Sicherheit in einer mobilen und flexiblen Arbeitswelt: CIOs und CISOs als Wegbereiter für zukunftsfähige hybride Konzepte

In diesem detaillierten Forschungsbericht stellen wir effektive Techniken für die erfolgreiche Umstellung von einer gefährdeten Legacy-Infrastruktur auf eine Zero-Trust-Strategie vor.

EIN ANALYSEREPORT VON HMG STRATEGY MIT UNTERSTÜTZUNG VON ZSCALER

HMG STRATEGY

zscaler™

KURZFASSUNG

Mit dem Eintritt in die nächste Phase der weltweiten Coronapandemie wird für zahlreiche Unternehmen weltweit insbesondere eine Frage akut: Wie lässt sich – nach über zwei Jahren, in denen sich viele Mitarbeiter an die Freiheit und Flexibilität dezentraler Konzepte gewöhnt haben – die Rückkehr zur Präsenzarbeit bewältigen? Eine Umfrage nach der anderen ergibt, dass die Mehrzahl der Beschäftigten sich für die Zukunft einen Umstieg auf hybride Modelle wünscht – also eine Mischung aus Präsenz- und Remote-Arbeit – und im Zweifelsfall bereit ist, sich nach neuen Berufschancen umzusehen, wenn der Arbeitgeber ihnen keinen Freiraum gewährt.

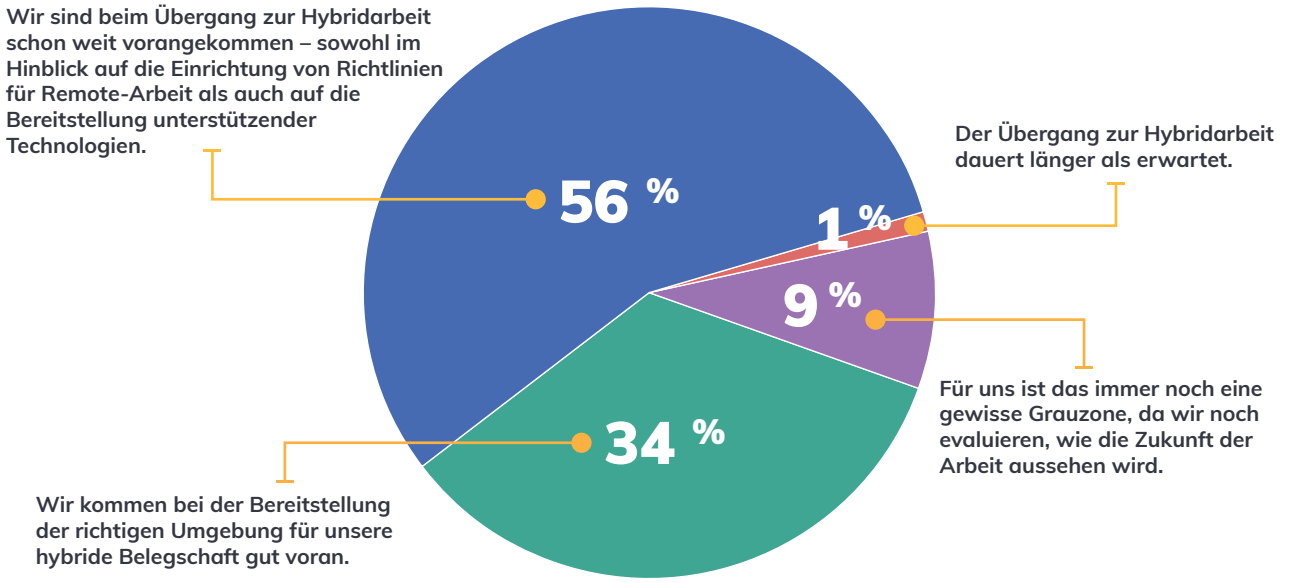
Aus Sicht der Organisationen stellt sich die Frage, wie die Umstellung auf Hybridarbeit möglichst effektiv und reibungslos gelingt. Speziell CIOs und CISOs sind hier gefordert, in Absprache mit Vorstandskollegen ein agiles und produktives Konzept zu erarbeiten, das zuverlässigen Schutz für die IT-Infrastruktur des Unternehmens gewährleistet.

In einer aktuellen Umfrage unter 138 CIOs, CISOs und Technologievorständen, die HMG Strategy im Auftrag von Zscaler durchgeführt hat, gaben 56 % der Befragten an, ihre Organisationen seien bei der Umstellung auf hybride Arbeitskonzepte bereits „weit fortgeschritten“. Berücksichtigt wurde dabei sowohl die Einrichtung entsprechender Richtlinien als auch die Bereitstellung von Technologien zur Unterstützung von Remote-Arbeit. 44 % bezeichneten die laufende Umstellung jedoch als noch nicht abgeschlossen.

Beinahe ein Fünftel der Befragten aus der zweiten Gruppe stimmte der Aussage zu, der Übergang sei für ihre Organisation „immer noch eine gewisse Grauzone, da wir noch evaluieren, wie die Zukunft der Arbeit aussehen wird“.

Umstellung auf hybride Arbeitskonzepte

Wie würden Sie den aktuellen Stand Ihrer Organisation beim Übergang von Remote- zur Hybridarbeit charakterisieren?



Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

„Die Mehrheit der Organisationen bewältigt die Umstellung von Remote- auf Hybridarbeit einigermaßen, ohne dass es sie jedoch wirklich voranbringt“, so die Einschätzung von **Bryan Green**, CISO Americas bei Zscaler. Als Beispiel verweist er auf die Investitionen in Übergangslösungen wie den Ausbau der VPN-Nutzung oder die Umgehung sensibler Anwendungen mit hohem Bandbreitenverbrauch (etwa Videokonferenzsysteme), mit denen viele Unternehmen die Corona-bedingte jähe Umstellung auf Remote-Arbeit ermöglichten. „Dabei werden jedoch nicht unbedingt die richtigen langfristigen Sicherheitsentscheidungen getroffen“, moniert Green.

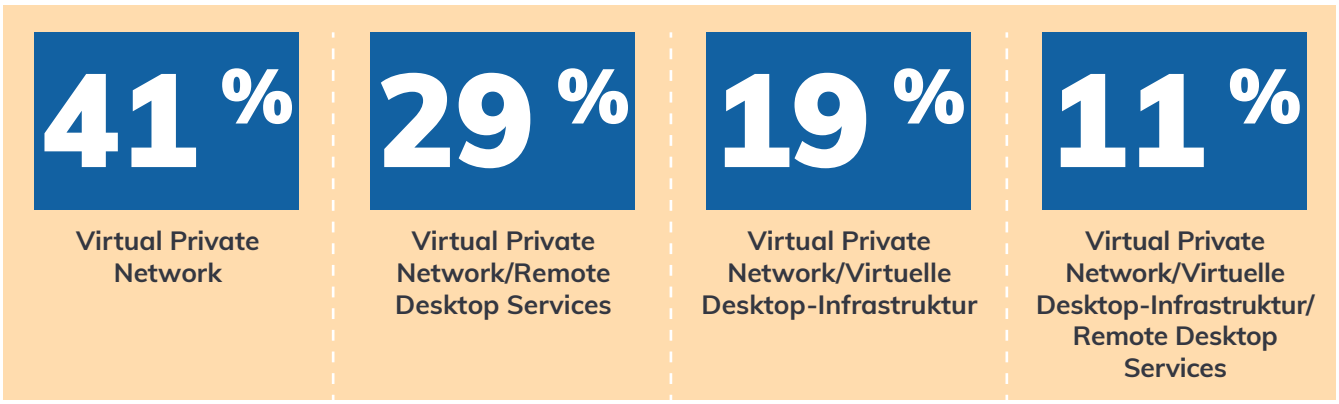
Als „Change Agents“, die während der Pandemie federführende Verantwortung für die Umstellung auf neue Arbeitskonzepte übernahmen, sind Technologievorstände bestens positioniert, ihre Organisationen auch erfolgreich durch die nächste Phase zu navigieren. Dabei wird es vor allem darum gehen, Technologien bereitzustellen, die die Ansprüche hybrider Belegschaften erfüllen und allen Usern standortunabhängig ein flexibles, produktives und sicheres Arbeiten ermöglichen. Die Studie von HMG Strategy belegt jedoch, dass bis zur Verwirklichung dieser Vorstellungen noch viel Arbeit auf die Organisationen zukommt.

In Zusammenarbeit mit HMG Strategy wollte Zscaler mehr darüber erfahren, welche Herausforderungen und Chancen sich aus Sicht der Betroffenen bei der Umstellung auf hybride Arbeitskonzepte ergeben. Insbesondere ging es uns um die Frage, welche technologischen und kulturellen Hindernisse der Umsetzung sicherer und flexibler hybrider Modelle bisher noch im Weg stehen. Der Report liefert wertvolle Erkenntnisse zu einer Reihe aktueller Themen:

- Technische Schwierigkeiten bei der Verwirklichung sicherer und flexibler hybrider Arbeitskonzepte, insbesondere die Mängel von Legacy-Infrastruktur wie VPN-Technologien
- Risiken in Bezug auf die Gewährleistung sicheren Anwendungszugriffs für hybride Belegschaften
- Sicherheitsbezogene Herausforderungen im Zusammenhang mit der Bereitstellung des Zugriffs auf private Unternehmensanwendungen für Remote- und Präsenzmitarbeiter
- Vorteile einer robusten Zero-Trust-Architektur zum Schutz hybrider Belegschaften

Wie wird der Anwendungszugriff ermöglicht?

Welche Technologien setzen Sie derzeit zur Ermöglichung des Anwendungszugriffs ein?



Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

„Die Mehrheit der Organisationen bewältigt die Umstellung von Remote- auf Hybridarbeit einigermaßen, ohne dass es sie jedoch wirklich voranbringt.“

BRYAN GREEN
CISO, Nord- und Südamerika
Zscaler

Ratschläge für die reibungslose Umsetzung sicherer und flexibler hybrider Arbeitskonzepte

Der Trend zur Umstellung auf SaaS-Angebote (Software-as-a-Service) und öffentliche Cloud-Umgebungen hält bereits seit einigen Jahren an. Dennoch ist bei vielen Organisationen die Cloud-Transformation noch längst nicht abgeschlossen. Einer Studie von Foundry zufolge soll der Anteil der Unternehmen, die ihre IT-Infrastruktur größtenteils oder ganz in die Cloud verlagert haben, im Laufe des nächsten Jahres von aktuell 41 % auf 63 % ansteigen.

Dem rapide voranschreitenden Wechsel in die Cloud stehen massive Altinvestitionen in Rechenzentren und lokal installierte Infrastruktur gegenüber.

„AWS bietet zwar bereits seit 16 Jahren öffentliche und private Cloud-Infrastruktur an. Richtig in Fahrt kam die Umstellung auf Remote-Arbeit jedoch erst vor zwei Jahren aufgrund der Coronapandemie“, meint Green. „Entsprechend gibt es bei vielen Organisationen noch enormen Nachholbedarf im Hinblick auf die Bewältigung der damit verbundenen Herausforderungen und Komplikationen bei Menschen, Prozessen und Technologien.“

Teilweise stehen auch Widerstände auf der Führungsebene einem reibungslosen Übergang zur Hybridarbeit entgegen. Unternehmen, die hohe Summen in den Erwerb oder die Anmietung von Büroflächen investiert haben, haben ein berechtigtes Interesse an einer möglichst effektiven Auslastung dieser Immobilien. In manchen Organisationen werden Angestellte durch Anordnungen der Geschäftsführung verpflichtet, einen bestimmten Anteil ihrer Arbeitszeit am Unternehmensstandort abzusitzen. Bei den Mitarbeitern stoßen derartige Regelungen allerdings auf wenig Gegenliebe.

In der ersten Septemberwoche 2022 erreichte die Auslastung von Büroräumen in zehn US-amerikanischen Großstädten knapp 50 % des Niveaus von Anfang 2020, also vor der Pandemie, so das Ergebnis einer Studie des Wach- und Sicherheitsdienstes Kastle Systems, der den physischen Zugang zu Bürogebäuden überwacht. Mehrere weitere Studien haben nachgewiesen, dass der Anteil der Beschäftigten in Präsenzarbeit zwar in den vergangenen Monaten leicht wuchs. Trotzdem ist er weiterhin niedriger als vor der Pandemie.

„Führungskräfte vieler Organisationen müssen sich mit der Tatsache auseinandersetzen, dass sie massiv in Immobilien investiert haben“, so Green. „Sie möchten, dass die Mitarbeiter dorthin zurückkehren und zusammenarbeiten, was sehr schwierig ist.“

Optimierung der Cybersicherheit durch Umstellung auf zukunftsfähige Alternativen

Die schlagartige Umstellung auf Remote-Arbeit im März 2020 offenbarte bei vielen Unternehmen eine ganze Reihe von Mängeln in Bezug auf die bisherigen Konzepte zur Überwachung und Absicherung von Remote-Mitarbeitern. Insbesondere betrifft dies den Einsatz von Virtual Private Networks (VPNs) zum Verschicken und Empfangen von Daten über gemeinsam genutzte bzw. öffentliche Netzwerke. VPNs weisen gleich mehrere gravierende Schwachstellen auf:

- Jedes VPN-Gateway verfügt über eine Ereignisbehandlungsroutine für eingehende Verbindungen, die es als Angriffsfläche exponiert.
- Hacker nutzen VPN-Gateways gerne als Ausgangspunkt für komplexere Angriffe.
- VPNs sind standardmäßig offen konzipiert. Um zu verhindern, dass Mitarbeiter auf Anwendungen und Systeme zugreifen können, für die sie keine Berechtigungen haben bzw. haben sollten, müssen Sicherheitsbeauftragte sie explizit aussperren.

Zukunftsfähige Lösungen für hybride Belegschaften

Viele der Hindernisse, die dem Übergang zu sicheren und agilen hybriden Arbeitskonzepten im Weg stehen, werden durch eine Kombination aus veralteter IT-Infrastruktur und dem Fehlen zuverlässiger Tools gegen Datenverluste und unbefugten Anwendungszugriff verursacht.

Welche primären Hindernisse stehen der Umsetzung sicherer und flexibler hybrider Arbeitskonzepte entgegen?

30 %

Wir bieten zwar aktiv ein BYOD-Konzept an, verfügen aber nicht über die erforderlichen Tools, um das Risiko von Datenverlusten und unbefugtem Zugriff auf interne Ressourcen zu minimieren.

20 %

Unsere VPN-Infrastruktur verlangsamt die Internetverbindung deutlich und wirkt sich negativ auf die Produktivität der Mitarbeiter aus.

7 %

Wir bieten zwar aktiv ein BYOD-Konzept an, verfügen aber nicht über die erforderlichen Tools, um das Risiko von Datenverlusten und unbefugtem Zugriff auf interne Ressourcen zu minimieren. Unser Unternehmen ist auf die Zusammenarbeit mit externen Auftragnehmern und Geschäftspartnern angewiesen, jedoch ist die Gewährleistung sicheren Zugriffs auf interne Anwendungen mit Schwierigkeiten verbunden.

22 %

Unser Unternehmen ist auf die Zusammenarbeit mit externen Auftragnehmern und Geschäftspartnern angewiesen, jedoch ist die Gewährleistung sicheren Zugriffs auf interne Anwendungen mit Schwierigkeiten verbunden.

16 %

Unsere VDI-Netzwerklatenz frustriert die Mitarbeiter und führt dazu, dass selbst die einfachsten Aufgaben auf virtuellen Desktops unmöglich sind.

5 %

Unsere VDI-Netzwerklatenz frustriert die Mitarbeiter und führt dazu, dass selbst die einfachsten Aufgaben auf virtuellen Desktops unmöglich sind. Unser Unternehmen ist auf die Zusammenarbeit mit externen Auftragnehmern und Geschäftspartnern angewiesen, jedoch ist die Gewährleistung sicheren Zugriffs auf interne Anwendungen mit Schwierigkeiten verbunden.

Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

„Wenn man also eine Kombination aus Remote-Access-VPNs und Site-to-Site-VPNs einsetzt, entsteht dadurch eine massive Angriffsfläche, die potenziell die gesamte Infrastruktur für Bedrohungsakteure sichtbar macht.“

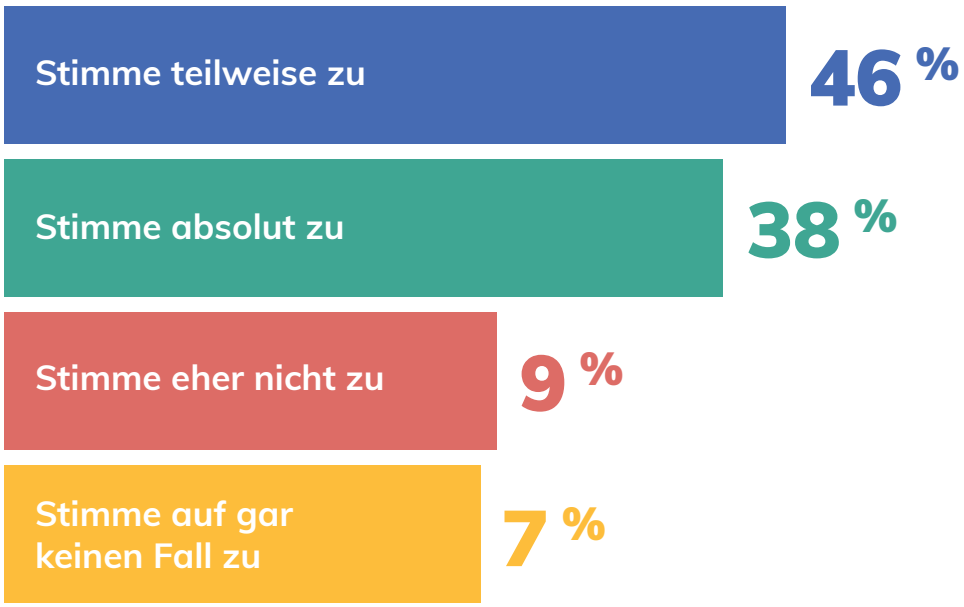
BRYAN GREEN
CISO, Nord- und Südamerika
Zscaler

„Mit jeder VPN-Verbindung, die Sie erstellen, wird das Unternehmensnetzwerk quasi bis zu den jeweiligen Standorten ausgeweitet“, erläutert Green, der ab 2003 bei Cisco an der Entwicklung von VPN-Konzentratoren arbeitete. „Wenn ein Unternehmen also eine Kombination aus Remote-Access-VPNs und Site-to-Site-VPNs einsetzt, entsteht dadurch eine massive Angriffsfläche, die potenziell die gesamte Infrastruktur für Bedrohungsakteure sichtbar macht. Sofern sie nicht durch bestimmte Arten von Firewalls bzw. bestimmte Methoden der Segmentierung geschützt wird, können sämtliche User frei darauf zugreifen.“

Produktivitätsbremse

Der Einsatz von VPNs für Remotezugriff und Verbindungen zwischen mehreren Unternehmensstandorten vergrößert nicht nur exponentiell die Angriffsfläche der Organisation, sondern lässt auch die Produktivität von Hybrid-Mitarbeitern stagnieren.

Inwieweit stimmen Sie der Aussage zu, dass sich eine frustrierend langsame VPN-Performance negativ auf die Produktivität von Hybrid-Mitarbeitern auswirkt?



Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

Durch Umstellung auf eine Zero-Trust-Architektur lassen sich nicht nur die Schwachstellen vermeiden, die durch den Einsatz von VPNs entstehen. Neben zuverlässigem Schutz vor Sicherheitsverletzungen sorgt das Zero-Trust-Modell für weniger Komplexität, besseren Datenschutz und optimierter User Experience für die Mitarbeiter bei minimaler Angriffsfläche.

In den folgenden Abschnitten geht es um die sicherheitsbezogenen Herausforderungen, die mit unnötigen Zugriffsberechtigungen verbunden sind. Außerdem wird detailliert auf die operativen und betriebswirtschaftlichen Vorteile einer Zero-Trust-Strategie eingegangen.

Zero Trust minimiert Risiken durch unnötige Zugriffsbe-rechtigungen und schafft sicherere hybride Umgebung

Bei vielen Organisationen ist Remote-Arbeit im kleineren Umfang bereits seit Jahren gang und gäbe. Die Corona-bedingte massive Umstellung im März 2020 führte jedoch quasi über Nacht zu einer exponentiellenBeschleunigung der Digitalisierung mit entsprechender Vergrößerung der Angriffsfläche.

Mit dem weiter anhaltenden Trend zur verstärkten Nutzung öffentlicher Clouds erhöht sich auch das Risiko der Vergabe unnötiger Zugriffsberechtigungen und der Exposition geschäftskritischer Daten.

Risikoexposition hybrider Belegschaften

Der Versuch, hybride Arbeitskonzepte mit Legacy-Infrastrukturen zu schützen, führt zur Entstehung mehrerer Sicherheitsrisiken, die die zuständigen Teams zu bewältigen haben. Dazu zählt die Vergabe unnötiger Zugriffsberechtigungen für Mitarbeiter und Auftragnehmer ebenso wie der potenzielle Zugriff kompromittierter User auf Netzwerkressourcen.

Welche Risiken sehen Sie in Bezug auf die Gewährleistung von sicherem Anwendungszugriff für hybride Belegschaften?

31 %

Unnötige Zugriffsberechtigungen für Mitarbeiter und externe User

26 %

Zugriff auf Netzwerkressourcen durch kompromittierte User

18 %

Versehentliche und böswillige Datenverluste

15 %

Zugriff auf Netzwerkressourcen über Geräte mit hohem Risiko (z. B. unbekannte oder nicht richtlinienkonforme Geräte)

10 %

Angriffe auf Anwendungen (z. B. Denial-of-Service, Cross-Site-Scripting, Injection)

Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

„Die Vergabe unnötiger Zugriffsberechtigungen stellt uns branchenweit vor ein massives Sicherheitsproblem“, so Green. Er verdeutlicht das Problem am Vergleich mit einer Bankfiliale: Kein Kunde würde auf die Idee kommen, allen Bankangestellten einen Schlüssel zu seinem Schließfach auszuhändigen. Hingegen lasse sich der logische rollenbasierte Zugriff für Mitarbeiter und User auf verschiedene Arten von Anwendungen sehr viel schwieriger implementieren als physische Zugangsberechtigungen.

Zur Bewältigung der Risiken, die durch die Vergabe unnötiger Berechtigungen entstehen, stehen glücklicherweise moderne Tools wie CIEM-Lösungen (Cloud Infrastructure Entitlement Management) zur Verfügung. Diese und ähnliche Tools unterstützen eine Strategie der minimalen Rechtevergabe, indem Organisationen umfassende Einblicke in sämtliche Cloud-Berechtigungen und das damit einhergehende Risiko unbefugter Zugriffe erhalten.

Im letzten Abschnitt des Reports geht es um die Faktoren, die Sicherheits- und Technologiebeauftragte zur Umstellung auf Zero-Trust-Sicherheitsstrategien bewegen, sowie operative und betriebswirtschaftliche Vorteile des Zero-Trust-Modells.

Mangelndes Vertrauen in vorhandene Sicherheitstools

Nur ein Drittel der befragten Sicherheits- und Technologieexperten setzte hohes Vertrauen in die Fähigkeit der aktuell eingesetzten Sicherheitstools, versuchte Zugriffe auf Netzwerkressourcen durch kompromittierte User oder Insider-Bedrohungen zu erkennen.

Wie viel Vertrauen setzen Sie in die Fähigkeit Ihrer aktuell eingesetzten Sicherheitstools, versuchte Zugriffe auf Netzwerkressourcen durch kompromittierte User oder Insider-Bedrohungen zu erkennen?

34 %

Hohes Vertrauen

62 %

Gewisses Vertrauen

4 %

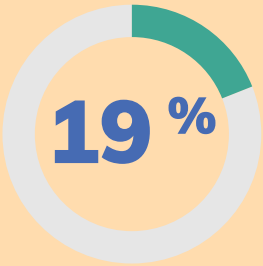
Sehr geringes Vertrauen

Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

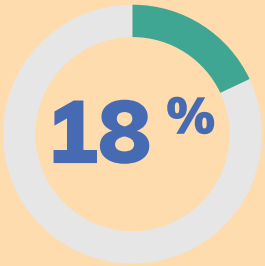
Die Sicherheitsmängel beim Zugriff auf private Anwendungen

Die beschriebenen Sicherheitsrisiken betreffen nicht nur öffentlich zugängliche Anwendungen. Auch private Anwendungen, die über Internetgateways bereitgestellt werden, können anfällig für Angriffe sein.

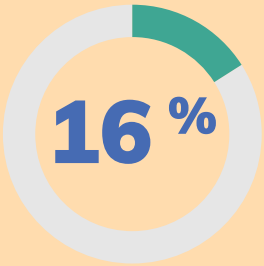
Welche der folgenden Szenarien haben Sie bei der Bereitstellung des Zugriffs auf private Anwendungen für Remote- und Präsenzmitarbeiter erlebt?



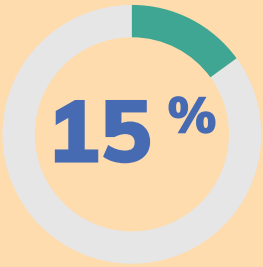
User sind aufgrund von inkonsistenten Zugriffsrichtlinien und Verbindungsproblemen frustriert.



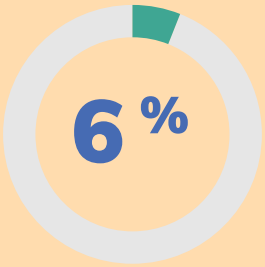
Private Anwendungen sind für die Bereitstellung des Zugriffs im Internet exponiert und für Angriffe anfällig.



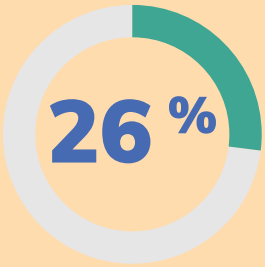
Mitarbeiter und externe User haben vollständigen Zugriff auf das Unternehmensnetzwerk, was das Risiko lateraler Bewegungen erhöht.



Wir leiten Remote-User im Backhauling-Verfahren in unsere Rechenzentren um, damit sie auf private Anwendungen zugreifen können – dadurch wird ihre Internetverbindung jedoch langsamer.



Wir verbinden User im Büro oder in Zweigstellen mit unserem Rechenzentrum und stellen dadurch Zugriff auf private Anwendungen her – das ergibt Engpässe und wirkt sich negativ auf die Performance aus.



Bei uns ist noch keines der beschriebenen Szenarien vorgekommen.

Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

Umstellung auf eine Zero-Trust-Strategie

Als zusätzlicher Risikofaktor im Zusammenhang mit der Umstellung auf hybride Arbeitskonzepte erweist sich der Zugriff auf Unternehmensressourcen über nicht verwaltete Privatgeräte, die von Usern im Homeoffice genutzt werden. Durch das Festhalten an Virtual Private Networks (VPNs) sind viele Organisationen gefährdet. Angesichts dieser Vielfalt von Risiken führt kein Weg an der Erkenntnis vorbei, dass die Legacy-Infrastruktur, die viele Organisationen zur Unterstützung hybrider Belegschaften einsetzen, den heutigen – ganz zu schweigen von den morgigen – Anforderungen schlichtweg nicht gewachsen ist.

Das sind nur einige von vielen Gründen, welche die Mehrheit der CISOs und Sicherheitsbeauftragten zur Umstellung auf moderne Zero-Trust-Architekturen veranlassen, um das Schutzniveau ihrer Organisation zu stärken und lückenlose Sicherheit zu gewährleisten.

„Mit einer Zero-Trust-Lösung für den Netzwerkzugriff lässt sich das Sicherheitsniveau erhöhen, indem die Angriffsfläche verkleinert wird“, so Green. „ZTNA sorgt zudem für eine deutliche Verbesserung der User Experience und Performance.“

Angesichts der zunehmenden Umstellung auf hybride Arbeitskonzepte machen sich Technologievorstände bei vielen Organisationen ernsthaft Gedanken über Alternativen zu Legacy-Architekturen. Die Stärkung der Sicherheit bei gleichzeitiger Steigerung der Produktivität gab für die Mehrheit der Organisationen den Ausschlag für die Implementierung von ZTNA. Alle befragten Organisationen, die den Umstieg auf ein Zero-Trust-Konzept erfolgreich abgeschlossen haben, erzielten eine erhebliche Reduzierung ihrer Kosten und Komplexität, die ihnen eine stärkere Fokussierung auf betriebswirtschaftliche Aspekte ermöglicht hat.

Hauptgründe für die Umstellung auf Zero Trust

Über 35 % der Befragten nennen den Schutz ihrer IT-Ressourcen und User in der hybriden Arbeitswelt als Beweggrund für die Umstellung von Legacy-Lösungen auf ein Zero-Trust-Konzept.

Welche Faktoren haben Ihre Organisation zur Umstellung auf eine Zero-Trust-Sicherheitsstrategie veranlasst?

29 %

Wir erwägen derzeit die Umstellung auf Zero-Trust-Sicherheit, haben aber noch keine endgültige Entscheidung getroffen.

Wir haben erkannt, dass herkömmliche Firewalls und VPNs leichter von Angreifern zu umgehen sind und laterale Bewegungen ungehindert zulassen.	21 %
Wir sind auf eine Zero-Trust-Strategie umgestiegen, um sichere und flexible Konnektivität für unsere hybride Belegschaft zu gewährleisten.	20 %
Wir haben erkannt, dass herkömmliche Firewalls und VPNs zur Entstehung einer massiven Angriffsfläche führen.	15 %
Wir planen derzeit keine Umstellung auf eine Zero-Trust-Sicherheitsstrategie.	15 %

Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

„Einmal angenommen, einem Bedrohungsakteur gelingt es, in Ihre IT-Umgebung einzudringen oder Ihre Infrastruktur zu kompromittieren. Unter dem Gesichtspunkt der Kill Chain müssen Sie unbedingt verhindern, dass sich dieser Akteur ungehindert lateral durch Ihr Unternehmensnetzwerk bewegen kann“, so Green. „Vor allem darf er keine Daten aus Ihrer Umgebung exfiltrieren, damit er kein vertrauliches geistiges Eigentum, Geschäftsgeheimnisse oder Kundendaten stehlen kann. Zusammen bilden diese drei Punkte eines der Hauptargumente für den Umstieg auf eine Zero-Trust-basierte Zugriffslösung.“

Eine Zero-Trust-Strategie bietet darüber hinaus in einem angespannten Arbeitsmarkt zusätzliche Vorteile. In der Forschungsstudie von HMG Strategy stimmten **84 %** der befragten Technologievorstände der Einschätzung zu, dass die Unterstützung eines flexiblen und sicheren hybriden Arbeitskonzepts dazu beigetragen hat, dass ihre Organisation Fachkräfte anwerben und dauerhaft binden kann.

„An dem hohen Prozentsatz der Führungskräfte, die hier einen Zusammenhang sehen, zeigt sich die erhebliche Bedeutung von Flexibilität und Freiheit aus Sicht der Arbeitnehmer“, ist Green überzeugt.

In der Forschungsstudie von HMG Strategy gaben 55 % der Befragten an, dass die Umstellung auf Hybridarbeit ihre Organisationen zur erneuten Evaluierung ihrer Legacy-Infrastruktur zur Gewährleistung von Remotezugriff veranlasst habe.

Mit der zunehmenden Kostenorientierung vieler Unternehmensvorstände gewinnt auch die Erkenntnis an Gewicht, dass die Umstellung von kostspieligen Legacy-Kontrollmechanismen auf eine zukunftsfähige Zero-Trust-Infrastruktur Organisationen nicht nur ermöglicht, schnell und flexibel auf veränderte Marktbedingungen zu reagieren, sondern dabei zugleich Kosten und Risiken zu reduzieren.

Zudem unterstützen Organisationen, die veraltete Einzellösungen durch eine ganzheitliche Zero-Trust-Architektur ersetzen, die zuständigen Teams bei der Optimierung und effektiveren Verwaltung der Sicherheitskontrollen. „Durch die Umstellung auf ein Zero-Trust-Modell lassen sich viele erforderliche Sicherheitskontrollen über eine zentrale Management-Konsole verwalten“, betont Green.

Seit der plötzlichen Umstellung im März 2020 haben die Angestellten vieler Organisationen nicht nur bewiesen, wie produktiv sie im Homeoffice arbeiten können, sondern auch, wie stark ihr Wunsch nach mehr Flexibilität im Privat- und Berufsleben ist. Eine Rückkehr zur Vollzeit-Präsenzarbeit im herkömmlichen Sinne erscheint zunehmend unwahrscheinlich. Ebenso eindeutig hat sich jedoch erwiesen, dass Legacy-Technologien wie VPN nicht das erforderliche Schutzniveau und die Flexibilität gewährleisten, um vertrauliche Daten in hybriden Arbeitsumgebungen zuverlässig abzusichern. Stattdessen ist ein neuer und effektiverer Ansatz gefragt.

Green kommentiert: „Zero Trust bietet Organisationen eine hervorragende Möglichkeit zur Verbesserung ihrer betrieblichen Effizienz in einer hybriden Arbeitswelt.“

Welche Zero-Trust-Technologien werden aktuell zum Schutz hybrider Belegschaften eingesetzt?

Welche der folgenden Zero-Trust-Technologien setzt Ihre Organisation derzeit zur Unterstützung sicherer Hybridarbeit ein?

19 %
Mehrstufige Authentifizierung

16 %
Endgerätesicherheit

14 %
Cloud-Firewall

10 %
Data Loss Prevention

9 %
Secure Web Gateway

32 %
Sonstige

Quelle: Umfrage von HMG Strategy zum Thema sichere Hybridarbeit unter 138 CIOs, CISOs und Technologievorständen im 2. und 3. Quartal 2022

Über HMG Strategy

HMG Strategy ist die weltweit führende digitale Plattform für die Vernetzung von Führungskräften aus der Technologiebranche, die Impulse für neue Unternehmenskonzepte setzen und die Zukunft der Wirtschaftswelt mitgestalten wollen. Dem globalen Netzwerk von HMG Strategy gehören über 400.000 CIOs, CTOs, CISOs, CDOs, Technologievorstände, Führungskräfte aus der Suchmaschinenbranche, Risikokapitalgeber, Branchenexperten und weltweit führende Vordenker an.

Über Zscaler

Zscaler beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die in 150 Rechenzentren auf der ganzen Welt verfügbare SSE-basierte Zero Trust Exchange ist die weltweit größte Inline-Cloud-Sicherheits-plattform.