: 56 %	• Collaboration-Tools: 73 % • Cybersicherheits-maßnahmen: 68 % • Cloud-basierte Dokumentfreigabe: 63 %
Eingesetzte IT-Lösungen nach Wichtigkeit geordnet (% der Unternehmen, die die Lösung als wichtigste eingestuft haben)	• Collaboration-Tools: 54 % • Cybersicherheits-maßnahmen: 46 % • Cloud-basierte Dokumentfreigabe: 31 %	• Cybersicherheits-maßnahmen: 55 % • Collaboration-Tools: 48 % • Professional Services: 25 %	• Cybersicherheits-maßnahmen: 52 % • Collaboration-Tools: 41 % • Professional Services: 27 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Die drei wichtigsten Änderungen von Cybersicherheitsrichtlinien zur Unterstützung von Remote-Arbeit	• Erhöhte VPN-Kapazität: 64 % • Implementierung von Multi-Faktor-Authentifizierung: 44 % • Endpunktschutz: 40 %	• Erhöhte VPN-Kapazität: 64 % • Implementierung von Multi-Faktor-Authentifizierung: 38 % • Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 34 %	• Erhöhte VPN-Kapazität: 59 % • Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 55 % • Implementierung von Multi-Faktor-Authentifizierung: 53 %
Anteil der permanenten Änderungen an Cybersicherheitsrichtlinien	• 30 % oder weniger: 57 % • Mehr als 30 %: 38 %	• 30 % oder weniger: 45 % • Mehr als 30 %: 48 %	• 30 % oder weniger: 50 % • Mehr als 30 %: 45 %
Die 3 größten Herausforderungen bei der Durchsetzung von Cybersicherheitsprotokollen	• Zu viele zu verwaltende Tools/Lösungen: 55 % • Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 49 % • Inkonsistente Schnittstellen: 23 %	• Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 54 % • Zu viele zu verwaltende Tools/Lösungen: 43 % • Inkonsistente Schnittstellen: 22 %	• Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 59 % • Zu viele zu verwaltende Tools/Lösungen: 50 % • Inkonsistente Schnittstellen: 35 %
Investitionen in Cybersicherheit nehmen zu			
Änderung der zukünftigen Investitionen von Unternehmen in die Cybersicherheit aufgrund von COVID-19	• Zunahme: 56 % • Rückgang: 6 % • Keine Änderung: 34 %	• Zunahme: 52 % • Rückgang: 6 % • Keine Änderung: 37 %	• Zunahme: 66 % • Rückgang: 9 % • Keine Änderung: 22 %
Anteil des Anstiegs künftiger Investitionen in die Cybersicherheit	• 30 % oder weniger: 77 % • Mehr als 30 %: 16 %	• 30 % oder weniger: 65 % Mehr als 30 %: 23 %	• 30 % oder weniger: 59 % • Mehr als 30 %: 36 %
Cybersicherheits-Investitionen nach Wichtigkeit geordnet (% der Unternehmen, die die Investition als wichtigste eingestuft haben)	• Netzwerkzugriff: 32 % • Allgemeiner Stand der Cybersicherheit: 28 % • Benutzer- und Geräteverifizierung: 22 % • Cloud-Sicherheit: 18 %	• Allgemeiner Stand der Cybersicherheit: 33 % • Netzwerkzugriff: 29 % • Benutzer- und Geräteverifizierung: 21 % • Cloud-Sicherheit: 17 %	• Allgemeiner Stand der Cybersicherheit: 34 % • Netzwerkzugriff: 24 % • Cloud-Sicherheit: 22 % • Benutzer- und Geräteverifizierung: 20 %

Italien

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Die Bedeutung von Cybersicherheit in einer hybriden Zukunft der Arbeit			
Anteil der Unternehmen, in denen ***mehr als die Hälfte*** der Belegschaft remote arbeitet	• Vor COVID-19: 15 % • Während COVID-19: 65 % • Nach COVID-19: 33 %	• Vor COVID-19: 16 % • Während COVID-19: 67 % • Nach COVID-19: 34 %	• Vor COVID-19: 19 % • Während COVID-19: 62 % • Nach COVID-19: 37 %
Bedeutung von Cybersicherheit für Unternehmen	• Extrem wichtig: 28 % • Wichtiger als zuvor: 57 % • Etwas wichtig: 15 %	• Extrem wichtig: 35 % • Wichtiger als zuvor: 46 % • Etwas wichtig: 18 %	• Extrem wichtig: 44 % • Wichtiger als zuvor: 41 % • Etwas wichtig: 15 %
Schutz durch Widerstandsfähigkeit: Angehen von Bedrohungen und Herausforderungen im Bereich Cybersicherheit			
Ausmaß der Zunahme von Cyberbedrohungen und -warnungen	• Zunahme um 25 % oder mehr: 43 % • Weiß nicht: 14 %	• Zunahme um 25 % oder mehr: 37 % • Weiß nicht: 17 %	• Zunahme um 25 % oder mehr: 61 % • Weiß nicht: 8 %
Die drei größten Herausforderungen im Bereich Cybersicherheit	• Sicherer Zugriff: 68 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 49 % • Datenschutz: 47 %	• Sicherer Zugriff: 57 % • Datenschutz: 41 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 39 %	• Sicherer Zugriff: 62 % • Datenschutz: 55 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 50 %
Herausforderung für den Schutz in einer Remote-Umgebung	• Private Endgeräte: 46 % • Dienstliche Laptops/ Desktop-PCs: 42 % • Kundendaten: 30 % • Cloud-Anwendungen: 21 %	• Private Endgeräte: 47 % • Dienstliche Laptops/ Desktop-PCs: 47 % • Kundendaten: 28 % • Cloud-Anwendungen: 27 %	• Dienstliche Laptops/ Desktop-PCs: 56 % • Private Endgeräte: 54 % • Kundeninformationen UND Cloud-Anwendungen: 46 % (GLEICHSTAND)
Vorbereitung auf den Übergang zu einer Remote-Arbeitsumgebung zu Beginn von COVID-19	• Sehr gut vorbereitet: 35 % • Etwas vorbereitet: 57 % • Nicht vorbereitet: 8 %	• Sehr gut vorbereitet: 45 % • Etwas vorbereitet: 50 % • Nicht vorbereitet: 6 %	• Sehr gut vorbereitet: 40 % • Etwas vorbereitet: 53 % • Nicht vorbereitet: 6 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Priorisierung von Cybersicherheit für Gegenwart und Zukunft			
Die 3 wichtigsten IT-Lösungen zur Ermöglichung von Remote-Arbeit	• Collaboration-Tools: 79 % • Cybersicherheits-maßnahmen: 68 % • Cloud-basierte Dokumentfreigabe: 62 %	• Collaboration-Tools: 76 % • Cybersicherheits-maßnahmen: 65 % • Cloud-basierte Dokumentfreigabe: 56 %	• Collaboration-Tools: 73 % • Cybersicherheits-maßnahmen: 68 % • Cloud-basierte Dokumentfreigabe: 63 %
Eingesetzte IT-Lösungen nach Wichtigkeit geordnet (% der Unternehmen, die die Lösung als wichtigste eingestuft haben)	• Cybersicherheits-maßnahmen: 58 % • Collaboration-Tools: 44 % • Cloud-basierte Dokumentfreigabe: 21 %	• Cybersicherheits-maßnahmen: 55 % • Collaboration-Tools: 48 % • Professional Service: 25 %	• Cybersicherheits-maßnahmen: 52 % • Collaboration-Tools: 41 % • Professional Services: 27 %
Die drei wichtigsten Änderungen von Cybersicher-heitsrichtlinien zur Unterstützung von Remote-Arbeit	• Erhöhte VPN-Kapazität: 66 % • Implementierung von Multi-Faktor-Authentifizierung: 40 % • Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 39 %	• Erhöhte VPN-Kapazität: 64 % • Implementierung von Multi-Faktor-Authentifizierung: 38 % • Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 34 %	• Erhöhte VPN-Kapazität: 59 % • Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 55 % • Implementierung von Multi-Faktor-Authentifizierung: 53 %
Anteil der permanenten Änderungen an Cybersicher-heitsrichtlinien	• 30 % oder weniger: 39 % • Mehr als 30 %: 46 %	• 30 % oder weniger: 45 % • Mehr als 30 %: 48 %	• 30 % oder weniger: 50 % • Mehr als 30 %: 45 %
Die 3 größten Herausforderungen bei der Durchsetzung von Cybersicher-heitsprotokollen	• Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 63 % • Zu viele zu verwaltende Tools/Lösungen: 41 % • Mangelnde Transparenz/ inkonsistente Schnittstellen: 15 %	• Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 54 % • Zu viele zu verwaltende Tools/Lösungen: 43 % • Inkonsistente Schnittstellen: 22 %	• Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 59 % • Zu viele zu verwaltende Tools/Lösungen: 50 % • Inkonsistente Schnittstellen: 35 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Investitionen in Cybersicherheit nehmen zu			
Änderung der zukünftigen Investitionen von Unternehmen in die Cybersicherheit aufgrund von COVID-19	• Zunahme: 52 % • Rückgang: 6 % • Keine Änderung: 37 %	• Zunahme: 52 % • Rückgang: 6 % • Keine Änderung: 37	• Zunahme: 66 % • Rückgang: 9 % • Keine Änderung: 22 %
Anteil des Anstiegs künftiger Investitionen in die Cybersicherheit	• 30 % oder weniger: 63 % • Mehr als 30 %: 26 %	• 30 % oder weniger: 65 % Mehr als 30 %: 23 %	• 30 % oder weniger: 59 % • Mehr als 30 %: 36 %
Cybersicherheits-Investitionen nach Wichtigkeit geordnet (% der Unternehmen, die die Investition als wichtigste eingestuft haben)	• Allgemeiner Stand der Cybersicherheit: 32 % • Netzwerkzugriff: 32 % • Benutzer- und Geräteverifizierung: 21 % • Cloud-Sicherheit: 15 %	• Allgemeiner Stand der Cybersicherheit: 33 % • Netzwerkzugriff: 29 % • Benutzer- und Geräteverifizierung: 21 % • Cloud-Sicherheit: 17 %	• Allgemeiner Stand der Cybersicherheit: 34 % • Netzwerkzugriff: 24 % • Cloud-Sicherheit: 22 % • Benutzer- und Geräteverifizierung: 20 %

Vereinigtes Königreich

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Die Bedeutung von Cybersicherheit in einer hybriden Zukunft der Arbeit			
Anteil der Unternehmen, in denen ***mehr als die Hälfte*** der Belegschaft remote arbeitet	• Vor COVID-19: 18 % • Während COVID-19: 85 % • Nach COVID-19: 50 %	• Vor COVID-19: 16 % • Während COVID-19: 67 % • Nach COVID-19: 34 %	• Vor COVID-19: 19 % • Während COVID-19: 62 % • Nach COVID-19: 37 %
Bedeutung von Cybersicherheit für Unternehmen	• Extrem wichtig: 46 % • Wichtiger als zuvor: 35 % • Etwas wichtig: 17 %	• Extrem wichtig: 35 % • Wichtiger als zuvor: 46 % • Etwas wichtig: 18 %	• Extrem wichtig: 44 % • Wichtiger als zuvor: 41 % • Etwas wichtig: 15 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Schutz durch Widerstandsfähigkeit: Angehen von Bedrohungen und Herausforderungen im Bereich Cybersicherheit			
Ausmaß der Zunahme von Cyberbedrohungen und -warnungen	• Zunahme um 25 % oder mehr: 24 % • Weiß nicht: 27 %	• Zunahme um 25 % oder mehr: 37 % • Weiß nicht: 17 %	• Zunahme um 25 % oder mehr: 61 % • Weiß nicht: 8 %
Die drei größten Herausforderungen im Bereich Cybersicherheit	• Sicherer Zugriff: 43 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 31 % • Schutz vor Malware: 27 %	• Sicherer Zugriff: 57 % • Datenschutz: 41 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 39 %	• Sicherer Zugriff: 62 % • Datenschutz: 55 % • Aufrechterhaltung von Kontroll- und Durchsetzungsrichtlinien: 50 %
Herausforderung für den Schutz in einer Remote-Umgebung	• Dienstliche Laptops/ Desktop-PCs: 46 % • Private Endgeräte: 39 % • Kundendaten: 27 % • Cloud-Anwendungen: 20 %	• Private Endgeräte: 47 % • Dienstliche Laptops/ Desktop-PCs: 47 % • Kundendaten: 28 % • Cloud-Anwendungen: 27 %	• Dienstliche Laptops/ Desktop-PCs: 56 % • Private Endgeräte: 54 % • Kundeninformationen UND Cloud-Anwendungen: 46 % (GLEICHSTAND)
Vorbereitung auf den Übergang zu einer Remote-Arbeitsumgebung zu Beginn von COVID-19	• Sehr gut vorbereitet: 59 % • Etwas vorbereitet: 39 % • Nicht vorbereitet: 2 %	• Sehr gut vorbereitet: 45 % • Etwas vorbereitet: 50 % • Nicht vorbereitet: 6 %	• Sehr gut vorbereitet: 40 % • Etwas vorbereitet: 53 % • Nicht vorbereitet: 6 %
Priorisierung von Cybersicherheit für Gegenwart und Zukunft			
Die 3 wichtigsten IT-Lösungen zur Ermöglichung von Remote-Arbeit	• Collaboration-Tools: 79 % • Cybersicherheits-maßnahmen: 65 % • Cloud-basierte Dokumentfreigabe: 57 %	• Collaboration-Tools: 76 % • Cybersicherheits-maßnahmen: 65 % • Cloud-basierte Dokumentfreigabe: 56 %	• Collaboration-Tools: 73 % • Cybersicherheits-maßnahmen: 68 % • Cloud-basierte Dokumentfreigabe: 63 %
Eingesetzte IT-Lösungen nach Wichtigkeit geordnet (% der Unternehmen, die die Lösung als wichtigste eingestuft haben)	• Cybersicherheits-maßnahmen: 63 % • Collaboration-Tools: 43 % • Cloud-basierte Dokumentfreigabe: 23 %	• Cybersicherheits-maßnahmen: 55 % • Collaboration-Tools: 48 % • Professional Services: 25 %	• Cybersicherheits-maßnahmen: 52 % • Collaboration-Tools: 41 % • Professional Services: 27 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Die drei wichtigsten Änderungen von Cybersicherheitsrichtlinien zur Unterstützung von Remote-Arbeit	· Erhöhte VPN-Kapazität: 65 % · Implementierung von Multi-Faktor-Authentifizierung: 35 % · Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 29 %	· Erhöhte VPN-Kapazität: 64 % · Implementierung von Multi-Faktor-Authentifizierung: 38 % · Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 34 %	· Erhöhte VPN-Kapazität: 59 % · Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 55 % · Implementierung von Multi-Faktor-Authentifizierung: 53 %
Anteil der permanenten Änderungen an Cybersicherheitsrichtlinien	· 30 % oder weniger: 30 % · Mehr als 30 %: 64 %	· 30 % oder weniger: 45 % · Mehr als 30 %: 48 %	· 30 % oder weniger: 50 % · Mehr als 30 %: 45 %
Die 3 größten Herausforderungen bei der Durchsetzung von Cybersicherheitsprotokollen	· Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 57 % · Zu viele zu verwaltende Tools/Lösungen: 29 % · Inkonsistente Schnittstellen: 21 %	· Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 54 % · Zu viele zu verwaltende Tools/Lösungen: 43 % · Inkonsistente Schnittstellen: 22 %	· Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 59 % · Zu viele zu verwaltende Tools/Lösungen: 50 % · Inkonsistente Schnittstellen: 35 %
Investitionen in Cybersicherheit nehmen zu			
Änderung der zukünftigen Investitionen von Unternehmen in die Cybersicherheit aufgrund von COVID-19	· Zunahme: 44 % · Rückgang: 1 % · Keine Änderung: 49 %	· Zunahme: 52 % · Rückgang: 6 % · Keine Änderung: 37 %	· Zunahme: 66 % · Rückgang: 9 % · Keine Änderung: 22 %
Anteil des Anstiegs künftiger Investitionen in die Cybersicherheit	· 30 % oder weniger: 57 % · Mehr als 30 %: 21 %	· 30 % oder weniger: 65 % Mehr als 30 %: 23 %	· 30 % oder weniger: 59 % · Mehr als 30 %: 36 %
Cybersicherheits-Investitionen nach Wichtigkeit geordnet (% der Unternehmen, die die Investition als wichtigste eingestuft haben)	· Allgemeiner Stand der Cybersicherheit: 48 % · Benutzer- und Geräteverifizierung: 20 % · Netzwerkzugriff: 17 % · Cloud-Sicherheit: 15 %	· Allgemeiner Stand der Cybersicherheit: 33 % · Netzwerkzugriff: 29 % · Benutzer- und Geräteverifizierung: 21 % · Cloud-Sicherheit: 17 %	· Allgemeiner Stand der Cybersicherheit: 34 % · Netzwerkzugriff: 24 % · Cloud-Sicherheit: 22 % · Benutzer- und Geräteverifizierung: 20 %

Studienparameter	% im Land	Regionaler Durchschnitt	Globaler Durchschnitt
Die drei wichtigsten Änderungen von Cybersicherheitsrichtlinien zur Unterstützung von Remote-Arbeit	· Erhöhte VPN-Kapazität: 65 % · Implementierung von Multi-Faktor-Authentifizierung: 35 % · Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 29 %	· Erhöhte VPN-Kapazität: 64 % · Implementierung von Multi-Faktor-Authentifizierung: 38 % · Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 34 %	· Erhöhte VPN-Kapazität: 59 % · Ausweitung der Webkontrollen und Richtlinien zur akzeptablen Nutzung: 55 % · Implementierung von Multi-Faktor-Authentifizierung: 53 %
Anteil der permanenten Änderungen an Cybersicherheitsrichtlinien	· 30 % oder weniger: 30 % · Mehr als 30 %: 64 %	· 30 % oder weniger: 45 % · Mehr als 30 %: 48 %	· 30 % oder weniger: 50 % · Mehr als 30 %: 45 %
Die 3 größten Herausforderungen bei der Durchsetzung von Cybersicherheitsprotokollen	· Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 57 % · Zu viele zu verwaltende Tools/Lösungen: 29 % · Inkonsistente Schnittstellen: 21 %	· Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 54 % · Zu viele zu verwaltende Tools/Lösungen: 43 % · Inkonsistente Schnittstellen: 22 %	· Mangelnde Sensibilisierung/ Aufklärung der Mitarbeiter: 59 % · Zu viele zu verwaltende Tools/Lösungen: 50 % · Inkonsistente Schnittstellen: 35 %
Investitionen in Cybersicherheit nehmen zu			
Änderung der zukünftigen Investitionen von Unternehmen in die Cybersicherheit aufgrund von COVID-19	· Zunahme: 44 % · Rückgang: 1 % · Keine Änderung: 49 %	· Zunahme: 52 % · Rückgang: 6 % · Keine Änderung: 37 %	· Zunahme: 66 % · Rückgang: 9 % · Keine Änderung: 22 %
Anteil des Anstiegs künftiger Investitionen in die Cybersicherheit	· 30 % oder weniger: 57 % · Mehr als 30 %: 21 %	· 30 % oder weniger: 65 % Mehr als 30 %: 23 %	· 30 % oder weniger: 59 % · Mehr als 30 %: 36 %
Cybersicherheits-Investitionen nach Wichtigkeit geordnet (% der Unternehmen, die die Investition als wichtigste eingestuft haben)	· Allgemeiner Stand der Cybersicherheit: 48 % · Benutzer- und Geräteverifizierung: 20 % · Netzwerkzugriff: 17 % · Cloud-Sicherheit: 15 %	· Allgemeiner Stand der Cybersicherheit: 33 % · Netzwerkzugriff: 29 % · Benutzer- und Geräteverifizierung: 21 % · Cloud-Sicherheit: 17 %	· Allgemeiner Stand der Cybersicherheit: 34 % · Netzwerkzugriff: 24 % · Cloud-Sicherheit: 22 % · Benutzer- und Geräteverifizierung: 20 %

DIE WICHTIGSTEN ERKENNTNISSE UND EMPFEHLUNGEN

DIE WICHTIGSTEN ERKENNTNISSE UND EMPFEHLUNGEN

#1 Die Zukunft der Arbeit ist dynamisch: Cybersicherheit muss den Bedürfnissen einer verteilten Belegschaft gerecht werden.

Es hat sich gezeigt, dass Mitarbeiter vernetzt und produktiv bleiben, während sie längere Zeit außerhalb des Büros arbeiten. Wahrscheinlich werden viele Unternehmen auf eine hybride Arbeitsumgebung umstellen, die sowohl die Mitarbeiter im Büro als auch Remote-Arbeit unterstützt. Dies bietet Arbeitgebern und Mitarbeitern mehr Auswahl und Flexibilität in Bezug auf Geschäfts- und Humankapital sowie mehr Vielfalt für die Belegschaft. Mit dem abrupten Umstieg sind aber auch eine Reihe von Cybersicherheits-Herausforderungen entstanden, z. B. die Fortführung des Geschäfts in einer völlig neuen Umgebung oder der sichere Zugriff im viel größeren Maßstab als bisher.

Mitarbeiter verbinden ihre Bürogeräte mit ihrem privaten WLAN oder externen Netzwerken oder nutzen ihre privaten Geräte, um sich mit Unternehmensanwendungen in der Cloud zu verbinden. Dies stellt eine unvorhergesehene Belastung für Sicherheits- und IT-Teams dar, die für eine nie dagewesene Anzahl an externen Mitarbeitern und deren Geräte einen schnellen Support bereitstellen müssen – und das, ohne die Sicherheit zu gefährden. Richtlinien und Kontrollen, die früher am Hauptsitz galten, müssen dem Mitarbeiter jetzt folgen, wo und wann immer er Zugriff benötigt. Darüber hinaus bringt die Gelegenheit zur Remote-Arbeit einen wesentlichen Nachteil mit sich: Moderne Angreifer haben mehr Phishing-Angriffe gestartet, um Benutzer zu täuschen und Informationen von ihnen zu stehlen, die Systeme der nun remote arbeitenden Belegschaft mit Malware zu kompromittieren oder Lücken in der sich entwickelnden Cybersicherheit eines Unternehmens auszunutzen.

Unternehmen müssen eine flexible und sichere hybride Arbeitsumgebung schaffen, in der Mitarbeiter innerhalb und außerhalb des Netzwerks mit ähnlichem Schutz arbeiten. Unternehmen und IT-Verantwortliche müssen wichtige Änderungen an ihren Technologie- und Geschäftsprioritäten vornehmen. Daher sollte die Cybersicherheit die Brücke sein, die es Unternehmen ermöglicht, ihr volles Potenzial auszuschöpfen.

#2 Der Erfolg einer flexiblen, hybriden Belegschaft hängt von Vorbereitung, Zusammenarbeit und Befähigung ab.

Eines der Hauptprobleme, die sich aus der Umstellung auf Remote-Arbeit in den letzten acht Monaten über Nacht ergeben haben, ist die Frage, wie gut Unternehmen den Übergang hinbekommen haben. Unternehmen, die vor der Pandemie inkrementelle und kontinuierliche Investitionen in Technologien wie Cloud-Security-Lösungen und Zero-Trust-Frameworks getätigt haben, waren am besten auf Remote-Arbeit vorbereitet. Auch die Verbesserung der Cybersicherheitsmaßnahmen, die solche Vorkehrungen unterstützen, hat Unternehmen in eine bessere Position versetzt, um der potenziellen Zunahme der Anzahl und Vielfalt von Cybersicherheitsangriffen zu begegnen.

Um jedoch die Vorteile eines flexiblen und hybriden Arbeitsplatzes voll ausschöpfen zu können, dürfen solche Investitionen nicht in einem Vakuum getätigt werden. Mit der Umstellung auf eine verteilte Belegschaft müssen Netzwerk- und Sicherheitsteams jederzeit und überall einen nahtlosen und sicheren Zugriff auf Anwendungen und Services bieten. Sicherheit, Vernetzung und Zusammenarbeit dürfen nicht länger getrennt betrachtet werden, sondern müssen Hand in Hand gehen. Neben diesen Funktionen müssen Führungskräfte zusätzliche Durchsetzungsprotokolle und verbesserte Cybersicherheitsrichtlinien einrichten. Dies sollte auch durch ein solides Schulungsprogramm für Mitarbeiter ergänzt werden, da Investitionen in eine gesunde Sicherheitskultur absolut entscheidend sind.

#3 Einfachere und effektivere Cybersicherheit ist entscheidend für die Stärkung der Business Resiliency.

Die Erfahrung der langfristigen Remote-Arbeit hat den Wert der Cybersicherheit in den in den Strategien von Unternehmen erhöht und langfristige Änderungen in den Unternehmens-Cybersicherheitsrichtlinien wahrscheinlich gemacht. Darüber hinaus haben viele Unternehmen erklärt, dass sie beabsichtigen, ihre Ausgaben für Cybersicherheit in Zukunft zu erhöhen.

Angesichts der vielen konkurrierenden Prioritäten für IT-Verantwortliche darf die Sicherheit kein nachträglicher Gedanke sein – sie sollte die Grundlage für den Erfolg jeder Digitalisierungsbemühung sein. Dies gewährleistet die Sicherheit, Skalierbarkeit und Anpassungsfähigkeit dieser Bemühungen. Um die Wahrscheinlichkeit und die Auswirkungen einer Cybersicherheitsverletzung zu verringern, müssen Unternehmen auch nach Wegen suchen, um die Komplexität ihrer Cybersicherheitsmaßnahmen zu reduzieren. Ein vereinfachter Ansatz für effektivere Sicherheit gewährleistet, dass sie die geschäftliche Entwicklung fördert und nicht behindert, was jetzt und in Zukunft erforderlich ist.

Empfehlungen:

Damit Unternehmen es ihren Mitarbeitern ermöglichen können, überall, jederzeit und auf jedem Gerät sicher zu arbeiten, sollte Cybersicherheit die Grundlage jeder IT-Investition sein. Dies erfordert einen plattformbasierten Ansatz, um hochwirksame Sicherheit im Netzwerk, auf Endpunkten und in der Cloud zu gewährleisten. Selbst herausragende Punktlösungen können einfach nicht mithalten. Da Sicherheit weniger komplex sein muss, müssen Lösungen zusammenarbeiten und benutzerfreundlich sein.

Um eine verteilte Belegschaft sicher zu unterstützen und die Flexibilität zu bieten, sich an die Zukunft der Arbeit anzupassen, sollten Unternehmen die folgenden Bedingungen sicherstellen:

- Identitätsverifizierung, um Vertrauen aufzubauen: Ist ein Benutzer wirklich der, für den er sich ausgibt?
- Arbeitsmöglichkeiten auf jedem Gerät und mit jeder Art von Verbindung – auf sichere Weise
- Zugriff auf die Unternehmensanwendungen und -daten, die Mitarbeiter benötigen
- Schutz von Benutzern vor Bedrohungen, sobald sie sich im Netzwerk befinden

Die Zukunft der Arbeit: zehn Erkenntnisse

1. Führen Sie eine Zero-Trust-Strategie ein, um die Identität aller Benutzer zu überprüfen, bevor Sie Zugriff auf vom Unternehmen genehmigte Anwendungen gewähren. So schützen Sie Mitarbeiter, Workloads und die Arbeitsumgebung.
2. Multi-Faktor-Authentifizierung (MFA) ist ein natürlicher erster Schritt beim Schutz verteilter Mitarbeiter, mit dem Sie die Identität von Mitarbeitern überprüfen können, die versuchen, auf Unternehmensressourcen zuzugreifen.
3. Implementierung eines VPN, das einen sicheren Tunnel zwischen Benutzern und Anwendungen bietet, damit Mitarbeiter unterwegs und von zu Hause aus produktiv arbeiten und vernetzt bleiben können. Die Lösung stellt sicher, dass nur autorisierte Benutzer Zugang erhalten. Sie bietet das richtige Maß an Sicherheit, ohne die Benutzerfreundlichkeit zu beeinträchtigen.
4. Verwendung von DNS. Die meisten Sicherheitsverletzungen zielen auf Endpunktbenutzer ab. Deshalb ist eine erste Verteidigungslinie auf DNS-Ebene erforderlich. Diese entscheidende erste Ebene blockiert Domänen, die mit schädlichem Verhalten in Zusammenhang stehen, bevor sie in Ihr Netzwerk gelangen, oder Malware enthalten, wenn sie sich bereits im Netzwerk befinden.
5. Schützen Sie Office 365-E-Mails vor modernen Bedrohungen. Da E-Mail der Angriffsvektor Nr. 1 ist, ist Schutz vor E-Mail-Bedrohungen wie Phishing, Ransomware, Business Email Compromise (BEC) usw. erforderlich. Dazu wird eine integrierte, Cloud-native Sicherheitslösung für Microsoft 365 benötigt, die Bedrohungen für Office 365 von internen und externen Absendern stoppt.
6. Setzen Sie auf sichere Endpunktlösungen als letzte Verteidigungslinie. Endpunktsicherheit verhindert nicht nur Cyberangriffe, sondern sorgt auch für eine schnelle Erkennung, Eindämmung und Behebung, wenn schädliche Dateien die ersten Verteidigungsmaßnahmen umgehen und auf die Endpunkte gelangen.
7. Beschleunigen Sie die strategische Einführung Cloud-basierter Sicherheitslösungen, um Ihre Mitarbeiter zu schützen, indem Sie eine nahtlose Verbindung zu Anwendungen in jeder Umgebung und an jedem Standort bereitstellen. Secure Access Service Edge (SASE) ist eine Netzwerkarchitektur, die VPN- und SD-WAN-Funktionen mit Cloud-nativen Sicherheitsfunktionen, z. B. sichere Web-Gateways, Cloud Access Security Broker und Firewalls, kombiniert – vollständig über die Cloud bereitgestellt.
8. Erzielen Sie größere Vorteile aus vorhandenen Produkten durch einen plattformbasierten Ansatz. Dies ermöglicht Transparenz über mehrere Sicherheitslösungen in einem einheitlichen Dashboard bei gleichzeitiger Integration mit Sicherheitslösungen von Drittanbietern.
9. Automatisieren Sie Security Operations Center (SOC)-Workflows wie Bedrohungsermittlung, Erkennung und Problembehebung, um die Effizienz und Präzision zu steigern und die Betriebskosten zu senken. So können Sicherheitsteams neue geschäftliche und technologische Anforderungen besser unterstützen und gleichzeitig einer sich ständig verändernden Bedrohungslandschaft immer einen Schritt voraus sein.
10. Denken Sie daran: Menschen können das stärkste Glied in jeder Verteidigung sein. Fördern Sie das Bewusstsein Ihrer Mitarbeiter für Cybersicherheit und ermächtigen Sie sie. Unternehmen müssen auch die Mitarbeiter dafür sensibilisieren, wie wichtig sicherheitsorientiertes Verhalten ist, z. B. die Fähigkeit zur Erkennung von Phishing-Angriffen, die Anwendung guter Kennwortrichtlinien und die Durchführung regelmäßiger Software-Updates. Cybersicherheitsschulungen dürfen keine einmal jährlich stattfindenden, Compliance-basierten Schulungen sein, die bei den meisten Mitarbeitern nicht sehr beliebt sind. Sie muss Teil der Unternehmenskultur sein.

Cisco SecureX™ ist eine Cloud-native, integrierte Plattform, die das Sicherheits- und Netzwerkportfolio von Cisco mit Ihrer bestehenden Infrastruktur verbindet. Sie ist integriert, einfach, zwecks Transparenz einheitlich und maximiert die Betriebseffizienz durch automatisierte Workflows.

ÜBER DEN BERICHT ZUR ZUKUNFT DER SICHEREN REMOTE-ARBEIT

Im Februar und März 2020 versuchten Unternehmen, ihre Mitarbeiter zu schützen, indem sie ihnen die Möglichkeit gaben, von zu Hause aus zu arbeiten. Diese Vorgehensweise war zwar für den Schutz von Menschen und Gemeinschaften notwendig, trennte die Sicherheitsexperten jedoch physisch von ihren eigenen Teams, von den Mitarbeitern, die von ihnen abhängig waren, und von den kritischen Systemen, für die sie verantwortlich waren. Die Organisation der Remote-Arbeit belastete auch bestehende Digitalrichtlinien und die Business-Continuity-Planung in einer ohnehin stressigen Zeit noch stärker.

Das soll nicht heißen, dass wir keine Möglichkeit gefunden hätten, uns an diese neue Arbeitsweise anzupassen. Vor diesem Hintergrund wurden vom 16. Juni bis 4. September 2020 mehr als 3.000 IT-Entscheidungsträger in Unternehmen aller Größe aus einem Spektrum von 30 Branchen befragt, darunter Finanzdienstleister, Gesundheitswesen, Architektur, Transportwesen usw., um zu verstehen, welche Auswirkungen die COVID-19-Krise im Bereich der Cybersicherheit auf sie hatte.

3.196
Befragte
in
21
Märkten

AMER:
- Brasilien
- Kanada
- Mexiko
- USA

EUROPA:
- Frankreich
- Deutschland
- Italien
- Vereinigtes Königreich

APJC:
- Australien
- China
- Hongkong
- Indien
- Indonesien
- Japan
- Südkorea
- Malaysia
- Philippinen
- Singapur
- Taiwan
- Thailand
- Vietnam

Branchen:
- Buchhaltung
- Architektur
- Unternehmensberatung
- Chemische Verfahrenstechnik oder Herstellung
- Bauwesen
- Bildungswesen
- Finanzdienstleistungen
- Behörden
- Gesundheitswesen
- Fertigung:
- Nicht computerbezogen
- Einzelhandel
- Softwareentwicklung
- Telekommunikation
- Transport- und Verkehrswesen
- Großhandel und Vertrieb
- Gemeinnützige Organisationen

Zielgruppe:
Fachleute, die für die IT ihres Unternehmens verantwortlich sind

Zu diesen Unternehmen zählen:
- klein (zwischen 1 und 249 Mitarbeiter),
- mittelgroß (zwischen 250 und 999 Mitarbeiter) und
- groß (1.000 Mitarbeiter oder mehr)

Ziele:

- Untersuchen der **Herausforderungen**, die sich ergeben, wenn die Belegschaft eines Unternehmens praktisch über Nacht ganz oder teilweise in eine **Remote-Arbeitsumgebungen** versetzt wird, sowie der **Bereitschaft** von Unternehmen auf der ganzen Welt, ihr Geschäft in einer Remote-Arbeitsausrichtung zu schützen

- Verstehen, wie sich Unternehmen an diesen plötzlichen Wandel angepasst haben, einschließlich der Veränderungen ihrer Prioritäten, Richtlinien und Investitionen im Bereich der Cybersicherheit

- Unternehmen ermöglichen, ein hybrides Arbeitsumfeld zu verstehen und sich darauf vorzubereiten, indem sie sich sicher anpassen, um gegenwärtige und zukünftige Unternehmensressourcen zu schützen

Studienparameter

1. Die Zunahme von Remote-Mitarbeitern während COVID-19 und die Bedeutung der Cybersicherheit zu ihrer Unterstützung

1) Anzahl der Personen, die vor, während und nach COVID-19 remote arbeiteten
2) Bedeutung der Cybersicherheit in der heutigen COVID-19- und Remote-Arbeitsumgebung

2. Vorbereitung auf die Cybersicherheit, Bedrohungen und Herausforderungen

1) Wie gut sind Unternehmen mit ihren Cybersicherheitsfunktionen/-lösungen auf den (plötzlichen) Übergang zum Remote-Betrieb vorbereitet?
2) Arten von Cybersicherheitsherausforderungen, die bei umfangreicher Remote-Arbeit auftreten, und deren Schweregrad nach Wichtigkeit
3) Die größten Schutz-Herausforderungen bei der Remote-Arbeit

3. Technologieprioritäten und -annahme zur Unterstützung der Remote-Arbeit

1) Art der eingesetzten Technologien
2) Einstufung und Reihenfolge ihrer Bedeutung

4. Veränderungen bei Cybersicherheitsrichtlinien und Durchsetzungsprotokollen zur Unterstützung von Remote-Mitarbeitern

1) Art der vorgenommenen Änderungen
2) Anteil der Änderungen an Cybersicherheitsrichtlinien
3) Herausforderungen bei der Durchsetzung von Cybersicherheitsprotokollen

5. Investitionen in die Cybersicherheit – heute und in Zukunft

1) Wird COVID-19 zukünftige Investitionen in die Cybersicherheit des Unternehmens verändern?
2) Prozentsatz der Zunahme oder Abnahme der Investitionen (falls zutreffend)
3) Einstufung der zukünftigen Investitionen in die Cybersicherheit nach Wichtigkeit

Bericht zur Zukunft der sicheren Remote-Arbeit

cisco SECURE