E-Book

Leitfaden für CIOs:

Beschleunigung einer sicheren digitalen Transformation

Fünf grundlegende Prinzipien, um schnell und sicher ans Ziel zu gelangen

Rasanter Wandel in der IT

Organisationen setzen Cloud-Anwendungen ein, das Volumen des Internet-Traffic hat sich vervielfacht und Mobile-first-Computing ist zur wichtigen strategischen Initiative vieler Unternehmen geworden.

Die digitale Transformation kann für IT-Organisationen sowohl nervenaufreibend als auch spannend sein. Sie kann sogar schlaflose Nächte bereiten, aber das muss nicht sein.

Diese fünf grundlegenden Prinzipien können bei der sicheren digitalen Transformation von Nutzen sein:

1. Veraltete Infrastruktur modernisieren ›
2. Sichere Internetverbindungen in Zweigstellen einrichten ›
3. Verteilte mobile Belegschaften sicher vernetzen ›
4. Microsoft-365-Erfahrung für User optimieren ›
5. IT-Integration bei M&As vereinfachen ›

Veraltete Infrastruktur modernisieren

Seit 30 Jahren bauen Organisationen komplexe Netzwerke auf, um User mit Anwendungen im Rechenzentrum zu verbinden. Um diese Netzwerke zu schützen, haben sie in eine Vielzahl von Appliances für die Netzwerksicherheit investiert. Angesichts der sich ständig weiterentwickelnden Bedrohungslandschaft ist es erforderlich, veraltete Infrastrukturen zu modernisieren oder zu ersetzen und neue Sicherheitskontrollen einzuführen — was die Kosten und Komplexität der Netzwerke in die Höhe treibt.

Da sich immer weniger User und Anwendungen im Netzwerk befinden und der Traffic zunehmend in die Cloud verlagert wird, ist das traditionelle Netzwerkmodell mittlerweile obsolet.

Es ist Zeit für einen zweckmäßigen Ansatz, der Ihren Sicherheitsansprüchen gerecht wird und Kosten senkt, indem Benutzer direkt mit ihren Zielen verbunden werden. Es ist an der Zeit, die Sicherheit in die Cloud zu verlagern.

Erste Schritte:

- **Verwenden Sie eine SASE-Architektur (Secure Access Service),** wie im Gartner-Report **„The Future of Network Security is in the Cloud“** besprochen und beziehen Sie sich auf **„Gartner Magic Quadrant for Secure Web Gateways“.**
- **Transformieren Sie Ihr Netzwerk** von Hub-and-Spoke zu Direct-to-Cloud und setzen Sie Security-as-a-Service aus der Cloud ein.
- **Bauen Sie schrittweise** Hardware und Software ab, um technische Talente zu entlasten und die tägliche Verwaltung und Wartung zu reduzieren.

KUNDENREFERENZ

SIEMENS

Für 350.000 User von Siemens in 192 Ländern wird die Cloud zum neuen Rechenzentrum und das Internet zum neuen Unternehmensnetzwerk. Dank einer modernen Netzwerkarchitektur, die für die Cloud konzipiert ist und jederzeit und überall sicheren, leistungsstarken Anwendungszugriff bietet, konnte Siemens seine Kosten erheblich reduzieren.

„Indem wir auf das Backhauling unseres Traffic verzichten und stattdessen das Internet direkt nutzen, können wir unsere Kosten voraussichtlich um 70% senken.“

Frederik Janssen
VP of IT Strategy & Governance
Siemens

Sichere Internetverbindungen in Zweigstellen einrichten

Wie lange dauert es, bis eine Organisation eine neue Zweigstelle oder ein Einzelhandelsgeschäft vernetzt hat? Ein Hub-and-Spoke-Netzwerk an einem neuen Standort zu integrieren, ist ein zeitaufwändiges und ressourcenintensives Unterfangen. Und auch wenn Standorte vernetzt sind, können Traffic-Engpässe und Latenzen auftreten — insbesondere wenn der Bandbreitenbedarf steigt und somit Firewalls überlastet, WAN-Kosten in die Höhe getrieben und Gateways blockiert werden. Legacy-Netzwerke lassen sich einfach nicht schnell genug skalieren.

Wenn Unternehmen auf SD-WAN umsteigen möchten, um den Betrieb in Zweigstellen zu vereinfachen und lokale Internet-Breakouts zu nutzen, müssen sie Sicherheitsvorkehrungen vom Rechenzentrum zur Netzwerk-Edge verlagern, um das Potenzial von SD-WAN voll auszuschöpfen.

Erste Schritte:

- **Sicherheit in die Cloud verlagern,** um den gesamten Traffic zu überprüfen, unabhängig davon, ob er aus dem Rechenzentrum, Cloud-Services oder Internet stammt.
- **Zweigstellen „ressourcenfrei“ gestalten**, indem an jedem Standort lokale Internetverbindungen eingerichtet werden und MPLS nach Möglichkeit entfernt wird.
- **Orientieren Sie Ihre lokalen IT-Talente um,** damit sie geschäftsdienlicher arbeiten und Transformationsinitiativen einleiten können.

KUNDENREFERENZ

AutoNation

Der größte Autohändler der USA, AutoNation, richtete lokale Breakouts ein, die Usern an 360 Standorten schnellen und sicheren Zugriff auf das Internet bieten. Dank Zscaler kann AutoNation Kosten reduzieren, neue Standorte einfacher vernetzen und seinen Sicherheitsstatus durch Inline-SSL-Überprüfung, Sandboxing und andere Funktionen optimieren.

„Mit Zscaler konnten wir den Bedarf für unsere 360 Zweigstellen auf lediglich je einen Router und Endgeräte reduzieren.“

Ken Athanasiou
CISO und Vice President
von AutoNation

Verteilte mobile Belegschaften sicher vernetzen

Da User von überall aus arbeiten und sich mit ihren Anwendungen verbinden, mussten sich Unternehmen auf VPN-Technologien verlassen, die ihre Netzwerke auf die Standorte der User ausdehnen. Aus Sicherheitsgründen war ein Backhauling des Traffics zu ihren Rechenzentren notwendig, was die Anwendererfahrung verschlechterte und häufig dazu führte, dass Remote-User das VPN und die Sicherheitsvorkehrungen umgingen, wodurch sich das Geschäftsrisiko erhöhte. Aus diesen und anderen Gründen schätzt Gartner, dass 60 % der Unternehmen VPN-Lösungen bis 2023[1] durch ZTNA-Lösungen (Zero Trust Network Access) ersetzen werden.

Endgerätesicherheit allein reicht nicht aus, um komplexe Bedrohungen abzuwehren. Wie kann man mithilfe einer Service Edge Security Cloud User schützen und eine erstklassige Anwendererfahrung erzielen?

Erste Schritte:

- **ZTNA-Architektur einführen,** damit User auf Anwendungen zugreifen können, ohne ins Netzwerk zu gelangen.
- **Sicherheitsvorkehrungen an die Edge verlagern,** um Usern standortunabhängig identische Sicherheit zu bieten und gleichzeitig eine schnelle Anwendererfahrung zu garantieren.
- **Gewähren oder verweigern Sie den Zugriff auf Anwendungen** über eine zentrale Identitätsverwaltung, die den Administrationsaufwand verringert.

KUNDENREFERENZ

nab

Bei der Cloud-Migration der National Australia Bank (NAB), Australiens größter Geschäftsbank, stand ursprünglich das Bestreben im Vordergrund, eine bessere Kundenerfahrung und mehr Sicherheit zu gewährleisten und die Betriebsabläufe zu optimieren. Heute setzt NAB auf Zero Trust zur Bereitstellung einer zukunftssicheren Netzwerkinfrastruktur, die das für alle Mitarbeiter geltende „Work from Anywhere"-Konzept unterstützt.

„Die Mitarbeiter schalten ihren PC im Homeoffice ein, und er funktioniert ganz genauso wie im Büro. Sie müssen sich keine Gedanken über zusätzliche Anmeldeschritte machen oder sich mit Sicherheits-Token herumschlagen, sondern es läuft einfach alles wie gewohnt."

Steve Day
EGM Infrastructure, Cloud and Workplace
National Australia Bank

Microsoft-365-Erfahrung für User optimieren

Da sich nahezu jeder auf Office 365 verlässt, ist die Anwendererfahrung ein wichtiger Maßstab für den Erfolg einer Bereitstellung. Allerdings erhöht der User-Traffic zu Office 365 die Netzwerkauslastung, wodurch Firewalls schnell überlastet sind und sich die Anwendererfahrung verschlechtert. Deshalb sind häufig kostspielige Hardware-Upgrades erforderlich, die die Komplexität erhöhen. Zudem müssen Firewalls regelmäßig aktualisiert werden — ein zeitaufwändiger Prozess.

Unternehmen benötigen eine schnelle und konsistente Microsoft-365-Erfahrung. Deshalb empfiehlt Microsoft Folgendes:

- Microsoft-365-Traffic identifizieren und priorisieren
- Lokale Austritte für Netzwerkverbindungen
- Die Umgehung von Proxies bewerten
- Netzwerkengpässen vermeiden

Erste Schritte:

- **Microsoft-365-Traffic** über lokale Internet-Breakouts leiten, wie von Microsoft empfohlen.
- **Den einzigen von Microsoft empfohlenen Anbieter von Cloud-Sicherheit nutzen,** um die schnellstmögliche Anwendererfahrung zu erzielen.
- **Bandbreitennutzung optimieren,** um Microsoft-365-Traffic gegenüber privatem Traffic zu priorisieren.

KUNDENREFERENZ

KELLY SERVICES

Kelly Services transformierte sein Netzwerk, um an 900 Standorten weltweit schnelle, sichere und direkte Internetverbindungen sowie schnellen Zugriff auf Microsoft 365 und andere Cloud-basierte Anwendungen bereitzustellen. Das Unternehmen sparte 60 Prozent seines MPLS-Budgets ein, verbesserte die Überprüfungsfunktionen und vereinfachte die Netzwerk- und Richtlinienverwaltung erheblich.

„Mit Zscaler konnten wir 30 % der gesamten Bandbreite Office 365 (Microsoft 365) zuweisen, diese aber auch auf 50 % begrenzen, damit die Übertragung von OneDrive-Dateien nicht alle anderen Vorgänge verlangsamt."

Darryl Staskowski
SVP & CIO
Kelly Services

IT-Integration bei M&As vereinfachen

Die Komplexität von IT-Integrationen verzögert M&As und stört die Geschäftstätigkeit. Sie müssen das Risiko kalkulieren, wenn Sie Benutzer ergänzen oder streichen, während Sie ihnen gleichzeitig Zugriff auf benötigte Anwendungen gewähren. Erschwerend kommt hinzu, dass Sie die Sicherheit standardisieren müssen, wenn Sie neue Unternehmensteile mit niedrigeren oder anderen Sicherheitsnormen integrieren. Dies kann das Risiko erhöhen und erfordert immer besondere Aufmerksamkeit.

Unternehmen können M&As und damit zusammenhängende Aktivitäten von Jahren auf Wochen verkürzen, indem sie Usern Zugriff auf Anwendungen gewähren, ohne die Netzwerkinfrastrukturen zusammenführen zu müssen. So lässt sich zudem das Geschäftsrisiko minimieren.

Erste Schritte:

- **ZTNA-Technologie nutzen,** damit User direkt auf Anwendungen zugreifen können, ohne ins Netzwerk zu gelangen.
- **Verwenden Sie einen schrittweisen, auf Identität basierten Ansatz.** Beginnen Sie mit Benutzern in beiden Entitäten, die an Aktivitäten im Zusammenhang mit M&A beteiligt sind, und bestimmen Sie, auf welche Anwendungen sie zugreifen müssen.
- **Liste der User und Anwendungen erweitern, während die Geschäftsintegration** voranschreitet.

KUNDENREFERENZ

Ein US-amerikanisches Fortune-500-Unternehmen im Gesundheitswesen verkürzte die geplante Integrationszeit um neun Monate, indem es Anwendungszugriff ohne Zugang zum Netzwerk bereitstellte und auf diese Weise neu erworbenen oder fusionierten Organisationen ein sicheres Onboarding ermöglichte. Dies trug zur Vereinfachung der M&A-Infrastruktur des Unternehmens bei und reduzierte die Komplexität der IT.

Über Zscaler

Zscaler wurde im Jahr 2008 auf der Grundlage eines einfachen aber wirkungsvollen Konzepts gegründet: Da Anwendungen in die Cloud verlagert werden, muss sich auch die Sicherheit dorthin bewegen. Heute helfen wir Tausenden von globalen Organisationen bei der Transformation zu Cloud-fähigen Betriebsabläufen.

CIO-Bibliothek

Weitere wichtige Ressourcen
von und für CIOs:

revolutionaries.zscaler.com

Oder kontaktieren Sie Ihren Vertriebsbeauftragten
für Peer-Referenzen.

zscaler™ | Experience your world, secured.™

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 Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen unter **zscaler.de** oder auf Twitter unter **@zscaler**.

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