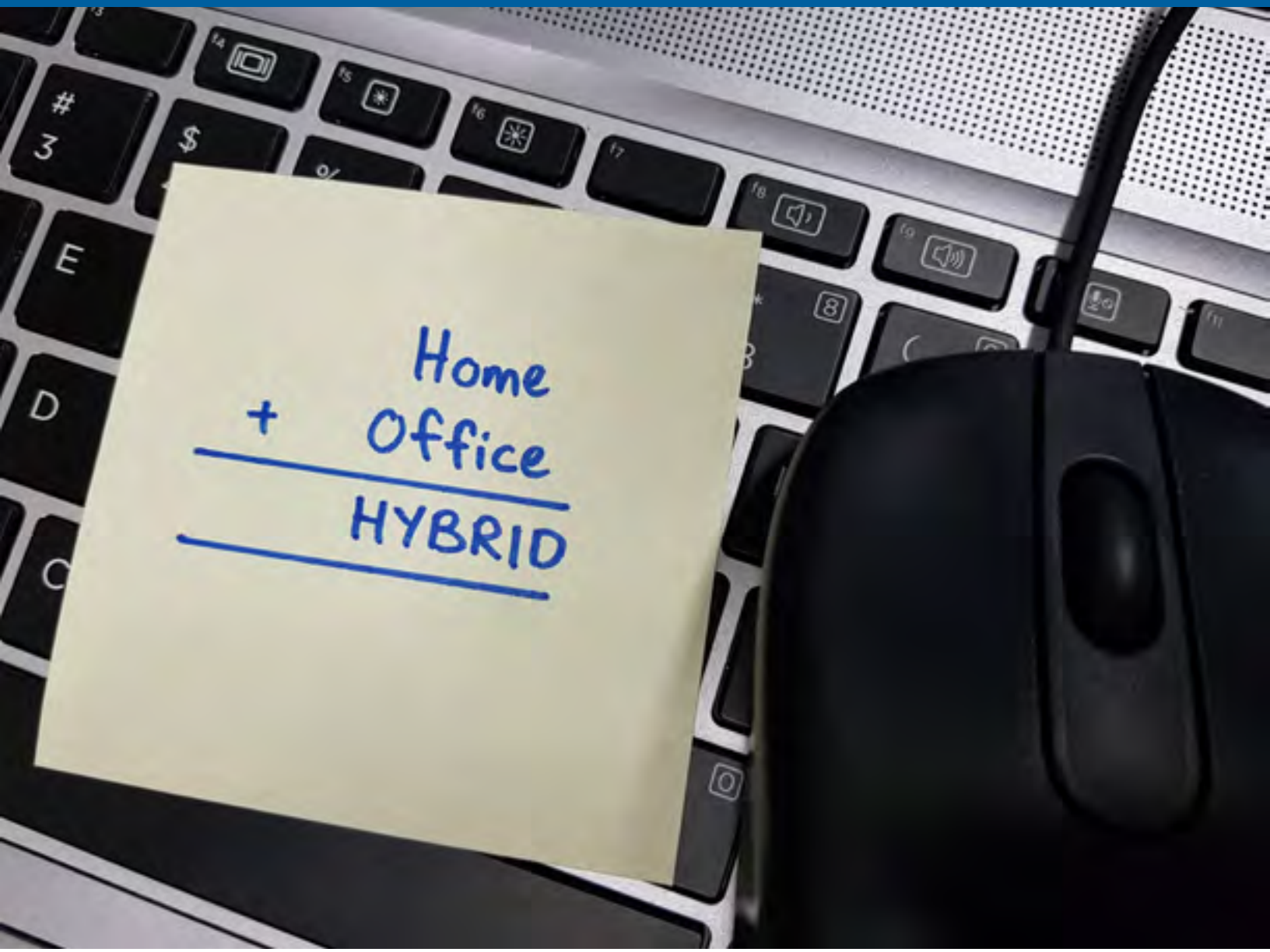
Zuverlässige Sicherheit für hybride Belegschaften mit Zero Trust

Tipps zum Einsatz von Zero Trust zur Gewährleistung eines höheren Schutzniveaus für hybride Arbeitskonzepte



EIN FORSCHUNGSBERICHT VON HMG STRATEGY MIT UNTERSTÜTZUNG VON ZSCALER

HMG STRATEGY

zscaler™

KURZFASSUNG

Die durch den Ausbruch der Corona-Pandemie im März 2020 bedingten schlagartigen Veränderungen stellten auch die CISOs und IT-Sicherheitsbeauftragten vieler Organisationen vor vollkommen neue Herausforderungen. Mit dem plötzlichen Umzug von Millionen von Arbeitnehmern ins Homeoffice wurde die Vorstellung eines klar definierten Netzwerkperimeters endgültig zur Makulatur.

Der Trend zur Remote-Arbeit hielt auch im weiteren Verlauf der Pandemie an – und rückte zunehmend die Unzulänglichkeiten vorhandener Netzwerkarchitekturen in den Blickpunkt, die keinen wirksamen Schutz für dezentrale Belegschaften mehr gewährleisten können. Parallel dazu beschleunigten zahlreiche Organisationen den Umzug ihrer Anwendungen vom Rechenzentrum in Cloud-Umgebungen und SaaS-Plattformen. Einer Studie von O'Reilly Media zufolge wollen 48 % der befragten Organisationen noch in diesem Jahr mindestens 50 % ihrer Anwendungen aus dem Rechenzentrum in die Cloud verlagern.[1]

Als zusätzlicher Risikofaktor im Zusammenhang mit der Umstellung auf hybride Arbeitskonzepte erweist sich der Zugriff auf Unternehmensressourcen über nicht verwaltete Privatgeräte, die von Usern im Homeoffice genutzt werden. Durch das Festhalten an Virtual Private Networks (VPNs) zur Bereitstellung des Remotezugriffs haben viele Organisationen ihre externe Angriffsfläche um ein Vielfaches vergrößert.

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

„Zu den wesentlichen Stärken des Zero-Trust-Ansatzes zählt die Möglichkeit, die Sicherheitskontrollen präzise auf die konkreten Risikofaktoren und Prioritäten des jeweiligen Anwendungsfalls abzustimmen", so **Lisa Lorenzin**, die als Field CTO bei Zscaler für die Region Nord- und Südamerika zuständig ist. *„Mit einer zukunftsfähigen Zero-Trust-Lösung ist hier ein hohes Maß an Abstraktion möglich. Statt zwischen Endgerät und Netzwerk können die Kontrollen inline zwischen einem User und der Anwendung platziert werden, mit der er verbunden wird."*

Im Zuge der weiteren Digitalisierung der Unternehmen sowie des damit einhergehenden Ausbaus ihrer digitalen Portfolios bildet eine Zero-Trust-Architektur die unverzichtbare Voraussetzung für den zuverlässigen und lückenlosen Schutz digitaler Geschäftsmodelle. **Entsprechend halten 61 % der CISOs und Sicherheitsbeauftragten das Zero-Trust-Sicherheitsmodell für einen effektiven Ansatz zur Absicherung ihres digitalen Ökosystems**, wie eine aktuelle Umfrage unter 118 Sicherheitsexperten von HMG Strategy und Zscaler ergab.

HMG Strategy hat in Zusammenarbeit mit Zscaler die Entwicklung der Bedrohungslage im Zuge der Umstellung zahlreicher Unternehmen auf hybride Arbeitskonzepte untersucht. Im Brennpunkt des Forschungsinteresses standen insbesondere die dadurch entstandenen kritischen Sicherheitsrisiken sowie die Vorteile und Chancen, die sich aus der Umstellung auf eine Zero-Trust-Architektur ergeben. Der Report liefert wertvolle Erkenntnisse zu folgenden Themen:

- Hauptrisiken und sicherheitsrelevante Herausforderungen im Zusammenhang mit der Umstellung auf hybride Arbeitskonzepte
- Nachteile bisher gängiger IT-Architekturen aus sicherheitstechnischer Sicht und daraus entstehende wirtschaftliche Verluste
- aktuelle Beispiele für Ransomware-Angriffe und Netzwerk-Sicherheitsverletzungen
- Argumente für eine möglichst schnelle Umstellung auf Zero Trust
- Praxisbeispiele für Unternehmen, die von einer erfolgreichen Umstellung auf Zero Trust profitieren
- Handlungsempfehlungen zur Implementierung einer Zero-Trust-Architektur zur Unterstützung hybrider Belegschaften

[1] *2021 Cloud Adoption Report, O'Reilly Media.*

Differenzierungsmerkmale des Zero-Trust-Konzepts

Welche der folgenden Definitionen trifft am besten auf Zero-Trust-Sicherheitsmodelle zu?

GRAFIK 1:

Zero Trust ist konzipiert als Framework für den Schutz digitaler Unternehmensressourcen in der zunehmend Cloud- und mobil-orientierten Geschäftswelt. Das Konzept beruht auf der Prämisse, dass kein User und keine Anwendung automatisch als vertrauenswürdig eingestuft werden darf, sowie der Überzeugung, dass der Netzwerkperimeter in der digitalen Welt keine Rolle mehr spielt.

52 %

Zero Trust ist ein Sicherheitskonzept, das auf der Überzeugung basiert, dass Organisationen nichts und niemanden – weder innerhalb noch außerhalb ihres Netzwerkperimeters – automatisch als vertrauenswürdig einstufen dürfen, sondern Verbindungen zu ihren Systemen erst nach gründlicher Überprüfung der jeweiligen Zugriffsanforderung herstellen sollten.

35,5 %

Niemand darf jemals als vertrauenswürdig eingestuft werden

12 %

Keine der genannten Optionen

0,5 %

Quelle: Understanding Zero Trust – Safeguarding the Hybrid Workforce; Studie von HMG Strategy/Zscaler basierend auf der Befragung von 118 CISOs und Sicherheitsbeauftragten

Zero Trust ist eine Cybersicherheitsstrategie unter Anwendung von Sicherheitsrichtlinien, die nicht auf inhärentem Vertrauen, sondern auf Kontext basieren. Dieser wird durch Zugangskontrollen mit minimaler Rechtevergabe und strenger User-Authentifizierung hergestellt. Durch eine optimal konfigurierte Zero-Trust-Architektur lässt sich die Netzwerkinfrastruktur vereinfachen, die User Experience verbessern und zuverlässigerer Schutz vor Cyberbedrohungen gewährleisten.

„Zu den wesentlichen Stärken des Zero-Trust-Ansatzes zählt die Möglichkeit, die Sicherheitskontrollen präzise auf die konkreten Risikofaktoren und Prioritäten des jeweiligen Anwendungsfalls abzustimmen.“

LISA LORENZIN
Field CTO, Nord- und Südamerika
Zscaler

Sicherheitsrelevante Herausforderungen hybrider Arbeitskonzepte und Hinweise zu ihrer Bewältigung

Der Trend zur Remote-Arbeit – mitsamt den Sicherheitsrisiken, die sich aus dem Zugriff über ungeschützte Heimnetzwerke und nicht verwaltete Privatgeräte ergeben – ließ sich bereits Jahre vor der Pandemie beobachten. Die drastischen Veränderungen, die im März 2020 die gesamte Wirtschaftswelt erschütterten, führten jedoch quasi von einem Tag zum nächsten zur massiven Beschleunigung der Digitalisierung – und damit zur Vervielfachung von Angriffsflächen und Sicherheitslücken.

Die Mitarbeiter haben oft wenig Ahnung von Netzwerksicherheit und machen sich kaum Gedanken darüber, wie sie sich selbst – geschweige denn vertrauliche Kundendaten und Geschäftsinformationen – effektiv schützen können. Stattdessen gehen sie davon aus, dass die unternehmenseigenen Firewalls und VPNs sichere Verbindungen zu Services und Ressourcen im Unternehmensnetzwerk gewährleisten. Dabei ist ihnen oft gar nicht bewusst, dass perimeterbasierte Sicherheitslösungen unter heutigen Vorzeichen keinen ausreichenden Schutz mehr bieten können.

Obwohl viele Organisationen ihre Mitarbeiter mittlerweile durch Simulationen für die Anzeichen und Risiken eines Phishing-Angriffs sensibilisieren, kommt es immer noch allzu häufig zu Sicherheitsverletzungen, die durch die Gutgläubigkeit einzelner User verursacht werden. Entsprechend befürchten 72 % der befragten CISOs und Sicherheitsbeauftragten, dass VPNs die Fähigkeit der IT beeinträchtigen, ihre Umgebungen effektiv zu schützen, wie der 2021 von Zscaler veröffentlichte Report zu VPN-Risiken zeigte.

Sicherheitsrisiken beim Einsatz von VPNs

Organisationen, die zum Schutz von Mitarbeitern und vertraulichen Unternehmensdaten auch weiterhin auf VPNs setzen, setzen sich dadurch einer Reihe zusätzlicher Sicherheitsrisiken aus.

Lorenzin weist insbesondere auf drei gravierende Nachteile von VPNs hin:

1. Jedes VPN-Gateway verfügt über eine Ereignisbehandlungsroutine für eingehende Verbindungen, die es als Angriffsfläche exponiert.
2. Das VPN-Gateway fungiert dann als Ausgangspunkt für komplexere Angriffe von Hackern.
3. VPNs sind standardmäßig offen konzipiert. Um zu verhindern, dass Mitarbeiter auf Anwendungen und Systeme zugreifen können, für die sie keine Berechtigungen haben bzw. haben sollten, müssen Sicherheitsbeauftragte sie explizit aussperren.

So wurde der verheerende Cyberangriff auf Colonial Pipeline im Mai 2021 über ein Legacy-VPN ohne Multifaktorauthentifizierung für User initiiert. Der Angriff veranschaulichte exemplarisch, wie viel Schaden Cyberkriminelle durch laterale Bewegungen innerhalb des Netzwerks einer Organisation anrichten können. Den Angreifern gelang es, sich mithilfe gestohlener VPN-Anmeldedaten Zugang zum Netzwerk von Colonial Pipeline zu verschaffen. Anschließend nutzten sie die ungehinderte laterale Bewegungsfreiheit innerhalb des Netzwerks aus, um auf geschäftskritische Finanzanwendungen zuzugreifen und vertrauliche Daten zu exfiltrieren, für die sie dann ein Lösegeld forderten.

Der Angriff führte zur Unterbrechung der Kraftstoffversorgung für einen Großteil der Ostküste und Südstaaten der USA und zwang das Unternehmen zur Zahlung eines Lösegelds in Höhe von 4,4 Mio. USD in Bitcoin.

Der Essener Chemiekonzern Brenntag zahlte nach einem erfolgreichen Angriff auf seine nordamerikanische Tochter ein Lösegeld in gleicher Höhe an die Ransomware-Gruppe Darkside, um verschlüsselte Geräte und gestohlene unverschlüsselte Daten freizukaufen.

Laut einer Studie von Accenture namens „The Cost of Cybercrime“ richten sich 57 % aller Cyberangriffe gegen Privatunternehmen aller Größen und Branchen. Die durchschnittliche Anzahl der Angriffe pro Unternehmen schoss 2021 um 31 % gegenüber dem Vorjahr in die Höhe, wie der Accenture-Report „How Aligning Security and the Business Creates Cyber Resilience“ zum aktuellen Stand der Cyberresilienz zeigte. Die durchschnittlichen Kosten einer Sicherheitsverletzung – einschließlich Geschäftsausfälle, Lösegeldzahlungen sowie die Kosten für Behebungsmaßnahmen, rechtliche Konsequenzen usw. – beziffert der Report auf 3,86 Mio. USD.

Umstieg auf eine effektivere und kostensparende Alternative

Abhilfe schafft hier die Umstellung auf eine Zero-Trust-Architektur, die dem Unternehmen zahlreiche Vorteile bietet. Neben zuverlässigem Schutz vor Sicherheitsverletzungen sorgt das Zero-Trust-Modell für weniger Komplexität und IT-Aufwand bei optimierter User Experience und minimaler Angriffsfläche.

Sanmina zählt zu den weltweit führenden Fertigungsdienstleistern für elektronische Komponenten und Komplettsysteme. Im Zuge der Cloud-Transformation zur Unterstützung zukunftsfähiger Smart-Factory-Initiativen hatte der Konzern bereits die teilweise Umstellung auf Zero-Trust-Grundsätze sowie den entsprechenden Umbau der IT-Architektur in Angriff genommen. Den Sicherheitsexperten von Sanmina wurde jedoch sehr bald klar, dass sich der Umstieg nicht mit herkömmlicher VPN-Technologie bewältigen ließ.

„Wir brauchten eine geeignete Zugriffslösung zur Absicherung zukunftsfähiger perimeterloser IT-Umgebungen“, erläutert **Matt Ramberg**, Vice President of Information Security bei Sanmina.

Wie viele andere Unternehmen stellte Sanmina im Zuge der COVID-19-Pandemie mit seinen 35.000 Mitarbeitern auf Remote-Arbeit um. Damit wurde die Zero-Trust-Transformation zur Priorität, um einer zunehmend mobilen und dezentralen Belegschaft sicheren Zugriff auf Unternehmensressourcen zu ermöglichen.

„Tag für Tag arbeiten bei uns mehrere Tausend User an Remote-Standorten und müssen von dort aus auf Zehntausende von IT-Ressourcen zugreifen“, berichtet Ramberg. *„Der Einsatz von VPNs war einfach nicht mehr zeitgemäß, sondern erhöhte sogar die Cybersicherheitsrisiken durch Entstehung zusätzlicher Angriffsflächen.“*

Sanmina prüfte mehrere Optionen und entschied sich letztlich, den Funktionsumfang der Zscaler Zero Trust Exchange™ durch Einsatz von Zscaler Private Access™ (ZPA) zu erweitern.

Als Grundbaustein der Zero Trust Exchange verbindet ZPA User und Geräte direkt mit der jeweils angeforderten Anwendung, anstatt ihnen Zugang zum Netzwerk zu gewähren. Im Unterschied zu Firewalls und VPNs[2] verhindert die Zero Trust Exchange die Entstehung von Hintertüren, über die Bedrohungen ins Unternehmensnetzwerk eindringen können. Stattdessen sind User und Anwendungen für externe Angreifer unsichtbar. Die laterale Ausbreitung von Bedrohungen innerhalb des Netzwerks wird durch die Einschränkung des User-Zugriffs auf die jeweils benötigten Anwendungen ebenfalls blockiert.

> ***„Wir brauchten eine geeignete Zugriffslösung zur Absicherung zukunftsfähiger perimeterloser IT-Umgebungen.“***
>
> **MATT RAMBERG**
> *Vice President of Information Security*
> **Sanmina**

[2] *Perimeter-Firewalls: Fünf Hauptrisiken und eine überzeugende Alternative – Zscaler*

Für Sanmina hat sich die Investition in die Zero Trust Exchange bereits in mehrfacher Hinsicht ausgezahlt. Die Plattform stellt den Cybersicherheitsexperten des Unternehmens effektive Funktionen zur granularen Kontrolle und Absicherung des gesamten Traffics zwischen Usern und Anwendungen bereit, die weit über die Kapazitäten von VPNs hinausgehen. Zugleich werden interne Anwendungen zuverlässig vor Sicherheitsrisiken geschützt.

Zusätzlich profitieren die User standortunabhängig von schnelleren nahtlosen Verbindungen zu öffentlichen und privat gehosteten Unternehmensanwendungen, als dies mit Firewalls und VPNs möglich war.

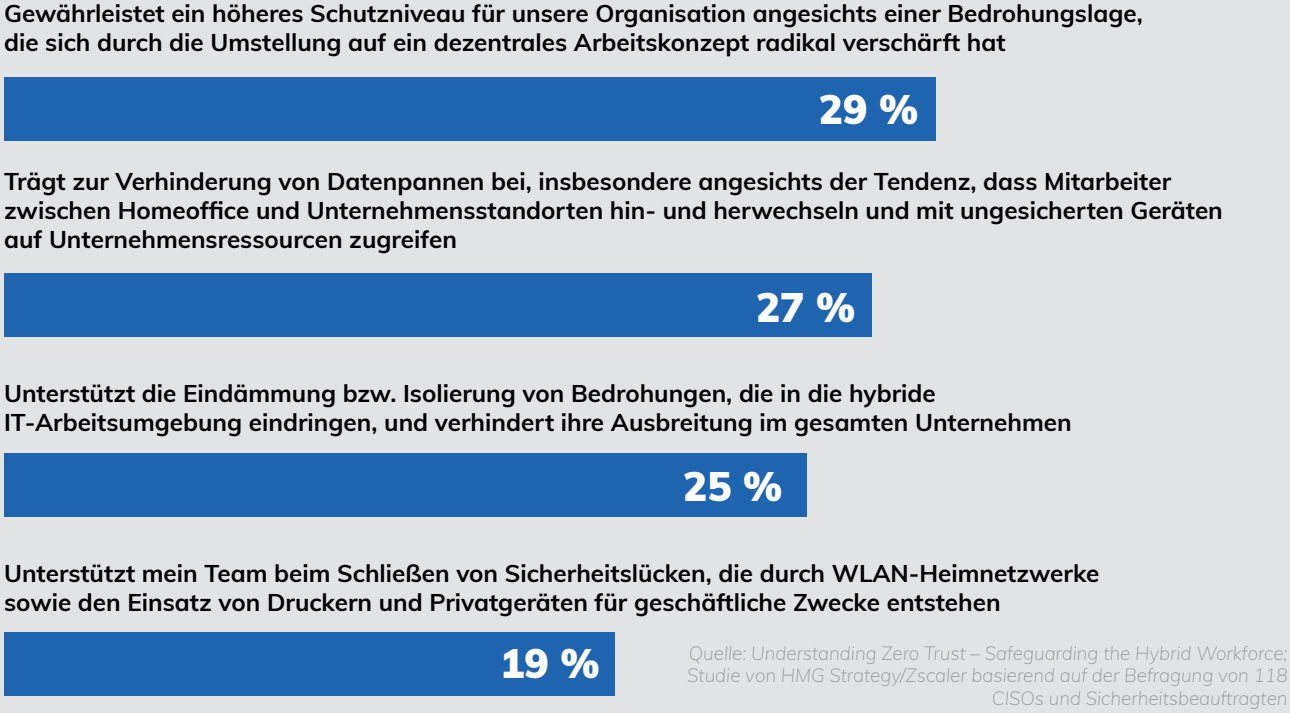
Die IT-Ausgaben sind im Vergleich zur Anschaffung, Konfiguration, Verwaltung und Aktualisierung herkömmlicher Firewalls, VPNs und Web-Gateways ebenfalls gesunken. *„Früher hatten wir weltweit zahlreiche physische Appliances im Einsatz, für die jeweils eigene Konfigurationen, Regeln, Patches, Updates und Wartungsverträge erforderlich waren“*, erinnert sich Ramberg.

Für Sanmina hat die Umstellung auf eine Zero-Trust-Architektur eine sichere Digitalisierung der Fertigungsverfahren im Rahmen von „Industrie 4.0“-Initiativen, eine Reduzierung der IT-Kosten sowie eine Verbesserung der Agilität durch beschleunigte M&A-Prozesse ermöglicht. Zudem profitieren die User von einer besseren Anwendererfahrung. Der nächste Abschnitt befasst sich mit den Faktoren, die eine möglichst schnelle Implementierung dieses bewährten Sicherheitskonzepts erforderlich machen. Außerdem werden Praxisbeispiele anderer Spitzenunternehmen vorgestellt, die bereits von der Umstellung auf Zero Trust profitieren.

Stärkung der Sicherheit durch Zero Trust

Welche primären sicherheitsrelevanten Vorteile ergeben sich aus der Anwendung eines Zero-Trust-Sicherheitsmodells zur Unterstützung hybrider Belegschaften?

GRAFIK 2:



Quelle: Understanding Zero Trust – Safeguarding the Hybrid Workforce; Studie von HMG Strategy/Zscaler basierend auf der Befragung von 118 CISOs und Sicherheitsbeauftragten

Als wichtigsten sicherheitsrelevanten Vorteil einer Implementierung des Zero-Trust-Sicherheitskonzepts zur Unterstützung hybrider Belegschaften nannten die befragten CISOs und Sicherheitsbeauftragten das höhere Schutzniveau angesichts einer Bedrohungslage, die sich im Zuge der Umstellung auf dezentrale Arbeitsmodelle drastisch verschärft hat.

Argumente für eine möglichst schnelle Umstellung auf Zero Trust

Die schrittweise Rückkehr zur Präsenzarbeit bzw. die Umstellung auf hybride Konzepte, bei denen die Belegschaft teils im Büro, teils an Remote-Standorten arbeitet, hat zur weiteren Vergrößerung der Angriffsfläche geführt sowie zusätzliche Sicherheitsrisiken entstehen lassen. Damit vermehren sich auch die Herausforderungen, die von CISOs und Sicherheitsbeauftragten zu bewältigen sind.

Je mehr Mitarbeiter von wechselnden Standorten aus über ungesicherte Geräte auf Unternehmensressourcen zugreifen, desto höher wird die Wahrscheinlichkeit, dass die Organisation von Datenpannen und anderen Sicherheitsverletzungen sowie erfolgreichen Angriffen von Cyberkriminellen und staatlichen Akteuren betroffen ist. Für die Sicherheitsexperten, die im Rahmen der Studie von HMG Strategy und Zscaler befragt wurden, zählt diese verschärfte Risikolage zu den wichtigsten Argumenten für die Umstellung auf Zero-Trust-Architekturen.

„Ganz egal, ob ich zu Hause im Homeoffice sitze oder im Café, an einem Unternehmensstandort oder an meinem Laptop, oder ob ich eine Verbindung über einen Cloud-basierten Desktop-as-a-Service aufbaue – ich muss in jedem Fall auf die IT-Ressourcen des Unternehmens zugreifen können und mich dabei darauf verlassen, dass mein ausgehender Traffic zuverlässig geschützt wird“, so Lorenzin. *„Ein Zero-Trust-Ansatz eignet sich dafür am besten, weil er eine zentrale Richtlinienverwaltung und lückenlosen Einblick in den gesamten Traffic gewährleistet. Dadurch lässt sich ein sehr viel höherer Grad an Koordination, Transparenz und Kontrolle erreichen, als es mit separaten Einzellösungen möglich wäre.“*

Careem vertraut beim Ausbau der globalen Remote-Belegschaft auf Zero Trust

Als führender Fahrdienstvermittlungsservice im Nahen Osten konnte **Careem** durch den Umstieg auf Zero Trust mehrere Probleme auf einmal lösen.

Bislang vertraute das 2012 gegründete Unternehmen mit Sitz in Dubai auf eine herkömmliche Sicherheitsarchitektur nach dem Prinzip „Festung mit Burggraben“. Angesichts des rasanten Wachstums sowie der zunehmenden Umstellung auf Remote-Arbeit im Laufe der vergangenen Jahre setzte sich bei der Geschäftsführung jedoch die Erkenntnis durch, dass die Legacy-Sicherheitsarchitektur zum Hemmschuh geworden war, der die weitere Expansion behinderte.

„Die prognostizierte Vervierfachung des Geschäftsvolumens ließ sich mit unserer Legacy-Sicherheit einfach nicht mehr bewältigen. Sie beeinträchtigte unsere Fähigkeit, genügend Arbeitskräfte anzuwerben, um unsere Geschäftsziele zu erreichen“, so **Peeyush Patel**, CIO und CISO bei Careem. *„Wir mussten unser gesamtes Sicherheitskonzept modernisieren.“*

Zur Unterstützung des Geschäftsmodells aus Cloud-basierter App-Entwicklung, Remote-Mitarbeitern und rasantem Wachstum ersetzte Careem die herkömmliche Sicherheitsinfrastruktur mit über 50 Firewalls und Dutzenden von VPN-Appliances durch einen Zero-Trust-Ansatz auf Basis der Zero-Trust-Exchange-Plattform von Zscaler.

„Die Zero-Trust-Exchange-Plattform war eindeutig die beste Wahl für die Entwicklung eines Zero-Trust-basierten SSE-Modells (Security Service Edge) zum Schutz unserer Daten, unserer Mitarbeiter und unserer Kunden“, bekräftigt Patel.

Zur Optimierung der Sicherheitsinfrastruktur nutzt Careem mehrere Services, die im Rahmen der Zero Trust Exchange bereitgestellt werden: Zscaler Internet Access™ (ZIA) zur Gewährleistung des sicheren Zugriffs auf SaaS-Anwendungen und Internet, Zscaler Private Access (ZPA) für einen sicheren Zugriff auf unternehmenseigene Anwendungen in öffentlichen Cloud-Umgebungen und im Rechenzentrum sowie Zscaler Digital Experience (ZDX) zur proaktiven Erkennung und Behebung von Zugriffsproblemen vor einer Beeinträchtigung der User Experience.

Careem setzt zudem den im Funktionsumfang der Plattform inbegriffenen Cloud Access Security Broker (CASB) zum Schutz ruhender Daten in SaaS-Anwendungen und IaaS-Umgebungen sowie die Cloud-DLP-Lösung (Data Loss Prevention) zur Gewährleistung der datenschutzrechtlichen Konformität bei der Verarbeitung personenbezogener Daten in der Cloud ein.

Die Implementierung der Zero Trust Exchange führte bei Careem sofort zu einer spürbaren Steigerung der Agilität und Produktivität. Angefangen bei der Eliminierung der mit herkömmlicher Netzwerksicherheit verbundenen Frustrationen und Kosten profitierte das gesamte Unternehmen von zahlreichen Effizienzgewinnen.

„Unsere Kollegen machten kein Hehl aus ihrer Unzufriedenheit mit dem VPN-Zugriff", erinnert sich Patel. *„Durch Implementierung der Plattform mitsamt ZPA konnten wir nicht nur diese Beschwerden beheben, sondern eine erhebliche Verbesserung der User Experience insgesamt erreichen – entsprechend verbesserte sich unser Net Promoter Score (NPS) bei unseren Mitarbeitern und externen Kundendienstfachkräften um 70 %."*

Die durch die Umstellung auf Zero Trust erzielten Kostenersparnisse setzten zusätzliches Investitionskapital zur Unterstützung der Entwicklung frei. *„Durch den vereinfachten Zugriff auf Anwendungen zur Softwareentwicklung sparen wir jährlich ca. 20.000 Arbeitsstunden ein"*, meint Patel. *„Die dadurch freigesetzten Ressourcen können wir stattdessen zum Ausbau der Wertschöpfung einsetzen."*

Die Erfahrung bei Careem zeigt, dass die Umstellung auf einen Zero-Trust-Ansatz nicht nur zur Stärkung der Kontrollen und Schutzmechanismen für das hybride Arbeitskonzept beiträgt, sondern auch mehr Agilität und Produktivität sowie signifikante Kostenersparnisse mit sich bringt. Im nächsten Abschnitt stellen wir abschließend konkrete Handlungsempfehlungen für die Implementierung einer Zero-Trust-Architektur vor, die zuverlässigen Schutz für hybride Belegschaften gewährleistet.

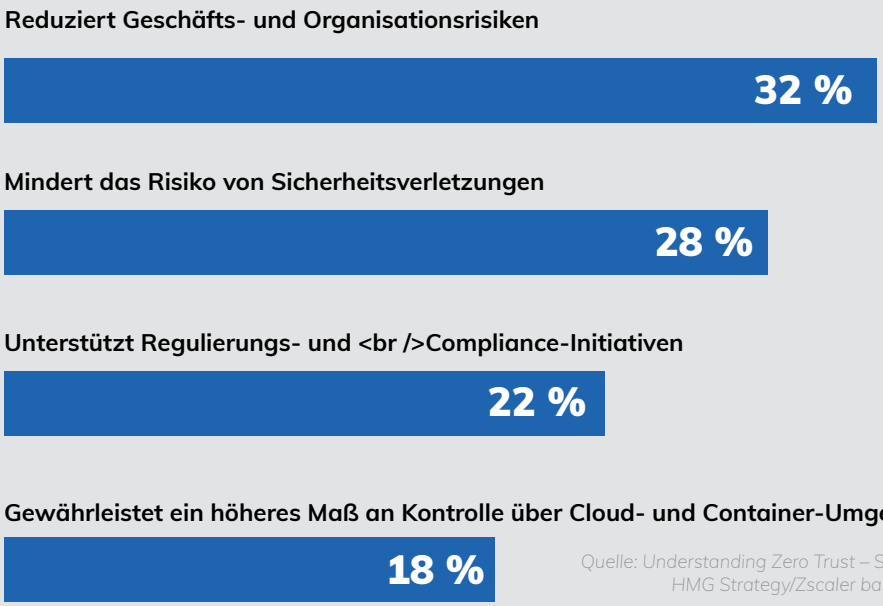
„Die Zero-Trust-Exchange-Plattform war eindeutig die beste Wahl für die Entwicklung eines Zero-Trust-basierten SSE-Modells (Security Service Edge) zum Schutz unserer Daten, unserer Mitarbeiter und unserer Kunden."

PEEYUSH PATEL
CIO und CISO
Careem

Vorteile von Zero Trust: Weniger Risiko, mehr Kontrolle

Welche primären betriebswirtschaftlichen und operativen Vorteile ergeben sich aus der Implementierung eines Zero-Trust-Sicherheitsmodells?

GRAFIK 3:



Quelle: Understanding Zero Trust – Safeguarding the Hybrid Workforce; Studie von HMG Strategy/Zscaler basierend auf der Befragung von 118 CISOs und Sicherheitsbeauftragten

BETRIEBSWIRTSCHAFTLICHE UND OPERATIVE VORTEILE EINES ZERO-TRUST-MODELLS

Die betriebswirtschaftlichen und operativen Vorteile, die bei Unternehmen wie Sanmina und Careem durch die Umstellung auf einen Zero-Trust-Ansatz realisiert wurden, entsprechen dem, was Lorenzin auch bei anderen Zscaler-Kunden beobachten konnte.

Lorenzin verweist auf vier Hauptvorteile, die sich aus der Umstellung auf Zero Trust ergeben: „**An allererster Stelle steht dabei Flexibilität und Resilienz** – und zwar insbesondere die zügige Bereitstellung sowie die Möglichkeit zur schnellen Anpassung im Zuge der weiteren Entwicklung der Organisation."

„Der zweite Vorteil besteht in der verbesserten Sicherheit", so Lorenzin weiter. „Vor allem ermöglicht Zero Trust die Minimierung der externen Angriffsfläche sowie die Einschränkung bzw. komplette Blockierung unbefugter lateraler Bewegungen."

Als dritten Vorteil nennt sie die optimierte User Experience. Insbesondere betrifft dies den schnelleren, vereinfachten und zuverlässigeren Zugriff auf Anwendungen.

Der vierte Hauptvorteil liegt in der Kostensenkung.

„Sie können sich die Investitionskosten sparen, und zwar nicht nur für die zahlreichen VPN-Gateways, die Sie weltweit einsetzen, sondern auch für die Stacks von Appliances und Funktionen – Load Balancing, DMZ-Firewalls, DDoS-Schutz – zur Absicherung dieser VPN-Gateways", so Lorenzin.

Die vier Vorteile einer Zero-Trust-Architektur

Erste Schritte auf dem Weg zur Zero-Trust-Architektur

Als Ausgangspunkt für die erfolgreiche Umstellung auf Zero Trust sollten CISOs und Sicherheitsbeauftragte zunächst einen geeigneten Anwendungsfall identifizieren und umsetzen, anhand dessen sich die Vorteile von Zero Trust im Vergleich zu den bisherigen Kontrollmaßnahmen eindeutig nachweisen lassen.

„Am besten suchen Sie sich einen vielversprechenden Anwendungsfall. Denken Sie daran: Es ist völlig in Ordnung, ein bisschen zu experimentieren. Versuchen Sie bloß nicht, das schwierigste Problem als Erstes anzugehen“, empfiehlt Lorenzin.

Daran anschließend empfiehlt sich ein Meeting mit dem CEO und Unternehmensvorstand. Als CISO oder Sicherheitsbeauftragter ist das Ihre Chance, die Vorteile einer Zero-Trust-Architektur im Vergleich zu herkömmlichen netzwerkzentrierten Sicherheitskonzepten zu kommunizieren und zu erläutern, wie sie zur Reduzierung von Risiken, Unterstützung des Geschäftswachstums und Optimierung der Flexibilität und Agilität beiträgt. Analogien können hier helfen, das Konzept so zu vermitteln, dass es auch für Vorstandsmitglieder ohne einschlägige technische Vorkenntnisse leicht verständlich wird.

Ebenfalls hilfreich ist der Verweis auf die im Zuge des Pilotprojekts erzielten Ergebnisse, um den Wert eines Zero-Trust-Ansatzes aufzuzeigen und verbindliche Zusagen für Investitionen in eine breiter angelegte Zero-Trust-Strategie einzuholen.

Darüber hinaus kann es sinnvoll sein, auf Feedback und Erkenntnisse von Branchenkollegen aus ihren jeweiligen Erfahrungen mit der Zero-Trust-Bereitstellung zurückzugreifen. Ein entsprechender Informationsaustausch findet beispielsweise im CXO REvolutionaries Forum statt. Unter anderem erhalten Sie hier Empfehlungen zur Auswahl eines vertrauenswürdigen Zero-Trust-Partners mit der richtigen Plattform für Ihre jeweiligen Prioritäten und strategischen Zero-Trust-Ziele.

„Machen Sie sich die Erfahrungen von Branchenkollegen zunutze, die mit der Umstellung auf Zero Trust schon weiter fortgeschritten sind“, rät Lorenzin.

Die Argumente für eine möglichst zügige Umstellung auf eine Zero-Trust-Architektur als unverzichtbare Voraussetzung für den Schutz hybrider Belegschaften und digital aufgestellter Unternehmen haben wir hier ausführlich erläutert. Die Studienergebnisse lassen keinen Zweifel daran, dass sich das Engagement zugunsten der Zero-Trust-Transformation für die betroffenen Organisationen in jedem Fall ausgezahlt hat.

Über HMG Strategy

HMG Strategy ist die weltweit führende digitale Plattform für die Vernetzung von Führungskräften aus der Technologiebranche, die Impulse für neue Unternehmenskonzepte setzen und die Zukunft der Geschäftswelt mitgestalten wollen. Mit regionalen und virtuellen Events im Rahmen der CIO and CISO Executive Leadership Series, Publikationen und einem digitalen Ressourcenzentrum engagieren wir uns für die Entwicklung und Veröffentlichung wertvoller Forschungserkenntnisse von CIOs, CISOs, CTOs und Technologieexperten zu Themen rund um Leadership, Innovation, digitale Transformation und Personalentwicklung.

Dem globalen Netzwerk von HMG Strategy gehören über 400.000 Spitzenkräfte aus dem IT-Bereich, Branchenexperten und Innovationsführer an.

Weitere Informationen zum branchenweit einzigartigen Geschäftsmodell von HMG Strategy, die sieben Säulen des Vertrauens, finden Sie hier.

HMG Strategy: die weltweit führende digitale Plattform für die Vernetzung von Führungskräften aus der Technologiebranche, die Impulse für neue Unternehmenskonzepte setzen und die Zukunft der Geschäftswelt mitgestalten wollen.

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 ist in über 150 Rechenzentren weltweit verteilt und die größte Inline-Cloud-Sicherheitsplattform der Welt. Informieren Sie sich auf zscaler.de oder folgen Sie uns auf Twitter unter @zscaler.