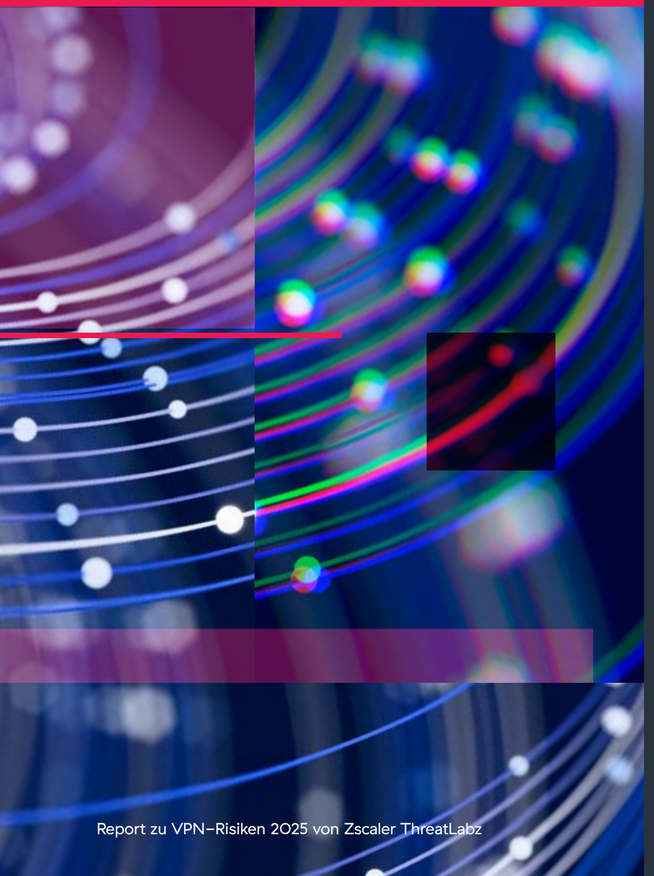
Cybersecurity INSIDERS

Zscaler ThreatLabz-Report zu VPN-Risiken 2025

Inhaltsverzeichnis



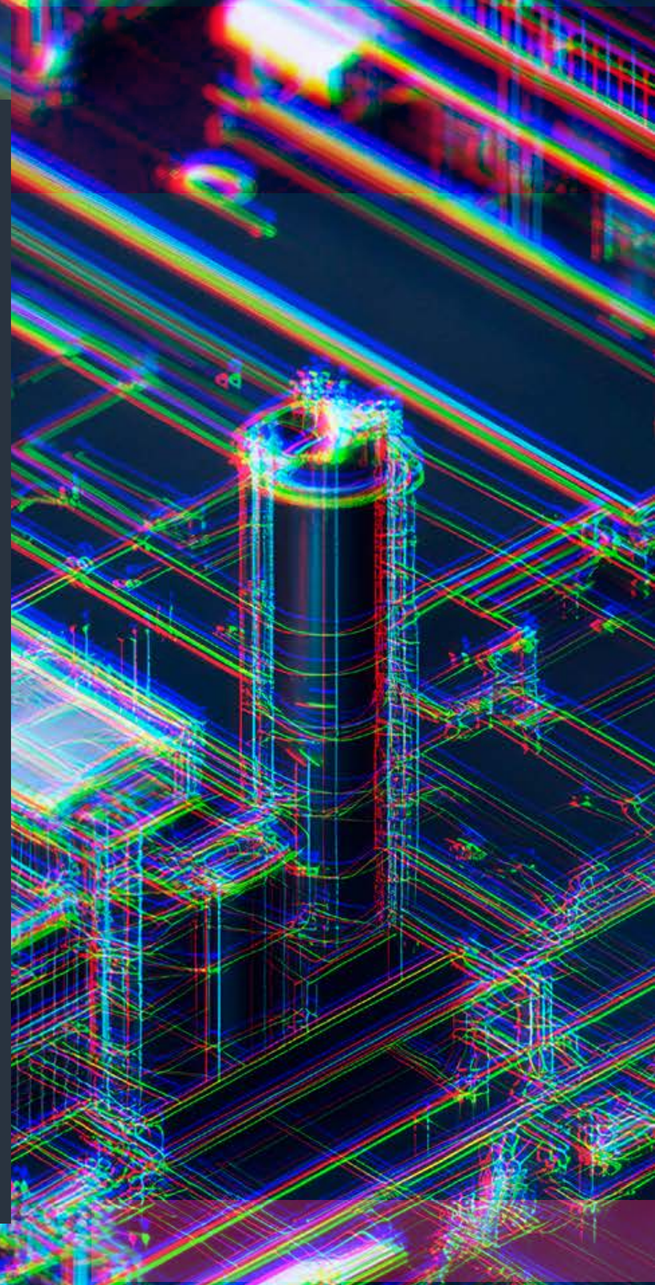
Kurzfassung

Der Report von Zscaler ThreatLabz zu VPN-Risiken 2025 liefert einen detaillierten Einblick in die Entwicklung der Risiken virtueller privater Netzwerke (VPNs) und unterstreicht die dringende Notwendigkeit der Umstellung auf Zero-Trust-Architekturen zur Erfüllung gegenwärtiger und zukünftiger Sicherheitsanforderungen. Einst als Rückgrat des Remotezugriffs gepriesen, entwickeln sich VPNs zunehmend zu Brennpunkten für Cyberbedrohungen und wandeln sich von unverzichtbaren Tools zu erheblichen Sicherheitsrisiken für Unternehmen weltweit. Dieser Bericht, der die Erkenntnisse aus einer Umfrage unter über 600 IT- und Sicherheitsexperten berücksichtigt, zeigt einen kritischen Wendepunkt in der Cybersicherheitslage auf: **Mehr als die Hälfte der befragten Unternehmen war allein im vergangenen Jahr von Angriffen aufgrund von VPN-Schwachstellen betroffen.** Dies unterstreicht die dringende Notwendigkeit eines neuen Ansatzes in den zunehmend hybriden Arbeitsumgebungen von heute.

Im Jahr 2025 hat die Unzufriedenheit mit herkömmlichen VPNs einen Wandel ausgelöst. Unternehmen erkennen zunehmend, dass die Behebung dieser Schwachstellen nicht länger praktikabel ist. Diese Erkenntnis treibt die Umstellung auf Zero-Trust-Modelle voran, die eine granulare Zugriffskontrolle versprechen und Sicherheitsrisiken deutlich reduzieren. **81 % der Unternehmen planen derzeit die Implementierung von Zero-Trust-Strategien bis 2026, wobei 65 % planen, VPNs im gleichen Zeitraum vollständig abzuschaffen.** Darüber hinaus haben betriebliche Probleme wie langsame Verbindungen, häufige Verbindungsabbrüche und komplexe Authentifizierungsprozesse die Dringlichkeit noch verstärkt und die Nachfrage nach Zero-Trust-Lösungen, die einen nahtlosen und sicheren Zugriff gewährleisten, stark ansteigen lassen.

Alle diese Veränderungen finden im Kontext der zunehmenden Risiken aufgrund KI-gestützter Bedrohungen statt. Tatsächlich wird die Zunahme KI-gesteuerter Cyberangriffe die VPN-Sicherheit in beispielloser Weise beeinträchtigen. Angreifer werden KI zunehmend zur automatischen Aufklärung von VPN-Schwachstellen nutzen, die über das öffentliche Internet problemlos gescannt werden können. Techniken wie intelligentes Password Spraying und die schnelle Entwicklung von Exploits ermöglichen es Bedrohungsakteuren, VPN-Anmeldedaten in größerem Umfang zu kompromittieren. Ganz am Anfang der Angriffskette wird es durch KI-gestützte Umgehungstechniken noch schwieriger, unbefugte Zugriffe über VPNs zu erkennen, bevor sie erheblichen Schaden anrichten können. Mit der Zunahme solcher KI-gesteuerten Bedrohungen werden sich auch die VPN-Risiken weiter verschärfen. Dies zwingt Unternehmen dazu, proaktive Sicherheitsmaßnahmen zu ergreifen, und beschleunigt den bereits deutlich ausgeprägten Wandel hin zur Umstellung auf Zero-Trust-Lösungen.

Der ThreatLabz-Report trägt diesen Veränderungen Rechnung und zeigt nicht nur den Niedergang von VPNs vom unverzichtbaren Tool zur untragbaren Belastung auf, sondern liefert auch umsetzbare Erkenntnisse für Unternehmen, die sich in diesem dynamischen Wandel zurechtfinden müssen.



Die wichtigsten Ergebnisse im Überblick

1. **Immer mehr Unternehmen vollziehen den Wandel weg von VPNs:**

   Bemerkenswerte 65 % der Unternehmen wollen ihre VPN-Services im nächsten Jahr ersetzen, was einem Anstieg von 23 % gegenüber 2024 entspricht. Dieser Trend ist vor allem darauf zurückzuführen, dass VPNs die Sicherheits- und Compliance-Anforderungen heutiger Unternehmen nicht erfüllen können: Statt Risiken zu mindern, verschärfen sie sie noch.

2. **Zunehmende Bedenken hinsichtlich des Missbrauchs von VPNs für Cyberangriffe und Ransomware:**

   Im vergangenen Jahr kam es zu einem besorgniserregenden Anstieg der Cyber-Vorfälle, die auf VPN-Schwachstellen zurückzuführen sind. 56 % der Unternehmen meldeten derartige Sicherheitsverstöße — ein alarmierender Anstieg im Vergleich zu früheren Zahlen. Gleichzeitig befürchten 92 % der Befragten, dass ungepatchte VPN-Schwachstellen direkt zu Ransomware-Angriffen führen könnten. Diese Erkenntnisse untermauern den Trend, dass Unternehmen, die mit der schnellen Behebung von Schwachstellen zu kämpfen haben, eine umfassende Überholung ihrer Sicherheitsmaßnahmen benötigen, um diese kritischen Sicherheitslücken zu schließen und die allgegenwärtigen Risiken der VPN-Ausnutzung zu mindern.

3. **Unzufriedenheit der Enduser beeinflusst die Umstrukturierung von Sicherheitsarchitekturen:**

   Die Frustration der User über Ineffizienzen bei VPNs — von langsamen Geschwindigkeiten bis hin zu umständlicher, komplexer oder fehlerhafter Authentifizierung — beeinflusst zunehmend die Unternehmensstrategien. Diese Unzufriedenheit der Enduser forciert die Umstellung auf Zero-Trust-Architekturen, die einen unterbrechungsfreien, sicheren Zugriff ohne die herkömmlichen Probleme bieten, die mit VPNs verbunden sind.

4. **Umstieg von VPNs auf Zero Trust — vom Konzept zur Umsetzung:**

   81 % der Unternehmen arbeiten aktiv daran, im nächsten Jahr Zero-Trust-Frameworks zu implementieren. Diese Zahl spiegelt einen signifikanten strategischen Wandel wider. Zudem markiert sie einen entscheidenden Übergang von der Betrachtung von Zero Trust als theoretisches Ideal hin zur Erkenntnis, dass es eine praktische Notwendigkeit ist, VPNs zu ersetzen und gleichzeitig die Sicherheit in dynamischen und verteilten IT-Umgebungen zu verbessern.

VPN-Risiken: Warum 81 % der Unternehmen bis 2026 auf Zero Trust umstellen wollen

VPNs wurden ursprünglich für den Remotezugriff entwickelt, doch die Zeiten haben sich geändert — und mit ihnen auch die Angreifer. Heutzutage dienen VPNs oft als Einstiegspunkte für Ransomware-Angriffe, Anmeldedatendiebstahl und Cyberspionage. Grund dafür sind Schwachstellen, die sich nur schwer schnell schließen lassen, implizite Vertrauensmodelle, die vollständigen Netzwerkzugriff ermöglichen, und weitreichende Zugriffsberechtigungen. Insgesamt sind Sicherheitslücken die größte VPN-bezogene Herausforderung für Unternehmen (laut 54 % der Befragten). Dies unterstreicht die Tatsache, dass Angreifer regelmäßig ungepatchte Schwachstellen ausnutzen oder Schutzmaßnahmen umgehen, um in Netzwerke einzudringen.

Die Risiken werden durch den VPN-Zugriff Dritter noch größer. 93 % der Befragten äußern Bedenken hinsichtlich Backdoor-Schwachstellen, die durch externe VPN-Verbindungen entstehen, da Angreifer zunehmend Anmeldedaten von Drittusern ausnutzen, um unbemerkt in Netzwerke einzudringen. Dabei geht es nicht nur um den Erstzugriff — vielmehr erhöhen VPNs auch das Schadenspotenzial von Angriffen. Im Gegensatz zu Zero-Trust-Lösungen, die granulare Richtlinien zur Verhinderung von Bewegungen innerhalb von Netzwerken durchsetzen, bieten VPNs einen breiten Zugriff, der es Angreifern ermöglicht, sich lateral auszubreiten und ihre Berechtigungen zu erweitern. Insgesamt sehen 71 % der Befragten laterale Bewegungen als Hauptproblem an und sind sich bewusst, dass sie den Umfang und die Auswirkungen eines Angriffs verstärken.

Diese Herausforderungen, kombiniert mit alltäglichen Problemen wie langsamer Leistung, komplexer Authentifizierung und häufigen Verbindungsabbrüchen, machen deutlich, warum Unternehmen von VPNs auf Zero-Trust-Modelle umsteigen. Der Report zu VPN-Risiken 2025 basiert auf den Erkenntnissen aus einer Umfrage unter 632 IT- und Cybersicherheitsexperten und soll Aufschluss über den Stand der VPN-Nutzung im Jahr 2025 geben, um Risiken und Herausforderungen besser zu verstehen und Unternehmen Best-Practice-Anleitungen zur Verbesserung ihrer Cybersicherheitslage und ihres Ansatzes für sicheren Remotezugriff zu bieten.

Die Ergebnisse dieses Berichts liefern IT- und Sicherheitsverantwortlichen datengestützte Einblicke und überzeugende Argumente für die Umstellung von veralteten VPNs auf eine zukunftsfähige cloudbasierte Zero-Trust-Architektur. Der Wechsel vom impliziten Vertrauen zur kontinuierlichen Überprüfung ist nicht länger optional — er ist für die Sicherheit der heutigen verteilten Unternehmen, die Reduzierung der IT-Komplexität und die Gewährleistung einer nahtlosen User Experience unerlässlich.

Bedenken hinsichtlich der Sicherheit von VPNs

Sicherheitsrisiken und frustrierte User

Unternehmen, die weiterhin auf VPNs für den Remotezugriff setzen, sehen sich zunehmend Sicherheitslücken, Betriebsineffizienzen und wachsender Unzufriedenheit der Enduser ausgesetzt. Damit setzt sich zunehmend die Erkenntnis durch, dass VPNs einer vergangenen Ära der Zugriffssicherheit angehören.

Die größte Herausforderung — Sicherheits- und Compliance-Risiken, die von 54 % der Befragten genannt wurden — verstärkt die kritische Anfälligkeit von VPNs gegenüber Ransomware, Rechteerweiterung und lateralen Angriffsbewegungen. Angreifer betrachten VPNs als Schwachstellen, die leicht ausgenutzt werden können, während Unternehmen Schwierigkeiten haben, diese veralteten Systeme schnell genug zu patchen, um mit komplexen Bedrohungen Schritt zu halten.

51 % der Befragten geben an, dass eine schlechte VPN-Performance — bedingt durch Faktoren wie träge Konnektivität, Verbindungsabbrüche und umständliche Authentifizierungsprotokolle — ein Produktivitätshemmnis darstellt. VPNs stellen weiterhin eine betriebliche Belastung dar: 41 % der Umfrageteilnehmer sprachen von Schwierigkeiten bei der Verwaltung und 37 % von hohen Kosten für die fortlaufende Wartung. Diese Zahlen veranschaulichen, wie ressourcenintensiv VPNs geworden sind, wie sehr sie die IT-Budgets belasten und die Teams dazu zwingen, unnötig viel Zeit mit Aufgaben zur Fehlerbehebung zu verschwenden.

Vorteile von Zero Trust als effektivere Alternative zu Legacy-Ansätzen

Eine kürzlich erfolgte Sicherheitsverletzung zeigt die Schwachstellen von VPNs deutlich auf. Im Januar 2025 nutzte eine chinesische Cyberspionagegruppe erfolgreich eine Zero-Day-Schwachstelle in Ivantis Pulse Secure VPN aus und verschaffte sich so unbefugten Zugriff auf Unternehmensnetzwerke. Dieser Angriff, einer von mehreren Angriffen auf VPN-Technologie in den letzten Monaten, verdeutlicht, warum Unternehmen es sich nicht länger leisten können, zum Schutz ihrer Infrastrukturen auf Legacy-Zugriffsmodelle zu vertrauen.

Angesichts dieser Herausforderungen haben zahlreiche Anbieter von Legacy-VPNs damit begonnen, aus der Cloud bereitgestellte virtuelle Maschinen als Zero-Trust-Lösungen zu vermarkten. Aus architektonischer Sicht weisen in der Cloud gehostete VPN-Services

Die Beseitigung von VPN-Abhängigkeiten ist kein optionales Upgrade mehr, sondern eine dringende Notwendigkeit. Unternehmen müssen auf echte Zero-Trust-Frameworks umsteigen, die identitätsgesteuerten Zugriff nach dem Prinzip der minimalen Rechtevergabe sowie granulare Segmentierung ermöglichen. Diese aus der Cloud bereitgestellten Architekturen tragen dazu bei, laterale Angriffsflächen zu reduzieren, die User Experience zu verbessern und die IT-Komplexität zu verringern — eine Kombination aus drei Vorteilen, die VPNs einfach nicht gewährleisten können.

Was sind Ihrer Meinung nach die größten Herausforderungen bei Ihren VPN-Lösungen?

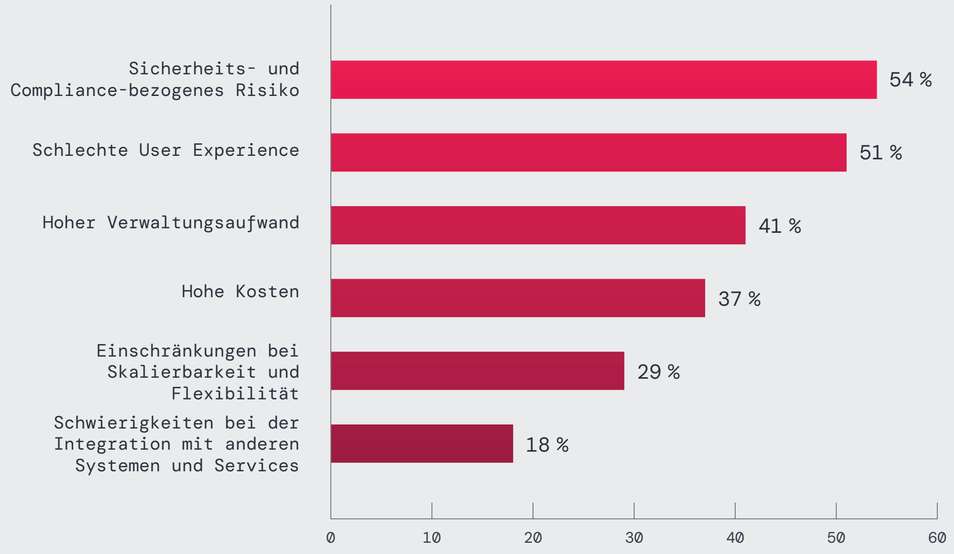


Abb. 1: Die größten Herausforderungen bei VPN-Lösungen.

jedoch grundsätzlich die gleichen Merkmale auf wie herkömmliche VPNs: Es handelt sich um mit dem Internet verbundene Services mit einer öffentlichen IP-Adresse, die kompromittiert werden kann. Ein typisches Beispiel: In der Branche kam es kürzlich zu massiven Spitzen bei der Scan-Aktivität, die auf über zwanzigtausend öffentliche VPN-IP-Adressen abzielte, die von einem der größten Sicherheitsanbieter gehostet werden. In früheren Fällen deuteten derartige Aktivitäten darauf hin, dass Angreifer möglicherweise die Ausnutzung noch nicht bekannt gegebener Schwachstellen in gezielten VPN-Ressourcen vorbereiten. Mit anderen Worten: Was erreichbar ist, kann angegriffen werden. Aus diesem Grund kann cloudbasierte VPN-Technologie aus architektonischer Sicht niemals echten Zero-Trust-Grundsätzen entsprechen.

Ransomware und VPNs: Zusammentreffen mehrerer Risikofaktoren

Ransomware-Gruppen nutzen weiterhin mit verheerender Präzision Schwachstellen in VPNs aus — sowohl Zero-Day-Schwachstellen als auch bereits bekannte Schwachstellen —, bevor Unternehmen Sicherheitspatches bereitstellen können. Aufgrund ihrer weiten Verbreitung und der Abhängigkeit von veralteten Modellen des impliziten Vertrauens innerhalb von Netzwerken werden VPNs von Angreifern als leichte Beute wahrgenommen.

Insgesamt äußerten 92 % der Umfrageteilnehmer große Besorgnis darüber, dass Ransomware auf ungepatchte VPN-Schwachstellen abzielt, was die dringende Notwendigkeit robusterer Schutzmechanismen unterstreicht. Diese Daten verdeutlichen, warum VPNs heute eher als Belastung denn als zuverlässiges Instrument zur Minderung moderner Cyberrisiken angesehen werden.

Beispiele aus der Praxis bestätigen diese Befürchtungen immer wieder. Im Januar 2023 wurden mehrere US-Unternehmen aus dem Gesundheitsbereich Opfer eines Ransomware-Angriffs, der durch eine ungepatchte Sicherheitslücke in Citrix NetScaler (CVE-2023-4966) begünstigt wurde. Durch diesen Exploit konnten Angreifer in Systeme eindringen, den Krankenhausbetrieb stören, Krankenakten sperren und Einrichtungen zwingen, kritische Notfallversorgung umzuleiten — nur weil die Sicherheitslücke nicht rechtzeitig geschlossen wurde. Dieser Vorfall unterstreicht das allgegenwärtige Risiko, das von ungepatchten VPNs ausgeht. Bedrohungsakteure suchen regelmäßig nach gefährdeten Systemen, um Schwachstellen auszunutzen, bevor Unternehmen Korrekturen anwenden. Dadurch sind Unternehmen dem Risiko von Kompromittierungen, Betriebsstörungen und finanziellen Verlusten ausgesetzt.

Unternehmen müssen aus der endlosen Tretmühle des Patchens aussteigen und proaktive Abwehrstrategien entwickeln, die auf neu auftretende Bedrohungen zugeschnitten sind. Zero-Trust-Frameworks priorisieren identitätsbasierte Zugriffskontrolle und kontinuierliche Überprüfung und sorgen so für eine deutliche Reduzierung des Ransomware-Risikos — selbst wenn Schwachstellen nicht behoben werden. Automatisierte Erkennungssysteme und dynamische Richtlinien dämmen potenzielle Sicherheitslücken zusätzlich ein und verhindern, dass Angreifer sich lateral durchs Netzwerk bewegen oder ihre Berechtigungen erweitern.

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

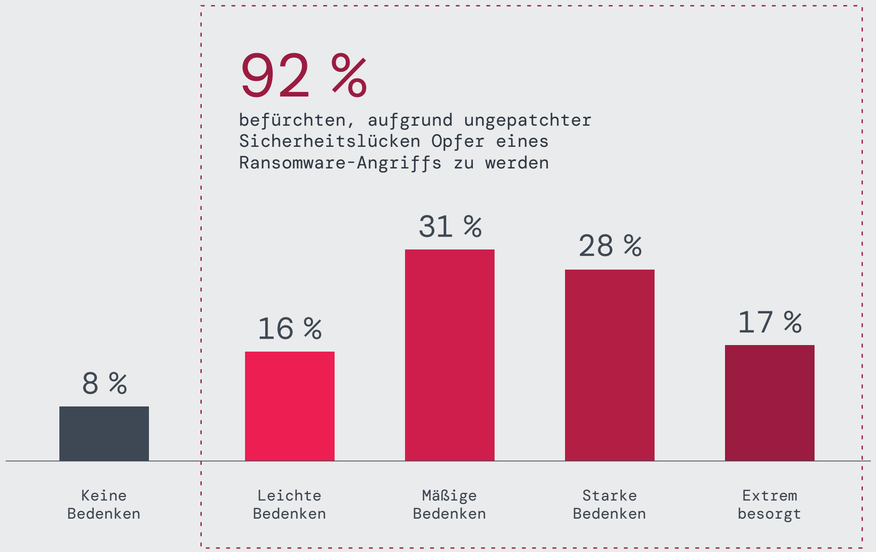


Abb. 2: Bedenken hinsichtlich Ransomware-Angriffen.

Laterale Bewegungsfreiheit in VPNs: Vermehrtes Schadenspotenzial bei Sicherheitsverstößen

VPNs ermöglichen nicht nur eine anfängliche Kompromittierung durch Ransomware und andere Bedrohungen, sondern erleichtern auch ihre laterale Ausbreitung — eine gefährliche Angriffstechnik. Angreifer nutzen den umfassenden Zugriff, den VPNs gewährleisten, um ihre Rechte zu erweitern und tiefer in die Zielnetzwerke einzudringen, was oft verheerende Folgen hat.

Insgesamt 71 % der Befragten äußerten ein gewisses Maß an Besorgnis hinsichtlich dieses Risikos, 32 % ein hohes Maß an Besorgnis. Diese Befürchtungen sind berechtigt, da VPNs typischerweise einen umfassenden Netzwerkzugriff gewähren und Angreifern dadurch ermöglichen, sich unentdeckt zu bewegen, ihre Berechtigungen zu erweitern und nach dem unbefugten Zugriff vertrauliche Daten abzugreifen.

Im September 2024 nutzten Angreifer mehrere Zero-Day-Schwachstellen in Ivantis Cloud Service Appliance (CSA), insbesondere CVE-2024-8963 und CVE-2024-8190, um sich unbefugten Zugriff auf die Netzwerke mehrerer Unternehmen zu verschaffen, wie die Cybersecurity and Infrastructure Security Agency (CISA) und das FBI bestätigten.

Angreifer umgingen administrative Kontrollen, führten willkürliche Befehle aus, erfassten Anmeldedaten und implantierten Web-Shells, um netzwerkübergreifend laterale Bewegungen zu ermöglichen. Trotz früherer Sicherheitsvorfälle mit Ivanti VPNs zeigen diese neuen Exploits, dass die grundlegenden Sicherheitsmängel netzwerkbasierter Remote-Access-Modelle auch durch Patchen oder Neustrukturieren von Legacy-VPN-Lösungen nicht behoben werden können.

Wie groß ist Ihre Sorge, dass Angreifer sich lateral in Ihrem Netzwerk bewegen, wenn ein VPN kompromittiert ist?

89 % sehen laterale Bewegungen als akute Bedrohung an

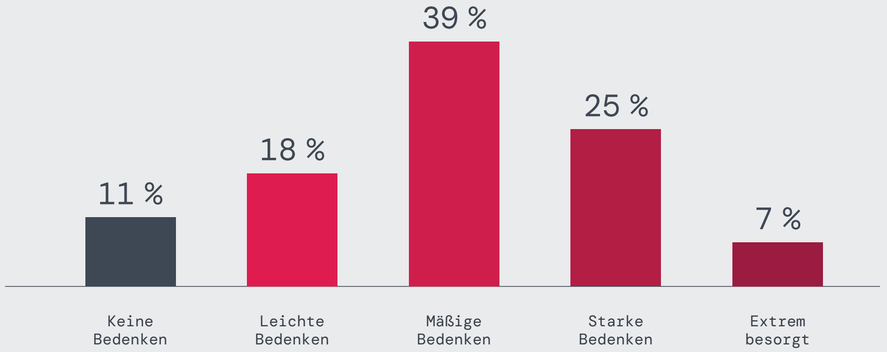


Abb. 3: Unternehmen befürchten, dass sich Bedrohungen durch Kompromittierung von VPNs lateral im Netzwerk ausbreiten.

Um diese Risiken zu mindern, müssen Unternehmen vom VPN-basierten Zugriff auf Zero Trust Network Access (ZTNA) mit strenger Segmentierung umsteigen. Im Gegensatz zu VPNs, die Usern umfassenden Netzwerkzugriff gewähren, ermöglicht ZTNA Einzelverbindungen auf Anwendungsebene basierend auf Identität und Kontext und stellt sicher, dass User nur auf die spezifischen Ressourcen zugreifen können, die sie benötigen. Dieser Ansatz verhindert laterale Bewegungen, selbst wenn es Angreifern gelingt, sich unbefugten Zugriff auf Anwendungen zu verschaffen, und reduziert so die Angriffsfläche und das Schadenspotenzial von Sicherheitsverstößen drastisch. Darüber hinaus erhöht die Implementierung von Netzwerk- und Mikrosegmentierung die Sicherheit, indem kritische Systeme isoliert und unbefugte Kommunikation zwischen kompromittierten und sicheren Assets verhindert werden.

VPN-CVEs von 2020 bis 2025: Signifikante Zunahme schwerwiegender Sicherheitslücken

Keine Software ist vor Sicherheitslücken gefeit. Bei VPN-Technologie können Schwachstellen, insbesondere Zero-Day-Bedrohungen, jedoch besonders schädlich sein, da Angreifer leicht nach betroffenen VPN-Infrastrukturen suchen und diese ausnutzen können, bevor ein Patch veröffentlicht oder installiert wurde. Die Meldung von CVEs ist sinnvoll, da diese gemeinschaftsweite Initiative Anbietern und Kunden hilft, Best Practices zu befolgen und ihre Cybersicherheitsmaßnahmen durch Patches und Offenlegung zu verbessern. Daran, wie diese CVEs entdeckt werden und welche Informationen sie enthalten, zeigen sich die Veränderungen der Bedrohungslage.

Zscaler ThreatLabz analysierte 411 VPN-bezogene Common Vulnerabilities and Exposures (CVEs) aus den Jahren 2020 bis 2025, die vom MITRE CVE-Programm gemeldet wurden. Die Ergebnisse deuten auf einen plötzlichen Anstieg der VPN-Schwachstellen hin, nachdem sie in der ersten Hälfte dieses Jahrzehnts stetig zugenommen hatten. Diese CVEs decken ein breites Spektrum an VPN-Fehlern ab — von der Ausnutzung webbasierter Verwaltungsschnittstellen über Schwachstellen bei der Befehlsinjektion und Eingabevalidierung bis hin zu kryptografischen Fehlern und DoS- und DDoS-Angriffen. Es gibt in letzter Zeit zahlreiche VPN-Sicherheitslücken, von denen viele zu schwerwiegenden Sicherheitsverstößen mit hoher Medienaufmerksamkeit geführt haben.

Viele dieser CVEs sind kritisch. Im Jahr 2024 wiesen beispielsweise 60 % der 83 vom NIST gemeldeten VPN-Schwachstellen einen hohen oder kritischen CVSS-Score auf. Die häufigsten VPN-bezogenen CVEs waren RCE-Schwachstellen (Remote Code Execution), die Angreifern die Ausführung willkürlicher Befehle und damit potenziell die Kompromittierung des Systems ermöglichen. Anders ausgedrückt: Die Mehrzahl der VPN-CVEs im vergangenen Jahr machte User extrem anfällig für Exploits, die Angreifer relativ einfach ausnutzen konnten. Darüber hinaus handelte es sich bei vielen dieser CVEs um Zero-Day-Exploits. Zu Beginn des Jahres 2025 wurden bereits einige schwerwiegende Schwachstellen bekannt, darunter zwei Zero-Day-Exploits, CVE-2025-0282 und CVE-2025-0283.

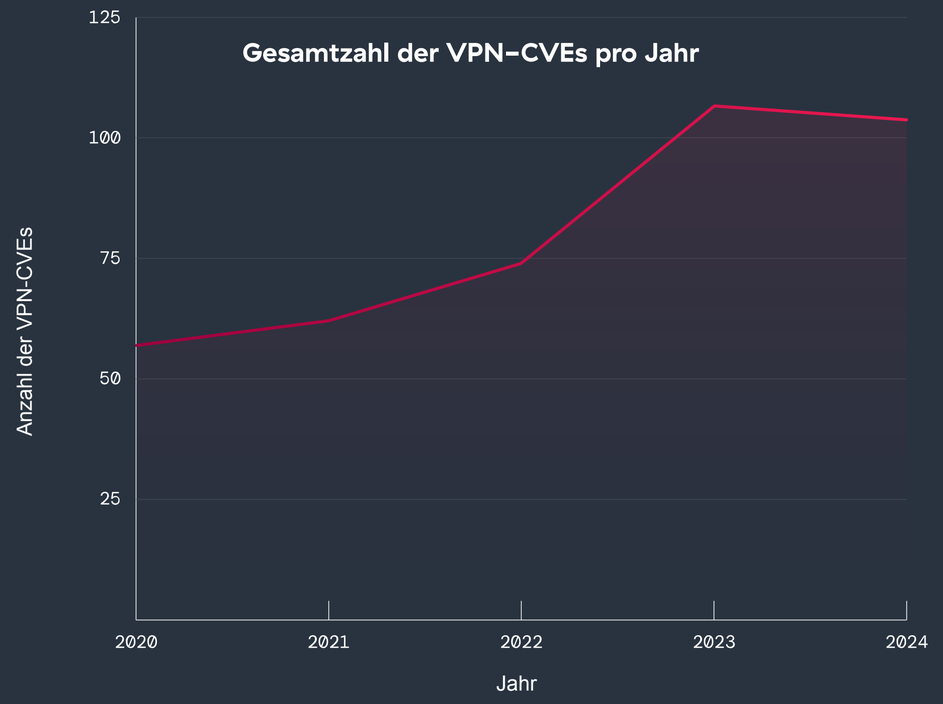


Abb. 4: Gesamtzahl der VPN-CVEs für jedes Jahr von 2020 bis 2024.

1. RCE bleibt die größte Bedrohung

- **Beobachtung:** RCE-Schwachstellen stehen in den vier Jahren des Beobachtungszeitraums an der Spitze der Liste, allein im Jahr 2024 waren es 32. Unter Mitberücksichtigung der Daten für 2025 entfallen auf RCE insgesamt 149 CVEs, damit sind sie der häufigste und kritischste Schwachstellentyp.
- **Folge:** RCE-Schwachstellen ermöglichen Angreifern die Ausführung willkürlicher Befehle auf VPN-Geräten, was möglicherweise zu einer vollständigen Systemkompromittierung führen kann. Unternehmen sollten dem Patchen und Schutz anfälliger Systeme Priorität einräumen.

2. Die Rechteerweiterung nimmt mit der Zeit stetig zu

- **Beobachtung:** Es wurde ein stetiger Anstieg von CVEs zur Rechteerweiterung beobachtet (66,7 %), der seinen Höhepunkt im Jahr 2024 mit 20 Schwachstellen erreichte.
- **Auswirkungen:** Angreifer nutzen zunehmend VPN-Schwachstellen aus, um ihre Rechte zu erweitern und so die administrative Kontrolle über Systeme zu erlangen. Unternehmen müssen sichere Systemkonfigurationen gewährleisten und den berechtigungsbasierten Zugriff streng einschränken.

3. DoS-Schwachstellen (Denial-of-Service) verzeichnen einen starken Anstieg um 200 %

- **Beobachtung:** DoS-bezogene CVEs haben sich von 9 im Jahr 2020 auf 27 im Jahr 2024 verdreifacht und sind damit in den letzten Jahren zum zweithäufigsten Typ geworden— unter Mitberücksichtigung der bisher vorliegenden Daten für 2025 wurden insgesamt 85 CVEs gemeldet.
- **Folge:** DoS-Angriffe werden immer raffinierter, was VPN-Systeme zu einem bevorzugten Ziel für Betriebsstörungen macht. Unternehmen sollten Geschwindigkeitsbegrenzung und Traffic Shaping einsetzen, um diese Risiken zu minimieren.

4. Verluste vertraulicher Daten sind seltener, aber dennoch kritisch

- **Beobachtung:** Schwachstellen, die zum Verlust vertraulicher Daten führen, sind mit insgesamt 41 CVEs vergleichsweise selten. Die Offenlegung unternehmenskritischer Anmeldedaten, Verschlüsselungscodes und Userdaten stellt jedoch ein beträchtliches Risiko dar.
- **Folge:** Diese Auswirkung ist besonders schädlich für Vertraulichkeit und Compliance. Unternehmen sollten robuste Verschlüsselung, sichere Codierungspraktiken und Trafficüberwachung implementieren, um Datenverlusten durch frühzeitge Erkennung vorzubeugen.

5. Stetiges Wachstum bei Sicherheitslücken zur Umgehung der Authentifizierung

- **Beobachtung:** Die Zahl der Fälle, bei denen es zu einer Umgehung der Authentifizierung kam, war relativ gering, blieb aber konstant. Sie stieg von 4 im Jahr 2020 auf einen Höchstwert von 6 im Jahr 2023 und fiel 2024 wieder auf 4 — insgesamt kam es zu 30 CVEs während des Beobachtungszeitraums.
- **Auswirkungen:** Angreifer nutzen Schwachstellen in der Multi-Faktor-Authentifizierung (MFA) und der Anmeldelogik, um sich als User auszugeben. Unternehmen sollten ihre MFA-Konfigurationen verstärken und auf ungewöhnliches Anmeldeverhalten achten.

Wichtige Trends: CVEs mit verschiedenen Auswirkungen

Um den potenziellen Schaden zu analysieren, den diese Schwachstellen im Falle ihrer Ausnutzung anrichten könnten, hat ThreatLabz VPN-CVEs anhand von fünf Angriffskategorien bewertet: Remote Code Execution (RCE), Rechteerweiterung, Informationslecks, Denial of Service (DoS) und Umgehung der Authentifizierung. Dabei ist zu beachten, dass es sich bei einigen Kategorien um Sammelgruppierungen für separate, aber eng miteinander verbundene Angriffsarten handelt: Beispielsweise umfasst die Umgehung der Authentifizierung sowohl Angriffe, die möglicherweise die Zwei-Faktor- oder Multi-Faktor-Authentifizierung (MFA) umgehen, als auch Angriff unter Umgehung einfacher Authentifizierungsmaßnahmen. Im Allgemeinen hat die Behebung von RCE-Sicherheitslücken für jedes Unternehmen höchste Priorität.

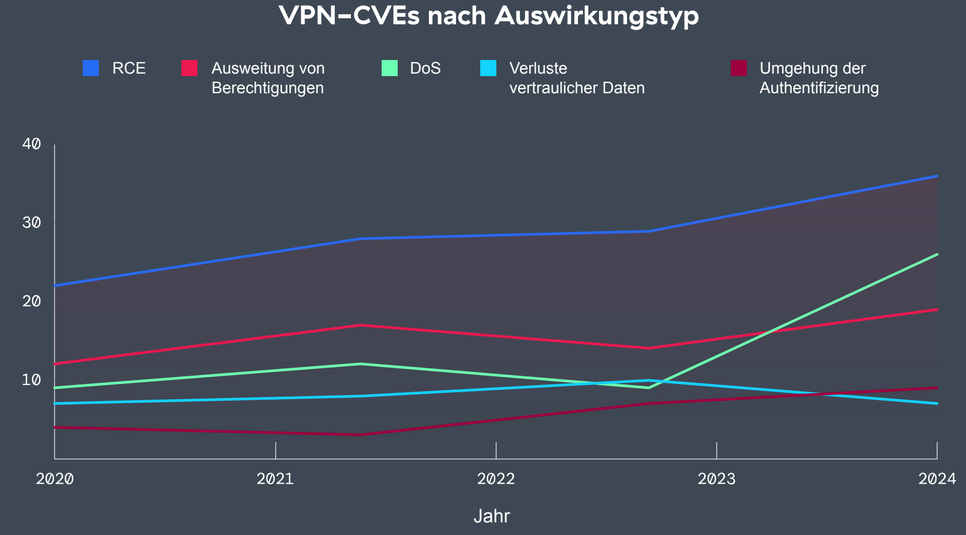


Abb. 5: VPN-CVEs mit unterschiedlichen Auswirkungen von 2020 bis 2024, einschließlich RCE, Rechteerweiterung, DoS, Verluste vertraulicher Daten und Umgehung der Authentifizierung.

Wichtige Trends: Kritische VPN-Schwachstellen

Neben den Auswirkungen analysierte ThreatLabz auch den Schweregrad von VPN-CVEs im Jahresvergleich. **Insgesamt stellte ThreatLabz fest, dass die CVEs mit CVSS-Werten von HOCH oder KRITISCH von 2020 bis 2024 um 38,9 % zunahmen.** Insgesamt wurden 66,3 % aller CVEs im Jahr 2024 als HOCH oder KRITISCH eingestuft, was auf potenziell schwerwiegende Auswirkungen für Unternehmen hindeutet, wenn solche CVEs ausgenutzt werden, bevor sie gepatcht werden. Darüber hinaus analysierte ThreatLabz kritische Trends bei verschiedenen Arten von Schwachstellen in den CVE-Daten, die Unternehmen kennen sollten, um sich besser vor neu auftretenden VPN-Bedrohungen zu schützen.

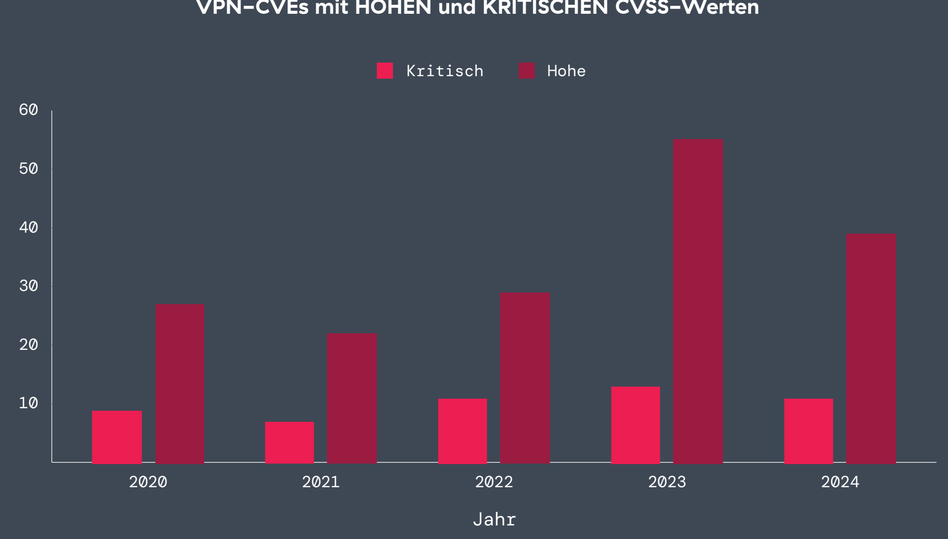


Abb. 6: Die Anzahl der VPN-CVEs mit HOHEN und KRITISCHEN CVSS-Werten von 2020-2024.

1. Zunehmende Nutzung webbasierter Verwaltungsschnittstellen

- **Trend:** Schwachstellen bei der Befehlseingabe und Eingabevalidierung nehmen stetig zu. Dies deutet darauf hin, dass Angreifer zunehmend Verwaltungs- und Managementportale ins Visier nehmen. Da diese Schnittstellen aufgrund ihrer Architektur im Internet exponiert sind, sind sie anfällig für Angriffe durch Cyberkriminelle.
- **Eskalation:** Diese Schwachstellen waren bereits in den Jahren 2020—2021 vorhanden, ab 2022 verstärkten sie sich jedoch deutlich. Dies lässt darauf schließen, dass Angreifer diese Verwaltungsschnittstellen als attraktive und leicht zugängliche Ziele betrachten, insbesondere aufgrund unzureichender Sicherheitscodierungspraktiken.

2. Weit verbreitete Authentifizierungs- und MFA-Umgehungen

- **Trend:** Angriffe, die speziell auf Authentifizierungsmethoden abzielen — insbesondere MFA-Umgehungen, Session-Hijacking und unsachgemäße Sitzungsverwaltung —, nehmen stetig zu.
- **Eskalation:** In den Jahren 2020—2021 kam es vor allem zu weniger komplexen Umgehungen der Authentifizierung, die sich 2023—2025 zu raffinierteren, automatisierten und persistenten Angriffen entwickelten, die explizit auf MFA-Schwachstellen abzielten und auf die Absicht der Angreifer hindeuteten, stärkere Sicherheitsmaßnahmen zu untergraben.

3. Zunahme von Exploits durch lokale Rechteerweiterung

- **Trend:** Schwachstellen, die eine Erweiterung der lokalen Zugriffsberechtigungen ermöglichen, treten immer häufiger auf und werden zunehmend schwerwiegender.
- **Eskalation:** Was 2020—2021 mit geringfügigen Konfigurationsfehlern begann, intensivierte sich bis 2024—2025 zu ausgefeilteren Methoden zur Rechteerweiterung, wie etwa DLL-Hijacking, wodurch Angreifer sich umfassenden Zugriff auf Systemebene verschafften.

4. Zunehmende Raffinesse von DoS- und DDoS-Angriffen

- **Trend:** DoS-Angriffe haben sich von der einfachen Erschöpfung der Ressourcen (2020—2021) zu ausgeklügelten DDoS-Verstärkungstechniken (2024—2025) entwickelt.
- **Eskalation:** Die Angreifer gingen von einfachen Störungen auf Basis fehlerhafter Pakete zu komplexeren, verstärkten Angriffen über, was eine strategische Eskalation zur Maximierung der Betriebsstörungen darstellt.

5. Anhaltende und verstärkte kryptografische Fehler

- **Trend:** Probleme im Zusammenhang mit der kryptografischen Implementierung — wie etwa unsachgemäße Zertifikatsvalidierung, offengelegte Schlüssel und unzureichende TLS-Verifizierung — haben deutlich zugenommen.
- **Eskalation:** Ab etwa 2022 kam es zu einem deutlichen Anstieg kryptografischer Schwachstellen, der 2024—2025 mit schwerwiegenden Fehlern seinen Höhepunkt erreichte. Dieser Anstieg zeigt das strategische Interesse der Angreifer, verschlüsselungsbezogene Schwachstellen auszunutzen, um die Vertraulichkeit von VPNs zu untergraben.

Bedenken hinsichtlich der Sicherheit von VPNs (Forts.)

Schwierigkeiten beim Implementieren von Segmentierung

Angesichts der Risiken lateraler Bewegung versuchen viele Unternehmen, die Ausbreitung von Angriffen durch Segmentierung einzuschränken. Obwohl die Segmentierung ein wichtiger Abwehrmechanismus zur Minimierung der Angriffsfläche ist, stellt ihre Umsetzung oft eine Herausforderung dar.

Die Umfrage unterstreicht diese Herausforderungen: 51 % der Unternehmen nennen komplexe Konfigurationen als potenzielles oder tatsächliches Problem. Darüber hinaus berichten 39 % von einem Mangel an Fachwissen und Ressourcen, während 24 % mit Performance-Engpässen zu kämpfen haben. Dies deutet darauf hin, dass Legacy-Netzwerkarchitekturen ungeeignet sind, um die granularen Zugriffskontrollen zu unterstützen, die für heutige IT-Umgebungen erforderlich sind.

Segmentierungsprobleme spielten beim Ransomware-Angriff auf MGM Resorts im Jahr 2023 eine wichtige Rolle. Die Angreifer verschafften sich durch Social Engineering zunächst Zugriff und konnten sich anschließend aufgrund unzureichender Segmentierung lateral im Netzwerk bewegen. Der Verstoß beeinträchtigte den Hotelbetrieb, Geldautomaten und Casino-Spielsysteme und kostete das Unternehmen schätzungsweise 100 Millionen USD Schadenersatz. Dieser Fall verdeutlicht, wie Angreifer durch mangelhafte Segmentierung in kritische Systeme eindringen und so die Auswirkungen eines Erstzugriffs verstärken können.

Um diese Herausforderungen zu bewältigen, sollten Unternehmen cloudbasierte, identitätsgesteuerte Segmentierungsmodelle implementieren, die die Richtliniendurchsetzung optimieren und den manuellen Aufwand reduzieren. Im Gegensatz zur herkömmlichen Netzwerksegmentierung, die auf komplexen Firewall-Regeln und VLAN-Konfigurationen basiert, ermöglicht ein Zero-Trust-Ansatz eine dynamische Segmentierung basierend auf Useridentität, Gerätestatus und Echtzeit-Risikobewertungen. Dadurch wird sichergestellt, dass nur autorisierte User auf bestimmte Anwendungen zugreifen können, während gleichzeitig die Sicherheit des gesamten Netzwerks gewährleistet bleibt.

Mit welchen Problemen wurde Ihr Unternehmen beim Implementieren der Segmentierung konfrontiert bzw. mit welchen Problemen haben Sie gerechnet?

Abb. 7: Die größten Herausforderungen für Unternehmen bei der Segmentierung.

VPNs erhöhen Cybersicherheitsrisiken bei Fusionen und Übernahmen

Neben den alltäglichen Sicherheitsherausforderungen stellen große IT-Übergänge — etwa infolge von Fusionen und Übernahmen — zusätzliche Risiken dar und vergrößern die Angriffsflächen. Bei diesen Übergängen werden häufig unterschiedliche Netzwerke, Anwendungen und Identitäten zusammengeführt, was zu übernommenen Schwachstellen, Fehlkonfigurationen und schwachen Sicherheitskontrollen führen kann.

Fast zwei Drittel (64 %) der Befragten äußerten sich besorgt über Cyberbedrohungen infolge von Fusionen und Übernahmen und waren sich der Sicherheitslücken bewusst, die bei IT-Integrationen entstehen.

Ein aktuelles Beispiel ist der Datendiebstahl bei Capita im Jahr 2023, bei dem Angreifer Sicherheitslücken nach einer Unternehmensübernahme ausnutzten und sich so unbefugten Zugriff auf vertrauliche Daten verschafften. Der Vorfall war auf eine mangelnde Abstimmung der Sicherheitsrichtlinien zwischen den fusionierten Unternehmen zurückzuführen, die es Bedrohungsakteuren ermöglichte, sich lateral im neu integrierten Netzwerk zu bewegen. Dieser Verstoß unterstreicht, wie inkonsistente Sicherheitskontrollen, veralteter VPN-Zugriff und unsegmentierte Umgebungen ideale Bedingungen für Cyberangriffe bei Fusionen und Übernahmen schaffen.

Um diese Risiken bei Fusionen und Übernahmen zu mindern, müssen Unternehmen der Sorgfaltspflicht in Bezug auf die Cybersicherheit Priorität einräumen, Zugriff nach dem Prinzip der minimalen Rechtevergabe durchsetzen und eine Segmentierung implementieren. Im Gegensatz zu VPN-basierten Zugriffsmodellen verhindert Zero Trust, dass in zusammengeführten IT-Umgebungen umfassende Zugriffsberechtigungen gelten, wodurch das Risiko lateraler Bewegungen und einer Rechteerweiterung effektiv verringert wird. Indem sie VPNs und perimeterbasierte Abwehrmaßnahmen durch identitätsgesteuerte Zugriffskontrollen ersetzen, die jede Anfrage validieren, können Unternehmen sowohl bisherige als auch neu integrierte IT-Umgebungen sichern.

Befürchten Sie eine erhöhte Anfälligkeit für Cyberangriffe infolge von Fusionen und Übernahmen?

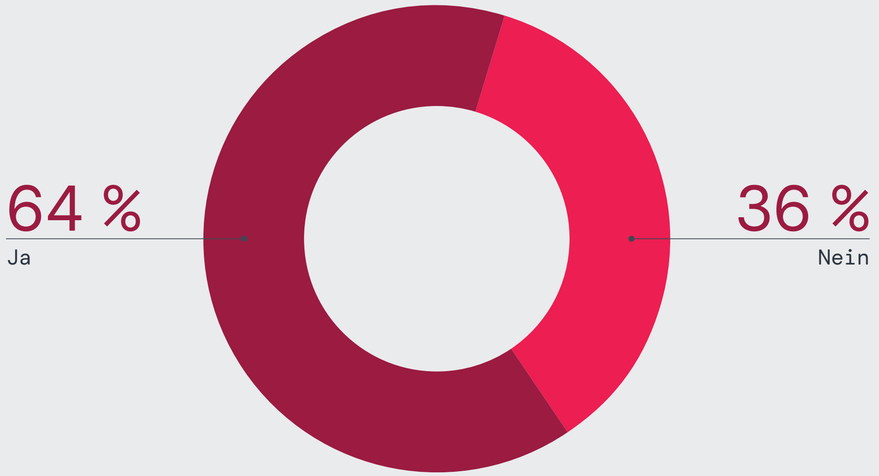


Abb. 8: Unternehmen sind besorgt über Cyberangriffe infolge von Fusionen und Übernahmen

VPN-Zugriff für Drittuser: Eine Hintertür für Angreifer

Der Zugriff für Drittuser hat sich als einer der häufigsten Einstiegspunkte für Angreifer herausgestellt. Herkömmliche VPNs sind von ihrer Konzeption her auf einen umfassenden Netzwerkzugriff nach abgeschlossener Authentifzierung angewiesen und weiten diese Berechtigung auf externe Anbieter und Partner aus. Dadurch entstehen Transparenzlücken, die Angreifer mit Vorliebe ausnutzen. Angreifer können gestohlene oder schwache Anmeldedaten, Fehlkonfigurationen und ungepatchte Schwachstellen ausnutzen, um diese als vertrauenswürdig eingestufte Verbindungen zu missbrauchen. 93 % der Befragten äußerten große Bedenken hinsichtlich Backdoor-Schwachstellen. Für Unternehmen, die auf statische, vertrauensbasierte Zugriffsmodelle angewiesen sind, stellt der Zugriff für Dritte eine tickende Zeitbombe dar.

Die Sorge ist begründet. Im August 2024 kam es bei der Enterprise Financial Group (EFG) zu einem schwerwiegenden Datenleck, bei dem die personenbezogenen Daten von fast 20.000 Kunden offengelegt wurden. Der Verstoß wurde auf Schwachstellen in einem von EFG genutzten VPN zurückgeführt, die Angreifer ausnutzten, um in das Netzwerk einzudringen und auf vertrauliche Daten zuzugreifen. Dieser Vorfall unterstreicht, wie durch VPN-Zugriff für Drittuser Sicherheitslücken entstehen, die Angreifer als Einstiegspunkte in Unternehmensnetzwerke ausnutzen können.

Unternehmen sollten zunächst den VPN-Zugriff für Drittuser überprüfen und strengere Richtlinienkontrollen durchsetzen, beispielsweise zeitlich begrenzten Zugriff, End-to-End-Trafficprüfung (vom Gerät zur Anwendung) und adaptive Authentifizierung. Die Umstellung auf ein Zero-Trust-Modell ermöglicht die Durchsetzung anwendungsspezifischer Zugriffe und stellt sicher, dass externe Partner nur den minimal erforderlichen Zugriff haben. Darüber hinaus können kontinuierliche Überwachung und risikobasierte Richtlinien die Schwachstellen aufgrund von Drittuser-Zugriff deutlich minimieren.

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

93 % befürchten, dass Angreifer sich über VPN-Zugriff für Drittuser unbefugten Zugang zum Unternehmensnetzwerk verschaffen könnten

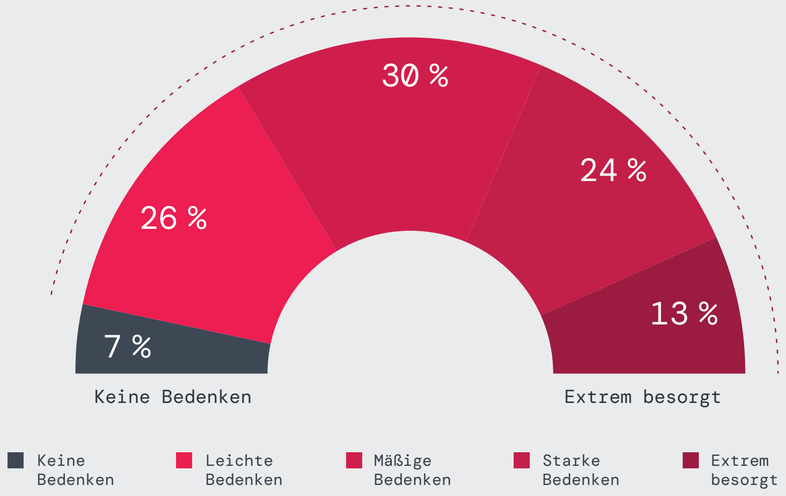


Abb. 9: Unternehmen befürchten, dass VPN-Zugriff für Drittuser Cyberangriffe begünstigen könnte.

Herausforderungen und Lücken bei herkömmlichen Schutzmaßnahmen

Legacy-Tools als Gefahr für private Unternehmensanwendungen

Der Schutz privater Unternehmensanwendungen vor zunehmend raffinierten webbasierten Bedrohungen — wie Ransomware, Anmeldedatendiebstahl und API-Missbrauch — ist zu einer geschäftskritischen Priorität geworden. Dennoch verlassen sich viele Unternehmen weiterhin auf Legacy-Tools, die der heutigen Bedrohungslage kaum gewachsen sind.

Laut den Umfrageergebnissen sind Firewalls (84 %), Web Application Firewalls (WAFs, 58 %) und VPNs (43 %) für Unternehmen nach wie vor die gängigsten Schutzmechanismen zur Abwehr von Webangriffen. Allerdings umgehen Angreifer diese Tools zunehmend, indem sie ungepatchte Geräte, schlechte Konfigurationen und inhärente Schwächen perimeterbasierter Sicherheitsmodelle ausnutzen. Dies zeigt, dass diese herkömmlichen Abwehrmaßnahmen heutigen Bedrohungen nicht mehr gewachsen sind.

Eine Reihe von Sicherheitsverstößen aus jüngster Zeit verdeutlichen die Schwächen solcher perimeterbasierten Abwehrmaßnahmen. Im August 2024 infiltrierten chinesische Hacker — eine Gruppe namens Salt Typhoon — große US-Telekommunikationsunternehmen, darunter AT&T und Verizon, indem sie Schwachstellen in ungepatchten Netzwerkgeräten und Routern ausnutzten. Dieser Angriff kompromittierte vertrauliche Metadaten von mehr als einer Millionen Usern und zeigte, wie raffinierte Angreifer traditionelle Sicherheitsmaßnahmen wie Firewalls und VPNs umgehen können.

Die einzige praktikable Lösung für den effektiven Schutz privater Unternehmnsanwendungen besteht darin, von Legacy-Perimeterschutzmaßnahmen auf Zero-Trust-Zugriffsmodelle umzusteigen. Im Gegensatz zu Firewalls und VPNs ermöglichen Zero-Trust-Architekturen Usern den Direktzugriff auf Anwendungen gemäß strikt durchgesetzten granularen Richtlinien nach dem Prinzip der minimalen Rechtevergabe. Dieser Ansatz macht netzwerkbasierte Sicherheit überflüssig, blockiert unbefugte Zugriffsversuche und verhindert laterale Bewegungen, Session Hijacking und den Diebstahl von Anmeldedaten — Taktiken, die Angreifer häufig verwenden, um traditionelle Perimeterschutzmaßnahmen zu umgehen.

Welche Produkte verwenden Sie zum Schutz privater Unternehmensanwendungen vor webbasierten Angriffen?

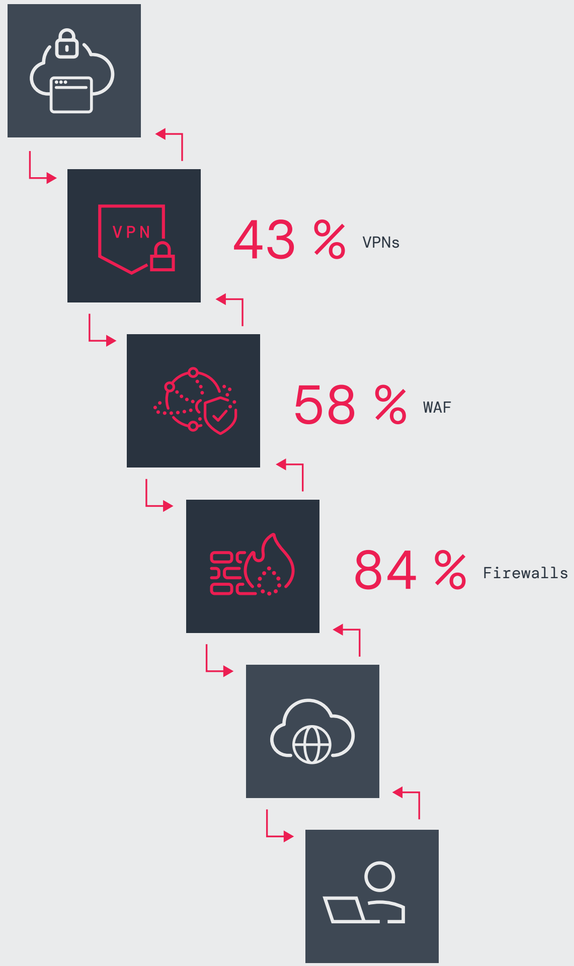


Abb. 10: Die verwendeten Sicherheitsprodukte zum Schutz privater Unternehmensanwendungen vor webbasierten Bedrohungen.

NAC-Bereitstellung in VPN-Umgebungen: Begrenzter Schutz

Bemerkenswerte 54 % der befragten Unternehmen geben an, NAC zu verwenden, um den VPN-Zugriff auf private Unternehmensressourcen zu sichern. Allerdings konnten diese Implementierungen bisher die Sicherheitsverstöße und Exploits, die üblicherweise mit VPN-Schwachstellen in Verbindung gebracht werden, nicht verhindern. Daran wird ersichtlich, dass sich die systemischen Risiken netzwerkbasierter Zugriffsmodelle mit NAC nicht bewältigen lassen.

NAC-Lösungen erzwingen Gerätestatusprüfungen, Authentifizierung und Netzwerksegmentierung. Sie lösen jedoch nicht die zentralen VPN-Sicherheitsprobleme wie umfassende Zugriffsberechtigungen, Risiken lateraler Bewegungen und die Abhängigkeit von implizitem Vertrauen.

Jüngste Sicherheitsverstöße zeigen, dass VPN-Sicherheitslücken trotz vorhandenem NAC weiterhin eine kritische Schwachstelle darstellen. Im November 2023 bestätigte das US-Energieministerium einen schwerwiegenden Sicherheitsvorfall im Zusammenhang mit kompromittierten VPN-Anmeldedaten, der es Angreifern ermöglichte, Kontrollmechanismen zu umgehen und sich Zugriff auf vertrauliche interne Systeme zu verschaffen. Dies verdeutlicht, wie Angreifer VPN-Schwachstellen direkt ausnutzen können, sei es durch gestohlene Anmeldedaten, ungepatchte Sicherheitslücken oder Session Hijacking. NAC erweist sich als unzureichender Schutz, wenn das zugrunde liegende Zugriffsmodell unverändert bleibt.

Verwenden Sie NAC (Network Access Control) zwischen Ihrem VPN und privaten Unternehmensressourcen?

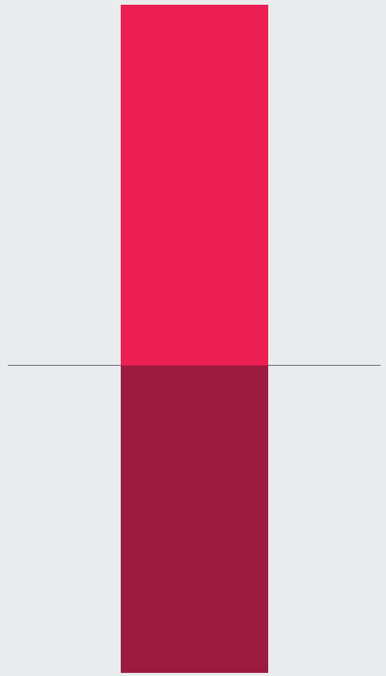


Abb. 11: Anteil der Unternehmen, die NAC zwischen VPNs und privaten Ressourcen einsetzen.

Um die Einschränkungen von NAC und Legacy-VPN-Architekturen zu überwinden, müssen Unternehmen auf ein Zero-Trust-Sicherheitsmodell umsteigen. Zero Trust eliminiert die laterale Bewegungsfreiheit innerhalb des Netzwerks und ermöglicht Usern stattdessen, sich unter kontinuierlich validierten Richtlinien, die an Identität, Gerätestatus und Kontext gebunden sind, direkt mit den jeweils benötigten Anwendungen zu verbinden. Zero Trust blockiert nicht nur unbefugte Zugriffe, sondern verhindert auch, dass Angreifer ihre Berechtigungen erweitern oder Daten exfiltrieren können.

Probleme mit der User Experience und Verwaltung von VPNs

Probleme mit der Performance von VPNs: Frustrierte User und überforderte IT

VPNs stellen nicht nur ein Sicherheitsrisiko dar, sie sind auch eine Hauptquelle der Unzufriedenheit der User. Enduser äußern zunehmend ihre Frustration über Probleme mit der Performance von VPNs, die die Produktivität beeinträchtigen und die IT-Teams zusätzlich belasten.

Langsame Verbindungsgeschwindigkeiten sind die häufigste Beschwerde (23 %). Dies bestätigt den schlechten Ruf von VPNs hinsichtlich Latenz, Überlastung und schlechter Leistung beim Remote-Zugriff auf Cloud-Anwendungen. Auch Authentifizierungsprobleme bleiben ein erhebliches Problem: 20 % der Befragten berichten von komplexen Anmeldeprozessen und 17 % haben aufgrund von Authentifizierungsfehlern Probleme mit dem Anwendungszugriff.

Diese Leistungsprobleme stören den täglichen Geschäftsbetrieb, beeinträchtigen die Produktivität und machen den IT-Helpdesk zu einem Engpass, da die Teams mit häufigen Anfragen zur Fehlerbehebung zu kämpfen haben — ein Problem, das sich mit der zunehmenden Komplexität von Remote- und Hybrid-Arbeitsumgebungen nur noch verschärft.

Das Ersetzen von VPNs durch Zero Trust Network Access (ZTNA) beseitigt nicht nur die Bandbreitenüberlastung, sondern verbessert auch die User Experience der Enduser erheblich, indem direkte, sichere und latenzfreie Verbindungen zu Anwendungen ermöglicht werden. Im Gegensatz zu VPNs, die den gesamten Traffic über ein zentrales Gateway leiten und Performance-Engpässe verursachen, ermöglicht ZTNA den direkten und sicheren Zugriff auf Anwendungen ohne Leistungseinbußen.
Durch Umstellung auf identitätsbasierte Zugriffskontrollen, kontinuierliche Überprüfung und cloudbasierte Sicherheit können Unternehmen nicht nur häufig auftretende Probleme mit VPNs vermeiden, sondern auch die Produktivität ihrer Mitarbeiter steigern und den IT-Aufwand für die Fehlerbehebung und Unterstützung unflexibler VPN-Frameworks verringern.

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

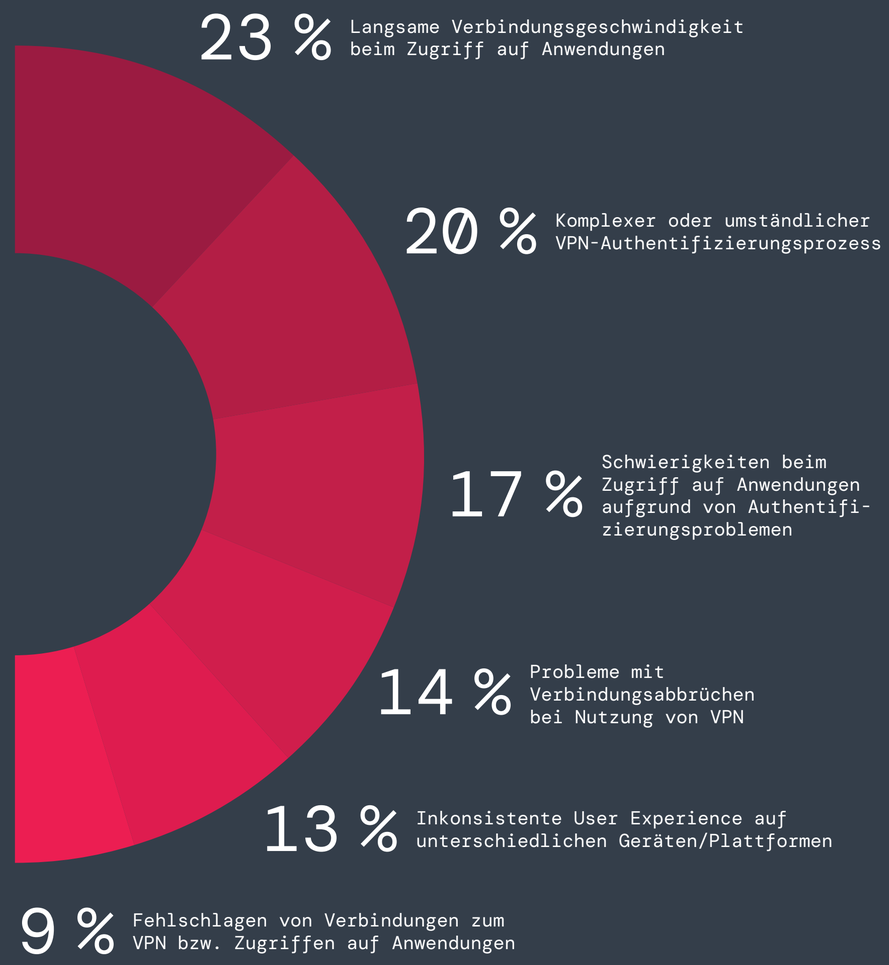


Abb. 12: Die häufigsten Beschwerden unter VPN-Usern.

VPN-Verwaltung: Überlastung von IT-Teams und Exposition von Schwachstellen

VPNs überlasten IT-Teams mit ständigen Sicherheitslücken, ressourcenintensiven Wartungsanforderungen und veralteten Zugriffsmodellen, die nicht mehr den Anforderungen der heutigen cloudorientierten Unternehmensumgebungen entsprechen. Die größte Sorge dieser Teams (52 %) sind Sicherheitslücken, die zu Sicherheitsvorfällen führen — dies verdeutlicht die anhaltenden Risiken im Zusammenhang mit dem Diebstahl von Anmeldedaten, der Ausnutzung ungepatchter Software sowie Angreifern, die den VPN-Zugriff für unkontrollierte laterale Bewegungen ausnutzen. Diese Risiken unterstreichen, warum VPNs zunehmend als Zugriffslösungen mit hohem Risiko angesehen werden.

VPNs sind für IT-Teams zu einer finanziellen und betrieblichen Belastung geworden. 41 % der Befragten wiesen auf die unverhältnismäßig hohen Ressourcenkosten hin, die mit ihrer Instandhaltung verbunden sind. Der unerbittliche Zyklus aus Patches, Fehlerbehebung und Protokollüberwachung, der erforderlich ist, um Legacy-Infrastrukturen zu sichern, führt dazu, dass die Teams überlastet sind und sich nicht auf höherwertige Aktivitäten konzentrieren können.

Eine weitere kritische Schwäche, die von 35 % der Befragten genannt wurde, ist die Unfähigkeit von VPNs, granulare Zugriffskontrollen durchzusetzen. Anstatt präzisen, identitätsbasierten Zugriff auf bestimmte Anwendungen zu gewähren, stellen VPNs häufig eine umfassende, uneingeschränkte Netzwerkkonnektivität bereit, wodurch das Risiko von Insider-Bedrohungen und lateralen Bewegungen von Angreifern dramatisch steigt. Darüber hinaus nennen 26 % den Betriebsaufwand für die Verwaltung von VPN-Konzentratoren und anderen Geräten, was die Komplexität der Wartung von Hardwaregeräten, Netzwerktunneln und Zugangs-Gateways zur Aufrechterhaltung der Remote-Konnektivität verdeutlicht. Diese Komplexitäten sind unhaltbar zu einem Zeitpunkt, an dem Cloud-native und Remote-Arbeitsumgebungen agilere und skalierbarere Lösungen erfordern.

Was sind die häufigsten Bedenken Ihrer IT/ Sicherheitsbeauftragten bei der Unterstützung von VPNs?

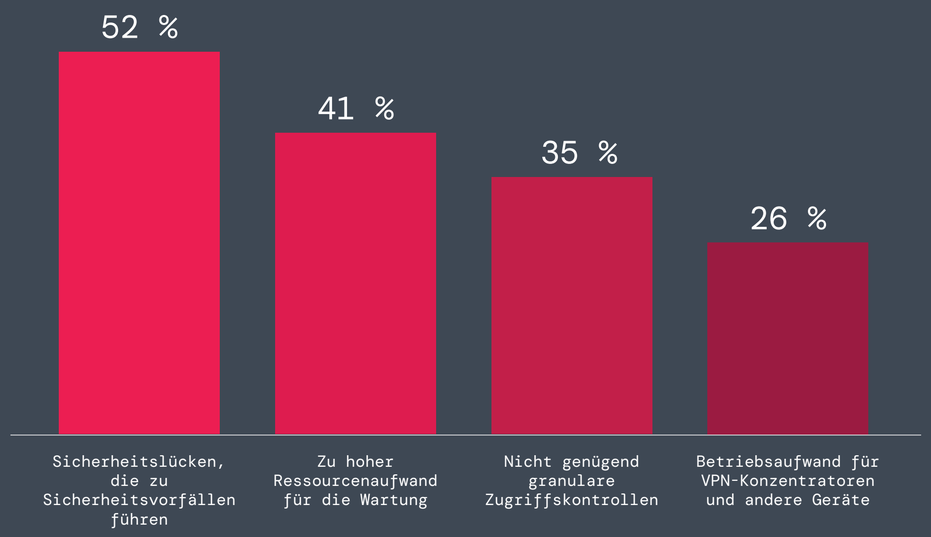


Abb. 13: Die größten Bedenken der IT- und Sicherheitsbeauftragten bei der Unterstützung von VPNs.

Um diese Herausforderungen zu bewältigen, sollten Unternehmen vom netzwerkbasierten VPN-Zugriff auf ein cloudbasiertes Zero-Trust-Modell umsteigen, das implizites Vertrauen eliminiert, Angriffsflächen reduziert und den IT-Betrieb rationalisiert. Durch die Umstellung auf Zero Trust wird der VPN-bezogene Betriebsaufwand verringert, die Zugriffsverwaltung vereinfacht und Sicherheitsrisiken im großen Maßstab minimiert. IT-Teams werden von der Last ständiger Wartungsaufgaben befreit und können sich auf proaktive Sicherheitsinitiativen konzentrieren und gleichzeitig zügigere, nahtlose User Experience unterstützen.

Hoher Verwaltungsaufwand für VPN

Die Verwaltung der VPN-Infrastruktur stellt weiterhin eine Belastung für die IT-Teams dar, wobei die größten Bedenken hinsichtlich Zuverlässigkeit, Performance und Wartungsaufwand bestehen. Die größte Herausforderung bleibt die Behebung von Problemen mit der VPN-Konnektivität und -Stabilität, die von 54 % der Befragten genannt wurde. IT-Beauftragte kämpfen ständig damit, eine konstante VPN-Verfügbarkeit aufrechtzuerhalten. Verbindungsausfälle führen zu weitreichenden Störungen, die die Produktivität mindern, die Sicherheit gefährden und die Mitarbeiter frustrieren.

Die Balance zwischen VPN-Performance und User Experience bleibt ebenfalls eine große Herausforderung (50 %) da VPNs häufig zu Latenz, Verbindungsabbrüchen und inkonsistenten Geschwindigkeiten führen, insbesondere in Cloud-First-Umgebungen. Darüber hinaus heben 47 % der IT-Experten den häufigen Patch-Bedarf und die Ressourcenkosten als große Hürden hervor und unterstreichen damit die betrieblichen Herausforderungen bei der Beseitigung hartnäckiger Schwachstellen und der Wartung veralteter Systeme.

Diese Herausforderungen haben bei mehreren spektakulären Datenschutzverletzungen eine Rolle gespielt. Von Dezember 2023 bis Anfang 2024 waren mehrere US-Regierungsbehörden von VPN-bezogenen Angriffen betroffen. Verzögerungen beim Patchen einer weithin bekannten Sicherheitslücke ermöglichten es Bedrohungsakteuren, veraltete VPN-Software auszunutzen und sich so unbefugten Netzwerkzugriff zu verschaffen. Dieser Fall verdeutlicht die Unzulänglichkeit reaktiver Patch-Zyklen, selbst bei Unternehmen mit dedizierten IT-Abteilungen, und zeigt, wie kritische Sektoren durch unvollständige VPN-Abwehrmaßnahmen neuen Bedrohungen ausgesetzt sind.

Da die VPN-Infrastruktur erhebliche IT-Ressourcen für die Fehlerbehebung bei der Konnektivität, das Einspielen von Sicherheitspatches und die Leistungsoptimierung in Anspruch nimmt, müssen Unternehmen die langfristige Rentabilität eines VPN-basierten Zugriffs neu bewerten. Durch den Ersatz von VPN-Konzentratoren und Netzwerkgeräten wie Firewalls und NACs durch eine Cloud-native Architektur können IT-Beauftragte Infrastrukturengpässe beseitigen, Patchzyklen verkürzen und die manuelle Fehlerbehebung bei Verbindungsfehlern überflüssig machen.

Durch den richtliniengesteuerten Zugriff nach dem Prinzip der minimalen Rechtevergabe wird sichergestellt, dass User nur auf autorisierte Anwendungen zugreifen können — ohne dass sie komplexe Firewall-Regeln oder Richtlinien zur Netzwerksegmentierung verwalten müssen. Durch Umstellung auf ein cloudbasiertes Zero-Trust-Modell können Unternehmen VPN-bedingte Engpässe beseitigen und gleichzeitig einen nahtlosen, richtliniengesteuerten Zugriff auf Anwendungen gewährleisten — ohne den Aufwand der Verwaltung der Netzwerkinfrastruktur, von Software-Patches oder komplexer Skalierungsmaßnahmen.

Was sind die drei Hauptbedenken bei der Verwaltung Ihrer VPN-Infrastruktur?

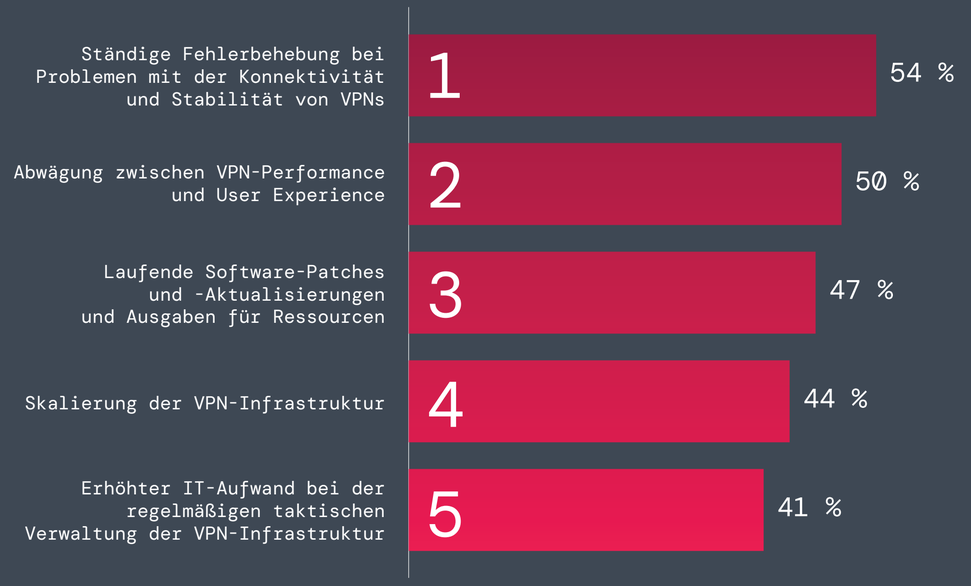


Abb. 14: Hauptbedenken der IT-Beauftragten, die die VPN-Infrastruktur verwalten.

Weitreichende VPN-Zugriffsberechtigungen: eine kritische Sicherheitslücke

Die Hauptursache für viele VPN-Sicherheitsrisiken liegt in der Art und Weise, wie VPNs den Zugriff definieren. Anstatt präzisen, anwendungsspezifischen Zugriff zu gewähren, ermöglichen viele Unternehmen immer noch umfassenden Netzwerkzugriff und verlassen sich auf implizite Vertrauensmodelle, wodurch kritische Systeme ungeschützt bleiben.

Die Ergebnisse der Umfrage zeigen, dass 52 % der Unternehmen immer noch auf veraltete Zugriffsmodelle wie statische Netzwerk-Firewall-Regeln (28 %) oder offenen Zugriff für authentifizierte User (24 %) setzen. Diese veralteten Kontrollen machen es Angreifern leicht, unbemerkt in Netzwerke einzudringen, Berechtigungen zu erweitern und kritische Daten zu exfiltrieren, sobald sie Zugriff erlangt haben.

Mehrere Vorfälle aus jüngerer Zeit unterstreichen die Gefahren eines derart umfassenden Zugangs. Anfang 2024 kam es bei Global Affairs Canada (GAC) zu einer erheblichen Sicherheitsverletzung aufgrund eines kompromittierten VPN, das von Mitarbeitern für den Zugriff auf die Zentrale in Ottawa genutzt wurde. Angreifer nutzten Schwachstellen im VPN aus, verschafften sich unbefugten Zugriff auf das Netzwerk und legten möglicherweise vertrauliche Informationen offen. Das Ereignis zeigte, wie uneingeschränkter und überprivilegierter Netzwerkzugriff einen idealen Rahmen für laterale Bewegungen und tiefere Infiltration bietet.

Um diese Risiken zu mindern, sollten Unternehmen implizites Vertrauen beseitigen und granulare, identitätsgesteuerte Zugriffskontrollen durchsetzen. Durch die Umstellung von umfassenden netzwerkbasierten Zugriffsmodellen auf eine direkte Segmentierung auf Anwendungsebene wird sichergestellt, dass jeder User nur auf die für seine Rolle erforderlichen Ressourcen zugreifen kann. Dadurch werden Angriffsflächen erheblich reduziert und laterale Bewegungen verhindert.

Wie definieren Sie den Zugriff von VPN-Usern auf Anwendungen?

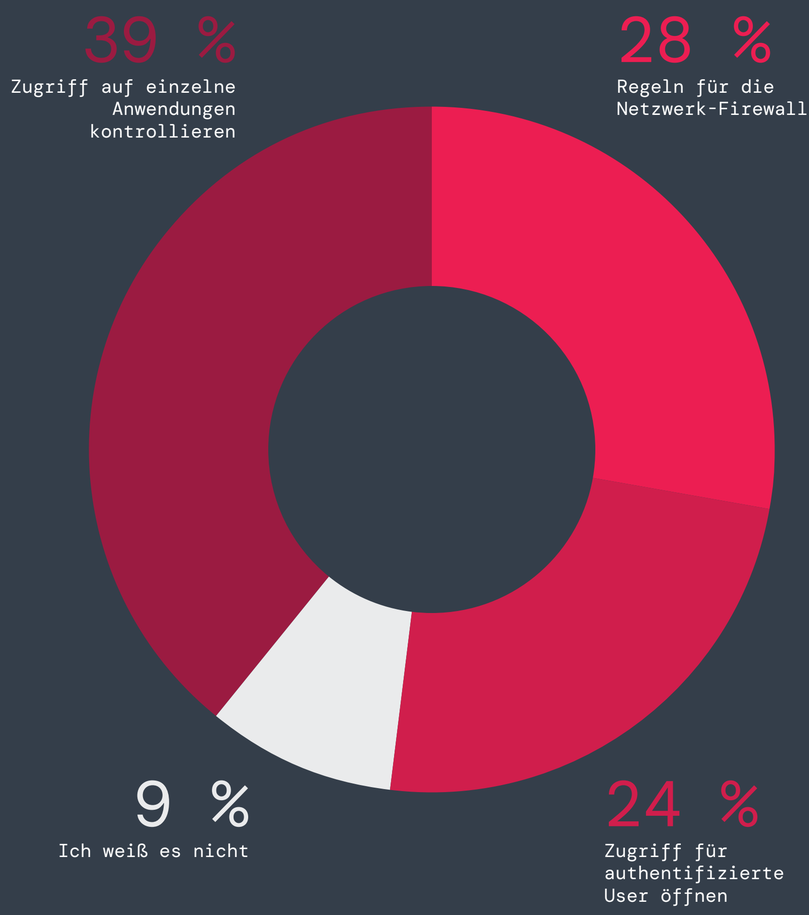


Abb. 15: So definieren Unternehmen den Zugriff von VPN-Usern auf Anwendungen.

Alternativen zu VPN: Umstellung auf sicheren Zugriff

Die zunehmenden Sicherheitslücken, Herausforderungen hinsichtlich der Userfreundlichkeit und der hohe Wartungsaufwand von VPNs veranlassen Unternehmen dazu, ihren Übergang zu zukunftsfähigen Technologien für die Zugriffssicherung wie ZTNA zu beschleunigen. Dieser Wandel signalisiert die wachsende Erkenntnis, dass VPNs nicht länger in der Lage sind, heutige Sicherheits- und Betriebsanforderungen zu erfüllen.

Die Umfrage bestätigt diese Dynamik: 65 % der Befragten gaben an, dass ihre Unternehmen entweder bereits dabei sind, ihre VPNs zu ersetzen, oder dies innerhalb des nächsten Jahres planen.

Da Unternehmen zunehmend auf VPNs verzichten, müssen sie der Einführung von cloudbasierten Sicherheitsmodellen Priorität einräumen, die einen granularen Zugriff auf Anwendungsebene statt einer umfassenden Netzwerkkonnektivität erzwingen. ZTNA eliminiert VPN-bezogene Risiken, indem es sicherstellt, dass User basierend auf Identität und Sicherheitsstatus nur auf die Ressourcen zugreifen können, die sie benötigen, ohne sie jemals in das Unternehmensnetzwerk einzubinden. Dieser Ansatz erhöht die Sicherheit, verringert die Betriebskomplexität und verbessert die User Experience, sodass der VPN-Ersatz für zukunftsfähige Unternehmen ein dringender und unverzichtbarer Schritt ist.

Welche Pläne haben Sie, Ihren aktuellen VPN-Service zu ersetzen?

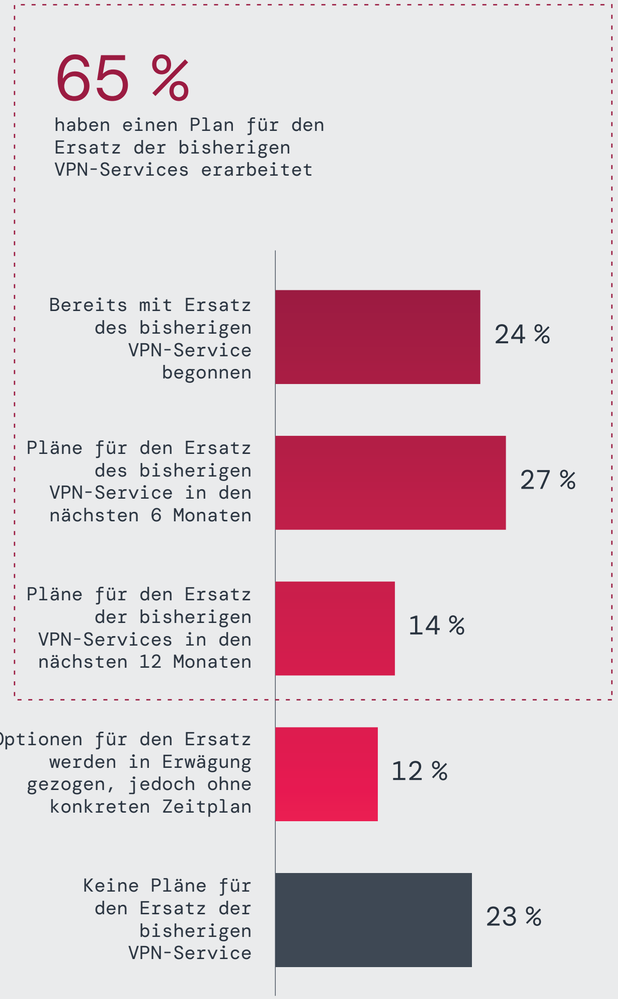
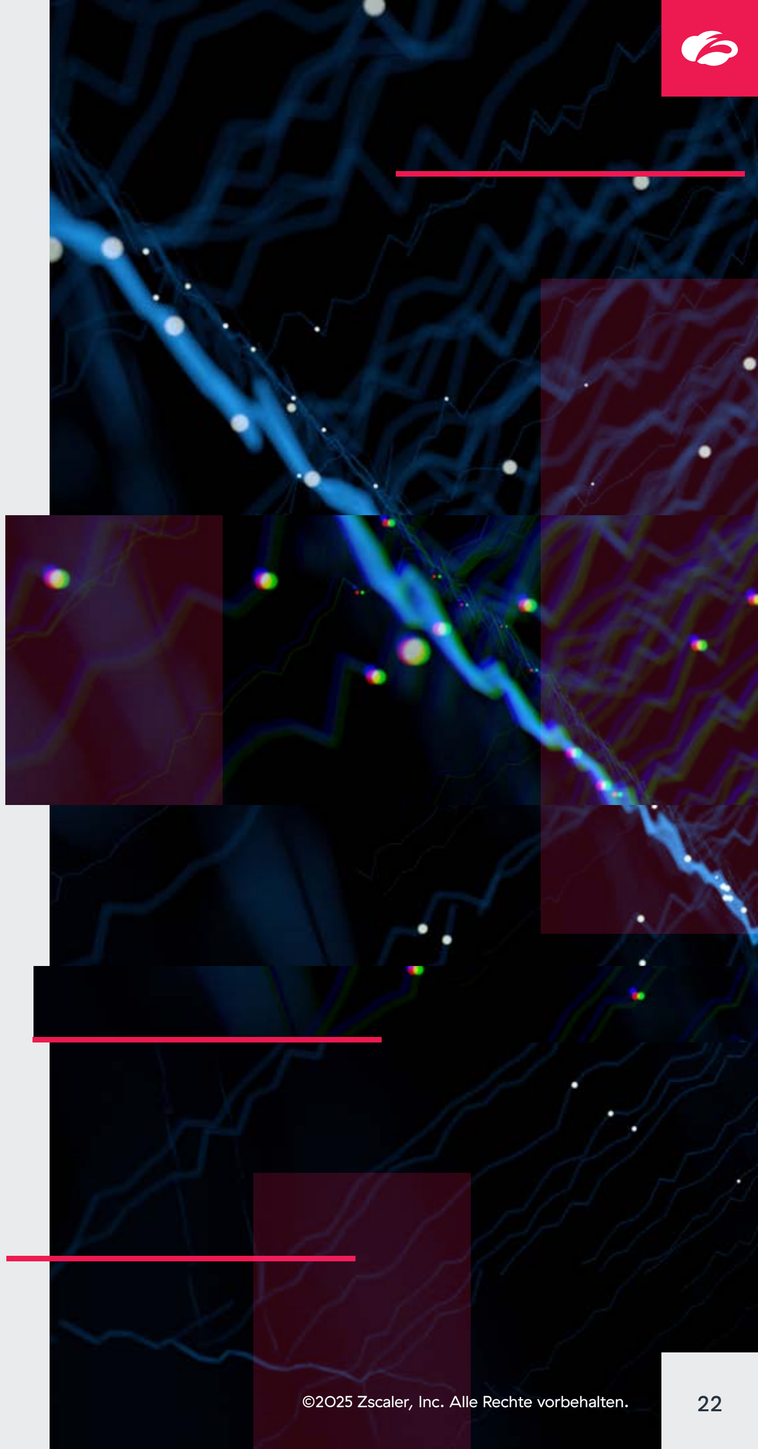


Abb. 16: Pläne der Unternehmen, bestehende VPN-Services zu ersetzen.



Umstellung auf Zero Trust

Zero Trust ersetzt VPN im großen Maßstab

Da sich der Trend zum VPN-Ersatz beschleunigt, setzt die große Mehrheit der Unternehmen auf Zero-Trust-Architekturen, um granulare Zugriffskontrollen zu ermöglichen, ihre Angriffsflächen zu reduzieren und die Userproduktivität zu verbessern. Die Umfrageergebnisse unterstreichen die wachsende Dynamik dieses Paradigmenwechsels: 81 % der Befragten geben an, dass sie planen, Zero Trust noch in diesem Jahr einzuführen. 35 % von ihnen implementieren bereits Zero-Trust-Lösungen, 24 % rechnen mit der Einführung innerhalb von sechs Monaten und 22 % haben Bereitstellungsstrategien für das folgende Jahr geplant. Damit erweist sich Zero Trust als branchenweit führende Strategie zum Ersetzen veralteter Zugriffstechnologien wie VPNs.

Voraussetzung für eine erfolgreiche Umstellung auf Zero Trust ist die Abstimmung zwischen Sicherheitsbeauftragten und Fachabteilungen. Unternehmen sollten Risikobewertungen durchführen, um ihre anfälligsten Zugriffspunkte zu identifizieren — ob Remotezugriff, Integrationen von Drittanbietern oder geschäftskritische Anwendungen — und der Zero-Trust-Bereitstellung entsprechend Priorität einräumen. Durch Automatisierung der Richtliniendurchsetzung kann der Übergang beschleunigt und gleichzeitig der Verwaltungsaufwand verringert werden.

Hat Ihr Unternehmen Pläne für die Umstellung auf eine Zero-Trust-Strategie?

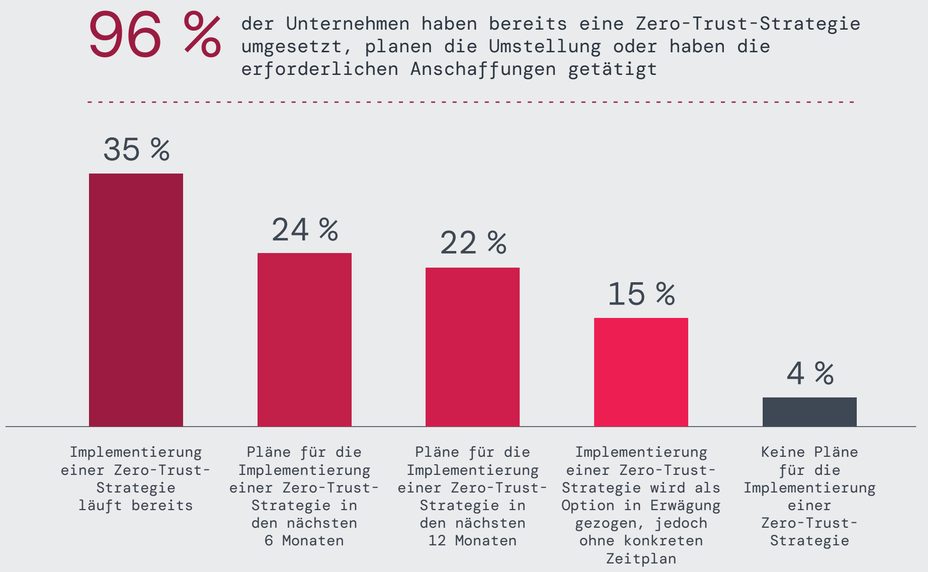


Abb. 17: Pläne der Unternehmen zur Implementierung einer Zero-Trust-Strategie.

Zero Trust-Prioritäten: Umstellung wird durch Remote-Arbeit forciert

Die Abkehr von herkömmlichen VPNs unterstreicht einen bedeutenden Wandel: Unternehmen setzen auf Zero-Trust-Architekturen, um Sicherheitslücken zu schließen, IT-Abläufe zu optimieren und den Anforderungen dezentralisierter Remote-Arbeitskräfte gerecht zu werden. Dieser strategische Wandel unterstreicht die Bedeutung von Zero Trust als zukunftsfähige Lösung zur Minderung von VPN-Risiken und zur Vereinfachung des Sicherheitsmanagements.

Umfrageergebnisse zeigen, dass die Absicherung der Remote-Belegschaft der Hauptgrund für diesen Wandel ist: 37 % der Unternehmen konzentrieren sich auf die Remote-Arbeit und 28 % auf die Sicherheit der hybriden Belegschaft. Dieser Schritt spiegelt einen breiteren Trend zu Sicherheitsmodellen wider, die direkten, anwendungsspezifischen Zugriff bieten und so die Komplexität reduzieren, die mit der Verwaltung mehrerer Einzelprodukte verbunden ist, wie sie in herkömmlichen VPN-Setups üblich sind.

Die Implementierung eines Zero-Trust-Frameworks erhöht nicht nur die Sicherheit, sondern verringert auch den operativen Aufwand für die Verwaltung zahlreicher Sicherheitslösungen. Durch die Zusammenführung von Sicherheitsrichtlinien und -kontrollen in einem zusammenhängenden System können Unternehmen den Verwaltungsaufwand senken und ihre Abläufe optimieren. Beispielsweise kann eine Zero-Trust-Plattform, die mehrere Richtlinienaktionen in einem einzigen Scan ausführt, die Notwendigkeit beseitigen, verschiedene Lösungen miteinander zu verketten. Dies vereinfacht die User Experience und gewährleistet gleichzeitig eine robuste Sicherheit.

Um Remote- und Hybrid-Belegschaften mit einer Zero-Trust-Architektur wirksam zu schützen, sollten Unternehmen den Schwerpunkt auf die Integration von Sicherheitsmaßnahmen legen, die die Komplexität minimieren. Durch Implementieren einer einheitlichen Zero-Trust-Plattform können verschiedene Sicherheitsfunktionen konsolidiert werden, wodurch der Bedarf an mehreren Einzelprodukten reduziert und die Verwaltung vereinfacht wird. Dieser Ansatz verbessert die Sicherheit und die Betriebseffizienz und ermöglicht IT-Fachkräften, sich auf strategische Initiativen zu konzentrieren, anstatt eine komplexe Reihe von Sicherheitstools verwalten zu müssen.

Was ist der primäre Anwendungsfall für die Bereitstellung einer Zero-Trust-Lösung?

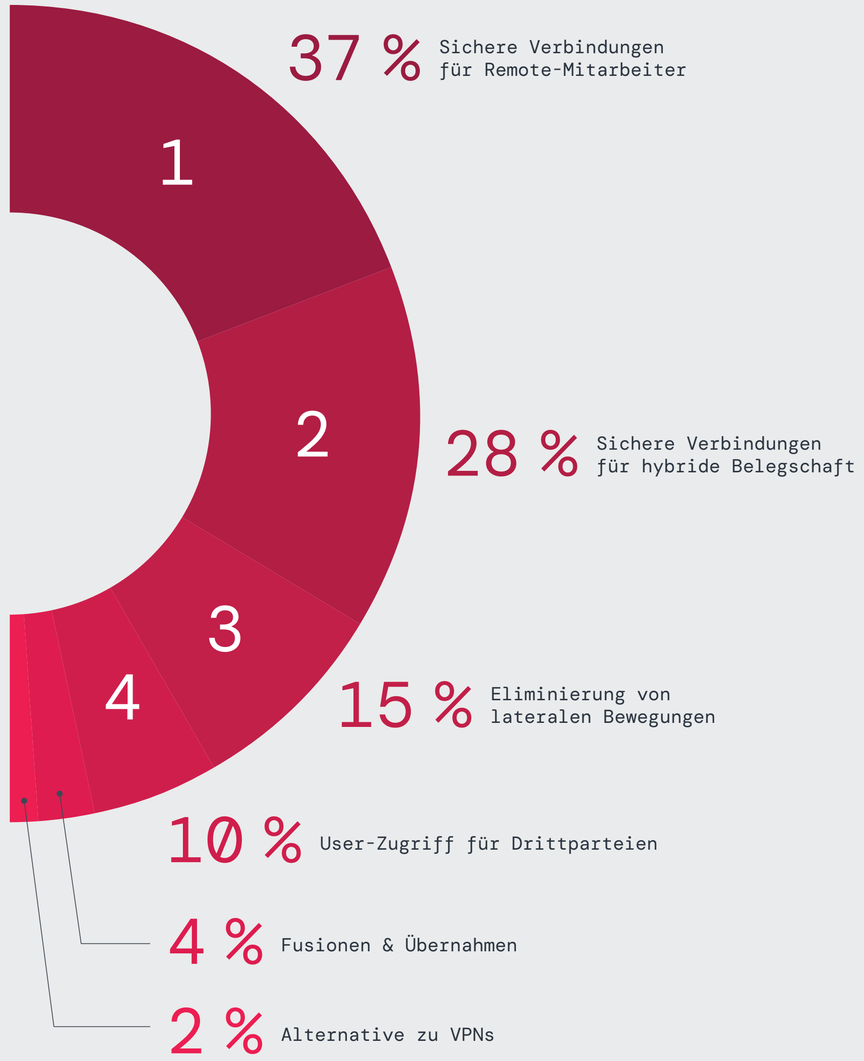


Abb. 18: Primärer Anwendungsfall für Zero-Trust-Lösungen in Unternehmen.

Hauptvorteile des Umstiegs von VPNs auf Zero Trust

Die Umstellung auf Zero-Trust-Lösungen verändert die Unternehmenssicherheit und bietet weitreichende Vorteile, die über den sicheren Zugriff hinausgehen — insbesondere vereinfachte Verwaltung, verbesserte Performance und Skalierbarkeit, eine drastische Reduzierung der Angriffsfläche und eine Verbesserung der Ressourceneffizienz. Bei der Umstellung von VPN-Modellen auf Zero Trust geht es nicht nur um ein Tool-Upgrade; vielmehr machen Unternehmen damit ihre gesamte Remote-Access-Strategie zukunftssicher.

Die überwiegende Mehrheit der Befragten (76 %) sieht verbesserte Sicherheit und Compliance als Hauptvorteil an, was unterstreicht, wie Zero Trust den bisherigen Netzwerkzugriff mit implizitem Vertrauen ersetzt und die Anfälligkeit für Ransomware, Diebstahl von Anmeldedaten und Risiken durch laterale Bewegungen verringert.

Darüber hinaus nennen 64 % Verbesserungen bei der Verwaltungsvereinfachung, Skalierbarkeit und Userfreundlichkeit als Hauptvorteil, da Zero Trust den Betriebsaufwand für die Verwaltung von VPN-Konzentratoren, ständiges Patchen und die Fehlerbehebung beim Zugriff eliminiert.

Fast die Hälfte (45 %) der Befragten nennen den Ersatz von VPN durch eine Zero-Trust-Lösung als entscheidenden Schritt hin zu einer vollständigen Zero-Trust-Architektur. Gleichzeitig betonen 34 % die überlegene Skalierbarkeit und Flexibilität, die Zero Trust zu einer effektiveren Lösung für die Absicherung von Remote- und Hybrid-Arbeitskräften machen. Als weitere Vorteile von Zero Trust nannten die Befragten insbesondere die verbesserte User Experience für Enduser (32 %), nahtlose systemübergreifende Integrationen (28 %), und reduzierte Betriebskosten durch Ressourceneinsparungen (18 %). Zusammengenommen verdeutlichen diese Vorteile, warum Unternehmen die Umstellung von Legacy-VPNs auf Zero Trust forcieren.

ManpowerGroup, ein weltweit führender Anbieter von Personallösungen, liefert eine überzeugende Fallstudie zur Zugriffssicherung mit Zero Trust. Zur Bewältigung der Aufgabe, eine große Anzahl von Remote-Mitarbeitern zu unterstützen, ersetzte das Unternehmen erfolgreich seine bestehende VPN-Infrastruktur durch eine Zero-Trust-Lösung von Zscaler. Bemerkenswerterweise skalierte ManpowerGroup innerhalb von nur 18 Tagen den sicheren Anwendungszugriff auf über 30.000 User, erreichte eine unterbrechungsfreie Geschäftskontinuität und reduzierte gleichzeitig die Helpdesk-Tickets drastisch um 97 %. Diese Bereitstellung unterstreicht die Fähigkeit einer Zero-Trust-Architektur, schnell zu skalieren, Abläufe zu vereinfachen und messbare Ergebnisse hinsichtlich Produktivität und Sicherheit zu erzielen.

Wenn Sie eine VPN-Lösung durch eine Zero-Trust-Lösung ersetzt haben, was sind für Sie die Hauptvorteile im Vergleich zur vorherigen VPN-Lösung?

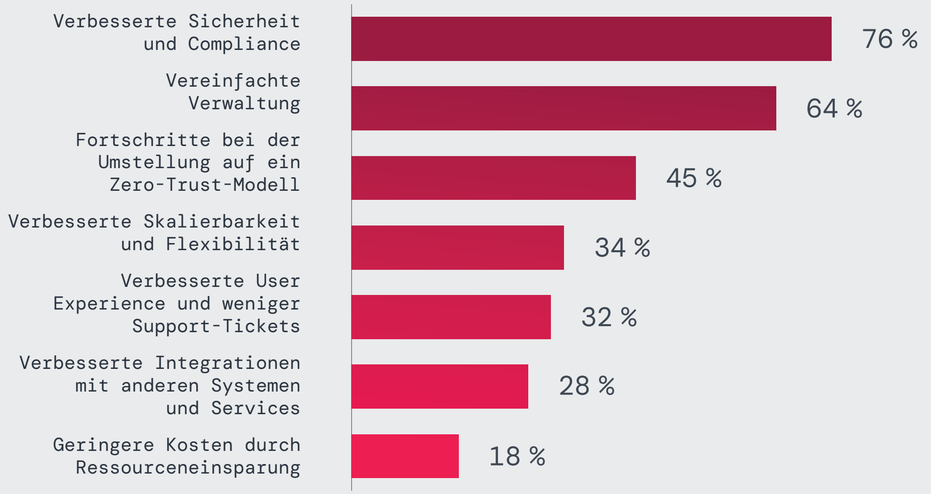


Abb. 19: Unternehmen berichten über die Hauptvorteile einer Zero-Trust-Lösung im Vergleich zu einer früheren VPN-Lösung.

Die Umstellung auf Zero Trust sollte mit taktischen Änderungen beginnen, die VPN-basierten Netzwerkzugriff zugunsten direkter Verbindungen auf Anwendungsebene eliminieren, um Risiken durch laterale Bewegungen entgegenzuwirken. Unternehmen können den Ersatz von Legacy-Zugriffen für kritische Anwendungsfälle, wie beispielsweise die Sicherung von Remote- und Drittuserverbindungen, priorisieren, bevor sie Zero-Trust-Funktionen in ihrem gesamten IT-Ökosystem skalieren. Die Automatisierung von Zugriffsrichtlinien — mithilfe eines einzigen Richtliniensatzes — und die Integration identitätsbasierter Sicherheit vereinfachen das Zero-Trust-Management weiter und ermöglichen gleichzeitig die Skalierbarkeit über verteilte Systeme hinweg. Diese intelligenten Frameworks ermöglichen IT-Beauftragten die Echtzeit-Sicherheitskontrolle ohne Einbußen bei Agilität und Effizienz.

VPN-Risikoprognosen für 2025

Kritische VPN-Schwachstellen werden weiter zunehmen

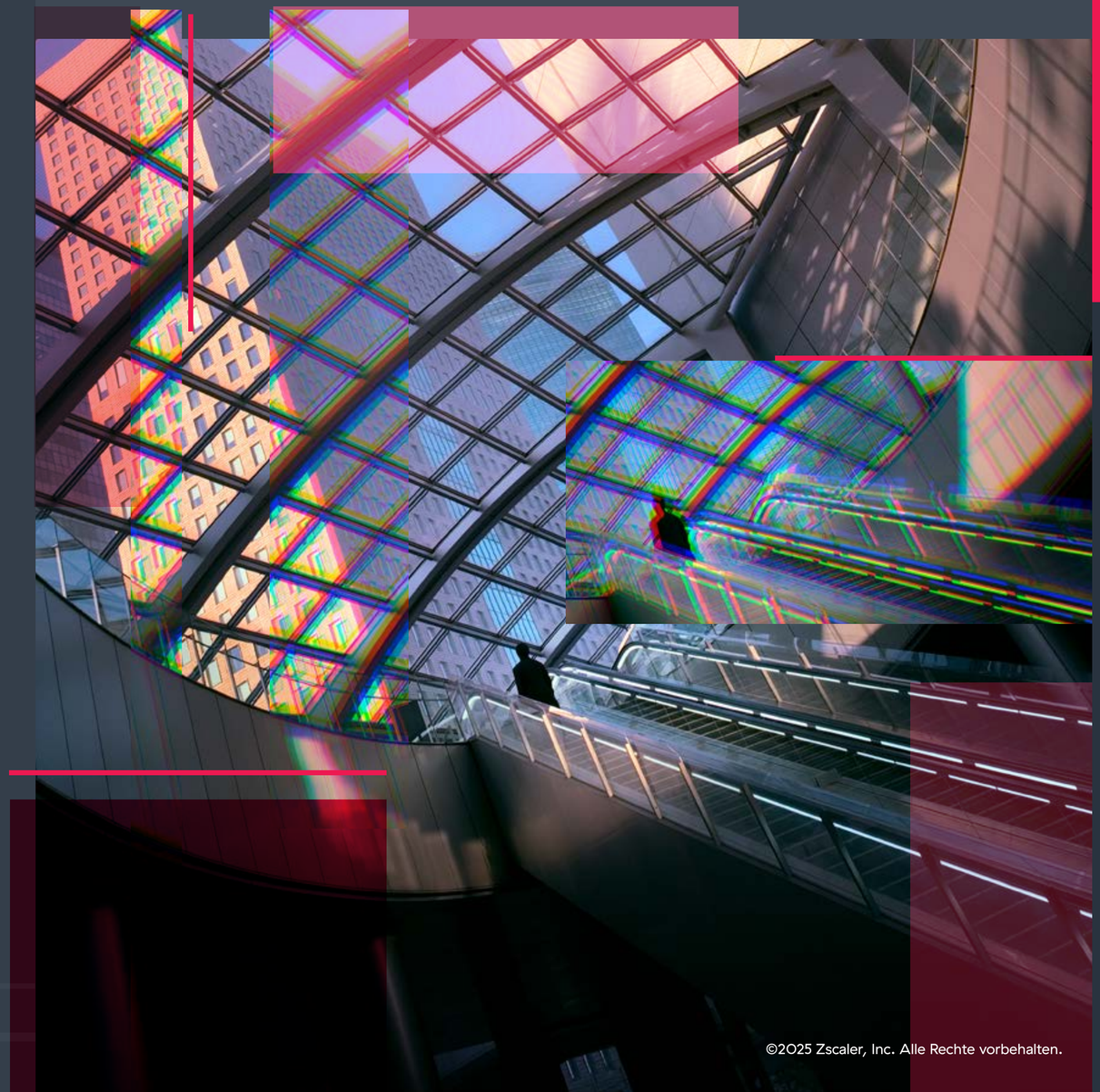
In den letzten Jahren war eine Zunahme der VPN-Exploits zu beobachten, die sich 2025 noch beschleunigen dürfte. VPN-Technologien sind ein Hauptziel für Angreifer, da sie unternehmenseigene IT-Assets im Internet exponieren und Schwachstellen dadurch leicht gescannt und ausgenutzt werden können. Während Unternehmen Probleme haben, VPN-Schwachstellen rechtzeitig zu beheben, werden Angreifer weiterhin neue, schwerwiegende Schwachstellen entdecken und als Waffe einsetzen, wie der Angriff auf Ivanti Pulse Secure im Januar 2025 gezeigt hat. Sowohl Sicherheitsanalysten als auch Cyberkriminelle suchen aktiv nach Sicherheitslücken in VPN-Infrastrukturen, was die fortlaufende Offenlegung kritischer CVEs unvermeidlich macht.

Ransomware-Gruppen werden VPN-Exploits intensivieren

Da 92 % der Umfrageteilnehmer Bedenken hinsichtlich ungepatchter VPN-Sicherheitslücken äußern, ist damit zu rechnen, dass Ransomware-Akteure auch weiterhin bekannte und Zero-Day-VPN-Schwachstellen als primäre Methode für den Erstzugriff ausnutzen. Ransomware-as-a-Service-Gruppen (RaaS) suchen häufig nach exponierten VPNs mit ungepatchten Schwachstellen und können so Ransomware einsetzen, bevor IT-Beauftragte reagieren können. Die Ransomware-Kampagne vom Januar 2025, die sich gegen US-Unternehmen aus dem Gesundheitswesen richtete, zeigt, wie VPN-Sicherheitslücken Angreifern direkten Zugriff auf vertrauliche Systeme ermöglichen. Da diese Angriffe zunehmend automatisiert werden, wird die Umstellung auf Zero-Trust-Sicherheit noch dringlicher.

Laterale Bewegungen über VPNs werden zu zerstörerischeren Angriffen führen

Angreifer nutzen den umfassenden Zugriff, den VPNs bieten, um sich lateral zu bewegen, Berechtigungen zu erweitern und Daten zu exfiltrieren — eine der effektivsten Techniken von Cyberkriminellen und staatlich unterstützten Bedrohungsakteuren. Da 71 % der Unternehmen dieses Risiko als besorgniserregend einstufen, wird die Netzwerksegmentierung oft als Lösung angesehen. Ihre Komplexität erschwert jedoch die Implementierung. Vielen Unternehmen fehlt es an qualifiziertem Personal, um die Segmentierung wirksam zu verwalten. Dies führt dazu, dass Projekte Monate in Anspruch nehmen oder ganz zum Stillstand kommen. Um diese Herausforderungen zu bewältigen, sollten Unternehmen auf Zero-Trust-Segmentierung setzen. Diese erzwingt die strikte Durchsetzung des Anwendungszugriffs nach dem Prinzip der minimalen Rechtevergabe und eliminiert laterale Bewegungspfade ohne den operativen Aufwand einer herkömmlichen Netzwerksegmentierung.



VPN-Zugriff für Drittuser bleibt ein wichtiger Bedrohungsvektor

Da 93 % der Befragten Bedenken hinsichtlich der Schwachstellen von VPNs von Drittanbietern äußern, kann davon ausgegangen werden, dass Angreifer auch weiterhin schwache externe Zugriffspunkte ins Visier nehmen. Gestohlene Anmeldedaten von Drittusern und falsch konfigurierte VPN-Zugänge gehören weiterhin zu den häufigsten Einstiegspunkten für Cyberkriminelle. Der Datendiebstahl bei der Enterprise Financial Group (EFG) im Jahr 2024 hat gezeigt, wie Angreifer VPN-Verbindungen für Drittuser ausnutzen, um in Unternehmensumgebungen einzudringen. Unternehmen haben häufig nur unzureichenden Einblick in die Zugriffsberechtigungen Dritter, was die Durchsetzung von Sicherheitsrichtlinien erschwert. Um diese Risiken zu mindern, müssen Unternehmen zu einem Zero-Trust-Framework übergehen, das einen strikten Zugriff nach dem Prinzip der minimalen Rechtevergabe und eine kontinuierliche Überprüfung aller externen Verbindungen durchsetzt.

KI-gestützte VPN-Exploits werden zunehmen

Die Zunahme KI-gestützter Cyberangriffe wird die VPN-Sicherheit in beispiellosem Ausmaß beeinträchtigen. Angreifer nutzen KI zunehmend für automatisierte Aufklärung, intelligentes Passwort-Spraying und die schnelle Entwicklung von Exploits, wodurch sie VPN-Anmeldedaten in großem Umfang kompromittieren können. KI-gestützte Umgehungstechniken erschweren es zusätzlich, VPN-basierte Angriffe zu erkennen, bevor erheblicher Schaden entsteht. Gleichzeitig können KI-gestützte VPN-Sicherheitslösungen zur Entstehung unvorhergesehener Sicherheitslücken führen und so neue Angriffsvektoren öffnen. Angesichts der zunehmenden KI-Bedrohungen müssen Unternehmen proaktive Sicherheitsmaßnahmen wie kontinuierliche Identitätsprüfung und Zero-Trust-Zugriffskontrollen ergreifen.

Schwerwiegende VPN-bezogene Sicherheitsverstöße werden Schlagzeilen machen

Nach mehreren spektakulären Sicherheitsverstößen im Jahr 2024 werden Unternehmen einem größeren Druck ausgesetzt sein, VPN-bezogene Cybervorfälle offenzulegen. Durch die neuen SEC-Vorschriften, die Transparenz in Bezug auf Cybersicherheitsrisiken vorschreiben, werden Unternehmen, die von VPN-Exploits betroffen sind, mit verstärkter behördlicher Kontrolle, Reputationsschäden und möglichen Geldstrafen konfrontiert sein. Da VPNs weiterhin als primärer Einstiegspunkt für Angriffe dienen, werden Unternehmen gezwungen sein, Legacy-Zugriffsmodelle zu überdenken. Dies wird die Umstellung auf Zero-Trust-Sicherheit weiter forcieren.

Investitionen in Zero Trust werden stark ansteigen

65 % der Unternehmen sind bereits dabei, ihre VPNs zu ersetzen, oder planen, dies innerhalb eines Jahres zu tun. Die Investitionen in Zero-Trust-Sicherheit nehmen zu und verändern den Markt für Remotezugriffsprodukte grundlegend. Aufgrund gesetzlicher Anforderungen und Vorschriften zur Cyber-Versicherung müssen Unternehmen von VPNs auf effektivere Alternativen umsteigen, da herkömmliche Lösungen die Anforderungen an Sicherheit, Skalierbarkeit und Compliance nicht mehr erfüllen. Die Umstellung auf Zero Trust reduziert nicht nur das Cyberrisiko, sondern eliminiert auch die hohen Kosten für die Wartung von VPN-Konzentratoren, Netzwerkgeräten und kontinuierlichen Patchzyklen. Infolgedessen werden VPNs zunehmend als veraltet wahrgenommen, was zu einer branchenweiten Verlagerung hin zu Zero-Trust-Sicherheitsmodellen führt.

Diese Prognosen unterstreichen einen wachsenden Konsens: Unternehmen, die die Einführung von Zero Trust verzögern, bleiben angesichts der zunehmenden Zahl von VPN-Exploits äußerst anfällig. Die Zukunft des sicheren Zugriffs hängt von einer proaktiven Risikominderung ab, nicht von reaktiven Patches. Jetzt ist es an der Zeit, über VPNs hinauszugehen.

Best Practices für sicheren Zugriff

Reduzieren Sie VPN-Risiken und stärken Sie die Zero-Trust-Sicherheit

1. **Entfernen Sie netzwerkbasierten Zugriff, um die Angriffsfläche zu minimieren.**
Verhindern Sie, dass Angreifer exponierte Netzwerkeintrittspunkte ausnutzen, indem Sie VPNs und netzwerkbasierten Zugriff durch direkte, anwendungsspezifische Konnektivität ersetzen. Umfragedaten zeigen, dass 54 % der Unternehmen Sicherheitsrisiken als größte VPN-Herausforderung nennen. Dies verdeutlicht die Notwendigkeit, VPN-Abhängigkeiten und Firewall-basierte Sicherheitsmodelle zu beseitigen, die Unternehmen Angriffen aussetzen.

2. **Verhindern Sie Angriffe durch Inline-Bedrohungsprävention.**
Überprüfen Sie den gesamten verschlüsselten und unverschlüsselten Datenverkehr inline, um Zero-Day-Exploits, Malware und Ransomware-Payloads zu blockieren, bevor sie die User erreichen. Da 92 % der Unternehmen befürchten, dass Ransomware VPN-Schwachstellen ausnutzt, sind Echtzeit-Trafficprüfungen und richtlinienbasierte Blockierungen unerlässlich. Ein Cloud-natives Sicherheitsmodell macht lokale Firewalls überflüssig und reduziert die Angriffsfläche.

3. **Verbessern Sie Authentifizierung und Identitätssicherheit.**
Implementieren Sie Phishing-resistente Multifaktor-Authentifizierung (MFA), beispielsweise mit FIDO2-Anmeldedaten, Biometrie oder Hardware-Token, um den Userzugriff zu verifizieren. Vermeiden Sie veraltete Authentifizierungsmethoden wie SMS-basierte MFA und Push-Benachrichtigungen, die von Angreifern häufig umgangen werden. Integrieren Sie identitätsbasierte Sicherheit mit kontinuierlicher Verifizierung, anstatt sich auf eine einmalige Authentifizierung zu verlassen.

4. **Erzwingen Sie mit ZTNA den kontextbasierten Zugriff nach dem Prinzip der minimalen Rechtevergabe.**
Ersetzen Sie den umfassenden VPN-Zugriff durch Zero Trust Network Access (ZTNA), um sicherzustellen, dass User nur Verbindungen zu autorisierten Anwendungen herstellen — niemals zum Netzwerk selbst. Granulare Just-in-Time-Zugriffskontrollen (JIT) basierend auf Identität, Gerätestatus und Echtzeit-Risikoanalyse stellen sicher, dass User ausschließlich bedarfsgerechten Direktzugriff auf einzelne Anwendungen erhalten.

5. **Eliminieren Sie laterale Bewegungen mit Zero-Trust-Segmentierung.**
Verbinden Sie User direkt mit Anwendungen, nicht mit dem Netzwerk. So verhindern Sie, dass Angreifer nach dem Erstzugriff systemübergreifend agieren können. Zero-Trust-Segmentierung und identitätsbasierte Mikrosegmentierung stellen sicher, dass Angreifer selbst nach erfolgreicher Kompromittierung eines Users nicht auf andere Ressourcen ausweichen oder ihre Berechtigungen erweitern können. ZTNA eliminiert VPN-Tunnel, die laterale Bewegungen ermöglichen.

6. **Sichern Sie den Zugriff von Dritt- und externen Usern mit identitätsbasierten Kontrollen.**
Setzen Sie den Zugriff nach dem Prinzip der minimalen Rechtevergabe für Drittuser, Geschäftspartner und Auftragnehmer durch strenge Sitzungskontrollen, Gerätezustandsprüfungen und kontinuierliche Überwachung durch. Der Ersatz des VPN-basierten Drittuserzugriffs durch ZTNA reduziert das Risiko kompromittierter Anmeldedaten erheblich — eine willkommene Nachricht für die 93 % der Unternehmen, die sich über die Risiken von Drittuser-VPNs Sorgen machen.

7. **Verbessern Sie die Data Protection mit integrierten Zero-Trust-Richtlinien.** Setzen Sie Inline-Kontrollen zur Datenverlustprävention (DLP) und Cloud Access Security Broker (CASB) ein, um den Traffic zu prüfen und zu verschlüsseln und unbefugte Datenbewegungen in Echtzeit zu verhindern. Ein Zero-Trust-Sicherheitsframework stellt sicher, dass der gesamte User-Traffic überprüft und kontrolliert wird, auch in SaaS-Anwendungen und Cloud-Umgebungen.

8. **Setzen Sie KI-gestützte Sicherheit und kontinuierliche Überwachung ein.** Nutzen Sie KI-gestützte Echtzeitanalysen, Deception Technology und automatisierte Verhaltenserkennung, um Bedrohungen zu stoppen, bevor sie eskalieren. ZTNA-Lösungen bieten eine Risikobewertung in Echtzeit und verhindern so, dass kompromittierte Konten auf vertrauliche Anwendungen zugreifen. Tägliche proaktive Bedrohungssuche und risikobasierte Zugriffskontrollen reduzieren die Auswirkungen von Sicherheitsverstößen erheblich.

9. **Bewerten und passen Sie Ihren Sicherheitsstatus kontinuierlich an.** Führen Sie automatisierte Risikobewertungen, Penetrationstests und Angriffssimulationen durch, um Zero-Trust-Sicherheitsrichtlinien dynamisch anzupassen. Fehlkonfigurationen und mangelnde Durchsetzung tragen maßgeblich zu schwerwiegenden Sicherheitsverstößen bei. Daher ist eine automatisierte, richtliniengesteuerte Durchsetzung zur Reduzierung menschlicher Fehler unerlässlich.

10. **Verzichten Sie auf VPN-Infrastrukturen und automatisieren Sie die Durchsetzung von Sicherheitsrichtlinien.** Mit einem cloudbasierten Zero-Trust-Modell sind VPN-Konzentratoren, Firewall-Regelverwaltung und manuelle Zugriffskontrolllisten nicht mehr nötig. ZTNA ermöglicht dynamische Sicherheitsrichtlinien, die sich in Echtzeit an Compliance-Änderungen, regulatorische Updates und neue Cyberbedrohungen anpassen — ohne manuelle Konfiguration oder Hardwareabhängigkeiten.

Durch die Implementierung dieser Best Practices können Unternehmen die Sicherheitsrisiken von VPNs mit einem robusten Zero-Trust-Sicherheitsframework eliminieren und so eine kontinuierliche Überprüfung, die Durchsetzung des Prinzips der minimalen Rechtevergabe und eine proaktive Bedrohungsminderung gewährleisten.

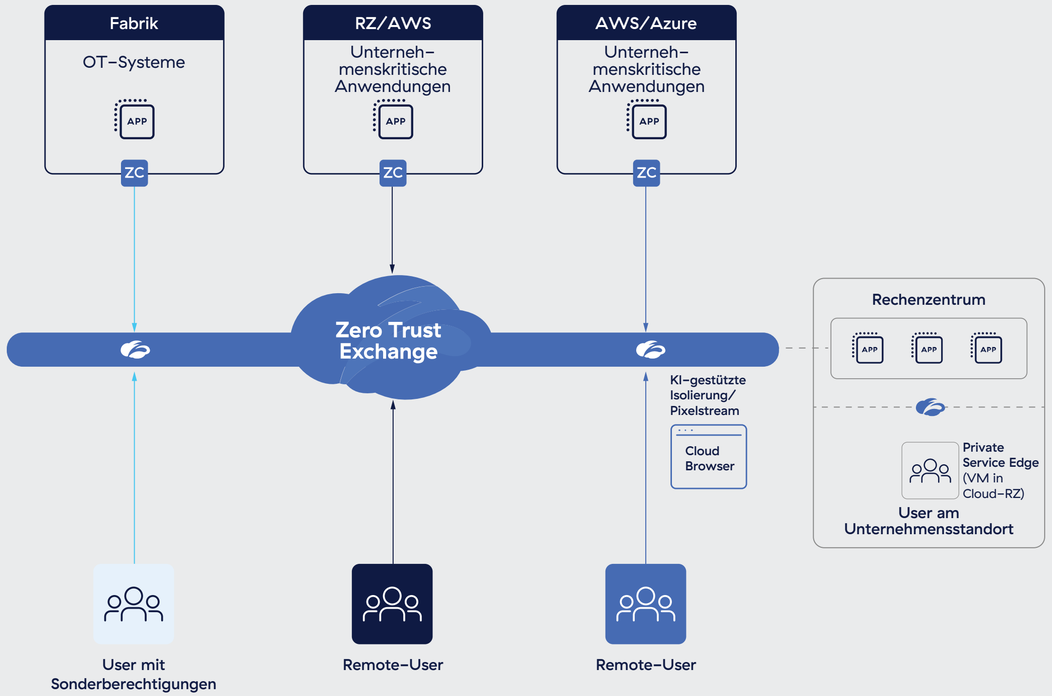
Wie Zscaler den sicheren Zugriff transformiert

Herkömmliche VPNs und Firewalls vergrößern die Angriffsfläche eines Unternehmens erheblich, indem sie User direkt im Netzwerk platzieren. Dieser umfassende Zugriff erleichtert es Angreifern, Schwachstellen auszunutzen, sich unbefugten Zugriff zu verschaffen und sich lateral innerhalb der Umgebung zu bewegen. Da sich die Bedrohungen ständig weiterentwickeln und hybrides Arbeiten zur Norm wird, führt das Vertrauen auf diese veralteten Technologien zu kritischen Sicherheitsrisiken.

Zscaler Private Access™ (ZPA) bietet eine sichere, skalierbare Alternative zu herkömmlichen Remote-Access-Lösungen wie VPNs. Als Cloud-native Lösung ermöglicht ZPA allen Usern Zero-Trust-Zugriff durch direkte Konnektivität zu privaten Unternehmensanwendungen. Um die Angriffsfläche zu minimieren, werden Anwendungen hinter der Zscaler Zero Trust Exchange™ unsichtbar gemacht. Dieser Ansatz verhindert laterale Bewegungen durch KI-gestützte Segmentierung einzelner Verbindungen und schützt durch integrierte Trafficprüfung sowie Anwendungsschutz und Data Protection vor komplexen Bedrohungen.

ZPA kann innerhalb weniger Stunden bereitgestellt werden und ersetzt Legacy-VPNs und Tools für den Remotezugriff durch eine ganzheitliche Zero-Trust-Plattform. ZPA wird von der weltweit größten Sicherheits-Cloud betrieben und bietet Usern überall auf der Welt schnelle, zuverlässige Konnektivität mit geringer Latenz. Die Cloud-native Architektur gewährleistet elastische Skalierbarkeit und unterstützt nahtlos die Anforderungen verteilter und hybrider Belegschaften in verschiedenen Regionen.

Mit ZPA können Unternehmen Cloud-First- und Hybridarbeit-Modelle mit der Gewissheit einführen, dass ihre Ressourcen geschützt, ihre User produktiv und ihre IT-Abläufe zukunftssicher sind.



Hauptvorteile von Zscaler Private Access (ZPA)

Minimieren Sie die Angriffsfläche zum Schutz vor Ransomware-Angriffen

VPN-Schwachstellen setzen Unternehmen dem Risiko des Missbrauchs durch böswillige User aus, was zu Ransomware-Angriffen und Diebstahl von Anmeldedaten führen kann. ZPA eliminiert dieses Risiko, indem alle Anwendungen hinter der Zero Trust Exchange verborgen werden und Usern direkter Zero Trust-Zugriff ausschließlich auf autorisierte Anwendungen gewährt wird. Indem ZPA verhindert, dass nicht autorisierte User, einschließlich Drittuser und Auftragnehmer, Anwendungen entdecken und sich lateral im Netzwerk bewegen, schützt es wirksam vor Ransomware-Angriffen. Es ermöglicht sicheren Remotezugriff auf alle Anwendungen, einschließlich privater Unternehmensanwendungen, netzwerkbasierter Anwendungen wie VoIP und Server-zu-Client-Apps. Darüber hinaus minimiert ZPA die Auswirkungen von Störungen durch eine umfassende Business-Continuity-Lösung und unterstützt Unternehmen dabei, strenge Compliance-Anforderungen zu erfüllen.

Keine laterale Ausbreitung von Bedrohungen

ZPA erzwingt Zugriff nach dem Prinzip der minimalen Rechtevergabe, indem User direkt mit bestimmten Anwendungen verbunden und so der Zugriff auf andere Anwendungen im Netzwerk verhindert wird. Durch visuelle Einblicke in den AnwendungszugriffKI-gestützte generiert automatisch Empfehlungen für App-Segmente und -Richtlinien. Dies vereinfacht die Implementierung der Segmentierung und gewährleistet gleichzeitig Skalierbarkeit und robuste Sicherheit.

Detaillierte Transparenz und Analysen: ZPA bietet detaillierte Echtzeit-Einblicke in Anwendungsnutzung, Userverhalten und Zugriffsmuster. IT-Fachkräfte können diese Daten nutzen, um potenzielle Bedrohungen zu überwachen, zu prüfen und schnell zu identifizieren und so den allgemeinen Sicherheitsstatus zu verbessern. Dadurch wird zugleich die Einhaltung aufsichtsrechtlicher Vorschriften gewährleistet.

Bieten Sie clientlosen Zugriff, um Schwachstellen durch Drittuser-Zugriff zu minimieren

ZPA Clientless Access vereinfacht den Zugriff durch Dritte, indem es Auftragnehmern und Geschäftspartnern ermöglicht, sich über jeden Browser sicher und ohne Client mit Anwendungen zu verbinden. ZPA Clientless Access isoliert nicht verwaltete Geräte vom Unternehmensnetzwerk, schützt vertrauliche Daten und ist in den Google Chrome Enterprise Browser integriert, um die BYOD-Sicherheit zu verbessern. Dieser zukunftsfähige Ansatz reduziert Kosten, minimiert die mit dem Drittuser-Zugriff verbundenen Risiken und macht die Abhängigkeit vom herkömmlichen VDI-Management überflüssig.

Keine kompromittierten privaten Anwendungen

ZPA minimiert das Risiko der Kompromittierung privater Unternehmensanwendungen und von Datenverlusten durch lückenlose Inline-Prüfung des gesamten Traffics von und zu privaten Unternehmensanwendungen. Robuste Funktionen zur Verhinderung von Datenverlusten sorgen dafür, dass vertrauliche Informationen geschützt bleiben, während unbefugter Zugriff blockiert wird. Indem ZPA Anwendungen vor dem öffentlichen Internet verbirgt und sichere User-zu-App-Verbindungen auf Basis von Zero-Trust-Prinzipien ermöglicht, reduziert es die Angriffsfläche, verhindert laterale Bewegungen und schützt vor Sicherheitsverstößen.

Vereinfachen Sie die Richtlinienverwaltung und beschleunigen Sie die Bereitstellung

ZPA rationalisiert den IT-Betrieb, indem es die Bereitstellung des Remotezugriffs, die Richtlinienverwaltung und die Segmentierung von Einzelverbindungen vereinfacht. Ehemals zeitaufwendige Aufgaben wie das Onboarding von Usern, das Patchen und Upgrades können jetzt in wenigen Minuten erledigt werden, was den IT-Aufwand erheblich reduziert. Durch zentrales Management und automatisierte Richtlinienempfehlungen ermöglicht ZPA IT-Fachkräften, die Effizienz zu steigern, die Komplexität zu minimieren und sich auf strategische Initiativen statt auf das Tagesgeschäft zu konzentrieren.

Erzwingen Sie eine Gerätestatus-basierte Zugriffskontrolle

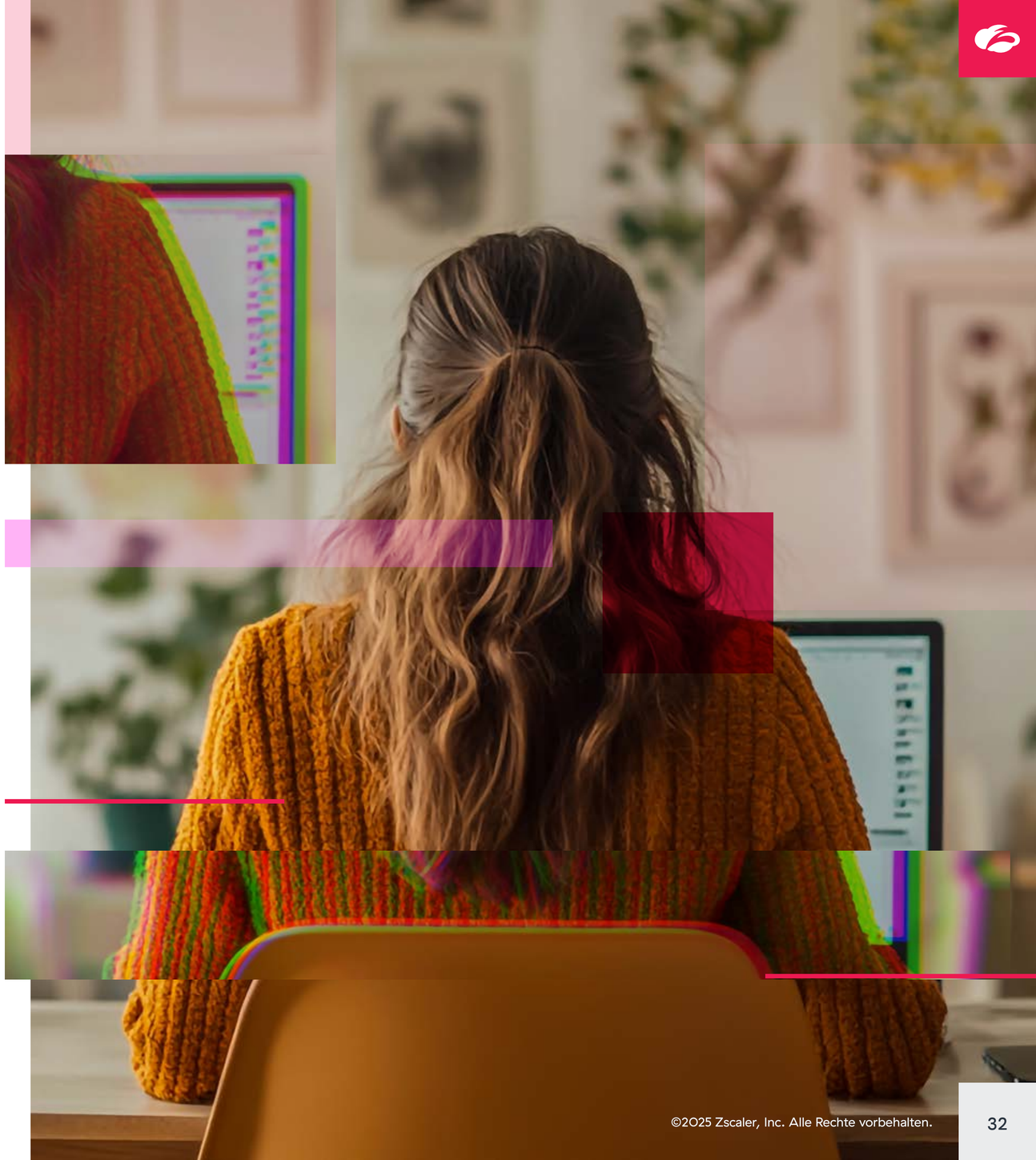
ZPA lässt sich in Tools zur Bewertung der Endgerätesicherheit integrieren, um den Sicherheitsstatus von Usergeräten zu überprüfen, bevor eine Zugriffsanfrage genehmigt wird. Dadurch wird sichergestellt, dass nur richtlinienkonforme Geräte eine Verbindung herstellen können. Entsprechend werden die Risiken durch nicht verwaltete oder kompromittierte Geräte gemindert.

Bereitstellung erstklassiger User Experience

ZPA gewährleistet optimale User Experience, indem es eine schnelle, nahtlose und sichere Konnektivität zu geschäftskritischen Anwendungen bereitstellt. Im Gegensatz zu VPNs, die den Traffic über ein zentrales Rechenzentrum zurückleiten, ermöglicht ZPA Direktverbindungen über die Zero Trust Exchange. Dadurch wird die Latenzzeit drastisch reduziert und die Anwendungsleistung verbessert, unabhängig davon, ob die User in der Unternehmenszentrale, an Remote-Standorten oder unterwegs auf Anwendungen zugreifen. Durch die Minimierung wiederholter Anmeldungen und der Abhängigkeit von clientbasierter Software vereinfacht ZPA den Zugriff und steigert die Produktivität. Darüber hinaus optimieren die proaktiven Überwachungsfunktionen von ZPA die Problemlösung und gewährleisten einen unterbrechungsfreien und qualitativ hochwertigen Zugriff für alle Uszer.

Niedrigere Gesamtbetriebskosten

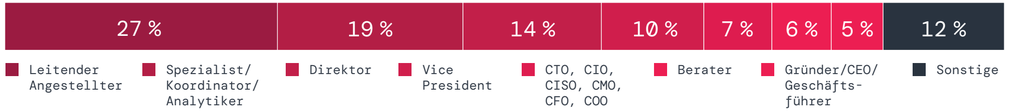
ZPA senkt die Gesamtbetriebskosten erheblich, da keine weiteren Einzelprodukte wie VPNs, Firewalls, NACs und VPN-Konzentratoren mehr erforderlich sind. ZPA basiert auf einer Cloud-nativen Zero-Trust-Architektur und eliminiert Infrastrukturkosten im Zusammenhang mit Hardware-Support, Wartung, Reparaturen und Updates. Die vereinfachte Verwaltung und die automatisierte Richtliniendurchsetzung reduzieren den Betriebsaufwand, sodass IT-Beauftragte Zeit und Ressourcen sparen und gleichzeitig die Sicherheit und Skalierbarkeit verbessern können.



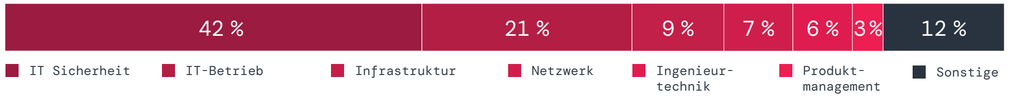
Methodik und demografische Daten

Dieser Bericht basiert auf einer umfassenden Umfrage unter 632 IT- und Cybersicherheitsexperten, die Anfang 2025 durchgeführt wurde und VPN-Sicherheitsrisiken, Trends beim Unternehmenszugriff und die Umstellung auf Zero-Trust-Architekturen untersuchte. Zu den Befragten zählten Führungskräfte, IT-Sicherheitsexperten und Verantwortliche für Netzwerkinfrastrukturen aus verschiedenen Branchen. Die Erkenntnisse in diesem Bericht liefern eine datenbasierte Perspektive auf den Rückgang von VPNs und die Umstellung auf Zero Trust und bieten wichtige Erkenntnisse für Unternehmen, die ihre Strategien im Bereich Zugriffssicherheit modernisieren wollen.

Position im Unternehmen

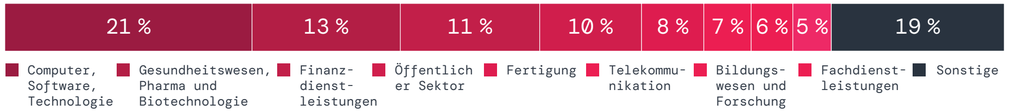


Abteilung



Firmengröße

Branche



Über Zscaler

Zscaler (NASDAQ: ZS) 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.com/de**

Über ThreatLabZ

ThreatLabz ist als Forschungsabteilung von Zscaler für die Früherkennung neuer Bedrohungen zuständig. Dieses erstklassige Team sorgt dafür, dass die Tausenden von Unternehmen, 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.com** veröffentlicht.

Über Cybersecurity Insiders

CYBERSECURITY INSIDERS — IHRE VERTRAUENSWÜRDIGE QUELLE FÜR DATENBASIERTE ERKENNTNISSE ZUR CYBERSICHERHEIT

Cybersecurity Insiders liefert beweisgestützte Erkenntnisse und Validierung durch Dritte und befähigt Führungskräfte im Bereich Cybersicherheit, fundierte, strategische Entscheidungen zu treffen. Auf der Basis von mehr als einem Jahrzehnt Forschung und einem globalen Netzwerk von über 600.000 Cybersicherheitsexperten liefern wir umsetzbare Informationen, die Führungskräfte dabei unterstützen, den Überblick über die dynamische Bedrohungslage zu behalten, neue Technologien zu bewerten und mit Zuversicht zukunftsweisende Strategien zu entwickeln.

Für Anbieter von Cybersicherheitslösungen verwandeln wir Forschungserkenntnisse in Ergebnisse. Wir schaffen Glaubwürdigkeit, Sichtbarkeit und Vertrauen durch wirkungsvolle Formate wie datenbasierte Marktberichte und Webinare, die eine Vordenkerrolle etablieren, CISO-Leitfäden, die Best Practices präsentieren, Produktbewertungen, die Lösungen validieren, praktische Anleitungen für Käufer, und Auszeichnungen, die den Markenruf stärken.

Durch die Kombination dieser Inhalte mit integrierter Verbreitung helfen wir Marken, Vertrauen zu gewinnen, den Bekanntheitsgrad zu steigern und im hart umkämpften Markt für Cybersicherheit die Nachfrage anzukurbeln.

Weitere Informationen: cybersecurity-insiders.com

Holger Schulze
CEO und Gründer
von Cybersecurity Insiders

zscaler™ | Zero Trust Everywhere

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt unzählige Kunden mit standortunabhängig sicheren Verbindungen zwischen Usern, Geräten und Anwendungen vor Cyberangriffen und Datenverlusten. Die in 150 Rechenzentren auf der ganzen Welt verfügbare SSE-basierte Zero Trust Exchange ist die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.com/de** oder folgen Sie uns auf Twitter**@zscaler**

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