Report zu VPN-Risiken 2024 von Zscaler ThreatLabz

Cybersecurity INSIDERS

Informieren Sie sich über die wichtigsten Trends in den Bereichen VPN-Sicherheit, Risiken und User Experience, da die Umstellung auf Zero Trust sich zunehmend als unerlässliche Notwendigkeit erweist.

Inhalt

Überblick

Der zunehmende Trend zu verteilten und cloudzentrierten Arbeitsumgebungen hat eine Verlagerung der Zugriffsmethoden von herkömmlichen virtuellen privaten Netzwerken (VPNs) zu robusteren Sicherheitsrahmen wie Zero Trust ausgelöst. Traditionell stellten VPNs wichtige Funktionen für die Anbindung einzelner User oder ganzer Unternehmensstandorte bereit. Allerdings haben die zunehmende Komplexität der Cyberbedrohungen sowie die zunehmende Anzahl von Remote-Arbeitsplätzen und Cloud-Technologien erhebliche Schwachstellen in VPNs offengelegt. Aufgrund ihrer Legacy-Architektur gewähren VPNs nach der Überprüfung der Anmeldedaten einen zu umfassenden Netzwerkzugriff, wodurch das Risiko von Cyberangriffen erheblich steigt, wenn diese Anmeldedaten kompromittiert werden.

In letzter Zeit erregten Angriffe unter Ausnutzung von VPN-Geräten Aufsehen, die kritische Schwachstellen (insbesondere CVE-2023-46805, CVE-2024-21887 und CVE-2024-21893) in systemrelevanten Sektoren, darunter auch der US-amerikanischen Rüstungsbranche, aufzeigten. Diese Schwachstellen ermöglichen Angreifern, die Authentifizierung zu umgehen, Befehle mit erweiterten Rechten auszuführen und die Persistenz auch nach Zurücksetzen des Geräts aufrechtzuerhalten. Als Reaktion darauf erließ die US-amerikanische Cybersecurity and Infrastructure Security Agency (CISA) eine Notfallanweisung an die Bundesbehörden, betroffene VPN-Geräte aufgrund erheblicher Sicherheitsrisiken umgehend zu trennen.

Mit der Executive Order 14028 schreibt die US-Regierung nun die Umstellung auf Zero-Trust-Architekturen zur Verbesserung der Cybersicherheit vor und setzt damit eine Abkehr von herkömmlichen VPNs voraus. Diese Richtlinie ist Teil einer umfassenden Strategie zur Stärkung der nationalen Cybersicherheit und weist die Bundesbehörden an, ein Zero-Trust-Prinzip umzusetzen, bei dem sämtliche Zugriffsanfragen unabhängig von ihrer Herkunft überprüft werden. Das Office of Management and Budget (OMB) unterstützt diese Initiative zusätzlich mit einer detaillierten Federal Zero Trust Strategy und unterstreicht die Abkehr vom VPN-basierten impliziten Vertrauen innerhalb von Netzwerkperimetern hin zur kontinuierlichen Überprüfung sämtlicher Zugriffsanforderungen. Diese Richtlinien und Empfehlungen spiegeln den Konsens innerhalb der Cybersicherheits-Community wider, dass Zero Trust einen robusteren Schutz vor komplexen und neu entstehenden Cyberbedrohungen bietet — eine Notwendigkeit, die durch die jüngsten Schwachstellen und Angriffe auf herkömmliche VPNs unterstrichen wird.

Infolgedessen implementieren Unternehmen zunehmend Zero-Trust-Modelle, die keinem User oder Gerät innerhalb oder außerhalb des Netzwerkperimeters grundsätzlich vertrauen und für jede Zugriffsanforderung eine detaillierte Überprüfung erfordern. Dieses Modell ist besonders wirksam bei der Verhinderung lateraler Bewegungen innerhalb von Netzwerken — ein Exploit, den Angreifer häufig nutzen, um sich nach dem Erstzugriff im Netzwerk auszubreiten.

Dieser Bericht basiert auf einer Umfrage unter 647 IT-Fachleuten und Cybersicherheitsexperten und untersucht die vielschichtigen Herausforderungen von VPNs in Bezug auf Sicherheit und User Experience. Er zeigt die Komplexität des heutigen Zugriffsmanagements, die Anfälligkeit für verschiedene Cyberangriffe und das Potenzial zur Beeinträchtigung des allgemeinen Sicherheitsstatus von Unternehmen auf. Der Bericht skizziert außerdem effektivere Sicherheitsmodelle, insbesondere Zero Trust, das sich als robustes und zukunftssicheres Framework zur Sicherung und Beschleunigung der digitalen Transformation etabliert hat.

Wir danken den Experten von Zscaler für ihren Beitrag zu dieser VPN-Risikoumfrage. Ihre Expertise im Bereich Zero Trust und sichere Zugriffslösungen hat unsere Erkenntnisse erheblich bereichert. Mit den hier vorgestellten Erkenntnissen wollen wir IT-Fachkräften und Cybersicherheitsexperten eine wertvolle Ressource an die Hand geben, die sie bei der Umsetzung zuverlässiger Zero-Trust-Sicherheit unterstützen sollen.

Vielen Dank,
Holger Schulze, Gründer, Cybersecurity Insiders

„Im vergangenen Jahr wurden zahlreiche kritische VPN-Schwachstellen als erfolgreiche Einstiegspunkte für Angriffe auf große Unternehmen und Bundesbehörden ausgenutzt. Angesichts dieser wiederholten Ergebnisse müssen Unternehmen unbedingt damit rechnen, dass Bedrohungsakteure in zunehmendem Maße diese veralteten, im Internet exponierten Ressourcen — physische und virtuelle Geräte — ausnutzen, die es ihnen ermöglichen, sich problemlos lateral durch herkömmliche flache Netzwerke zu bewegen. Die Umstellung auf eine Zero-Trust-Architektur ist unerlässlich. Sie reduziert die Angriffsfläche erheblich, indem sie Legacy-Technologien wie VPNs und Firewalls eliminiert, konsistente Sicherheitskontrollen mit TLS-Inspektion durchsetzt und das Schadenspotenzial durch Segmentierung und Täuschung begrenzt und so schädliche Sicherheitsverletzungen verhindert.“

—DEEPEN DESAI, CHIEF SECURITY OFFICER, ZSCALER

Haupterkenntnisse

VPN-Angriffe nehmen zu.

56 % der Organisationen wurden im letzten Jahr Opfer eines oder mehrerer VPN-bezogener Cyberangriffe — im Jahr davor waren es nur 45 %. Dies verdeutlicht die zunehmende Häufigkeit und Raffinesse von Angriffen auf VPNs.

VPNs sind Ransomware, Malware und DDoS-Angriffen nicht gewachsen.

Die Befragten identifizierten Ransomware (42 %), Schadsoftware (35 %) und DDoS-Angriffe (30 %) als größte Bedrohungen, die sich VPN-Schwachstellen zunutze machen. Dies unterstreicht die Bandbreite der Risiken, denen Organisationen aufgrund der inhärenten Schwächen herkömmlicher VPN-Architekturen ausgesetzt sind.

Die überwiegende Mehrheit stellt auf Zero-Trust-Architekturen um.

78 % der Organisationen planen, in den nächsten 12 Monaten Zero-Trust-Strategien umzusetzen. Mittlerweile stimmen 62 % der Unternehmen der Aussage zu, dass VPNs mit dem Zero-Trust-Prinzip unvereinbar sind.

Das Risiko lateraler Bewegungen darf nicht unterschätzt werden.

53 % der Unternehmen, deren Zugriff über VPN-Schwachstellen erfolgte, geben an, dass sich die Bedrohungsakteure lateral im Netzwerk ausbreiteten. Dies deutet auf Fehler bei der Eindämmung am ersten Angriffspunkt hin, die die Risiken herkömmlicher, flacher Netzwerke unterstreichen.

Die Mehrheit hat Zweifel an der Sicherheit von VPNs.

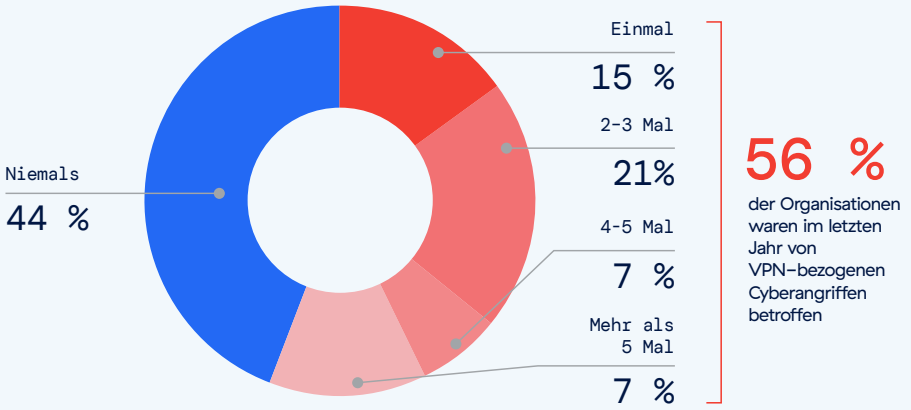
91 % der Befragten äußerten Bedenken, dass VPNs ihre IT-Sicherheitsumgebung gefährden könnten. Die jüngsten Sicherheitsverstöße verdeutlichten dabei die Risiken, die mit dem Festhalten an veralteten oder ungepatchten VPN-Infrastrukturen verbunden sind.

Sicherheitsrelevante Nachteile von VPN

VPN-Angriffe nehmen zu

Die Häufigkeit und Schwere von Angriffen, die sich VPN-Schwachstellen zunutze machen, verdeutlichen die Ineffektivität herkömmlicher Cybersicherheitsmaßnahmen und unterstreichen die anhaltenden Risiken, die von der Exposition des Netzwerks ausgehen. Unsere Umfrage zeigt, dass 56 % der Organisationen im letzten Jahr Opfer von Cyberangriffen wurden, bei denen VPN-Schwachstellen ausgenutzt wurden. Dies stellt einen deutlichen Anstieg im Vergleich zum Vorjahr dar (45 %). Besonders besorgniserregend ist, dass 41 % der Organisationen von zwei oder mehr VPN-bezogenen Angriffen berichteten, was auf schwerwiegende Sicherheitslücken hinweist.

War Ihre Organisation in den vergangenen zwölf Monaten von einem Angriff betroffen, bei dem Sicherheitslücken in Ihren VPN-Servern ausgenutzt wurden?

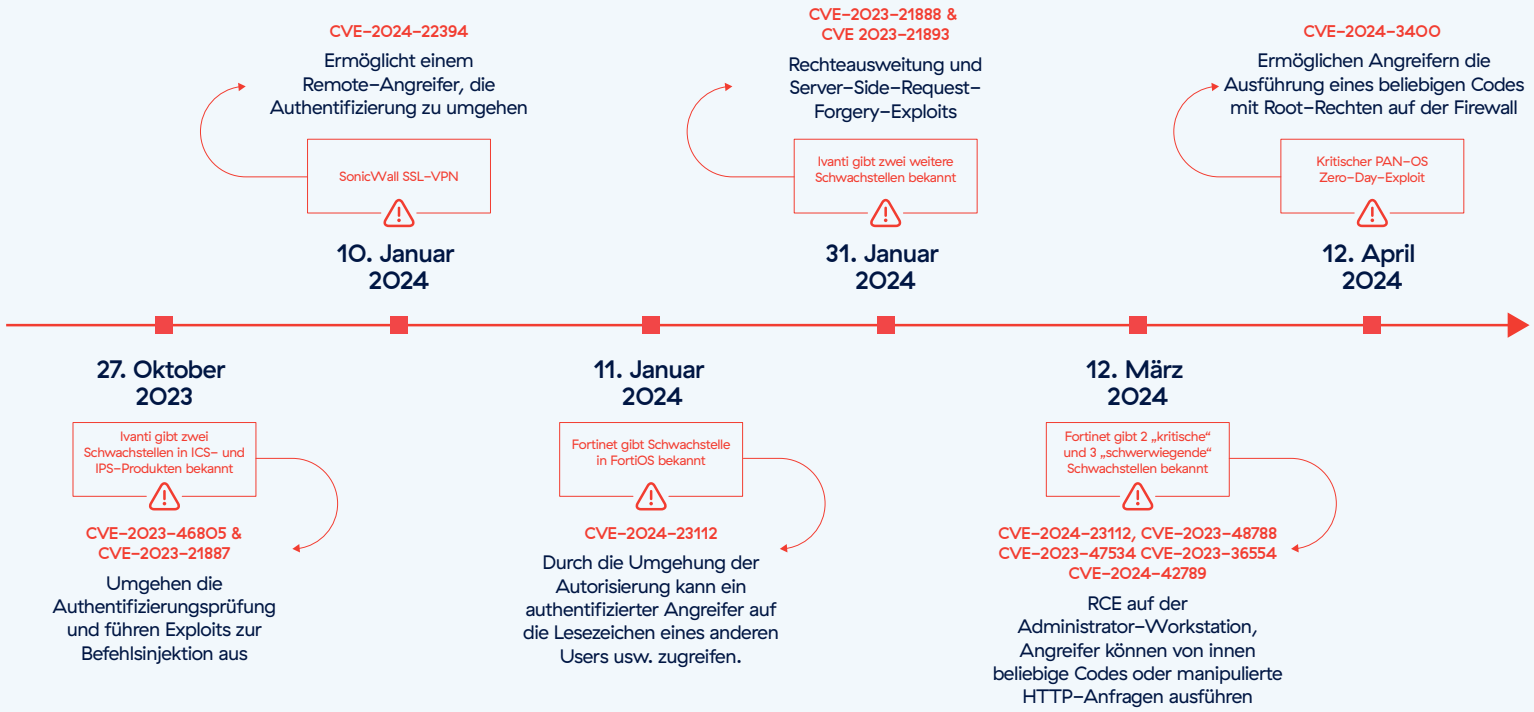


Aktuelle Trends bestätigen, dass Angriffe auf VPNs nicht nur häufiger, sondern auch raffinierter werden. So verdeutlichen etwa die zunehmenden Fälle von Ransomware, die VPN-Schwachstellen ausnutzen — insbesondere nach der Veröffentlichung von Sicherheitslücken — die kritischen Schwächen herkömmlicher VPNs. Solche Schwachstellen bieten Angreifern einfache Einstiegspunkte für die Infiltration von Netzwerken und ermöglichen laterale Bewegungen, was zu erheblichen Datenverlusten und Betriebsstörungen führen kann.

Signifikante VPN-Sicherheitslücken im vergangenen Jahr

Angesichts der jüngsten Reihe schwerwiegender CVEs, die VPN-Produkte betreffen, ist es keine Überraschung, dass Unternehmen mehr Angriffe melden, bei denen derartige Schwachstellen ausgenutzt werden. Natürlich kann kein einzelner Anbieter und keine bestimmte Technologie vor Softwareschwachstellen gefeit sein. Im Falle von VPN besteht die Herausforderung für Unternehmen darin, dass jede CVE einen einzelnen Sicherheitsfehlerpunkt für das Unternehmen darstellen kann: einen Brückenkopf, der es Angreifern ermöglicht, eine VPN-Ressource zu kompromittieren, Persistenz aufzubauen, sich lateral durch das Netzwerk zu bewegen und Daten zu stehlen. Da VPN-CVEs weiterhin in diesem Tempo offengelegt werden, stellen sie ein anhaltendes Risiko für Unternehmen dar, die VPNs für die Remote-Konnektivität verwenden.

Eine Reihe neuer CVEs weist auf einen Architekturfehler hin



Umgang mit VPN-Sicherheitsbedenken

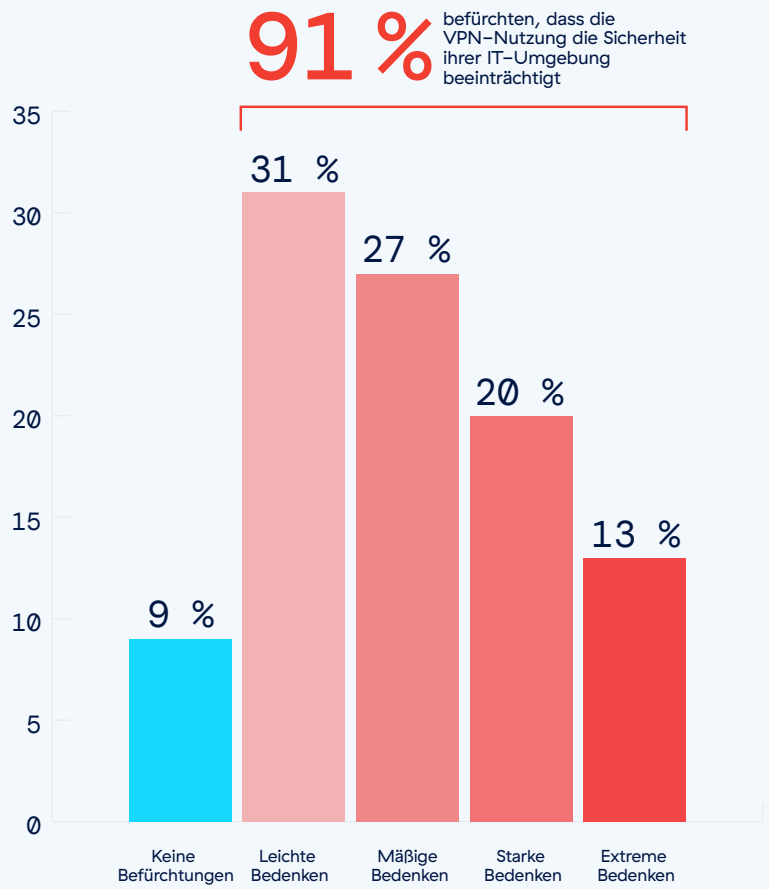
Die Ergebnisse der Umfrage spiegeln die tiefsitzende Sorge wider, dass VPNs die Sicherheitsumgebung gefährden könnten, und verdeutlichen anhaltende Trends und zunehmende Schwachstellen in VPN-Technologien. Eine überwältigende Mehrheit der Befragten (91%, im Jahr 2023 waren es 88 %) äußerte Bedenken, dass VPNs ihre IT-Sicherheit gefährden könnten, was das gestiegene Bewusstsein für VPN-bezogene Risiken in Unternehmen unterstreicht.

Diese Sorge wird durch die jüngsten Exploits gegen Ivanti VPNs gerechtfertigt, bei denen Angreifer schwerwiegende Schwachstellen ausnutzten, um in Netzwerke einzudringen und vertrauliche Daten zu exfiltrieren. Diese Vorfälle, bei denen es um Schwachstellen wie CVE-2024-21888 und CVE-2024-21893 geht, verdeutlichen die Risiken, die mit der Wartung und Sicherung veralteter oder ungepatchter VPN-Infrastrukturen verbunden sind. Darüber hinaus birgt die inhärente Architektur von VPNs erhebliche Sicherheitsrisiken in der heutigen perimeterlosen digitalen Landschaft. Mit der zunehmenden Nutzung von Cloud-Diensten und Weiterentwicklung von Remote-Arbeitskonzepten stehen VPNs vor neuen Sicherheitsherausforderungen, darunter die Verwaltung umfassender Zugriffsrechte und die Absicherung einer wachsenden Angriffsfläche.

Diese Schwachstellen und architektonischen Einschränkungen unterstreichen einen grundlegenden Wandel in der Wahrnehmung der VPN-Sicherheit und stehen im Einklang mit umfassenderen Trends in der Cybersicherheit, die dynamischere und widerstandsfähigere Frameworks wie Zero Trust propagieren.

Zukunftsorientierte Organisationen gehen zu Zero-Trust-Architekturen über, um eine präzisere Kontrolle zu erlangen und die Angriffsfläche deutlich zu reduzieren, indem keinem User automatisch vertraut wird, weder innerhalb noch außerhalb eines Netzwerkperimeters. Die Einführung einer solchen Strategie behebt die unmittelbaren Schwachstellen herkömmlicher VPNs und geht mit einem proaktiven Ansatz zur Cybersicherheit einher, der für die Anpassung an die dynamische Bedrohungslange von entscheidender Bedeutung ist.

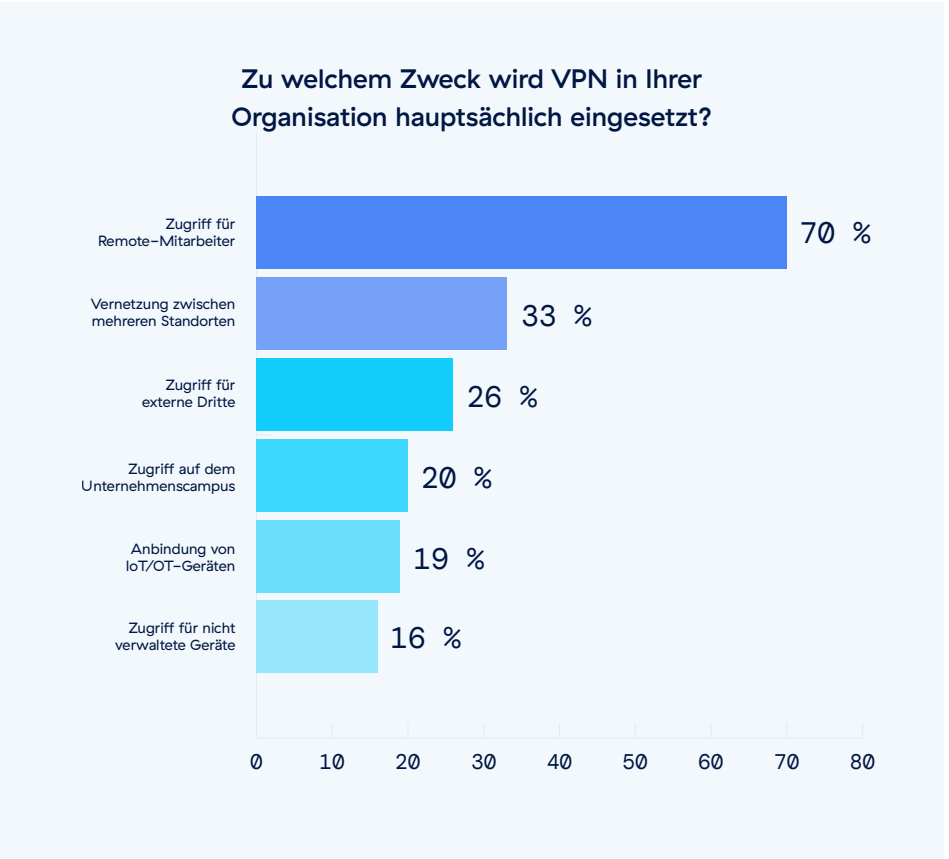
Inwieweit haben Sie Bedenken, dass VPN Ihre Fähigkeit beeinträchtigen könnte, Ihre Umgebungen zu sichern?



Wichtige Anwendungsszenarien für sicheren Zugriff

Es ist wichtig zu verstehen, warum Organisationen VPNs verwenden, da es verdeutlicht, wie sie dem sicheren Zugriff in verschiedenen Geschäftsszenarien Priorität einräumen. Darüber hinaus zeigt es auf, welche Netzwerkanwendungsfälle den größten Sicherheitsrisiken ausgesetzt sind und weist auf Bereiche hin, die robustere und innovativere Strategien zur Zugriffssicherheit erfordern.

Bemerkenswerte 70 % der Organisationen nutzen VPNs hauptsächlich, um den Zugriff für Remote-Mitarbeiter zu sichern. Aufgrund dieser weiten Verbreitung ist der Remote-Zugriff ein bevorzugtes Ziel für Cyberangriffe. An zweiter Stelle steht die Verwendung von VPNs, um mehrere Standorte zu verbinden, bei 33 % der Organisationen. Dies birgt erhebliche Risiken, da diese Verbindungen als Vektoren für Cyberangriffe dienen können, wenn sie nicht ausreichend geschützt werden. An dritter Stelle wurde der Zugriff für Dritte genannt (26 %), was die Sicherheit aufgrund des unterschiedlichen Sicherheitsstatus verschiedener externer Interessengruppen und der fehlenden Kontrolle über Sicherheitsrichtlinien weiter erschwert. Darüber hinaus nutzen 20 % der Organisationen VPNs für den Zugriff innerhalb des Standorts und 19 % für die Anbindung von IoT/OT-Geräten.



Angesichts der dynamischen Cyberbedrohungslage bieten VPNs für kritische Zugriffsfälle keine ausreichende Sicherheit mehr, da sie auf veralteten Modellen basieren, die nach einer einfachen User-Authentifizierung umfassenden Netzwerkzugriff gewähren. Dieser umfassende Zugriff setzt Unternehmen erheblichen Risiken aus, da potenzielle Angreifer über einen einzigen Zugangspunkt im gesamten Netzwerk auf vertrauliche Daten zugreifen und diese extrahieren können.

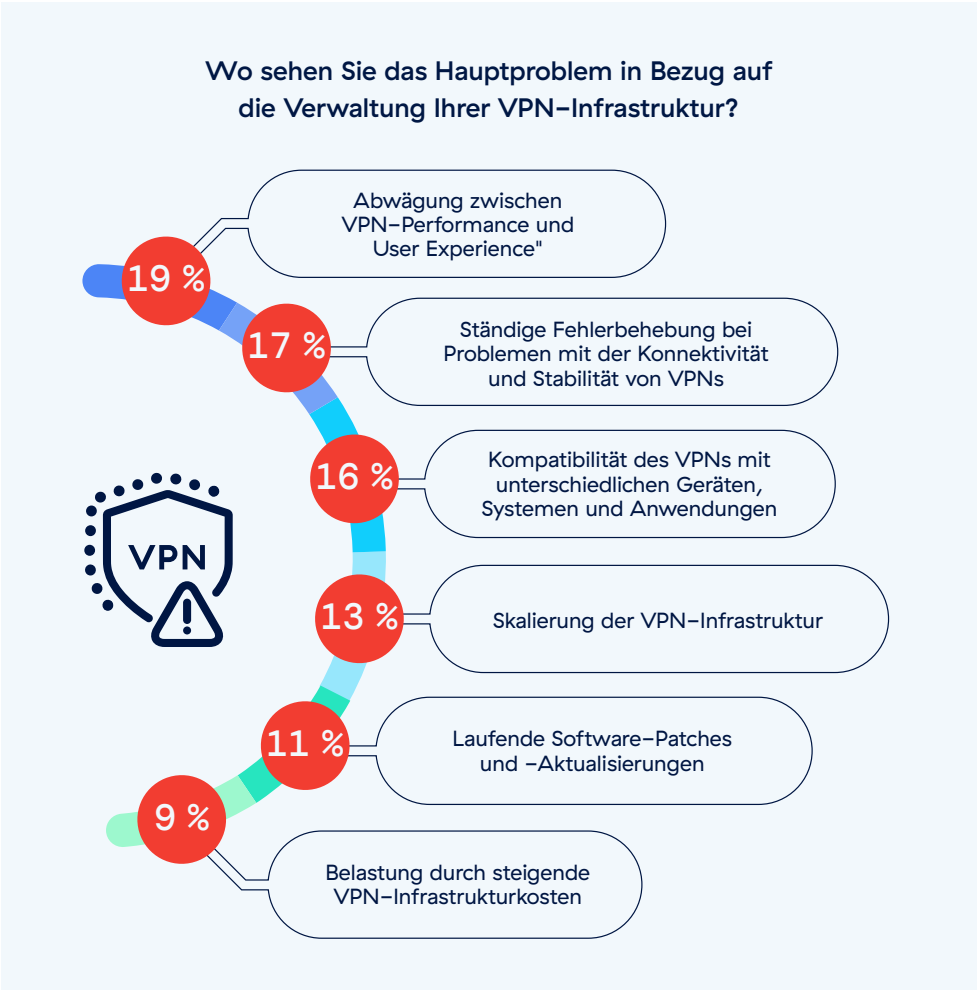
VPN: Verwaltung, Performance und User Experience

Probleme bei der VPN-Verwaltung

Zusätzlich zu den inhärenten Sicherheitsrisiken stellt die Verwaltung von VPN-Infrastrukturen erhebliche Herausforderungen für IT-Teams dar, da die Anforderungen an robuste Zugriffslösungen in verteilten, Cloud-zentrierten Arbeitsumgebungen steigen. Als größte Management-Herausforderung nennen IT-Experten die Abwägung zwischen VPN-Performance und User Experience (19 %). Dieses Problem hat direkte Auswirkungen auf die Produktivität: Wenn das VPN das Netzwerk verlangsamt oder sich die Nutzung als zu umständlich erweist, kann dies zu einer geringeren Mitarbeiterzufriedenheit und langsamen, ineffizienten Geschäftsprozessen führen.

Die zweithäufigste Sorge, die von 17 % der Befragten genannt wird, ist die ständige Fehlerbehebung bei VPN-Konnektivitäts- und Stabilitätsproblemen. Diese Probleme sind nicht nur zeitaufwendig für das IT-Personal, sondern verursachen auch frustrierende Störungen für die User. Zu den weiteren nennenswerten Herausforderungen gehört die mangelnde Kompatibilität von VPNs mit einer Vielzahl von Geräten, Betriebssystemen und Anwendungen, die etwa 16 % der IT-Experten als belastend empfinden. Darüber hinaus haben 13 % der Befragten mit der Komplexität und dem Arbeitsaufwand bei der Skalierung der VPN-Infrastruktur zu kämpfen. Dies stellt ein kritisches Problem dar, da Unternehmen wachsen und ihre Anforderungen weiter steigen, während der eklatante Mangel an qualifizierten Cybersicherheitsfachkräften anhält.

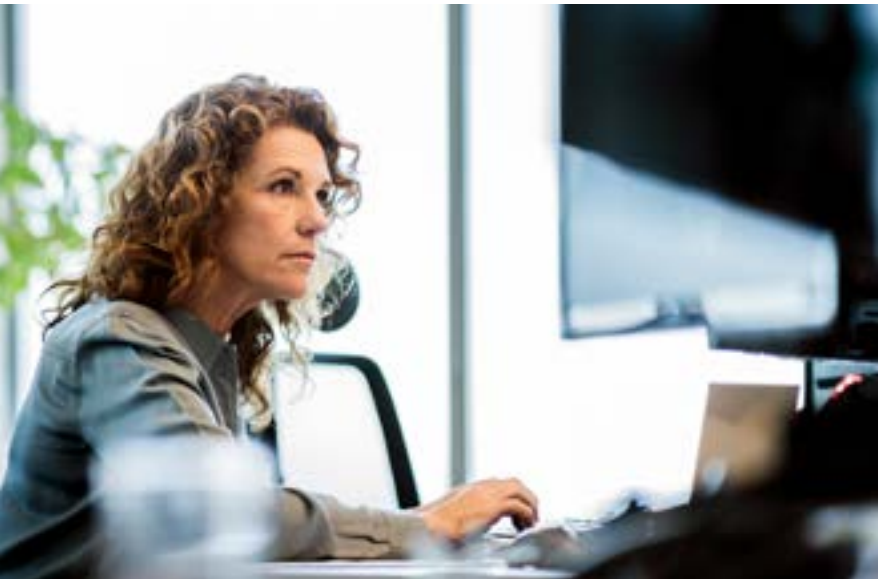
Diese Erkenntnisse unterstreichen die Notwendigkeit für Unternehmen, die Umstellung auf agilere, benutzerfreundlichere und weniger ressourcenintensive Alternativen wie etwa Zero Trust Network Access (ZTNA) zu prüfen. ZTNA gewährleistet eine detailliertere Kontrolle, verbesserte Skalierbarkeit und einen geringeren Verwaltungsaufwand und ist damit in der heutigen dynamischen Cybersicherheitslage eine bessere Wahl als herkömmliche VPNs.



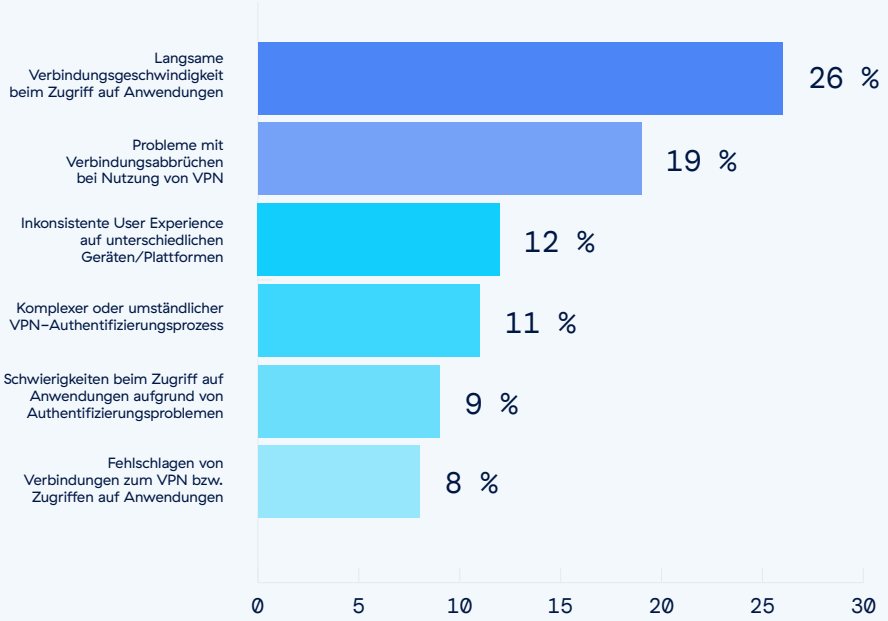
Häufige Probleme für VPN-User

Die häufigste Beschwerde seitens der User von VPNs betrifft laut 26 % der Befragten die langsame Verbindungsgeschwindigkeit. Dies verdeutlicht ein kritisches Problem hinsichtlich der Userproduktivität und -zufriedenheit, da langsame Geschwindigkeiten die Effizienz von Routineaufgaben und den Zugriff auf cloudbasierte Ressourcen erheblich reduzieren können, insbesondere in Homeoffice-Umgebungen.

Unterbrechungen der VPN-Verbindung sind laut 19 % der Befragten das zweithäufigste Problem. Dieses Problem kann laufende Aufgaben und die Kommunikation unterbrechen und so die User Experience und die Betriebskontinuität erheblich beeinträchtigen. 12 % der User berichten von inkonsistenten Anwendererfahrungen auf unterschiedlichen Geräten und Plattformen. Dies weist auf die Notwendigkeit einer einheitlicheren Zugriffsleistung hin.

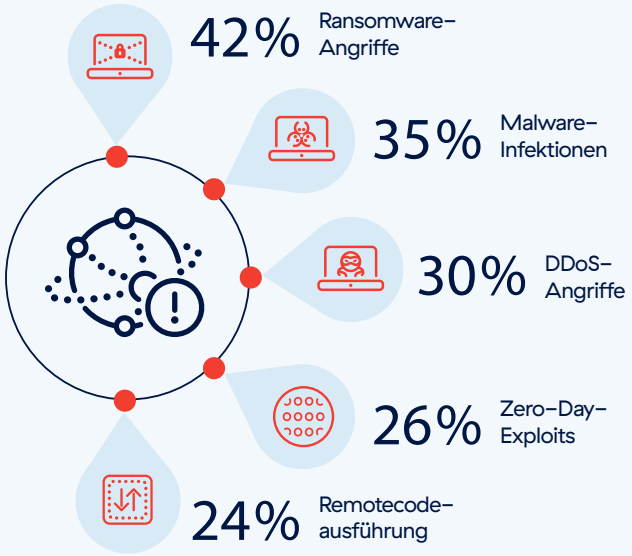


Welches der folgenden Probleme wird von Ihren Usern beim Zugriff auf Anwendungen über VPN am häufigsten gemeldet?



Um diese Bedenken auszuräumen, sollten Organisationen die Umstellung auf Netzwerkzugriffslösungen in Betracht ziehen, die plattformübergreifend mehr Stabilität und Konsistenz gewährleisten. Als besonders effektive Alternative empfiehlt sich die Implementierung einer Zero-Trust-Architektur, da sie die Sicherheit erhöht, ohne Leistungsengpässe zu verursachen. Zero-Trust-Netzwerke stellen sicher, dass die Sicherheit durch Verbindungsprobleme nicht beeinträchtigt wird und dass die Zugriffskontrolle zwar streng, aber dynamisch an unterschiedliche User-Umgebungen anpassbar ist.

Von welchen Arten von Cyberangriffen geht Ihrer Meinung nach das höchste Risiko in Bezug auf die Ausnutzung von Sicherheitslücken im VPN Ihrer Organisation aus?



Um diesen Schwachstellen entgegenzuwirken, sollten Organisationen auf proaktive Sicherheitsmaßnahmen wie ein Zero-Trust-Modell umstellen. Zero Trust erzwingt strenge Zugriffskontrollen und eine kontinuierliche Überprüfung aller Netzwerkverbindungen unabhängig von ihrem Ursprung. Mit dieser Strategie können Sie die Risiken einer breiten Palette von Angriffen, die VPN-Schwachstellen ausnutzen, wirksam verringern, die laterale Bewegungen einschränken und robuste Zugriffskontrollen verstärken.

Ausnutzung von VPN-Sicherheitslücken

Die Vielfalt der Cyberangriffe, bei denen Schwachstellen von VPNs ausgenutzt werden, verdeutlicht die Bandbreite der Risiken, denen Unternehmen ausgesetzt sind. Aus der Umfrage geht hervor, dass 42 % der Befragten die Erfahrung gemacht haben, dass VPN-Schwachstellen am häufigsten durch Ransomware-Angriffe ausgenutzt werden. Es folgen Malware-Infektionen, die von 35 % der Befragten gemeldet wurden, und DDoS-Angriffe (30 %), die sowohl die Verfügbarkeit als auch die Vertraulichkeit und Integrität der Systeme gefährden.

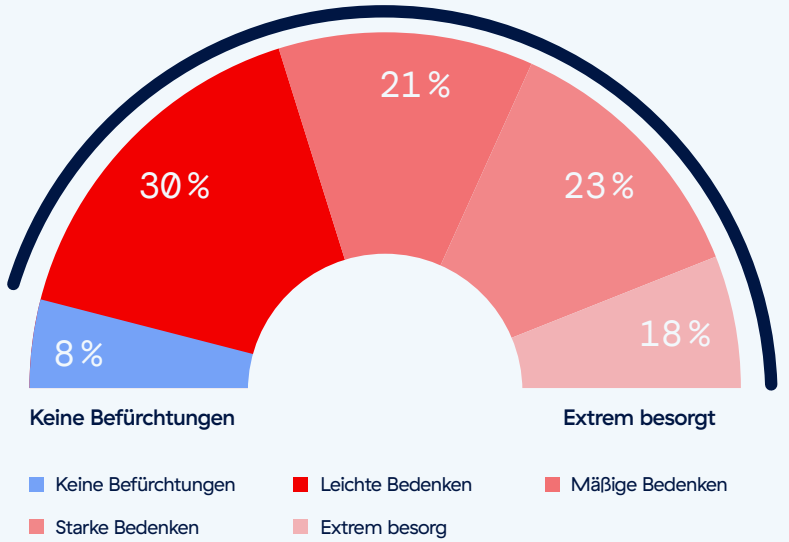
VPN-Risiken durch Drittuser

Die Umfrage unterstreicht die erhebliche Besorgnis hinsichtlich des VPN-Zugriffs Dritter als Sicherheitslücke im Netzwerk. Bemerkenswerte 92 % der Befragten äußern Bedenken hinsichtlich dieses Risikos, was einen leichten Anstieg gegenüber 90 % im Jahr 2023 darstellt. Diese wachsende Besorgnis verdeutlicht das Risiko, dass der Zugriff Dritter als Einfallspunkt für Cyberbedrohungen ausgenutzt wird.

Neue Erkenntnisse zu VPN-Schwachstellen und Sicherheitsverletzungen haben diese Bedenken weiter bestätigt. Herkömmliche VPNs ermöglichen in der Regel einen umfassenden Netzwerkzugriff nach der Validierung der Anmeldedaten. Dies birgt Risiken, wenn die Sicherheitsmaßnahmen von Drittanbietern kompromittiert werden.

Haben Sie Bedenken, dass Angreifer sich über VPN-Zugriff für Drittuser unbefugten Zugang zu Ihrem Unternehmensnetzwerk verschaffen könnten?

92 % befürchten, dass Angreifer sich über VPN-Zugriff für Drittuser unbefugten Zugang zum Unternehmensnetzwerk verschaffen könnten



Organisationen sollten die Umstellung von herkömmlichen VPNs zu Zero-Trust-Architekturen beschleunigen. Dieser Wandel beinhaltet die Implementierung von Systemen, die Zugriffsanforderungen streng auf Grundlage von Identität und Kontextdaten prüfen und Drittuser ausschließlich mit Ressourcen verbinden, die für ihre Aufgaben unerlässlich sind.

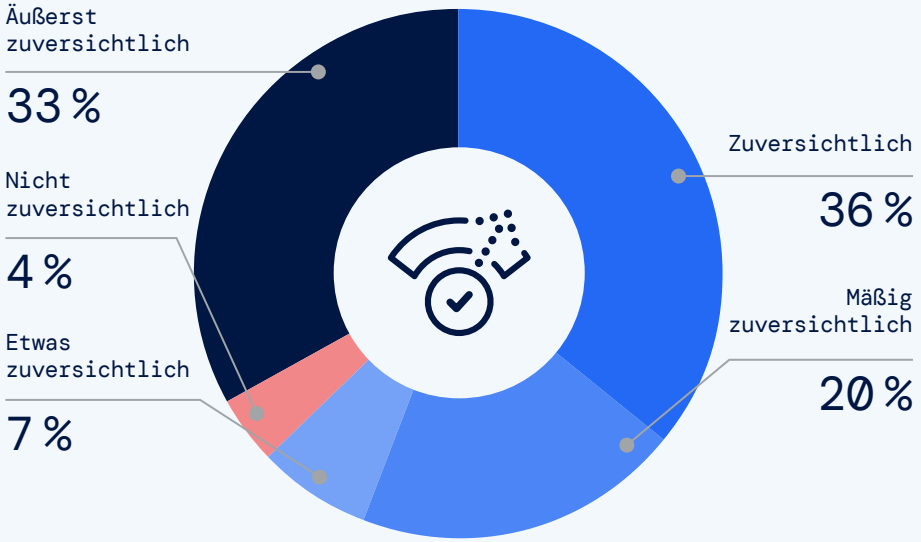
Sicherheitsprobleme mit der VPN-Infrastruktur

Übermäßiges Vertrauen in VPN-Sicherheit

Der jüngste Anstieg der VPN-Sicherheitsverletzungen macht deutlich, dass eine Diskrepanz zwischen wahrgenommener Sicherheit und tatsächlichem Risiko besteht. Jüngste Angriffe mit hohem Schweregrad in VPN-Produkten unterstreichen, dass selbst gut vorbereitete Organisationen die Fähigkeiten von Cyber-Angreifern, die für die VPN-Technologie typische Schwachstellen ausnutzen, möglicherweise unterschätzen. Bemerkenswerte 69 % der Umfrageteilnehmer äußerten großes Vertrauen in die Fähigkeit ihres Unternehmens, mit VPN-Schwachstellen umzugehen. Diese Wahrnehmung entspricht möglicherweise nicht vollständig der eskalierenden Bedrohungslage, in der raffinierte Akteure selbst geringfügige Schwachstellen sehr schnell ausnutzen. Angesichts der Komplexität und Hartnäckigkeit der jüngsten VPN-Angriffe kann Selbstüberschätzung besonders riskant sein. Dies zeigen Vorfälle, in die staatlich geförderte Gruppen und cyberkriminelle Banden verwickelt waren, die über längere Zeiträume ungepatchte Systeme ins Visier nahmen.

Organisationen müssen ihren Sicherheitsstatus durch strenge Schwachstellenanalysen, regelmäßige Updates und umfassende Schulungen zur Sensibilisierung für Sicherheitsaspekte stärken. Für einen umfassenden Schutz empfiehlt sich die Umstellung auf einen mehrschichtigen Sicherheitsansatz, der nicht übermäßig auf VPNs setzt. Dieser Ansatz sollte erweitertes Monitoring, Erkennung von Anomalien und die Integration von Zero-Trust-Prinzipien umfassen.

Wie zuversichtlich sind Sie, dass Ihr Unternehmen in der Lage ist, VPN-Schwachstellen zu erkennen und zu beseitigen, die es Cybersicherheitsangriffen aussetzen?

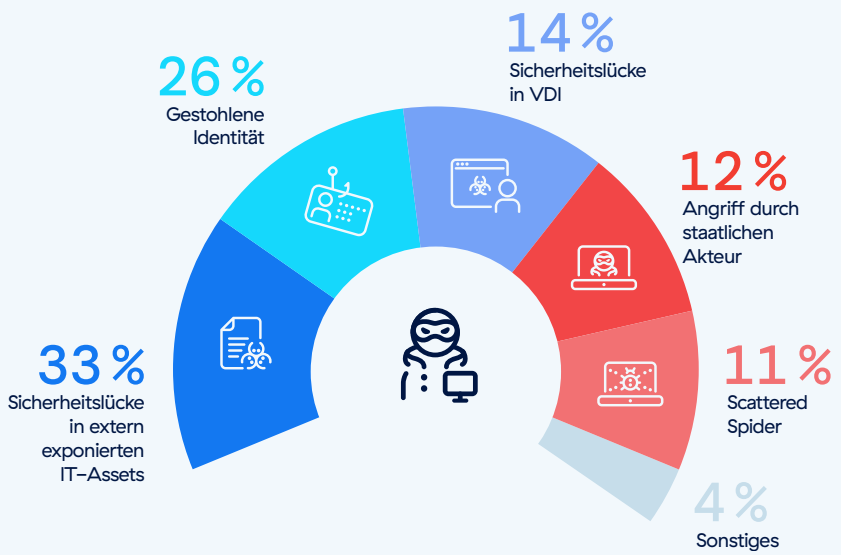


Ransomware-Angriffsvektoren

Aus der Umfrage geht eindeutig hervor, dass Schwachstellen in extern exponierten IT-Assets den besorgniserregendsten potenziellen Angriffsvektor für Ransomware darstellen: 33 % der Befragten gaben dies an. Dies deutet darauf hin, dass die Risiken exponierter Netzwerkdienste oder Webanwendungen, die häufig den ersten Einstiegspunkt für Ransomware-Angriffe darstellen, weithin bekannt sind.

Gestohlene Identitäten folgen dicht dahinter mit 26 %. Dies unterstreicht die Rolle kompromittierter Anmeldedaten, die es Angreifern ermöglichen, Sicherheitsmaßnahmen zu umgehen und Zugriff zu erhalten, um Ransomware-Payloads auszuliefern. Bedenken hinsichtlich Schwachstellen in virtuellen Desktop-Infrastrukturen (VDI) und Angriffen durch staatliche Akteure (14 % bzw. 12 %) unterstreichen die vielfältigen Ursprünge der Ransomware-Bedrohungen, vor denen sich Organisationen schützen müssen. 11 % der Befragten sind besorgt über Scattered Spider (eine Gruppe von Cyberkriminellen, die ausgefeilte Social-Engineering-Taktiken wie Phishing, Multifaktor-Authentifizierungs-Ermüdungsangriffe und SIM-Swapping verwendet).

Worin sehen Sie die Hauptursache für erfolgreiche Ransomware-Angriffe?



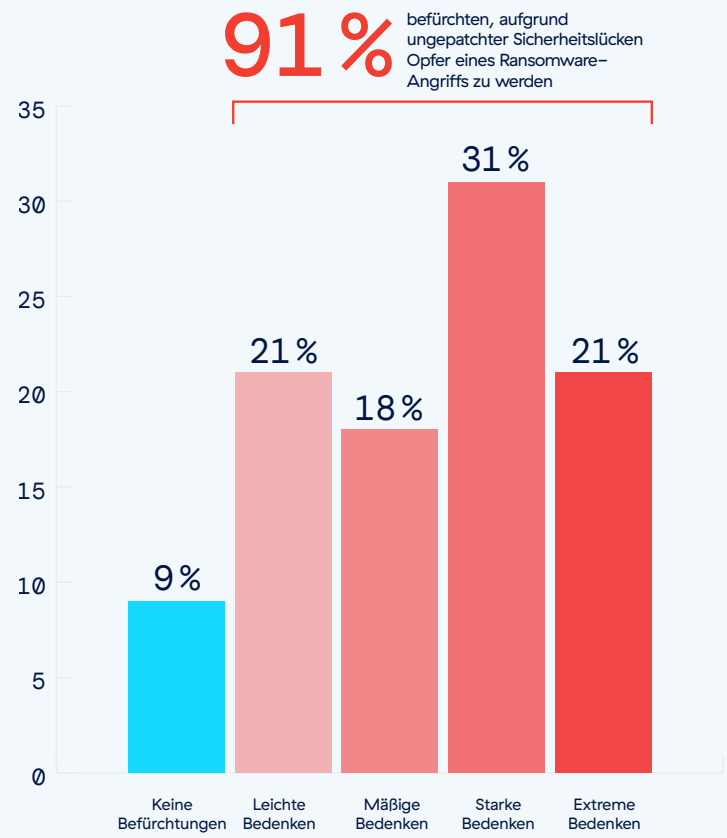
Organisationen sollten ihre Abwehrmaßnahmen und Identitätsmanagementprotokolle verbessern. Durch die Implementierung umfassender Prozesse zum Schwachstellenmanagement und die Umstellung auf ein Zero-Trust-Sicherheitsmodell kann das Risiko von Ransomware-Angriffen wirksam verringert werden, indem der Zugriff auf Netzwerkressourcen und die laterale Ausbreitung verweigert werden.

Bedenken hinsichtlich Ransomware

Die Umfrageergebnisse zeigen, dass 52 % der Befragten aufgrund ungepatchter Schwachstellen sehr oder äußerst besorgt über die Bedrohung durch Ransomware sind. Dies ist gerechtfertigt, da ungepatchte Schwachstellen weiterhin einen primären Angriffsvektor für Ransomware darstellen. Aktuelle Analysen zeigen, dass ein erheblicher Teil der Ransomware-Angriffe diese Schwachstellen ausnutzt, wobei die Auswirkungen im Vergleich zu anderen Arten von Cyberangriffen bemerkenswert schwerwiegend sind.

Ransomware-Gruppen werden immer raffinierter. Viele verwenden mittlerweile hochentwickelte Taktiken, mit denen sie neu entdeckte Schwachstellen schnell ausnutzen können, bevor die Organisationen sie patchen können. Dieser schnelle Ausnutzungszyklus verkürzt das Zeitfenster für die Reaktion auf kritische Schwachstellen erheblich und unterstreicht die dringende Notwendigkeit erweiterter Sicherheitsmaßnahmen zur Minimierung der Angriffsfläche.

Wie stark ist Ihre Befürchtung, aufgrund ungepatchter Sicherheitslücken Opfer eines Ransomware-Angriffs zu werden?



Laterale Bewegung bei VPN-Angriffen

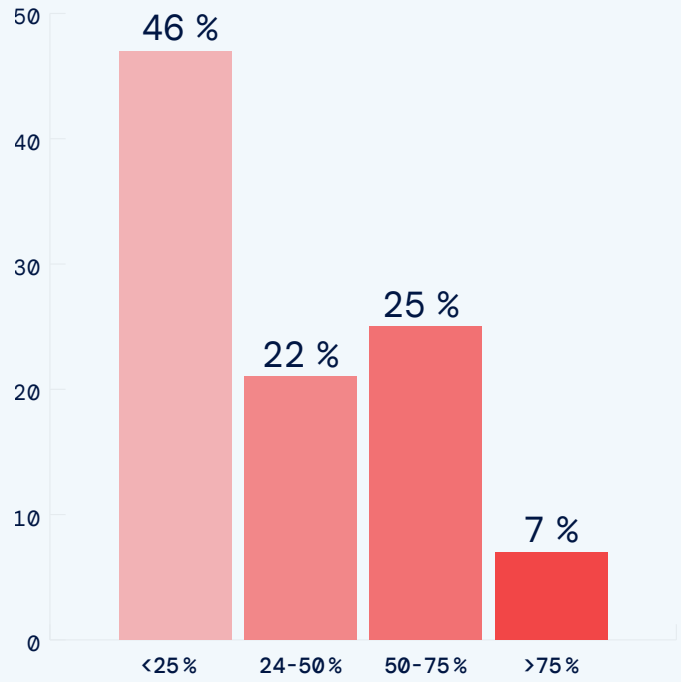
Eine Mehrzahl der Befragten (53 %) berichtet, dass über 25 % der VPN-bezogenen Angriffe laterale Bewegungen beinhalteten, was auf erhebliche Fehler bei der Eindämmung am ersten Angriffspunkt hinweist. Knapp ein Drittel (32 %) verzeichnete laterale Bewegungen bei über der Hälfte aller Angriffe, was auf große Probleme bei der Eindämmung der Bedrohungsausbreitung nach erfolgreichem Erstzugriff schließen lässt.

Bei VPNs besteht ein erhebliches Risiko lateraler Bewegungen, da Angreifer ähnlich umfassenden Netzwerkzugriff wie ein authentifizierter User erlangen können. Auf diese Weise können sie sich unbemerkt durch das Netzwerk bewegen und sensible Bereiche angreifen.

Dadurch können VPNs die Risiken verstärken und den Umfang eines Angriffs über seinen ursprünglichen Eintrittspunkt hinaus erweitern. Um dieses Problem zu lösen, ist eine strenge Segmentierung — idealerweise mit User-zu-Anwendung-Traffic über eine Zero-Trust-Architektur — und eine kontinuierliche Überwachung erforderlich. Dadurch wird das Schadenspotenzial durch laterale Bewegungen erheblich verringert, indem jedem einzelnen User granularer Zugriff auf eine kleinere Anzahl von Anwendungen ermöglicht wird, während der Rest unsichtbar bleibt.

Die zunehmende Raffinesse von Angriffen, die VPN-Schwachstellen ausnutzen, unterstreicht die Notwendigkeit einer Umstellung auf ein Zero-Trust-Framework. Durch die Durchsetzung strenger Zugriffskontrollen und kontinuierlicher Überprüfung begrenzt Zero Trust unbefugte laterale Bewegungen und verbessert die Sicherheit in wachsenden digitalen Umgebungen.

Bei wie vielen der Angriffe auf Ihre Organisation kam es zu lateralen Bewegungen von Bedrohungen, nachdem sie sich über VPN Zugriff verschafft hatten?

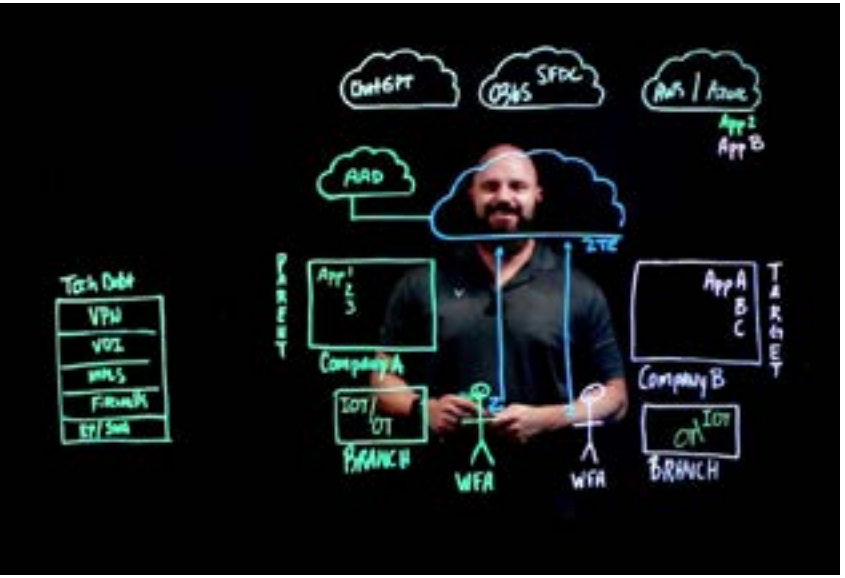


Bedenken hinsichtlich der Sicherheit von VPNs

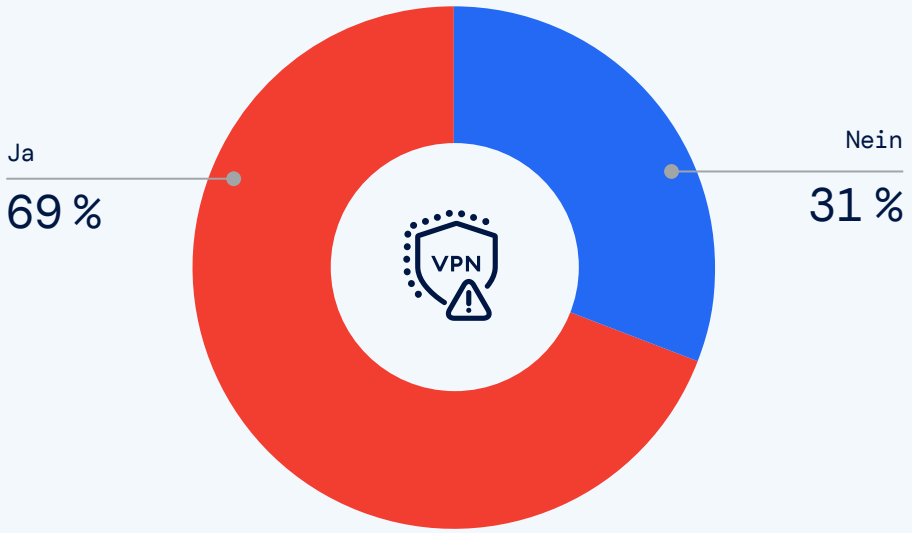
Nach Fusionen und Übernahmen

Bedenken hinsichtlich der Auswirkungen von Fusionen und Übernahmen auf die vorhandene VPN-Infrastruktur beleuchten die potenziellen Schwachstellen, die sich aus organisatorischen Änderungen und der Integration unterschiedlicher Netzwerke ergeben.

Bemerkenswerte 69 % der Befragten äußern Besorgnis über Cyberangriffe infolge von Fusionen und Übernahmen, was die weitverbreitete Besorgnis über die Sicherheitsrisiken unterstreicht, die mit diesen Unternehmenstransaktionen einhergehen. Dieses Ergebnis zeigt, dass sich die Befragten der Gefahr bewusst sind, dass Fusionen und Übernahmen vorhandene Sicherheit-Frameworks destabilisieren und die Anfälligkeit gegenüber Cyberbedrohungen erhöhen können.



Befürchten Sie, mit Ihrer aktuellen Infrastruktur von einem Angriff infolge von Fusionen und Übernahmen betroffen zu werden?



Übergangsfristen während Fusionen und Übernahmen bieten Organisationen einzigartige Möglichkeiten, veraltete und anfällige VPN-Technologien durch Zero-Trust-Frameworks zu ersetzen. Insbesondere erhöhen Zero-Trust-Architekturen die Sicherheit, indem sie eine umfassende Segmentierung der Umgebung zwischen Usern und Anwendungen, mehreren Workloads, Zweigstellenstandorten und Geräten ermöglichen, unabhängig davon, ob es sich um verwaltete Geräte, nicht verwaltete Geräte, IoT- oder OT-Systeme handelt. Dieser Ansatz erhöht die Sicherheit während und nach einer Umstellung erheblich durch eine strenge Überprüfung aller User und Geräte, eine umfassende Segmentierung und die strikte Durchsetzung von Zugriffskontrollen nach dem Prinzip der minimalen Rechtevergabe.

Umstellung auf Zero Trust in Unternehmen

Fortschritte bei der Einführung von Zero Trust

Die Umfrage spiegelt einen starken Trend zur Einführung von Zero-Trust-Sicherheits-Frameworks wider und unterstreicht die wachsende Anerkennung ihrer Bedeutung bei der Verbesserung der organisatorischen Cybersicherheit. Bemerkenswerte 31 % der Befragten implementieren bereits Zero Trust (gegenüber 27 % im Jahr 2023). Dies deutet auf eine wachsende proaktive Anstrengung zum besseren Schutz von Netzwerkressourcen hin.

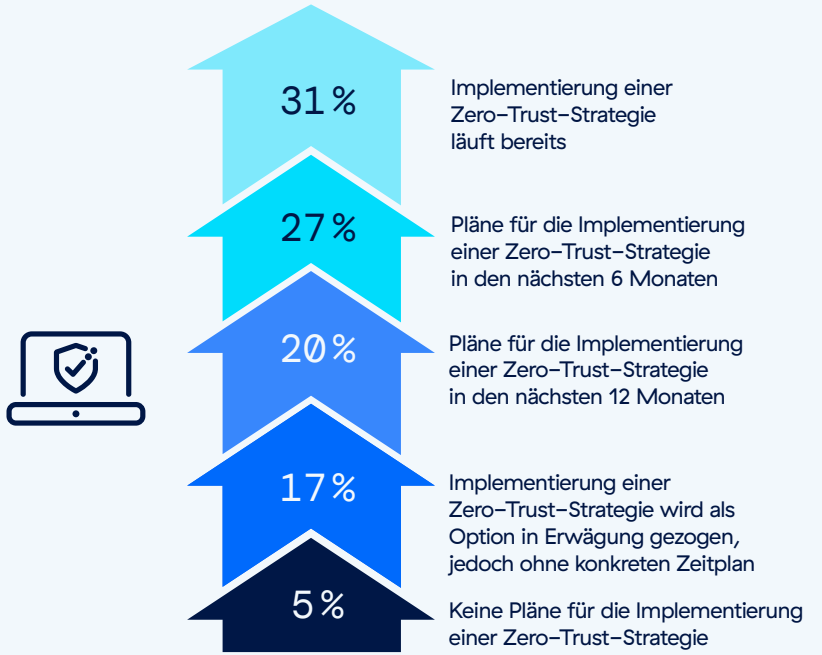
Darüber hinaus planen 27 % der Organisationen, innerhalb der nächsten sechs Monate eine Zero-Trust-Strategie umzusetzen (gegenüber 18 % im Jahr 2023), und weitere 20 % der Organisationen planen, die Umstellung innerhalb der nächsten 12 Monate vorzunehmen, was ein weit verbreitetes Engagement für den Übergang zu Zero Trust in naher Zukunft zeigt. Dies bestätigt, dass mehr als drei Viertel der Umfrageteilnehmer (78 %) die Dringlichkeit der Umstellung und die Vorteile von Zero Trust erkennen.

Allerdings ziehen 17 % der Befragten noch immer eine Zero-Trust-Strategie in Erwägung, ohne einen konkreten Zeitplan vorzugeben (gegenüber 23 % im Jahr 2023). Dies deutet auf eine gewisse Zurückhaltung oder potenzielle Herausforderungen bei der Planung oder Einleitung der Umstellung hin. Nur ein kleiner Bruchteil (5 %) hat keine Pläne zur Einführung von Zero Trust (gegenüber 8 % im Jahr 2023), möglicherweise aufgrund fehlender Ressourcen.

Eine Analyse nach Unternehmensgröße zeigt, dass die größeren Organisationen in unserer Umfrage, insbesondere solche mit über 20.000 Mitarbeitern, eher und schneller Zero-Trust-Strategien einführen; 33 % setzen sie bereits um. Im Gegensatz dazu weisen kleinere Unternehmen mit 1.000 bis 5.000 Mitarbeitern eine etwas geringere Akzeptanzrate von 29 % auf. Dies deutet darauf hin, dass Umfang und Ressourcenverfügbarkeit das Tempo und den Umfang der Zero-Trust-Integration beeinflussen können.

Organisationen, die noch unentschieden sind oder sich erst in der Planungsphase befinden, sollten zunächst ihren aktuellen Sicherheitsstatus und ihre Netzwerkarchitektur bewerten, um spezifische Anforderungen und potenzielle Herausforderungen zu identifizieren.

Welche Pläne haben Sie für die Einführung einer Zero-Trust-Strategie in Ihrem Unternehmen?

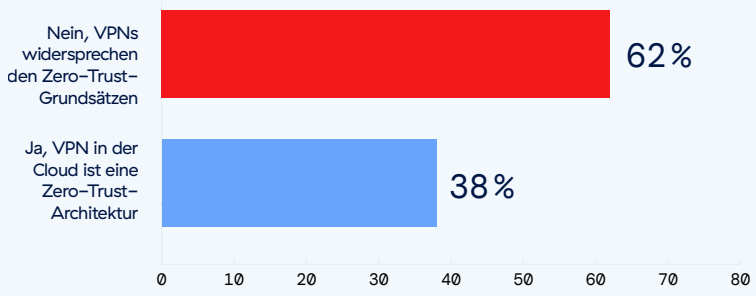


Keine Zero-Trust-Sicherheit mit VPN

Aus den Umfrageergebnisse geht hervor, dass die Ansichten über die Kompatibilität von VPNs mit Zero-Trust-Sicherheitsframeworks stark auseinandergehen. Die Mehrzahl der Befragten (62 %) ist der Ansicht, dass VPNs grundsätzlich nicht mit den Prinzipien von Zero Trust vereinbar sind. Umgekehrt sind 38 % der Befragten der Ansicht, dass VPNs, insbesondere cloudbasierte Plattformen, mit Zero-Trust-Architekturen kompatibel sind.

Diese Sichtweise rührt möglicherweise daher, dass VPN-Anbieter behaupten, ihre cloudbasierten Lösungen entsprächen den Zero-Trust-Prinzipien. Um so wichtiger ist es, diese Aussagen kritisch zu prüfen. Das bloße Hosten eines VPN-Dienstes in der Cloud verleiht beispielsweise nicht automatisch Zero-Trust-Attribute. Für Zero-Trust-Sicherheit ist mehr als nur eine sichere Hosting-Umgebung erforderlich. Sie erfordert eine grundlegende Abkehr von perimeterbasierten Abwehrmaßnahmen hin zu einem Modell, bei dem die Sicherheit dynamisch, granular und kontextbasiert ist.

Glauben Sie, dass Sie mit VPNs Zero-Trust-Sicherheit erreichen können?



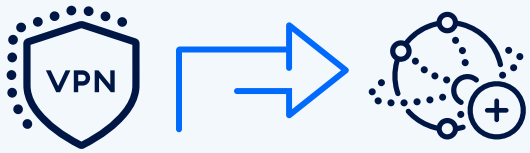
Echte Zero-Trust-Sicherheit beinhaltet die kontinuierliche Validierung aller User und Geräte, die konsequente Umsetzung des Prinzips der minimalen Rechtevergabe und die Segmentierung des gesamten Traffics, um laterale Bewegungen zu verhindern — Funktionen, die herkömmliche VPNs, selbst cloudbasierte, nicht bieten. Daher müssen Organisationen überprüfen, inwieweit vermeintliche „Zero Trust"-VPNs diese Kernprinzipien tatsächlich umsetzen, anstatt sich ausschließlich auf Marketingversprechen zu verlassen.

Vom VPN zum Zero Trust Network Access

Die Umfrageergebnisse zeigen, dass die meisten Organisationen einen strategischen Wandel vornehmen: 53 % der Befragten gaben an, dass sie planen, ihre vorhandenen VPN-Lösungen in naher Zukunft durch ZTNA-Lösungen zu ersetzen. ZTNA bietet einen flexibleren und sichereren Ansatz, indem Richtlinien basierend auf User-Kontext, Standort und Gerätesicherheit durchgesetzt werden, ohne Anfragen basierend auf dem Netzwerkstandort automatisch als vertrauenswürdig einzustufen. Dies steht im Gegensatz zu herkömmlichen VPNs, die im Allgemeinen einen umfassenden Zugriff auf ein Netzwerk gewähren und dadurch Sicherheitslücken entstehen lassen.

Für die 53 % der Unternehmen, die auf ZTNA umsteigen, ist es von entscheidender Bedeutung, einen reibungslosen Übergang sicherzustellen, indem sie umfassende Risikobewertungen planen, Zugriffsrichtlinien aktualisieren und User über neue Protokolle informieren. Unterdessen sollten die 47 %, die noch keinen Wechsel planen, ihre aktuellen Sicherheitsherausforderungen bewerten und überlegen, ob diese mit ZTNA wirksamer gelöst werden können als mit VPN.

Gibt es in Ihrer Organisation Pläne, Ihre VPN-Lösung in naher Zukunft durch eine ZTNA-Lösung zu ersetzen?



53 %

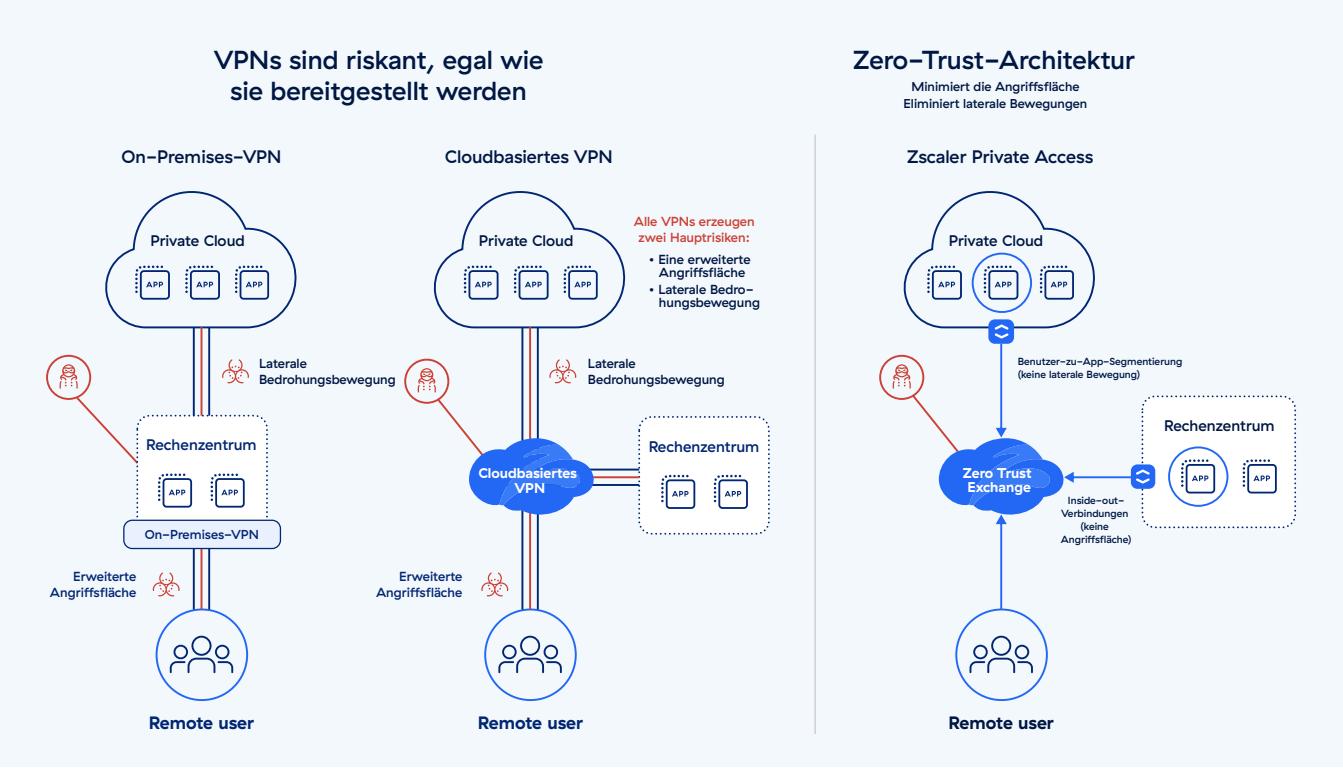
planen, VPN in naher Zukunft durch eine ZTNA-Lösung zu ersetzen

Warum Zero Trust sicherer ist als VPN

Architektonisch sind Zero Trust und ZTNA aus mehreren Gründen sicherer als herkömmliche VPNs, vor allem aufgrund eines robusten Sicherheitsframeworks, das einzelne Verbindungen niemals automatisch als vertrauenswürdig einstuft. Herkömmliche VPN-basierte Architekturen sind anfällig für einen einzelnen Ausfallpunkt. Wenn ein VPN oder Gerät kompromittiert wird (beispielsweise durch eine neue CVE), können Bedrohungsakteure das in einem flachen Netzwerk inhärente Vertrauen ausnutzen, um Zugriff auf das gesamte Netzwerk zu erhalten, sich lateral zu bewegen, Daten zu stehlen und Ransomware auszuliefern. Aus diesem Grund sind Sicherheitsexperten zunehmend besorgt über die Sicherheitsrisiken von VPN.

On-Prem und in der Cloud bereitgestellte VPNs weisen ähnliche Sicherheitslücken auf. Darüber hinaus führen VPNs zu Komplexität und damit zu unnötigem Mehraufwand sowie zeitaufwendigen Aufgaben wie User Provisioning, Routing-Tabellenverwaltung, Konnektivitätsfehlerbehebung, Patchen, Überwachung und Leistungsoptimierung.

In einer Zero-Trust-Architektur wird keine einzelne Verbindung jemals inhärent als vertrauenswürdig eingestuft. User stellen eine Direktverbindung zu Anwendungen her — niemals zum zugrunde liegenden Netzwerk. Darüber hinaus wird jede Verbindung unabhängig vom Ursprung automatisch beendet, bevor sie durch sieben Ebenen von Zero-Trust-Sicherheitskontrollen überprüft wird. Mithilfe der Zero-Trust-Architektur können Organisationen ihre Umgebungen umfassend und mit granularem Zugriff segmentieren — zwischen Usern und Anwendungen, mehreren Workloads, Zweigstellen und Geräten, einschließlich IoT- und OT-Geräten.



Wichtige Unterschiede und Vorteile

Deutlich reduzierte Angriffsfläche
Eine Zero-Trust-Architektur ermöglicht Inside-Out-Konnektivität, die kritische Assets, Anwendungen, Server und mehr vor dem öffentlichen Internet verbirgt und gleichzeitig den Einsatz anfälliger Assets wie VPNs und Firewalls überflüssig macht. Auf diese Weise können Unternehmen ihren Mitarbeitern hybride Konnektivität bereitstellen und gleichzeitig ihre Angriffsfläche erheblich verkleinern. Im Gegensatz dazu erfordern VPN- und Firewall-basierte Architekturen, dass Unternehmen die Angriffsfläche erweitern, um eine erhöhte Konnektivität zu ermöglichen.

Kontinuierliche Überprüfung
Zero-Trust-Modelle erzwingen eine kontinuierliche Sicherheitsüberprüfung von Anmeldedaten und Sicherheitsstatus, bevor Zugriff auf Ressourcen gewährt wird. Dadurch wird es für unbefugte Entitäten viel schwieriger, Zugriff auf vertrauliche Informationen und Systeme zu erhalten und aufrechtzuerhalten. Bei VPNs hingegen erhält der User oder das Gerät oft umfassenden Zugriff auf Netzwerkressourcen, sobald der Zugriff gewährt wurde.

Zugriff nach dem Prinzip der minimalen Rechtevergabe:
Zero-Trust-Prinzipien setzen Zugriffsrichtlinien nach dem Prinzip der minimalen Rechtevergabe durch und stellen sicher, dass User und Geräte nur auf die Ressourcen zugreifen können, die für ihre spezifischen Rollen erforderlich sind. Dies minimiert das Risiko interner Bedrohungen und lateraler Bewegungen innerhalb eines Netzwerks, die häufige Schwachstellen in VPN-Setups darstellen.

Granularer Zugriff und Segmentierung
Durch die Aufteilung der Netzwerkressourcen in separate Segmente — zwischen Usern und Apps, zwischen Workloads, zwischen Geräten — isoliert Zero Trust potenzielle Sicherheitslücken auf kleinere Zonen und reduziert so die Auswirkungen eines Angriffs erheblich. Bei Versuchen, Netzwerkumgebungen zu segmentieren, handelt es sich um einen betrieblich komplexen und kostspieligen Prozess, der in der Praxis oft unvollständig bleibt, Hunderte diskreter Firewall-Regeln erfordert und authentifizierten Usern größere Netzwerkbereiche zugänglich macht.

Unterstützung zukunftsfähiger hybrider Arbeitskonzepte:
Zero Trust ermöglicht die einfache Ausweitung des blitzschnellen Zugriffs auf private Anwendungen auf Remote-User sowie auf Unternehmenszentralen, Zweigstellen und Drittanbieterpartner.

Verbesserte User Experience und reduzierte Komplexität
Zero Trust verbessert die User Experience, da der gesamte Remote-Traffic nicht mehr über einen zentralen Netzwerkpunkt geleitet werden muss, was bei VPNs häufig zu Leistungsengpässen führt. Diese Architektur kann die Skalierungsanforderungen moderner Netzwerke, die IoT- und BYOD-Richtlinien umfassen, besser bewältigen. Darüber hinaus reduziert Zero Trust den Verwaltungsaufwand, indem Sicherheitskontrollen automatisiert und die Durchsetzung von Sicherheitsrichtlinien im gesamten Netzwerk vereinfacht wird.

Diese architektonischen Vorteile machen Zero Trust zu einer überzeugenden Alternative zu herkömmlichen VPNs, insbesondere angesichts einer zunehmend unübersichtlichen und unberechenbaren Bedrohungslage. Für Organisationen, die ihre Cybersicherheitsabwehr stärken möchten, gewährleistet die Umstellung auf einen Zero-Trust-Ansatz eine robustere, flexiblere und skalierbarere Sicherheitsinfrastruktur.

Prognosen für 2024 und darüber hinaus

1 Schwerwiegende VPN-Schwachstellen und Exploits werden zunehmen

Angesichts der Häufigkeit, Schwere und des Ausmaßes der im vergangenen Jahr bekannt gewordenen VPN-Schwachstellen müssen Unternehmen damit rechnen, dass sich dieser Trend fortsetzt. Bedrohungsakteure und Sicherheitsforscher sind sich des erhöhten Risikos schwerwiegender Schwachstellen in VPN-Produkten bewusst. Im Gegenzug suchen sie aktiv nach weiteren CVEs, sodass es wahrscheinlich ist, dass in den kommenden Monaten und Jahren noch weitere CVEs gefunden werden.

2 Aufsehenerregende Angriffe über VPNs stehen im Rampenlicht

Eng verbunden mit unserer ersten Vorhersage ist davon auszugehen, dass mehr große Organisationen Sicherheitsverletzungen offenlegen, die auf die Ausnutzung von VPN-Schwachstellen zurückzuführen sind. Dies liegt teilweise an den neuen Richtlinien der SEC, die börsennotierte Unternehmen dazu verpflichten, Angaben zu Verstößen mit wesentlichen Auswirkungen offenzulegen. Wie wir gesehen haben, schaffen Bedrohungsakteure beim Auftreten von VPN-Schwachstellen immer wieder Hintertüren in Zielumgebungen, um diese zu einem späteren Zeitpunkt auszunutzen, selbst nachdem diese Schwachstellen gepatcht wurden. Im Laufe des Jahres werden weitere davon in öffentlichen Unterlagen der SEC bekannt gegeben und in den Medien Schlagzeilen machen.

3 Die Zunahme KI-gestützter VPN-Lösungen wird Sicherheits- und Datenschutzbedenken aufwerfen

Im Zuge weiterer Fortschritte im Bereich der künstlichen Intelligenz werden KI-gestützte VPN-Lösungen den Markt überschwemmen. Unternehmen sollten diese Angebote jedoch mit Vorsicht prüfen. Zwar versprechen sie eine verbesserte Leistung, doch durch die Integration künstlicher Intelligenz steigen auch die Sicherheitsrisiken und die Möglichkeiten für Angreifer, VPN-Schwachstellen auszunutzen. Darüber hinaus entstehen Datenschutzbedenken durch die umfangreiche Datenanalyse, die das Risiko einer Offenlegung vertraulicher Informationen erhöht.

4 Password-Spraying-Angriffe auf VPNs werden weiter zunehmen

Angreifer finden zunehmend Möglichkeiten, Schwächen bei der Passwortverwaltung und ungenutzte Standard-VPN-Verbindungsprofile durch Password-Spraying-Angriffe auszunutzen. Bei diesen Angriffen probieren Bedrohungsakteure dasselbe Kennwort für viele VPN-Konten aus, bis sie sich erfolgreich anmelden und unbefugten Zugriff erhalten. Angesichts der zahlreichen jüngsten und spektakulären VPN-Sicherheitsverletzungen, bei denen diese Technik effektiv ausgenutzt wurde, müssen Unternehmen damit rechnen, dass es auch weiterhin zu ähnlichen Angriffen kommt.

5 Investitionen werden sich von VPN hin zur Zero-Trust-Konnektivität verlagern

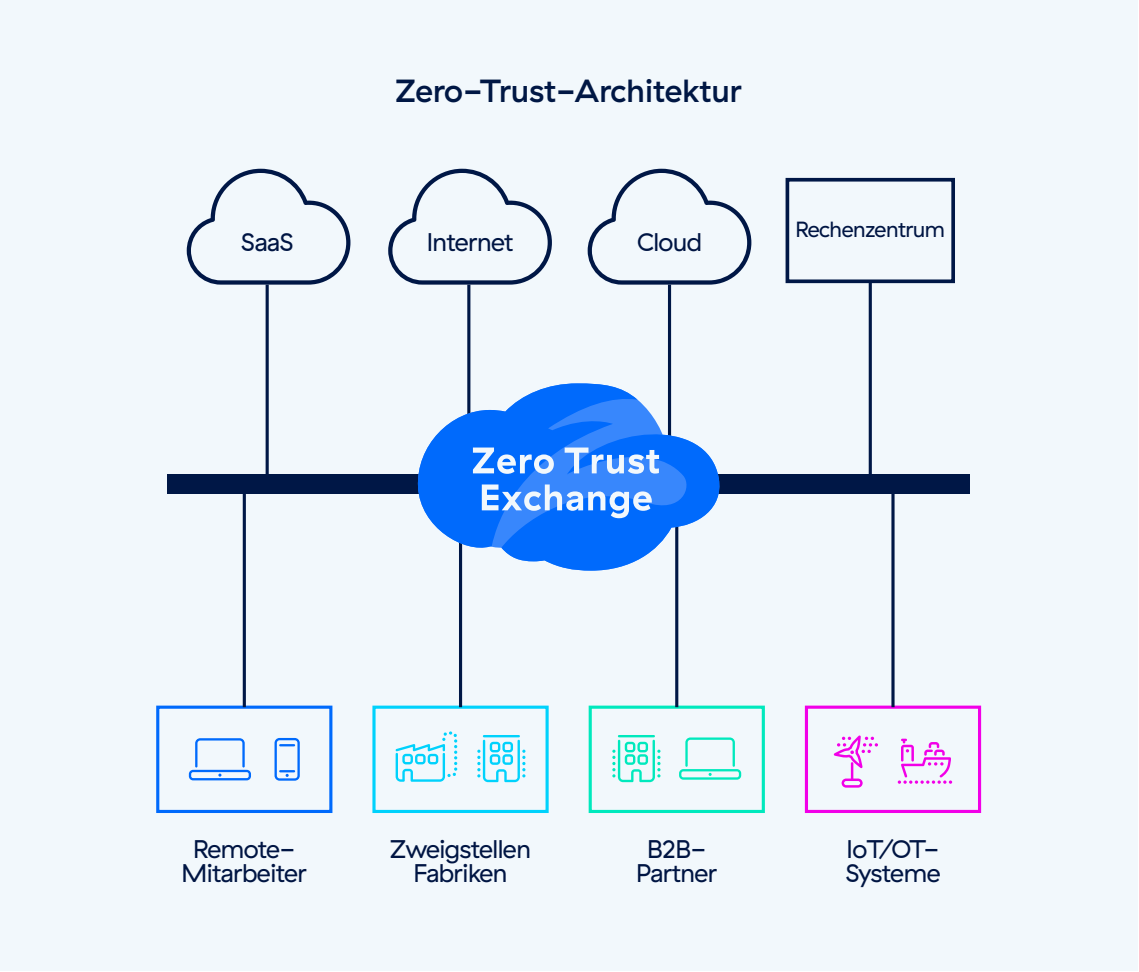
VPNs galten lange als probate Lösung zur Gewährleistung der Remote-Konnektivität, doch angesichts der anhaltenden und zunehmenden Sicherheitsherausforderungen dieser Technologie wird es immer schwieriger, langfristige Investitionen in die Technologie zu rechtfertigen. Da sich in Unternehmen ein Konsens über Zero Trust als bevorzugte Architektur für Sicherheit und Konnektivität herauskristallisiert, werden sich die Unternehmensbudgets weiterhin in Richtung Zero-Trust-Initiativen verschieben, um die Remote-Belegschaft zu schützen.

Zscaler-Lösungen zur Unterstützung von VPN-Alternativen und Zero-Trust-Transformation

Herkömmliche Firewalls und VPNs schaffen eine riesige Angriffsfläche, die es Angreifern ermöglicht, exponierte Ressourcen auszunutzen. Indem User im Netzwerk platziert werden und auf alle darin gehosteten Anwendungen zugreifen können, ermöglichen diese Legacy-Ansätze Angreifern einfachen Zugriff auf vertrauliche Daten. Sie machen es schwierig und zeitaufwendig, Drittanbietern, Auftragnehmern und Agenturen einen sicheren Zugriff zu gewähren oder Ressourcen zur gemeinsamen Nutzung freizugeben. Darüber hinaus verursachen sie zusätzliche Kosten und Komplexität und sind schlichtweg zu langsam für die Anforderungen zukunftsfähiger Remote-Belegschaften.

Die Zscaler Zero Trust Exchange™-Plattform, die weltweit größte Inline-Sicherheits-Cloud, verbindet sicher User, Workloads, IoT/OT, und B2B-Partner ohne Erweiterung des Netzwerkzugriffs.

Zscaler Private Access™ (ZPA™), ein wesentlicher Bestandteil der Zero Trust Exchange, gewährleistet Direktzugriff auf private Unternehmensanwendungen, die hinter der Zero Trust Exchange verborgen sind. Dadurch wird die Angriffsfläche minimiert und eine granulare Segmentierung einzelner Verbindungen zwischen Usern und Anwendungen ermöglicht, laterale Bewegungen verhindert, Funktionen zum Schutz für interne Anwendungen und zur Inline-Überprüfung des gesamten Traffics bereitgestellt und gleichzeitig Zero-Day-Bedrohungen gestoppt. Dadurch verbessert sich insgesamt Ihr Sicherheitsstatus. Als cloudnativer Service kann ZPA innerhalb weniger Stunden bereitgestellt werden und ersetzt Legacy-Tools für den Remotezugriff wie VPNs und VDI.



Zero Trust Networking

ZPA ermöglicht granularen, segmentierten Zugriff mit Inside-Out-Konnektivität zu privaten Unternehmensanwendungen und Workloads. Darüber hinaus beinhaltet ZPA eine umfassende Reihe von Zugriffskontrolldiensten, darunter KI-gestützte User-zu-App-Segmentierung — mit automatisierten Empfehlungen für Userzugriffsrichtlinien und Anwendungssegmente —, Workload-zu-Workload-Segmentierung, privilegierter Remote-Zugriff, privater Service-Edge, Browser-Zugriff und mehr.

Schutz vor Cyberbedrohungen

ZPA bietet erweiterte Cybersicherheitsfunktionen zum Schutz Ihres Unternehmens. Hierzu gehören App-Schutzfunktionen, die mithilfe von Inline-Sicherheitsüberprüfungen die häufigsten Anwendungsangriffe und Zero-Day-Schwachstellen stoppen, sowie Deception-Technologien, die Angreifer mit Decoy-Anwendungen anlocken und das Erkennen komplexer Bedrohungen erleichtern.

Data Protection

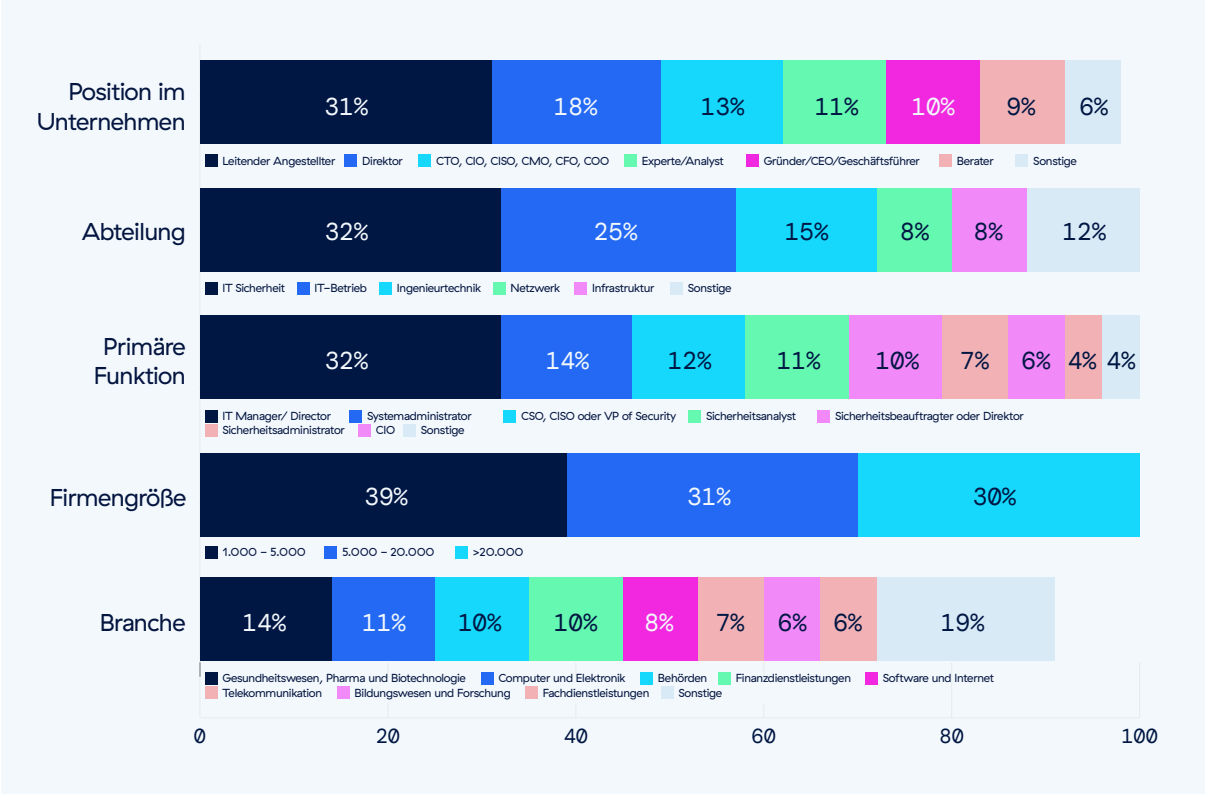
ZPA bietet ganzheitliche Data Protection und kanalübergreifende Funktionen zur Verhinderung von Datenverlusten mit Web Data Loss Prevention (DLP), Endpoint DLP und Browser-Isolierung, die Datenlecks für gefährdete User und BYOD-Endgeräte verhindert.

Best Practices für die Bewältigung von VPN-Risiken

- **Minimieren Sie die Angriffsfläche:** Ermöglichen Sie direkten Zugriff auf Anwendungen und sorgen Sie dafür, dass sowohl Anwendungen als auch User im Internet unsichtbar sind, um ihre Entdeckung und Nutzung für den Erstzugriff zu erschweren.
- **Verhindern Sie den Erstzugriff:** Überprüfen Sie den gesamten Traffic inline, um Zero-Day-Exploits, Malware oder andere komplexe Bedrohungen automatisch zu stoppen.
- **Blockieren Sie unbefugten Zugriff:** Verwenden Sie eine starke Multifaktor-Authentifizierung (MFA) wie Einmalpasswörter oder Token, Biometrie oder FIDO2-Anmeldeinformationen, um Zugriffsanforderungen zu validieren. Umgekehrt verwendet eine schwache MFA häufig Ansätze, die Fragen zum Zurücksetzen von Passwörtern verwenden.
- **Erzwingen Sie Zugriff mit minimaler Rechtevergabe:** Schränken Sie die Berechtigungen von Usern, Traffic, Systemen und Anwendungen anhand von Identität und Kontext ein und stellen Sie so sicher, dass nur autorisierte User auf bestimmte Ressourcen zugreifen können (bietet zusätzliche Sicherheit im Falle einer MFA-Kompromittierung oder eines Diebstahls von Anmeldedaten).
- **Unterbinden Sie laterale Bewegungen:** Verbinden Sie User direkt mit Anwendungen, nicht mit dem Netzwerk, um das Schadenspotenzial eines potenziellen Angriffs zu begrenzen und das Risiko lateraler Bewegungen zu minimieren.
- **Schalten Sie kompromittierte User und Insider-Bedrohungen aus:** Aktivieren Sie die Inline-Überprüfung und -Überwachung, um kompromittierte User mit Zugriff auf Ihr Netzwerk, private Anwendungen und Daten zu erkennen.
- **Verhindern Sie Datenverluste:** Überprüfen Sie Daten während der Übertragung und Daten im Ruhezustand, um aktiven Datendiebstahl während eines Angriffs zu vermeiden.
- **Setzen Sie aktive Abwehrmaßnahmen ein:** Nutzen Sie die Deception-Technologie mit Decoys und führen Sie eine tägliche Bedrohungssuche durch, um Angriffe in Echtzeit zu vereiteln und abzufangen.
- **Testen Sie Ihren Sicherheitsstatus:** Lassen Sie regelmäßig Risikobewertungen durch Dritte vornehmen und führen Sie Aktivitäten in Purple Teams durch, um die Lücken in Ihrem Sicherheitsprogramm zu ermitteln und zu schließen. Fordern Sie Ihre Service-Anbieter und Technologiepartner auf, dasselbe zu tun, und teilen Sie die Ergebnisse dieser Berichte mit Ihrem Sicherheitsteam.

Methodik und demografische Daten

Diesem Bericht liegen die Ergebnisse einer umfassenden Online-Umfrage zugrunde, die im Juni 2023 unter 382 IT- und Cybersicherheitsexperten durchgeführt wurde, um aktuelle Trends, Herausforderungen, Lücken und Lösungspräferenzen im Zusammenhang mit VPN-Risiken in Unternehmen zu ermitteln. Der Kreis der Befragten umfasste Führungskräfte aus dem Technologiebereich sowie IT-Sicherheitsexperten. Sie repräsentieren einen ausgewogenen Querschnitt von Unternehmen unterschiedlicher Größe und verschiedener Branchen.



Über Zscaler

Zscaler beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen finden Sie unter www.zscaler.de.

Über ThreatLabZ

ThreatLabz ist als Forschungsabteilung von Zscaler für die Früherkennung neuer Bedrohungen zuständig. Dieses erstklassige Team sorgt dafür, dass die Tausenden von Organisationen, die weltweit mit der globalen Zscaler-Plattform arbeiten, jederzeit geschützt sind. Neben der Erforschung und Verhaltensanalyse von Malware-Bedrohungen tragen die ThreatLabz-Experten auch zur Entwicklung neuer Prototypen für Advanced Threat Protection auf der Zscaler-Plattform bei und führen regelmäßig interne Revisionen durch, um sicherzustellen, dass Zscaler-Produkte und -Infrastrukturen die geltenden Sicherheitsstandards erfüllen. Detaillierte Analysen neuer Bedrohungen werden regelmäßig unter research.zscaler.de veröffentlicht.

Über Cybersecurity Insiders

Cybersecurity Insiders ist ein Zusammenschluss aus über 600.000 IT-Sicherheitsexperten und führenden Technologieanbietern, die sich für intelligente Lösungsansätze und effektive Zusammenarbeit zur Bewältigung akuter Cybersicherheitsrisiken engagieren.

Den Schwerpunkt unserer Arbeit bildet die Erstellung und Bereitstellung sorgfältig ausgewählter Inhalte, die über aktuelle Trends, Lösungen und Best-Practice-Empfehlungen rund um das Thema Cybersicherheit informieren sollen. Wir sind bestrebt, Ressourcen bereitzustellen, die evidenzbasierte Antworten auf die komplexen Herausforderungen von heute liefern. Unser Angebot umfasst Forschungsstudien und unabhängige Produktbewertungen ebenso wie praxisbezogene E-Guides, Webinare und Textbeiträge.

Kontaktieren Sie uns noch heute, um zu erfahren, wie Cybersecurity Insiders Ihre Organisation bei der Stärkung von Nachfrage, Markenpräsenz und Innovationskraft unterstützen kann, um sich in einem wettbewerbsintensiven Markt erfolgreich zu positionieren.

Senden Sie uns eine E-Mail an info@cybersecurity-insiders.com oder besuchen Sie cybersecurity-insiders.com.

Erleben Sie Ihre Welt, sicher.

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen überall vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist weltweit in 150 Rechenzentren verfügbar und ist somit die größte Inline-Cloud-Sicherheitsplattform der Welt. Weitere Informationen finden Sie unter **www.zscaler.de**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA

zscaler.de