zscaler™

VPN — Die potenzielle Hintertür in Ihr Unternehmensnetzwerk

Der aktuelle Report über VPN-Risiken 2023

Report zu VPN-Risiken 2023

Cybersecurity INSIDERS

Die VPN-Schwachstellen bergen enorme Risiken. 84 % der Unternehmen realisieren den Remotezugriff über VPN.

Ein Überblick.

Virtuelle private Netzwerke (VPNs) kommen traditionell als einfache Möglichkeit zur Bereitstellung von Remotezugriff zum Einsatz. Der massive Trend zu neuen dezentralen Arbeitsmodellen und Cloudbasierten Technologien überfordert jedoch die Kapazitäten dieser Konnektivitätslösung, die ursprünglich nur für ein begrenztes Spektrum vergleichsweise unkomplizierter Anwendungsfälle vorgesehen war. Angesichts der ständigen Weiterentwicklung der Bedrohungslage wächst auch der Druck auf Unternehmen, sicheren, segmentierten Remotezugriff auf unternehmenseigene Ressourcen zu gewährleisten. Das können VPNs nicht leisten. Stattdessen gewähren sie Anwender:innen häufig uneingeschränkten Zugang auf das gesamte Unternehmensnetzwerk. Dadurch steigt das Risiko von Cyberangriffen, da Cyberkriminelle, denen es gelingt, beispielsweise über gestohlene Anmeldedaten auf das VPN zuzugreifen, sich ungehindert im Netzwerk bewegen und Schaden anrichten können. Viele Unternehmen nutzen VPNs ebenfalls, um mehrere Unternehmensstandorte miteinander zu vernetzen, externen Dritten Zugriff auf IT-Ressourcen zu geben, nicht verwaltete Geräte zu unterstützen und IoT-Geräte ans Netzwerk anzubinden. Diese komplexen Anwendungsfälle beanspruchen VPNs weit über ihren ursprünglichen Zweck hinaus und führen zur Entstehung von Sicherheitslücken.

Für den Report zu VPN-Risiken wurden 382 Cybersicherheitsexperten interviewt. Ziel war es, die Herausforderungen von Unternehmen bei der Verwaltung von VPNs zu verstehen. Dabei ging es um Anfälligkeiten für Cyberbedrohungen, mögliche negative Auswirkungen auf die Nutzererfahrung und den allgemeinen Sicherheitsstatus. Neben den Risiken und Herausforderungen werden auch effektivere Alternativen zu VPN thematisiert. Der Report zeigt auf, warum Zero Trust sich zunehmend als überzeugende Lösung zur Gewährleistung sicherer und zügiger Unternehmenstransformationen etabliert.

DAS SAGEN DIE EXPERTEN: DIE WICHTIGSTEN ERKENNTNISSE AUS DER UMFRAGE IM ÜBERBLICK:

Sicherheitsrisiken und sicherheitsrelevante Folgen der VPN-Nutzung:
Trotz der weit verbreiteten Nutzung von VPNs zu geschäftskritischen Zwecken sind sich die befragten Unternehmen der damit verbundenen Sicherheitsrisiken bewusst. Insgesamt 88 % äußerten Bedenken – von „leicht“ bis „sehr stark“ – in Bezug auf eine potenzielle Gefährdung der IT-Umgebung durch VPNs. Immerhin 45 % gaben an, in den vergangenen 12 Monaten mindestens einen Angriff erlebt zu haben, bei dem VPN-Schwachstellen ausgenutzt wurden. Bei einem Drittel der Angriffe handelte es sich um Ransomware. Angesichts der wachsenden Bedrohung durch Cyberangriffe unter Ausnutzung von VPN-Schwachstellen besteht dringender Handlungsbedarf zur Verbesserung der Sicherheit aktueller VPN-Architekturen.

Beeinträchtigte User Experience durch VPN-Nutzung:
VPNs werden für unterschiedliche Anwendungsfälle eingesetzt, wobei die Bereitstellung von Remotezugriff für Mitarbeitende für die Mehrzahl der Unternehmen (84 %) im Vordergrund steht. Den Umfrageergebnissen zufolge sind jedoch 72 % der Anwender:innen mit dem aktuellen VPN-Angebot unzufrieden. Auch hier zeigt sich ein dringender Handlungsbedarf zur Gewährleistung benutzerfreundlicher undzuverlässiger Lösungen für den Remotezugriff, die den Anforderungen digital aufgestellter Unternehmen gerecht werden.

Im Jahr 2022 waren 50 % der Unternehmen von VPN-Angriffen betroffen.

VPNs als Angriffsvektoren: Im vergangenen Jahr waren 50 % der Unternehmen von VPN-Angriffen betroffen. VPNs, die im Geschäftsalltag und in der Kommunikation eine zentrale Rolle spielen, sind ein potenzielles Angriffsziel und erfordern besondere Vorsicht. Ein zusätzliches Risiko besteht darin, dass Angreifer über VPN-Zugänge für externe Nutzer (z. B. Auftragnehmer, Lieferanten) unberechtigten Zugriff auf das Firmennetzwerk erhalten können. Laut einer Umfrage sehen 90 % der Unternehmen dieses Risiko kritisch.

Umstellung auf Zero Trust: Viele Unternehmen priorisieren den Wechsel zu einem Zero-Trust-Modell. 90 % der Befragten gaben an, dass die Implementierung von Zero Trust im Fokus ihrer Planung steht. Schon 27 % setzen ein Zero-Trust-System um, während 37 % den Wechsel von VPN zu ZTNA-Lösungen (Zero Trust Network Access) in Erwägung ziehen.

Ein besonderer Dank geht an Zscaler für die Unterstützung bei der Erstellung dieses VPN Risiko-Reports 2023. Mit ihrer Expertise im Bereich Zero Trust und Zugriffsschutz haben sie maßgeblich zur Einordnung unserer Forschungsergebnisse beigetragen.

Mit den hier vorgestellten Erkenntnissen wollen wir IT-Fachkräften und Cybersicherheitsexpert:innen eine wertvolle Ressource an die Hand geben, die Sie bei der Umsetzung zuverlässiger Zero-Trust-Sicherheit unterstützen sollen.

Mit freundlichen Grüßen

Holger Schulze

Holger Schulze
CEO und Gründer
Cybersecurity Insiders

Cybersecurity
INSIDERS

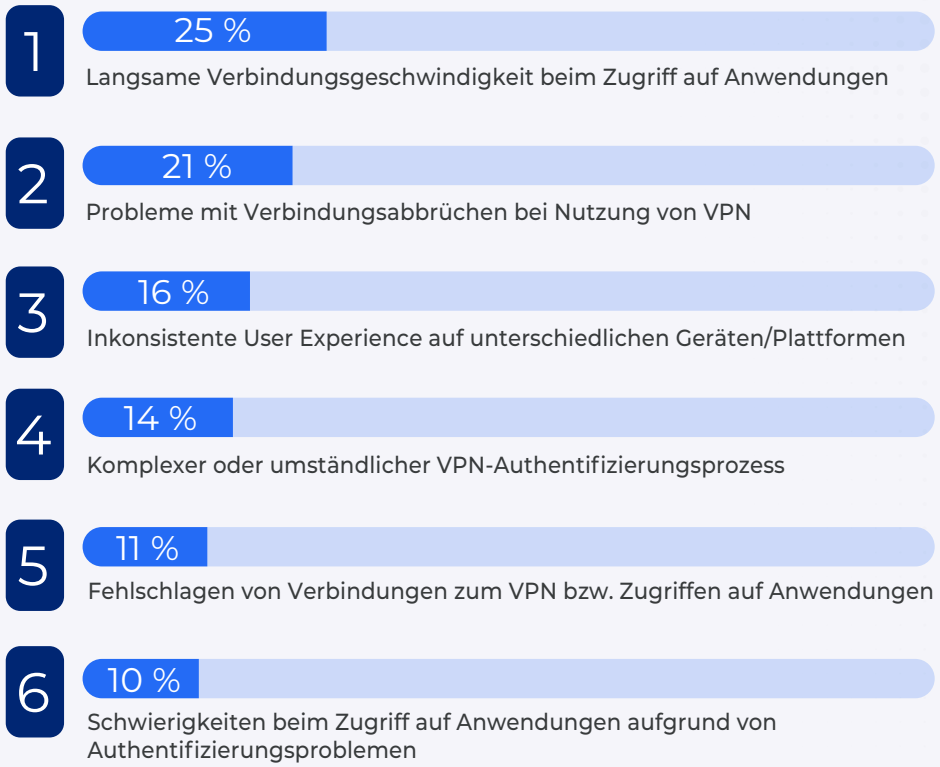
72 % der Anwender:innen sind mit dem VPN-Angebot insgesamt unzufrieden.

Auf die Frage, welche Probleme im Zusammenhang mit der VPN-Nutzung auftreten, nannten die Umfrageteilnehmer:innen am häufigsten die langsame Verbindungsgeschwindigkeit beim Zugriff auf Anwendungen (25 %). An zweiter und dritter Stelle folgten Probleme mit Verbindungsabbrüchen (21 %) sowie inkonsistente Anwendererfahrungen auf unterschiedlichen Geräten/Plattformen (16 %).

Diese Ergebnisse lassen keinen Zweifel daran, dass Unternehmen der Verbesserung der User Experience beim Remotezugriff hohe Priorität einräumen müssen. Unternehmen, die ihren Mitarbeitenden reibungslosen und zuverlässigen Zugriff auf IT-Ressourcen ermöglichen, steigern nicht nur die Produktivität, sondern in vielen Fällen auch die Sicherheit. Denn eine positive User Experience erhöht die Wahrscheinlichkeit, dass Sicherheitsrichtlinien tatsächlich eingehalten werden.

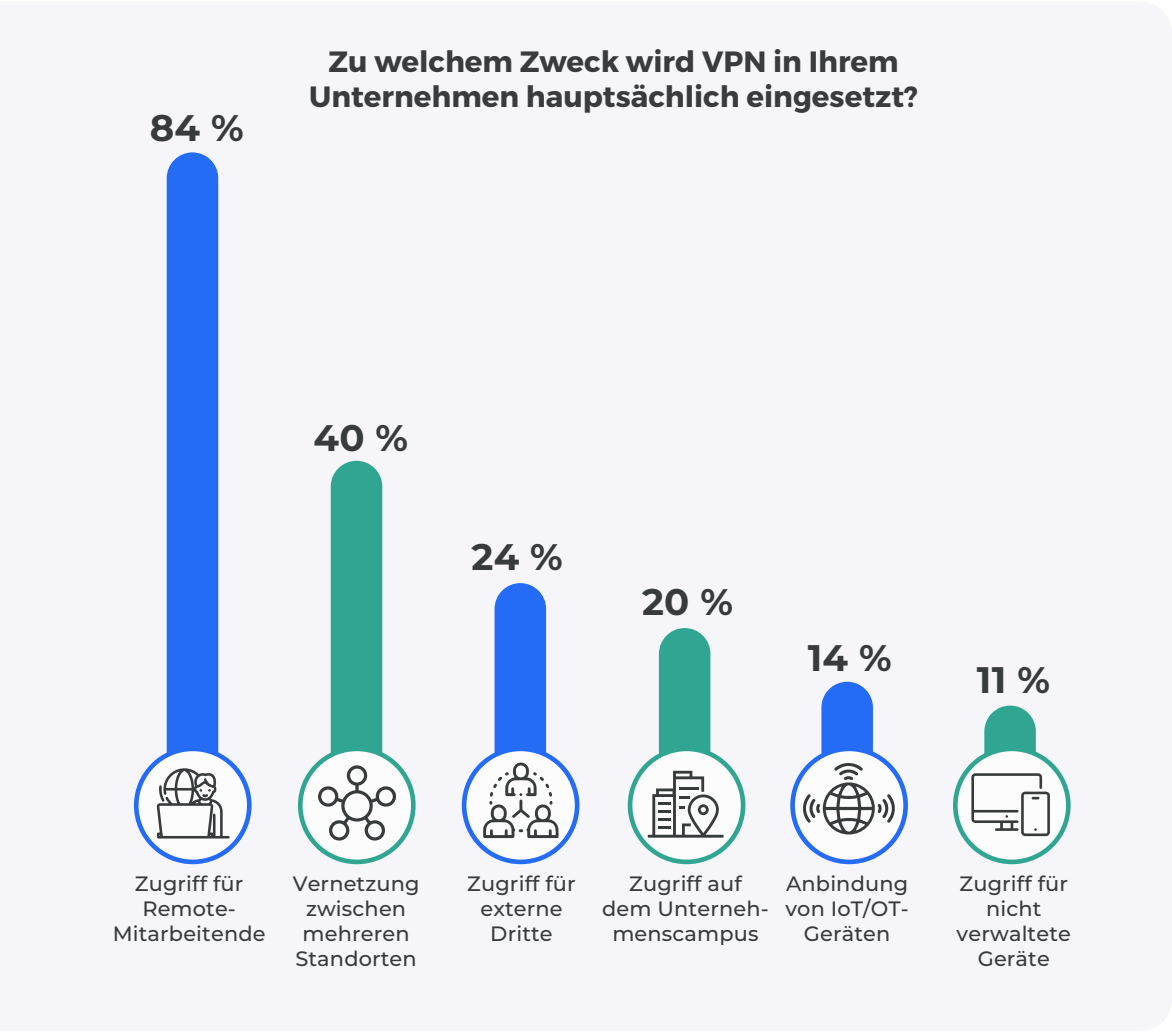
Verbesserungen lassen sich etwa durch Maßnahmen zur Optimierung der Netzwerkleistung erreichen, die die Wahrscheinlichkeit von geringen Verbindungsgeschwindigkeiten bzw. Verbindungsabbrüchen verringern. Auch eine Vereinfachung der Verfahren zur VPN-Authentifizierung sowie die Optimierung konsistenter Anwendererfahrungen auf unterschiedlichen Plattformen trägt dazu bei, dass die Zufriedenheit der User beim Arbeiten mit VPN zunimmt. Darüber hinaus empfiehlt sich die Einrichtung robuster Support-Mechanismen, die User bei der zügigen Behebung von Problemen im Zusammenhang mit der VPN-Nutzung unterstützen.

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



Sonstige 3 %

Remotezugriff für Mitarbeitende als vorrangiger Anwendungsfall für VPNs



Sonstige 3 %

VPNs werden traditionell vor allem zur Anbindung von Remote-Mitarbeitenden an das Unternehmens-netzwerk eingesetzt. Neben der Remote-Arbeit unter-stützen sie jedoch auch andere Anwendungsfälle, etwa zur Herstellung von Verbindungen für Drittuser (Kunden, Lieferanten etc.) oder, um mehrere Standorte des Unternehmens miteinander zu verbinden.

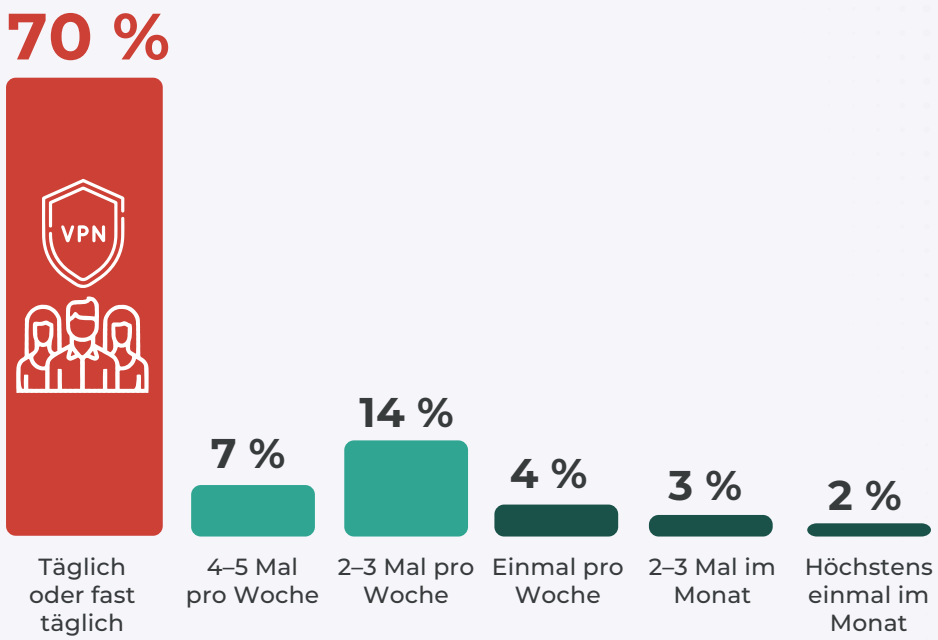
Entsprechend ergab auch unsere Umfrage, dass die große Mehrzahl der befragten Unternehmen (84 %) VPNs hauptsächlich zur Unterstützung des Zugriffs für Remote-Mitarbeitende einsetzt. Durch die deutliche Zunahme der Remote-Arbeit im Laufe der letzten Jahre dürfte daher auch die Nutzung von VPNs ange-stiegen sein. Ebenfalls erwähnenswert ist, dass nur 11 % der befragten Unternehmen VPNs zur Unterstützung des Zugriffs über nicht verwaltete Geräte einsetzen. Dieses Ergebnis deutet darauf hin, dass sich viele Unternehmen der damit verbundenen Sicherheits-risiken nicht unbedingt bewusst sind oder zumindest keine ausreichenden Maßnahmen zu ihrer Bewältigung ergreifen.

Hohe Abhängigkeit von VPNs für die tägliche Arbeit.

Mit 70 % gibt ein bemerkenswert hoher Prozentsatz von Endnutzer:innen an, täglich oder nahezu täglich VPNs für ihre Arbeit zu verwenden. Dies deutet klar auf eine intensive Abhängigkeit von dieser Technologie in den täglichen Geschäftsprozessen hin. Wenn man die Nutzer:innen berücksichtigt, die angeben, vier bis fünf Mal pro Woche VPNs zu nutzen, steigt der Anteil sogar auf 77 %. Das bedeutet, dass mehr als drei Viertel der Befragten fast jeden Tag auf die Nutzung von VPNs angewiesen sind. Ein weiterer bemerkenswerter Punkt ist, dass keiner der Teilnehmer:innen der Umfrage angab, nur einmal im Monat oder seltener VPNs zu nutzen. Dies unterstreicht die weit verbreitete Nutzung und Akzeptanz dieser Technologie in der Arbeitswelt.

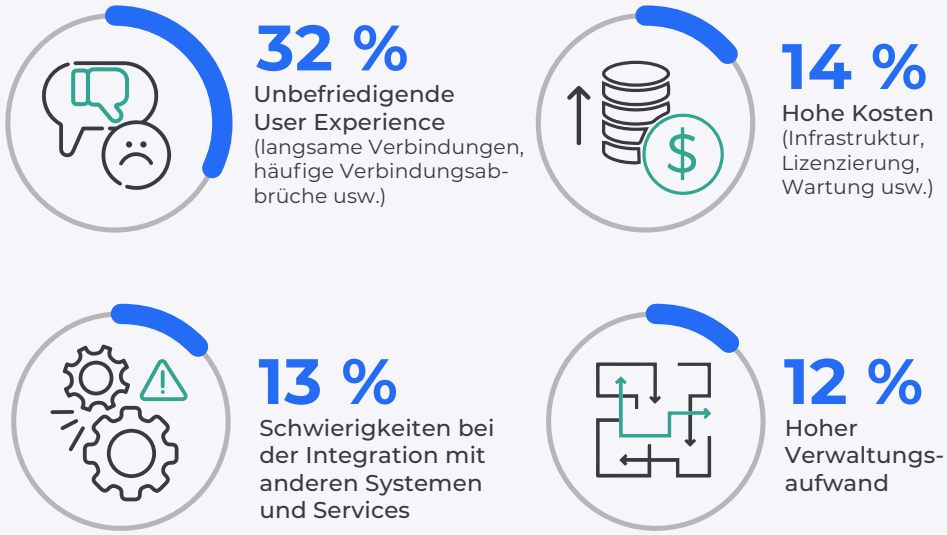
In Anbetracht dieser intensiven und regelmäßigen Nutzung von VPNs ist es von entscheidender Bedeutung, dass Remote-Access- und VPN-Dienste stets verfügbar und sicher sind. Sie sind ein wesentlicher Bestandteil für den störungsfreien Ablauf von Geschäftsprozessen und die Aufrechterhaltung der Produktivität in Unternehmen.

Wie oft verwenden Ihre Mitarbeitenden VPNs?



Empfindliche Störung des Geschäftsbetriebs.

Welche der genannten Optionen nehmen Sie als größten Nachteil Ihres aktuellen VPN-Services wahr?



Eingeschränkte Skalierbarkeit und Flexibilität 11 % | Unzureichende Sicherheit und Compliance 7 % | Keine ausreichende Unterstützung für Remote-Arbeit und virtuelle Zusammenarbeit 4 % | Sonstige 7 %

Die Performance und Qualität der User Experience vonVPN-Services hat erhebliche Auswirkungen auf die Produktivität der Unternehmen und die allgemeine betriebliche Effizienz. Langsame Verbindungsgeschwindigkeiten oder häufige Verbindungsabbrüche aufgrund von VPN-Nutzung können den Geschäftsbetrieb empfindlich stören und für Frust bei den Usern sorgen. Aus den Umfrageergebnissen geht hervor, dass unbefriedigende Anwendererfahrungen am häufigsten als Nachteil von VPNs wahrgenommen werden. 32 % der Befragten nannten langsame Verbindungsgeschwindigkeiten und dauernde Verbindungsabbrüche als Hauptprobleme in Bezug auf die VPN-Nutzung.

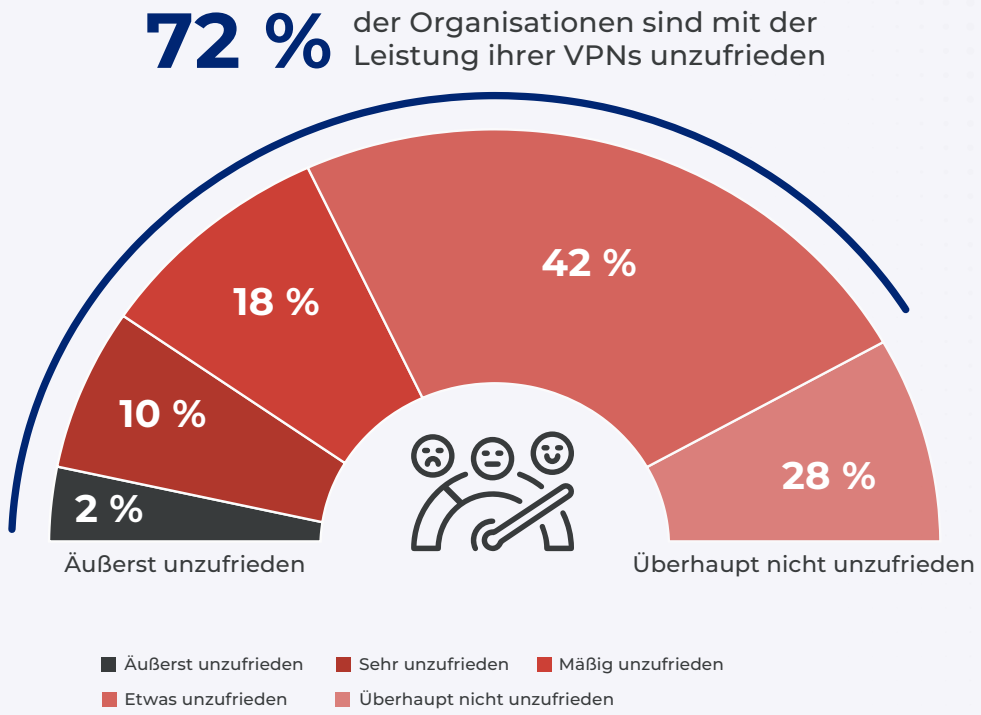
Angesichts dieser Ergebnisse sollten Unternehmen der Verbesserung ihrer Remote-Access-Lösungen in Bezug auf die User Experience hohe Priorität einräumen Erreichen lässt sich dies u. a. durch Erhöhung der Serverkapazität oder Umstellung auf sichere Zugriffslösungen, die mehr Geschwindigkeit und Stabilität gewährleisten. In diesem Zusammenhang ist ebenfalls erwähnenswert, dass Sicherheit relativ weit hinten unter den Hauptproblemen mit VPN rangierte – dabei waren viele der befragten Unternehmen im vergangenen Jahr mehrmals von VPN-bezogenen Angriffen betroffen.

VPNs sorgen für hohen Frust bei den Anwender:innen.

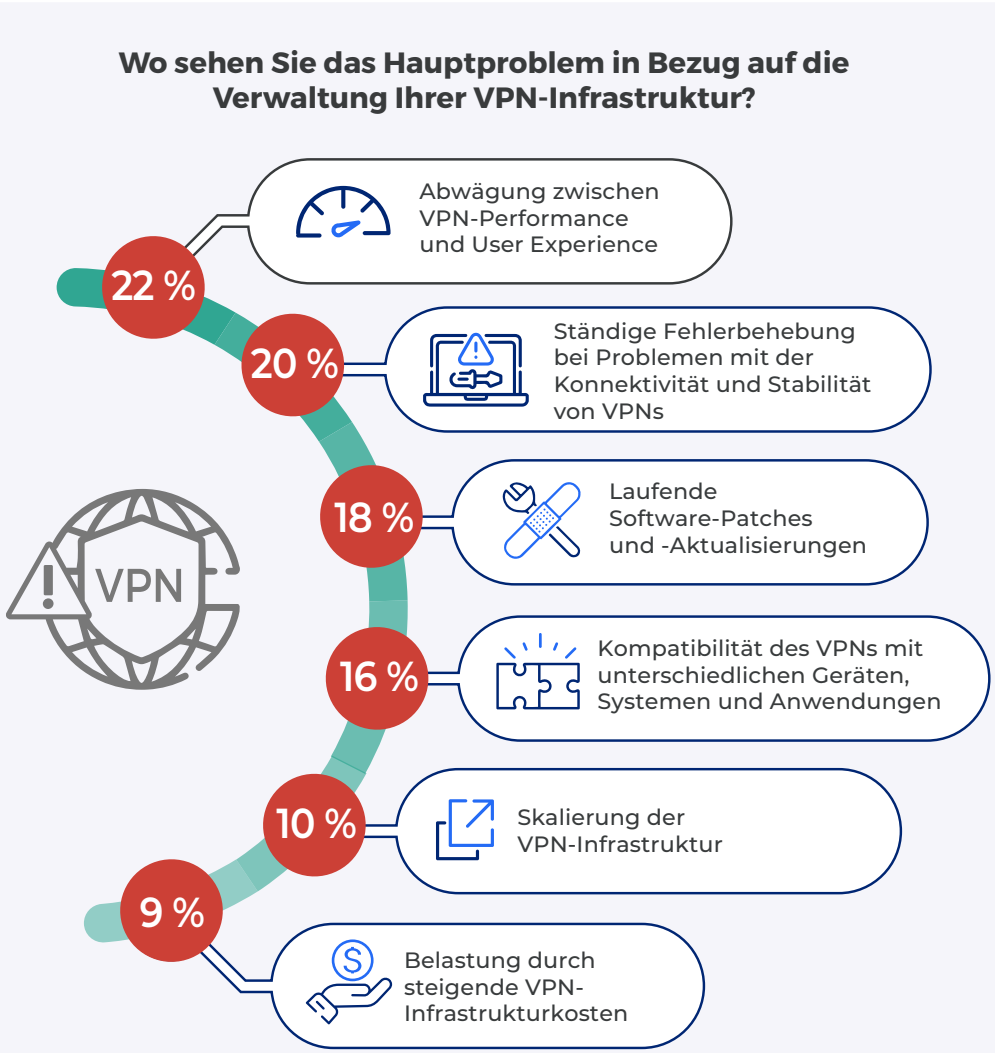
Die Zufriedenheit der Anwender:innen ist ein wichtiger Faktor, den Unternehmen auf keinen Fall ignorieren dürfen. Denn unbefriedigende Anwendererfahrungen sind nicht nur der Produktivität abträglich – sie können auch dazu führen, dass Sicherheitsrichtlinien nicht eingehalten werden, wodurch wiederum Sicherheitsrisiken entstehen.

Eine deutliche Mehrheit der Nutzer:innen (72 %) ist mit den aktuellen Zugriffsoptionen über VPN unzufrieden. Dies deutet darauf hin, dass Bedarf an benutzerfreundlicheren und zuverlässigeren Remote-Access-Lösungen zur Unterstützung digital aufgestellter Unternehmen besteht.

Wie schätzen Sie die Unzufriedenheit Ihrer Mitarbeitenden mit der Anwendererfahrung über VPN ein?



Probleme bei der Verwaltung von VPN: Performance vs. User Experience und ständige Fehlerbehebung



Sonstige 5 %

An erster Stelle unter den größten Herausforderungen im Umgang mit VPNs rangiert die Abwägung zwischen VPN-Performance und User Experience. 22 % der Befragten stuften diesen Aspekt als Hauptproblem bei der Verwaltung ihrer VPN-Infrastruktur ein.

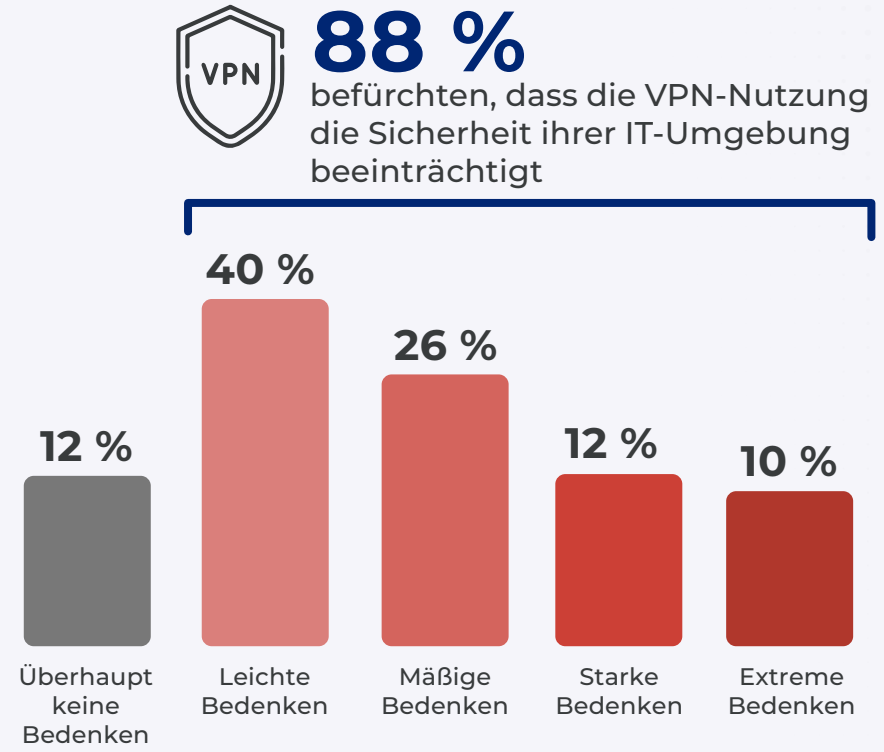
Die Fehlerbehebung bei Problemen mit der Konnektivität und Stabilität von VPNs wird ebenfalls als beträchtlicher Nachteil wahrgenommen und von knapp 20 % der Befragten als Hauptproblem bewertet. An dritter Stelle folgte der Aufwand durch laufende Software-Patches und -Aktualisierungen mit 18 %. Nur 9 % der Befragten nannten die Belastung durch steigende VPN-Infrastrukturkosten als Hauptproblem.

Potenzielle Sicherheitslücken führen zu Bedenken hinsichtlich der Sicherheit von VPNs

Cyberangriffe nehmen immer weiter zu und die Angriffe werden immer intelligenter. Angesichts einer zunehmend komplexen Bedrohungslage ist das Sicherheitsniveau der Remote-Access-Lösungen eine entscheidende Voraussetzung für den zuverlässigen Schutz vertraulicher Daten und Systeme. Je nachdem, wie gut sie konzipiert sind und verwaltet werden, können VPNs den Sicherheitsstatus eines Unternehmens entweder stärken oder gefährden.

Aus den Ergebnissen der Umfrage geht hervor, dass die überwältigende Mehrzahl der Teilnehmer:innen (88 %) befürchtet, dass die VPN-Nutzung die Sicherheit ihrer IT-Umgebung beeinträchtigt. Besonders hervorzuheben ist, dass insgesamt 22 % der Befragten „starke“ oder „sehr starke“ Bedenken im Hinblick auf VPNs als potenzielle Sicherheitslücken äußerten.

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

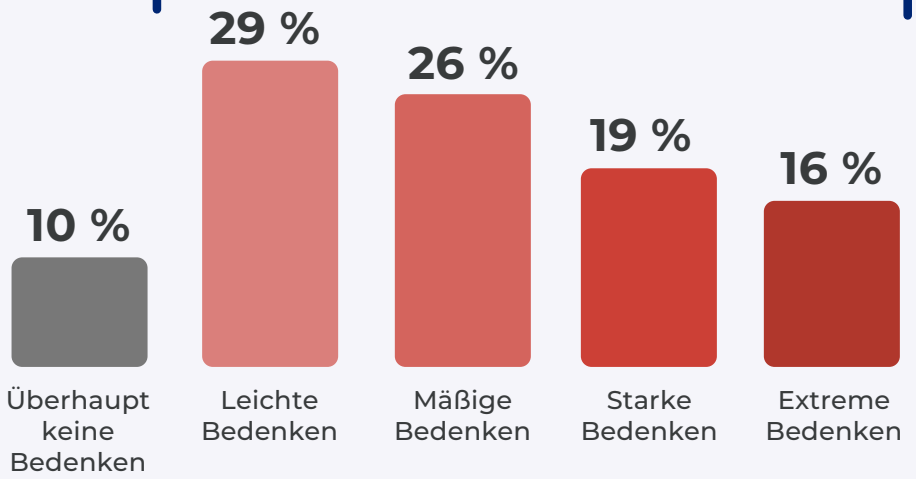


Hohe Sicherheitsbedenken in Bezug auf VPN-Zugriff für Drittuser

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

90 %

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



Um einen reibungslosen Geschäftsbetrieb zu gewährleisten, ist es manchmal notwendig, externen Nutzer:innen über ein VPN Zugang zu firmeninternen IT-Ressourcen zu ermöglichen. Dies birgt jedoch erhebliche Risiken. Vor allem, wenn diese externen Anbieter:innen nicht die gleichen hohen Cybersicherheitsstandards einhalten, können Sicherheitslücken entstehen. Diese könnten von Angreifer:innen genutzt werden, um heimlich ins Unternehmensnetzwerk einzudringen.

Eine überwältigende Mehrheit von 90 % der Befragten erkennt das Risiko, dass Cyberkriminelle über VPN-Zugänge für externe Nutzer:innen in das Netzwerk eindringen könnten. 35 % haben sogar „große“ bis „sehr große Bedenken“. Das zeigt deutlich, dass Sicherheitsexpert:innen dies als ernsthafte Bedrohung sehen.

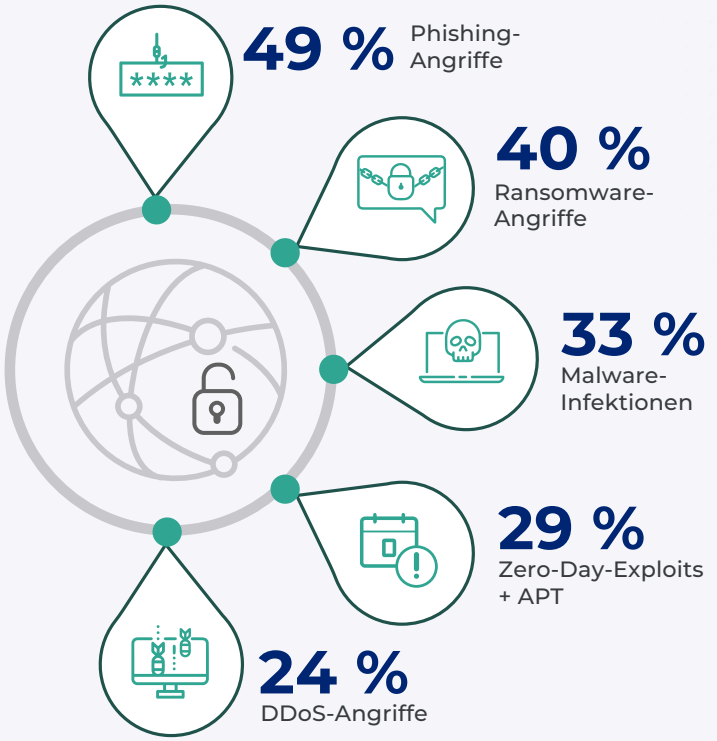
Zum Schutz sollten Unternehmen strikte Sicherheitsprotokolle für VPN-Zugänge externer Nutzer:innen implementieren. Dazu gehört die regelmäßige Kontrolle und Aktualisierung von Zugriffsrechten, die Einführung sicherer Passwortrichtlinien und die Überwachung des Netzwerks auf ungewöhnliche Aktivitäten. Externe Nutzer:innen sollten zudem verpflichtet werden, firmeneigene Cybersicherheitsrichtlinien einzuhalten. Weiteren Schutz bieten fortschrittliche Technologien wie Zero-Trust-Architekturen, die den Zugang streng nach dem Prinzip der minimalen Rechtevergabe durchsetzen.

Phishing-Angriffe werden als größte Gefahr wahrgenommen.

VPNs sind bekannt für ihre hohe Angriffsanfälligkeit, die ein ständiges Patchen erforderlich macht, um Sicherheitslücken und Schwachstellen in den Servern zu schließen.Entsprechend setzen Unternehmen sich durch ihre Nutzung erheblichen potenziellen Sicherheitsrisiken aus, zumal Cyberkriminelle zunehmend raffiniertere und kreativere Angriffstechniken entwickeln.

Nach Einschätzung der Umfrageteilnehmer:innen geht die Gefahr, dass VPN-Sicherheitslücken für Angriffe ausgenutzt werden, in erster Linie von Phishing-Angriffen (49 %) sowie Ransomware (40 %) aus. Bei diesen Angriffen geht es oft darum, Nutzer:innen durch Betrugsmaschen entweder zur Preisgabe vertraulicher Informationen oder zum Implementieren von Schadcode zu verleiten, der die Systeme der Unternehmen sperrt, bis das Angriffsopfer ein Lösegeld für ihre Freigabe zahlt.

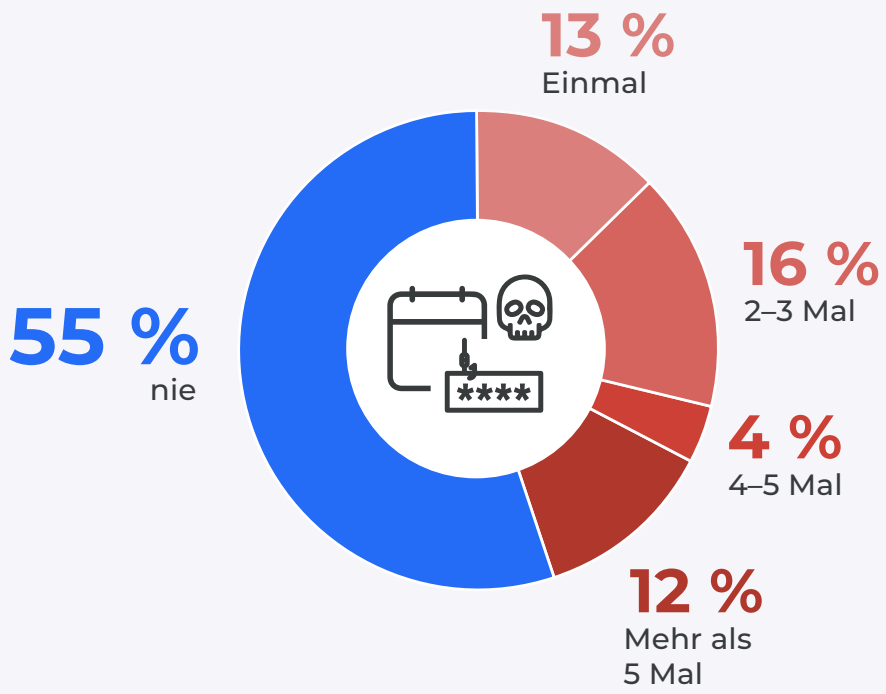
Von welchen Arten von Cyberangriffen geht Ihrer Meinung nach das höchste Risiko in Bezug auf die Ausnutzung von Sicherheitslücken im VPN Ihres Unternehmens aus?



Man-in-the-Middle-Angriffe 22 % | Unbefugte Rechteerhöhung 20 % | Angriffe mit Datenexfiltration 18 % | Brute-Force-Angriffe 11 % | Cross-Site Scripting 11% | Remote-Codeausführung 9 %

Jedes zweite Unternehmen war von Angriffen auf VPN-Server betroffen.

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



Die Sicherheit der VPN-Server ist eine wesentliche Voraussetzung für die Integrität und Vertraulichkeit der verarbeiteten Daten. Die zunehmende Abhängigkeit von VPNs für Remote-Arbeit macht sie zu einem um so attraktiveren Angriffsziel für Cyberkriminelle, die Schwachstellen und Sicherheitslücken geschickt und immer intelligenter auszunutzen wissen.

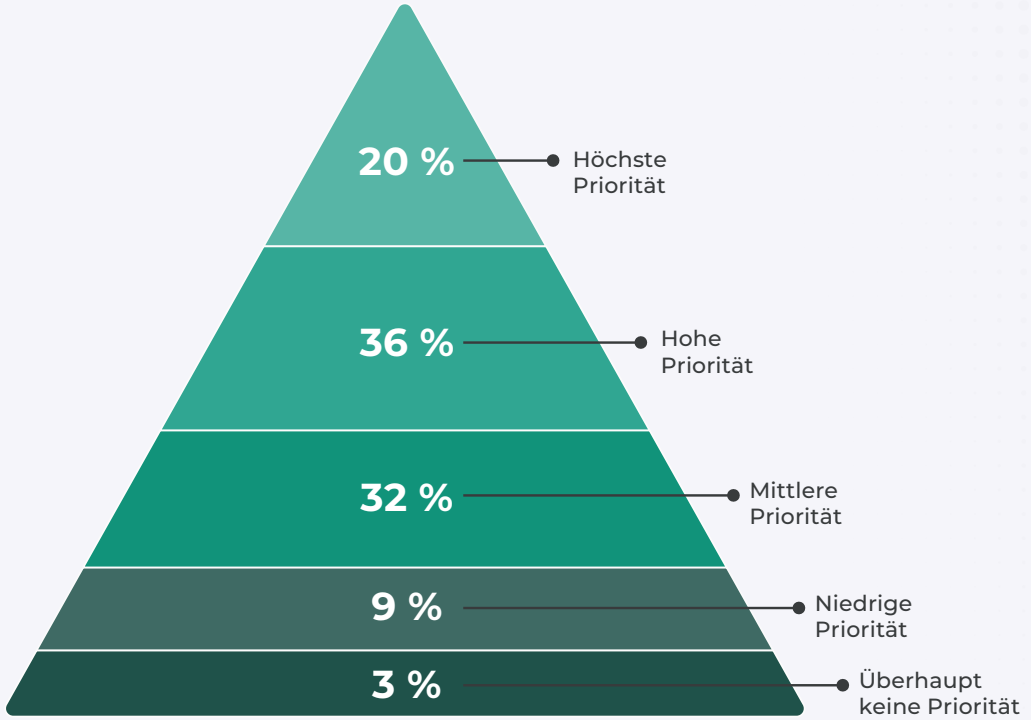
Und die Bedrohungslage verschgärft sich immer mehr. Fast die Hälfte der befragten Unternehmen (45 %) war in den vergangenen zwölf Monaten von einem oder mehreren Angriffen auf ihre VPN-Server unter Ausnutzung von Software-Sicherheitslücken betroffen. Diese Zahl zeigt eindeutig, dass ein dringender Bedarf an Remote-Access-Lösungen besteht, die mehr Sicherheit gewährleisten.

Minimale Rechtevergabe, mehr Sicherheit: Zero Trust wird bei Unternehmen als hohe Priorität eingestuft.

Neun von zehn der befragten Unternehmen stufen die Umstellung auf Zero Trust – ein Sicherheitskonzept, das auf dem Grundsatz „Niemals vertrauen, immer überprüfen“ aufbaut – als Priorität ein.

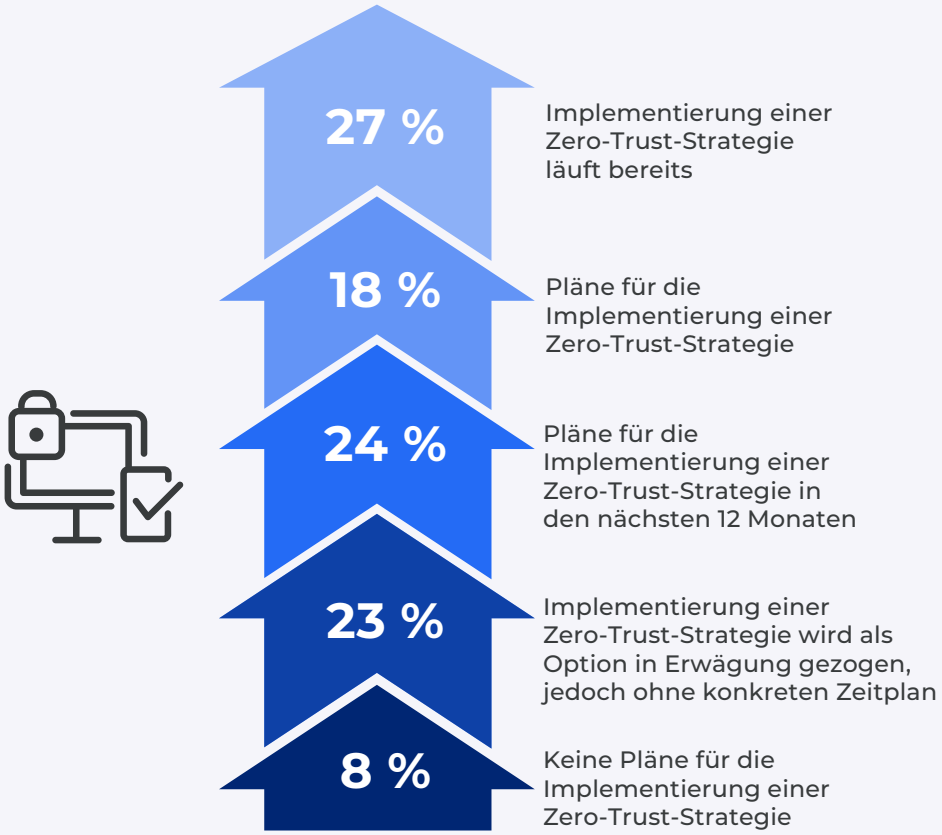
Damit Ihr Unternehmen von allen Vorteilen einer Zero-Trust-Architektur profitiert, sollten Sie Schlüsselelementen, die entscheidend zur Stärkung Ihres Sicherheitsstatus beitragen, absolute Priorität einräumen. Insbesondere betrifft dies eine starke Multifaktorauthentifizierung, kontinuierliche Überwachung des Netzwerks und Überprüfung des gesamten Traffics, Netzwerksegmentierung sowie eine minimale Rechtevergabe.

Welche Priorität hat die Umstellung auf eine Zero-Trust-Strategie für Ihr Unternehmen?



Bei mehr als zwei Drittel aller Unternehmen ist die Umstellung auf Zero Trust ist in vollem Gang

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



Insgesamt 92 % der befragten Unternehmen implementieren (27 %), planen (42 %) oder ziehen aktuell eine Zero-Trust-Strategie in Betracht. Daran zeigt sich der hohe Stellenwert und Bekanntheitsgrad des Konzepts in der heutigen Geschäftswelt. Zero Trust hat sich längst vom Modewort zur praxistauglichen VPN-Alternative entwickelt.

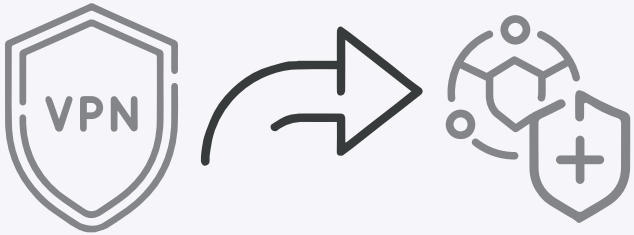
Unternehmen, die bislang keinen konkreten Zeitplan für die Implementierung festgelegt haben, sollten dies schleunigst in Angriff nehmen, um ihre Wettbewerbsfähigkeit und Sicherheit zu gewährleisten. Dies gilt erst recht für die Minderheit der befragten Unternehmen, die noch unentschlossen sind bzw. angaben, keine Umstellung auf Zero Trust zu planen.

Umstellung auf ZTNA oder ein Hybrid-Konzept: Die besseren Alternativen zu VPN.

Die Umstellung von VPN- auf ZTNA-Lösungen (Zero Trust Network Access) vollzieht sich vor dem Hintergrund eines Paradigmenwechsels im Cybersicherheitsdenken. Insbesondere den Grundsätzen der minimalen Rechtevergabe und der Mikrosegmentierung – beides essentielle Komponenten des ZTNA-Konzepts – kommt im Rahmen zukunftsfähiger Sicherheitsstrategien ein hoher Stellenwert zu. Vier von zehn befragten Unternehmen stellen aktuell auf ZTNA um und reagieren damit aktiv auf die Herausforderungen einer zunehmend dynamischen und unberechenbaren Bedrohungslage, die sich immer weiter verschärft.

Allen Unternehmen, die aktuell eine Umstellung planen oder zumindest in Erwägung ziehen, wird dringend empfohlen, bei der Bewertung und Auswahl geeigneter ZTNA-Lösungen ihre unternehmensspezifischen Sicherheits- und Geschäftsanforderungen in den Vordergrund zu stellen. Diejenigen, die derzeit keine Pläne für eine Umstellung auf ZTNA haben, sollten sich zumindest über die potenziellen Vorteile dieser Lösungen zur Verbesserung ihres Cybersicherheitsstatus informieren. Unternehmen, für die eine komplette Umstellung aus logistischen oder betriebswirtschaftlichen Erwägungen derzeit nicht in Frage kommt, könnten unter Umständen von einem Hybrid-Konzept profitieren, das die Vorteile von ZTNA mit der Option kombiniert, die vorhandene VPN-Infrastruktur weiterhin zu nutzen.

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



37 %

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

Best Practices für die Umstellung auf Zero Trust

Damit die Umstellung von einer herkömmlichen VPN-Infrastruktur auf eine zukunftsfähige Zero-Trust-Architektur möglichst reibungslos gelingt, empfehlen wir Ihnen, eine Reihe von Best-Practice-Hinweisen zu beachten:

Aktuelle Infrastruktur bewerten:

Beginnen Sie mit einer gründlichen Überprüfung Ihrer bisherigen VPN-Infrastruktur sowie der konkreten Probleme, mit denen Ihr Unternehmen zu kämpfen hat. Unsere Umfrage ergab, dass viele Unternehmen mit dem Ist-Zustand unzufrieden sind – 32 % berichteten über beeinträchtigte Anwendererfahrungen, 14 % über hohe Kosten.

Geeignete Lösung auswählen:

Bei der Suche nach der richtigen Zero-Trust-Lösung kommt es vor allem darauf an, Ihre konkreten Herausforderungen und Bedürfnisse zu kennen und zu berücksichtigen Mit einer Cloud-nativen, softwaredefinierten Lösung können Sie viele der häufigsten VPN-Probleme vermeiden, da sie die Verwaltung vereinfacht, die Kosten senkt und die User Experience beim Remotezugriff deutlich verbessert.

Minimale Rechtevergabe anwenden:

Ein Grundprinzip des Zero-Trust-Konzepts sieht vor, dass Zugriffsberechtigungen ausschließlich für Anwendungen vergeben werden, die der betreffende Mitarbeitende unbedingt zur Erledigung seiner rollenspezifischen Aufgaben benötigt.

Zukünftiges Wachstum einplanen:

Achten Sie darauf, eine skalierbare Lösung auszuwählen, die das weitere Wachstum Ihres Unternehmens unterstützt. Unsere Umfrage ergab, dass 11 % der Unternehmen die mangelnde Skalierbarkeit ihrer VPN-Lösungen als Problem wahrnehmen. Cloudbasierte Lösungen gewährleisten hochgradige Skalierbarkeit.

Sicherheitsrichtlinien regelmäßig überprüfen und aktualisieren:

Durch laufende Überprüfung und Aktualisierung Ihrer Sicherheitsrichtlinien leisten Sie einen entscheidenden Beitrag zur Aufrechterhaltung eines robusten Sicherheitsstatus.

Sicheren Zugriff für alle User bereitstellen:

Achten Sie darauf, eine Plattform auszuwählen, die alle Nutzer:innen unabhängig vom jeweiligen Standort und Gerät unterstützt. Die richtige Lösung sollte gleichermaßen sicheren Zugriff für Remote-Mitarbeitende, externe Drittuser und nicht verwaltete Geräte ermöglichen.

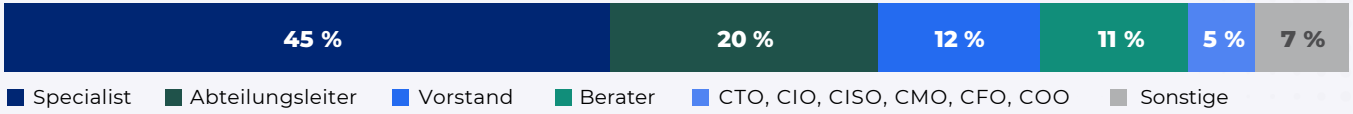
Kontinuierlich überwachen und optimieren:

Durch kontinuierliche Überwachung können Sie potenzielle Probleme erkennen und darauf reagieren, bevor sie eskalieren. Die proaktive Erkennung und Behebung von Problemen ist eine unverzichtbare Voraussetzung für eine starke Zero-Trust-Implementierung.

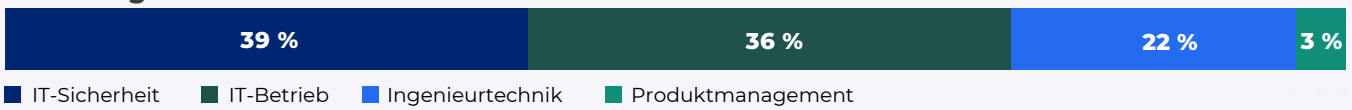
Methodik und demografische Daten

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

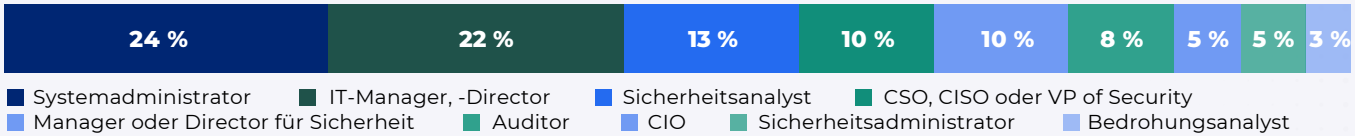
Position im Unternehmen



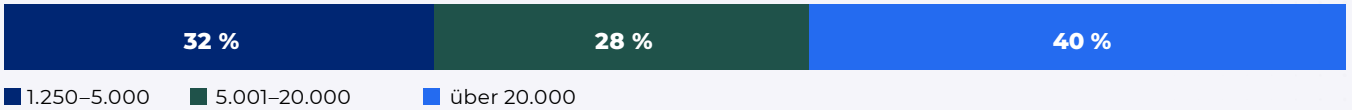
Abteilung



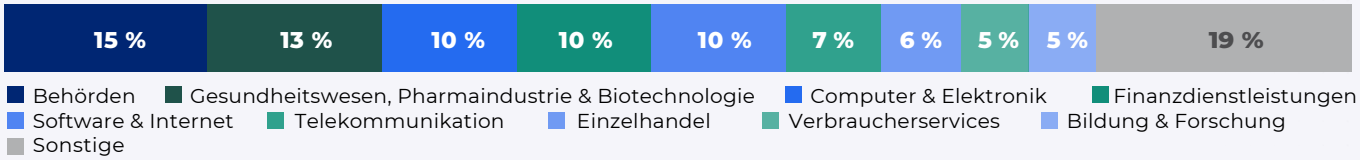
Primäre Funktion



Firmengröße



Industrie



Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange, die in 150 Rechenzentren auf der ganzen Welt verfügbar ist, ist die weltweit größte Inline-Cloud-Sicherheitsplattform.

Weitere Informationen finden Sie unter zscaler.de oder auf Twitter @zscaler.

zscaler.de

Cybersecurity
INSIDERS

Cybersecurity Insiders ist ein Zusammenschluss aus über 600.000 IT-Sicherheitsexpert:innen 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 Unternehmen bei der Stärkung von Nachfrage, Markenpräsenz und Innovationskraft unterstützen kann, um sich in einem wettbewerbsintensiven Markt erfolgreich zu positionieren.

Sie erreichen uns per E-Mail an **info@cybersecurity-insiders.com** oder im Internet unter **cybersecurity-insiders.com**