Absicherung von Fernarbeit:

Gewährleistung von Business Continuity mit Zscaler

zscaler™

Nichts ist derzeit wichtiger als die Gesundheit von Mitarbeitern und Mitgliedern der Gemeinschaft. Deshalb müssen Unternehmen das Risiko der Ansteckung mit dem Coronavirus (COVID-19) verringern. Gleichzeitig müssen Organisationen die Geschäftskontinuität sicherstellen und die Produktivität des Unternehmens erhalten, insbesondere wenn Mitarbeiter komplett auf Fernarbeit umsteigen. Plötzlich eine ganze Belegschaft von Remote-Mitarbeitern verwalten zu müssen, stellt Unternehmen vor enorme Herausforderungen.

> Dass sich die Investition in eine Cloud-First-Infrastruktur lohnt, zeigt sich besonders, wenn sie in einer VUCA-Umgebung [Volatility, Uncertainty, Complexity, Ambiguity] anwendbar ist.
>
> **Markus Sontheimer, CIO/CDO & Mitglied des Verwaltungsrats von DB Schenker**

Einige Unternehmen sind in der Lage, Remote-Management und eine komplette Belegschaft im Homeoffice zu bewältigen. Aber bei vielen Unternehmen überfordert die Aufgabe, alle Mitarbeiter (in manchen Fällen Hunderttausende von Benutzern) auf Remote-Access umzustellen, nicht nur die IT-Administratoren sondern auch die Architekturen, die sie verwalten.

Cyberkriminelle wittern in der Fernarbeitswelle eine Gelegenheit. Es gibt eine steigende Anzahl von Cyberangriffen unter dem Deckmantel Coronavirus, die sich gegen Menschen und Unternehmen auf der ganzen Welt richten. Betrüger verbreiten Malware, Ransomware, Bots usw., um unerfahrene Remote-Mitarbeiter und erweiterte Angriffsflächen auszunutzen.

Unternehmen müssen die Auswirkungen des Wechsels zur Fernarbeit erkennen:

Bandbreite

Für Unternehmen, die sich auf VPN-basierten Internetausgang für Fernarbeit verlassen, könnte es ein böses Erwachen geben. Ein rapider Anstieg des Traffic aus Video-Kollaborationen könnte bestehende Internetausgangsverbindungen überlasten. Zusätzliche VPN-Verbindungen werden die Infrastruktur überfordern.

Security-Übersicht

Fernarbeit muss sicher bleiben. Wie wird sich der Wechsel einer gesamten Belegschaft ins Homeoffice auf den Zugang zu benötigten Diensten und Applikationen auswirken? Kann der Security-Stack des Unternehmens die Traffic-Spitzen effektiv bewältigen?

Benutzererfahrung

SaaS-Anwendungen wie Office 365 erfordern ein optimiertes Routing – je mehr Netzwerkteilstrecken der Benutzer durchlaufen muss, desto größer ist die Verzögerung der Konnektivitätsleistung. Die Lage spitzt sich zu, wenn eine Vielzahl von Remote-Benutzern zuerst per VPN an einen zentralen Ort geleitet wird.

Kosten

Welche neue Software, IT-Ressourcen und Infrastruktur werden benötigt und wie viel kostet das alles?

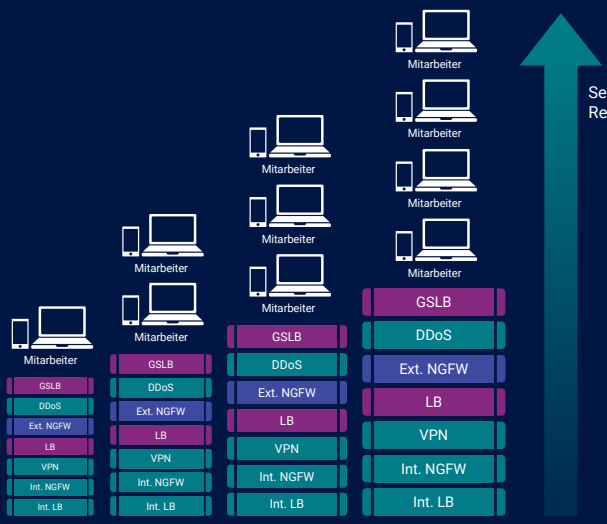
Zeitplanung

Wie schnell können Sie angesichts der Tatsache, dass die Einführung von Remote-tauglichen Betriebsmodellen Monate oder Jahre dauern kann, auf Fernarbeit umsteigen, und welche Strategie verfolgen Sie?

Regulatorisches Umfeld

In stark regulierten Branchen werden Compliance-Vorschriften in Krisenzeiten nicht unbedingt gelockert. Neue Remote-Mitarbeiter könnten versehentlich Zugang zu nicht genehmigten Anwendungen erhalten und dadurch das gesamte Unternehmen in Compliance-Verstöße verwickeln.

VPN-Probleme nehmen mit dem steigendem Bedarf der Remote-Benutzer zu



- Mehr Bedarf an Appliances aufgrund von Kapazitätsbeschränkungen
- Lizenzen für den „Ernstfall" bieten nur begrenzte Entlastung
- Bandbreitenverbrauch steigt sprunghaft an
- Betriebsaufwand wächst, während die Nutzererfahrung leidet

Abbildung 1. Mit der Zunahme von VPN-Benutzern und Traffic vermehren sich auch die Herausforderungen für Unternehmensnetzwerke.

VPN-Technologie erfordert Stacks von Gateway-Appliances mit unterstützender Infrastruktur (siehe Abbildung 1 oben), die nur begrenzte Bandbreiten- und Lizenzkapazität haben. Das VPN-Modell mit einem einzelnen Eintrittspunkt lässt eine externe Angriffsfläche offen und verursacht Leistungskosten für das Backhauling von Benutzer-Traffic zu Anwendungen in verteilten Umgebungen.

Zscaler Internet Access (ZIA) und Zscaler Private Access (ZPA) helfen dabei, Probleme mit Remote-Mitarbeitern zu mindern, da sie auf einem in der Cloud bereitgestellten Service basieren, der für den sicheren Zugriff auf SaaS, das Internet und private Anwendungen konzipiert ist.

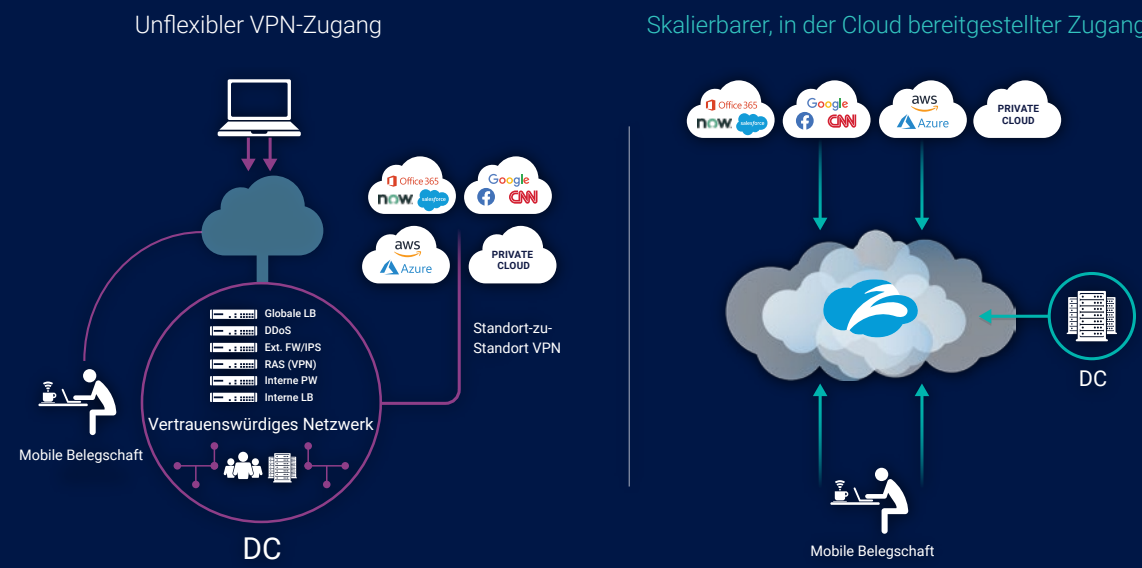


Abbildung 2. Das kostspielige, unflexible und nicht allzu sichere VPN-Zugangsmodell (links) ist bei Spitzen des Remote Access überlastet. In der Cloud bereitgestellter Remote Access wie bei Zscaler (rechts) skaliert, um steigender Fernarbeit gerecht zu werden.

Wie Zscaler sicheren Remote-Access ermöglicht

Geschäftsziele	Strategische Fähigkeiten	Kritische Taktik	Nutzung von Zscaler
Sicherstellen von Netzwerkkapazität (z. B. Schaltungsbandbreite, Hardware-Speicher oder Ressourcen usw.)	Unternehmen benötigen dynamische Skalierbarkeit, die für Bandbreite, Hardware, Speicher usw. nachhaltig ist, sowie Transparenz, um unwesentlichen Traffic eliminieren oder minimieren zu können.	Legen Sie die Netzwerkzeit für Benutzer nach Zeitzone und geografischem Standort fest. Priorisieren Sie Benutzer nach ihrer Rolle, sodass Schlüsselpersonen bei Bedarf auf das Netzwerk zugreifen können (C-Personal, Kundensupport).	Setzen Sie ZIA und ZPA ein, um direkt auf Applikationen und Daten im Internet zuzugreifen, und öffentliche Cloud-Dienste, damit Sicherheitsrichtlinien des Unternehmens für den gesamten Traffic ohne umständliches Weiterleiten durch Engpässe durchgesetzt werden.
Skalieren Sie flexibel mit minimalem Deployment-Aufwand	Integrieren Sie innerhalb kürzester Zeit eine stark erweiterte Gemeinschaft von Remote-Mitarbeitern, ohne das Betriebspersonal zu überlasten.	Nutzen Sie Cloud-basierten Anwendungszugang zur Vermeidung von Engpässen bei Applikationen, Lizenzierung und geografischer Verteilung.	Transferieren Sie Remote-Mitarbeiter zur Cloud-Plattform von Zscaler, um zuverlässigen, sicheren Anwendungszugang zu erhalten, der Hunderttausende neuer Benutzer innerhalb von Tagen, nicht Wochen oder Monaten, absorbieren kann.
Sicherer Mitarbeiterzugang zu Anwendungen und Daten	Mitarbeiter müssen auf Anwendungen und Daten zugreifen, wenn sie im Homeoffice arbeiten.	Legen Sie unternehmensspezifische Richtlinien und Sicherheitsvorschriften für Remote-Mitarbeiter fest, die auf Identität, Funktion, Zugangsbedingungen und geografischen Standorten basieren.	Setzen Sie ZPA und Connector ein und verwenden Sie die Zscaler App oder Browser-basierten Zugang, um Benutzer anhand individueller Richtlinien mit autorisierten Anwendungen zu verbinden. Dies ermöglicht sicheren Zugriff auf Anwendungen und Daten, eliminiert gleichzeitig eingehende Verbindungen von außen und reduziert die Angriffsfläche des Netzwerks.
Sichern Sie den Zugriff von Drittparteien auf Anwendungen und Daten ab.	Auftragnehmer, Berater, Anbieter und Partner müssen auf Anwendungen und Daten zugreifen können, ohne ins Netzwerk eingebunden zu sein.	Lassen Sie Drittparteien ausschließlich auf autorisierte Anwendungen zugreifen; durch Eliminieren der Netzwerkkonnektivität wird das Potenzial für laterale Bewegung minimiert.	Nutzen Sie ZPA für Browser-basierten Zugang, um Drittparteien granular kontrollieren und einsehen zu können – ohne Software installieren zu müssen.
Gewährleisten Sie nahtlosen Zugang zu privaten Anwendungen im Rechenzentrum und in der Multi-cloud	Benutzer müssen ohne teures Backhauling von einer Vielzahl von Backend-Umgebungen aus auf Anwendungen zugreifen können.	Stellen Sie dynamische, sichere, direkte Konnektivität zu Anwendungen an mehreren Standorten gleichzeitig bereit.	Setzen Sie ZPA-Connector in verschiedenen Backend-Anwendungsumgebungen ein; dynamische Pfadwahl gewährleistet transparenten, leistungsstarken Zugang für alle Remote-Mitarbeiter unabhängig vom Standort.
Schützen Sie die Geräte von Remote-Mitarbeitern	Geräte von Remote-Mitarbeitern müssen auch außerhalb der Sicherheitsgrenzen des Unternehmens geschützt werden.	Legen Sie zugangsspezifische Richtlinien fest, die je nach Situation auf Endgeräte angewendet werden.	Installieren Sie die Zscaler App auf allen Endgeräten, entweder über Push, das Self-Service-Portal oder über App Store oder Play Store. Nutzen Sie ZIA zur Durchsetzung von Richtlinien für diese Deployments der Zscaler App, um Schutz gemäß den Risikotoleranzniveaus zu garantieren.
Verwenden Sie SSL-Entschlüsselung für den gesamten ausgehenden Traffic	Untersuchen Sie sämtlichen Traffic zum Internet und zu SaaS-Applikationen, um sicherzustellen, dass Richtlinien, Bedrohungsanalysen, Erkennung und Wiederherstellung aktiviert sind, damit Bedrohungen gefunden und Infiltrationen verhindert werden.	Entscheiden Sie, ob alle Traffic-Kategorien untersucht werden müssen oder ob Ihr Risikoprofil Ausnahmen erlaubt (wie Compliance mit PCI DSS und HIPAA).	Aktivieren Sie SSL-Entschlüsselung für ZIA an allen Standorten und Endgeräten mithilfe von Zscaler-Zertifikaten (für das schnellste Deployment).
Stellen Sie fest, ob Dateien schädlich sind	Mitarbeiter müssen wahrscheinlich eine große Anzahl von Dateien zwischen internen wie externen Parteien austauschen.	Bestimmen Sie aus Risikosicht, welche Dateien von welchen Standorten eine Sandbox benötigen, und treffen Sie Entscheidungen auf Grundlage dessen, was das Unternehmen unterstützen kann.	Verwenden Sie ZIA, um eine Regel für das automatische Bereinigen der riskantesten Dateitypen zu aktivieren und Dateitypen für Quarantäne zu definieren.
Stellen Sie sicher, dass kritische Unternehmensdaten nicht exfiltriert werden	Unternehmen müssen dauerhaft sicherstellen, dass kritische Daten das Unternehmen nicht verlassen.	Präzisieren Sie die Regeln für Data Loss Prevention (DLP) und implementieren Sie Exact Data Match, um die Bewegung kritischer Daten effektiver einzuschränken.	Verwenden Sie vorab festgelegte und/oder benutzerdefinierte ZIA DLP-Regeln, um nach sensiblen Daten im Traffic-Fluss zu suchen.

Mit der richtigen Planung und den richtigen Maßnahmen können vom Ausbruch von Covid-19 betroffene Unternehmen die Sicherheit ihrer Mitarbeiter gewährleisten und gleichzeitig wichtige Geschäftsziele verfolgen. Die Cloud-basierte SASE-Plattform (Secure Access Service Edge) von Zscaler ist speziell dafür konzipiert, direkte Konnektivität über lokale Internet-Breakouts zu ermöglichen, damit Unternehmen (und ihre sämtlichen Remote-Mitarbeiter) auch in ungewissen Zeiten vorankommen können.

Um in dieser nie zuvor dagewesenen Situation zu helfen, führt Zscaler sein **Business Continuity Program** ein, das Organisationen dabei unterstützen soll, ihre Mitarbeiter zu schützen und die Produktivität des Unternehmens aufrecht zu erhalten.

Sichern Sie Ihre Remote-Belegschaft noch heute ab

zscaler™

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.