Zero-Trust-Zugriff auf firmeninterne Anwendungen für lokale und Remote-User mit Zscaler™

Im Zuge der COVID-Pandemie haben zahlreiche Organisationen die Umstellung von Präsenzarbeit auf dezentrale Konzepte erfolgreich über die Bühne gebracht. Zur Gewährleistung der Business Continuity waren dabei vielfältige Herausforderungen in Bezug auf Datenschutz, sicheren Remotezugriff und bedarfsgerechte Skalierung zu bewältigen. Viele Organisationen sahen sich zunächst überrumpelt und überfordert von der Notwendigkeit, den Großteil der Belegschaft quasi von einem Tag zum nächsten ins Homeoffice umzusiedeln. Zero-Trust-Services bewährten sich hier als effektivere Alternative zu herkömmlichen netzwerkzentrierten Techniken für die Sicherung des Zugriffs auf Unternehmensressourcen. Inzwischen deuten viele Anzeichen auf eine langfristige Beibehaltung der damaligen Notlösung hin. Dieser neuen Normalität müssen IT-Teams bei der strategischen Planung für die kommenden Jahre gerecht werden.

zscaler™

Aus der Perspektive der Sicherheitsverantwortlichen sind dezentrale bzw. hybride Arbeitskonzepte mit erhöhtem Risiko verbunden, da User mit eigenen Geräten von unterschiedlichen Standorten auf Anwendungen zugreifen. Dieses Risiko ist umso höher, wenn User – wie bei herkömmlichen Sicherheitsarchitekturen üblich – automatisch als vertrauenswürdig eingestuft werden und Zugriff auf das Unternehmensnetzwerk erhalten. Die User wiederum legen vor allem Wert auf einen möglichst reibungslosen Zugriff von jedem beliebigen Standort aus.

Drei Vorteile von Zero Trust, die IT-Teams bei der Zukunftsplanung berücksichtigen sollten

Neben geeigneten Hygienekonzepten zur Gewährleistung der gesundheitlichen Sicherheit aller Mitarbeiter und Besucher gibt es bei der Rückkehr zur Präsenzarbeit auch einige Punkte zu berücksichtigen, die eher ins Ressort des für Cyber- und Netzwerksicherheit zuständigen IT-Beauftragten fallen. Mit Zero Trust profitieren Organisationen insbesondere von drei Hauptvorteilen.

1 Die beste Lösung für alle User an allen Standorten

Ein weitverbreiteter Irrglaube lautet, dass Zero Trust nur für die Gewährleistung von Remotezugriff auf unternehmenseigene Anwendungen relevant ist. Entsprechend werden Zero-Trust-Services häufig als Alternative zu Technologien wie VPN oder VDI eingesetzt, die Remote-User im Netzwerk platzieren. Hingegen werden User, die an Unternehmensstandorten arbeiten – d. h. innerhalb des herkömmlichen Sicherheitsperimeters – wie gehabt mit dem Netzwerk verbunden, da sie inhärent als vertrauenswürdig gelten. Teilweise wurde als zusätzliche Sicherheitsmaßnahme Netzwerksegmentierung implementiert – was wiederum den Nachteil einer sehr viel komplizierteren Netzwerkarchitektur mit sich bringt. Durch den Einsatz effektiver Zero-Trust-Services erübrigt sich auch der mit Netzwerksegmentierung verbundene Aufwand. Ein Zero-Trust-Service gewährleistet identischen Schutz für User an Remote- und Unternehmensstandorten und kann zudem zur Segmentierung auf Anwendungsebene eingesetzt werden.

2 Identisches Schutzniveau bei optimaler User Experience

Mittlerweile liegen Ergebnisse aus mehreren Umfragen vor, die nachweisen, dass sowohl Arbeitgeber als auch Arbeitnehmer sich mit der Remote-Arbeit als dauerhafter Lösung angefreundet haben. Viele Organisationen verzeichnen steigende Produktivität, obwohl der Kern ihrer Belegschaft ganz oder größtenteils dezentral arbeitet. Die Mehrzahl der Mitarbeiter weiß vor allem die damit einhergehende Flexibilität zu schätzen. Deswegen setzt sich bei unseren Kunden zunehmend der Wunsch nach Umstieg auf hybride Arbeitsmodelle durch, bei denen die Mitarbeiter ihre Aufgaben teils im Büro, teils im Homeoffice erledigen. Entsprechend müssen die Netzwerk- und Sicherheitsbeauftragten für alle Mitarbeiter standortunabhängig reibungslosen Zugriff und ein identisches Schutzniveau gewährleisten.

3 Kein Netzwerkzugang für infizierte Geräte

Als weiterer Schlüsselfaktor ist dabei die wachsende Beliebtheit von Sicherheitsservices zum Schutz von Endgeräten bei der Remote-Arbeit zu berücksichtigen (CrowdStrike, Microsoft, Carbon Black usw.). User sind mittlerweile daran gewöhnt, mit eigenen Laptops und Smartphones über ihren privaten Internetanschluss auf Unternehmensanwendungen zuzugreifen. Wenn diese Geräte nun ins Büro mitgebracht werden, dürfen die IT-Verantwortlichen auf keinen Fall zulassen, dass damit aufs Netzwerk zugegriffen wird. Zur Reduzierung der Angriffsfläche und Abwehr potenzieller Bedrohungen unter den veränderten Vorzeichen hybrider Arbeitskonzepte ist es unbedingt erforderlich, zunächst den Sicherheitsstatus der einzelnen Geräte gründlich zu überprüfen.

Zero Trust: Keine Verbindung wird automatisch als vertrauenswürdig eingestuft

Zero Trust basiert auf zwei Kernelementen: Identität und Unternehmensrichtlinien.

Zugriffsrechte für User werden nicht aufgrund von IP-Adressen, sondern auf Basis der Identität bzw. des Kontexts gewährt. Anhand der Unternehmensrichtlinien kann das Netzwerk- bzw. Sicherheitsteam granular festlegen, auf welche unternehmenseigenen Anwendungen ein befugter User jeweils zugreifen darf. Diese Richtlinien werden auf der Zscaler Zero Trust Exchange™ gehostet und von ihr durchgesetzt. Wird der Zugriff genehmigt, vermittelt die Plattform die entsprechende Verbindung zwischen einem einzelnen User und einer einzelnen Anwendung für eine einzelne Sitzung.

Netzwerkzentrierte Zugriffskontrollen sind nicht mehr zeitgemäß, wenn User von unterschiedlichen und wechselnden Standorten aus auf Anwendungen zugreifen. Eine sichere Rückkehr zur Präsenzarbeit bzw. Umstellung auf ein hybrides Konzept setzt voraus, dass keine Verbindung automatisch als vertrauenswürdig eingestuft werden darf. Stattdessen ist eine Umstellung auf Zero-Trust-Richtlinien erforderlich. Aus User-Sicht gewährleistet Zero Trust Network Access standortunabhängig sicheren, zügigen und nahtlosen Zugriff auf Anwendungen. Aus IT-Sicht profitiert die Organisation zusätzlich von der hochgradigen Flexibilität und Skalierbarkeit der Lösung.

Zscaler Private Access als optimale Zero-Trust-Lösung für Remote-, Hybrid- und Präsenzarbeit

Zscaler Private Access™ (ZPA™) ist ein Cloud-Service von Zscaler zur Bereitstellung nahtlosen Zero-Trust-Zugriffs auf unternehmensinterne Anwendungen, die entweder in öffentlichen Cloud-Umgebungen oder im Rechenzentrum ausgeführt werden. Die Lösung eignet sich gleichermaßen zur Unterstützung von Legacy- und webbasierten Anwendungen. Anhand von Informationen, die von einem SAML-basierten ID-Anbieter bereitgestellt werden, sowie unternehmensspezifisch definierten Richtlinien verbindet der Service einen entsprechend befugten User direkt mit der jeweils benötigten Anwendung. Im Unterschied zu VPN oder VDI wird der User dabei niemals im Unternehmensnetzwerk platziert. Damit entfällt zugleich die Notwendigkeit eines Security-Stacks am Inbound-Gateway. Die Anwendung wird niemals im Internet exponiert und ist somit für potenzielle Angreifer unsichtbar – eine weitere entscheidende Voraussetzung für sicheren Remotezugriff.

ZPA vermittelt die Verbindung in Echtzeit über zwei ausgehende Tunnel – je einen von der Anwendung und vom User – an einem Service-Edge-Standort in möglichst unmittelbarer Nähe zum Gerät des Users. Dadurch wird der User auf dem kürzesten Pfad mit der Anwendung verbunden, ohne dass der Traffic über ein zentrales Rechenzentrum umgeleitet werden muss. Die betreffende Service Edge wird entweder öffentlich von Zscaler oder privat vom Kunden gehostet. In letzterem Fall bezieht sie die Zweigstelle bzw. das Rechenzentrum des Kunden zur lokalen Durchsetzung von Richtlinien ein. In beiden Fällen ist Zscaler für die Verwaltung der Service Edges verantwortlich.

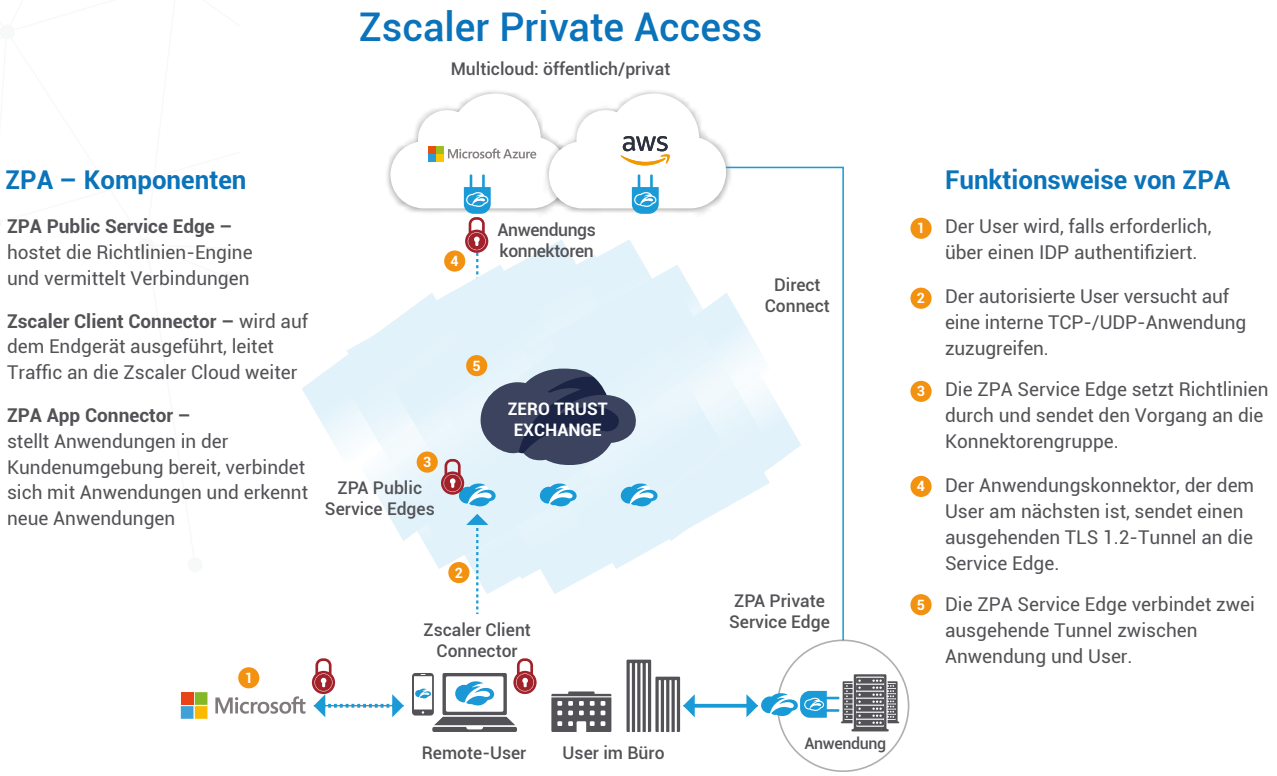
Da Verbindungen immer nur zwischen einzelnen Usern und einzelnen Anwendungen hergestellt werden, ist die Segmentierung auf Anwendungsebene gewährleistet, wobei die Notwendigkeit der Netzwerksegmentierung entfällt. Dies vereinfacht die Segmentierung und ermöglicht der IT, Richtlinien nach Benutzernamen und Hostnamen anstelle von IP-Adressen zu definieren.

ZPA vermittelt die Verbindung in Echtzeit über zwei ausgehende Tunnel – je einen von der Anwendung und vom User – an einem Service-Edge-Standort in möglichst unmittelbarer Nähe zum Gerät des Users.

Alle Vorteile einer Zero-Trust-Architektur, aber in der eigenen IT-Umgebung gehostet

Für Unternehmen, die das Hosting des ZPA Service Edge in der eigenen Umgebung vorziehen, bieten wir ZPA Private Service Edge als private Single-Tenant-Instanz mit dem gesamten Funktionsumfang einer öffentlich gehosteten ZPA Service Edge an. ZPA Private Service Edge kann wahlweise am physischen Unternehmensstandort oder in einer Cloud-Umgebung des Kunden gehostet werden und wird in jedem Fall von Zscaler verwaltet. ZPA Private Service Edge lädt alle relevanten Richtlinien und Konfigurationen aus der Cloud herunter und gewährleistet ihre lokale Durchsetzung.

ZPA Private Service Edge kann in Kombination mit klassischen ZPA-Services bereitgestellt werden, die von Zscaler gehostet werden. Um Latenzen zu vermeiden, stellt ZPA die Verbindung automatisch auf dem jeweils kürzesten Pfad zwischen User und Anwendung her.



Hauptvorteile von ZPA Private Service Edge

Geringere Komplexität und Kosten

Mit ZPA Private Service Edge erübrigt sich der Einsatz interner Firewalls und zusätzlicher Appliances. Dadurch lassen sich nicht nur die Kosten reduzieren, sondern es entfällt auch die Notwendigkeit einer aufwendigen Netzwerksegmentierung, um lokalen Usern sicheren Zugriff auf Anwendungen zu gewähren.

Hohe Verfügbarkeit

ZPA Private Service Edge speichert Zugriffsrichtlinien wochenlang im Cache, sodass User auch bei einem Ausfall der Internetverbindung sicher verbunden werden können. Dies gewährleistet die kontinuierliche Verfügbarkeit des Anwendungszugriffs unabhängig von der Konnektivität.

Zügiger Anwendungszugriff

Unter Priorisierung der lokalen ZPA Service Edge wählt ZPA automatisch den jeweils kürzesten und schnellsten Verbindungspfad zwischen User und Anwendung aus. Die dualen Zugriffsmöglichkeiten gewährleisten eine optimale Anwendererfahrung sowohl für lokale als auch für Remote-User, die auf On-Premise- oder Cloud-basierte Anwendungen zugreifen.

Compliance

In bestimmten Branchen, u. a. im Banken- und Finanzsektor, unterliegt die Nutzung Cloud-basierter Anwendungen strengen Regeln und Vorschriften. Durch die Option, die Services bei Bedarf lokal zu hosten, unterstützt ZPA Private Service Edge Unternehmen bei der Einhaltung dieser Vorschriften.

Zentral verwaltete Richtlinien mit lokaler Durchsetzung

Durch Verbindung mit dem ZPA-Cloud-Service wird gewährleistet, dass die von ZPA Private Service Edge durchgesetzten Unternehmensrichtlinien jederzeit auf dem aktuellen Stand sind. So kann sich die Organisation darauf verlassen, dass alle relevanten Richtlinien und Konfigurationen durchgesetzt werden. ZPA Private Service Edge speichert alle Richtlinien 14 Tage lang im Cache, um sie im Fall eines Internetausfalls für den lokalen User-Zugriff auf interne Anwendungen durchzusetzen.

ZPA Private Service Edge erleichtert Ihnen den sicheren Zugang zu privaten Anwendungen und bietet lokalen wie Remote-Benutzern eine identische Erfahrung beim Zugriff auf Applikationen im Rechenzentrum oder in der Cloud.

Fragen zu ZPA beantwortet unser Team jederzeit gerne unter: **sales@zscaler.com**.

Weitere Informationen zu **ZPA Private Service Edge**

Demo anfordern

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 auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA
+1 408 533 0288
www.zscaler.de