Lösungsprofil

Zscaler Resilience™

Ununterbrochene Business Continuity bei Stromausfällen, Brownouts und unvorhersehbaren Katastrophen

Business Continuity steht für IT-Führungskräfte an erster Stelle

Die gesamte Geschäftswelt hat sich innerhalb der letzten Jahre stark gewandelt und damit auch die Art und Weise, wie wir arbeiten. Business Continuity steht heute mit an erster Stelle, und eine der wichtigsten Aufgaben der IT-Verantwortlichen besteht darin, Unterbrechungen von geschäftskritischen Services zu verhindern und selbst bei Ausfällen anhaltende Produktivität sicherzustellen. Mit den richtigen Tools, Prozessen und Technologien können IT-Teams schnell und einfach die volle Funktionsfähigkeit ihrer Organisationen selbst im Katastrophenfall wiederherstellen.

Durch die Umstellung auf cloudbasierte Services für Storage, Computing und Sicherheit profitieren Organisationen von flexiblen und skalierbaren Systemen, optimierter Business Continuity, niedrigeren IT-Kosten und reduzierter Komplexität. Doch diese Vorteile reichen nicht aus, um auch im Falle unvorhersehbarer Ereignisse wie Naturkatastrophen, physischen Angriffen oder groß angelegten Cyberangriffen uneingeschränkte Business Continuity zu gewährleisten.

Zscaler Resilience kombiniert eine Vielzahl von robusten Funktionen, um Kunden im Fall von Stromausfällen, Brownouts und unvorhersehbaren Katastrophen diese unverzichtbare Business Continuity bereitzustellen. Die Lösung basiert auf der fortschrittlichen Architektur und der operativen Exzellenz der Zscaler Zero Trust Exchange™ und gewährleistet somit jederzeit hohe Verfügbarkeit und Servicebereitschaft. Unsere kundengesteuerten Funktionen zur Notfallwiederherstellung unterstützen in Kombination mit unterschiedlichsten robusten Failover-Optionen die Business-Continuity-Planung unserer Kunden für sämtliche Ausfallszenarien und machen die Security Cloud von Zscaler zur resilientesten der Branche

Warum ist Cloud-Resilienz so wichtig?

Ein wesentliches Ziel aller Führungskräfte besteht darin, eine Umgebung zu schaffen, in der ein Höchstmaß an Produktivität erreicht werden kann. IT-Teams müssen die wichtigsten Unternehmensfunktionen und die Produktivität selbst dann aufrechterhalten, wenn Konnektivitätseinschränkungen, Skalierungsprobleme oder Serviceausfälle den normalen Geschäftsbetrieb unterbrechen.

Um zuverlässige Business Continuity zu gewährleisten, ist es entscheidend, dass User jederzeit nahtlos auf geschäftskritische Anwendungen — SaaS, intern und privat — zugreifen können. Sollte es zu Unterbrechungen kommen, sind diese meist entweder auf einen Ausfall der Cloud oder der Anwendungskonnektivität zurückzuführen. Dementsprechend beinhaltet Cloud-Resilienz beide Aspekte: eine resiliente Cloud-Umgebung und resiliente Cloud-Verbindungen.

Resiliente Cloud-Umgebung
Eine resiliente Cloud-Umgebung basiert auf einer leistungsstarken Infrastruktur und verfügt über robuste Betriebsprozesse für alle gängigen Geschäftsfunktionen. Die Zscaler Cloud behebt viele kleinere Vorfälle wie Knotenausfälle oder Festplattenprobleme autonom, ohne dass Kunden eingreifen müssen, die Konnektivität beeinträchtigt wird oder die Performance leidet. Unsere stabilen, speziell entwickelten Hardwaresysteme mit überdimensionierter Verarbeitungskapazität und Redundanz bilden die Grundlage für eine hohe Resilienz.

Resiliente Cloud-Verbindungen
Resiliente Cloud-Verbindungen sind ein wesentlicher Aspekt einer umfassenden Cloud-Resilienz-Lösung. Damit User auf Anwendungen oder Daten zugreifen können, müssen sowohl die Cloud als auch entsprechende Verbindungswege verfügbar sein. Wenn der Zugriff auf die Cloud unterbrochen wird, muss ein alternativer, optimaler Pfad zu den Anwendungen gefunden werden. Dabei kommen verschiedene manuelle oder autonome Maßnahmen zum Einsatz, um Fehler zu beheben, die von einem Abfall der Netzwerkperformance bis hin zu vollständigen Ausfällen reichen. Zscaler Resilience kombiniert eine Vielzahl von robusten Funktionen, um Kunden sowohl bei geringfügigen Ausfällen als auch bei unvorhersehbaren Katastrophen verlässliche Business Continuity bereitzustellen.

Resiliente Cloud-Verbindungen bei verschiedensten Ausfallszenarien

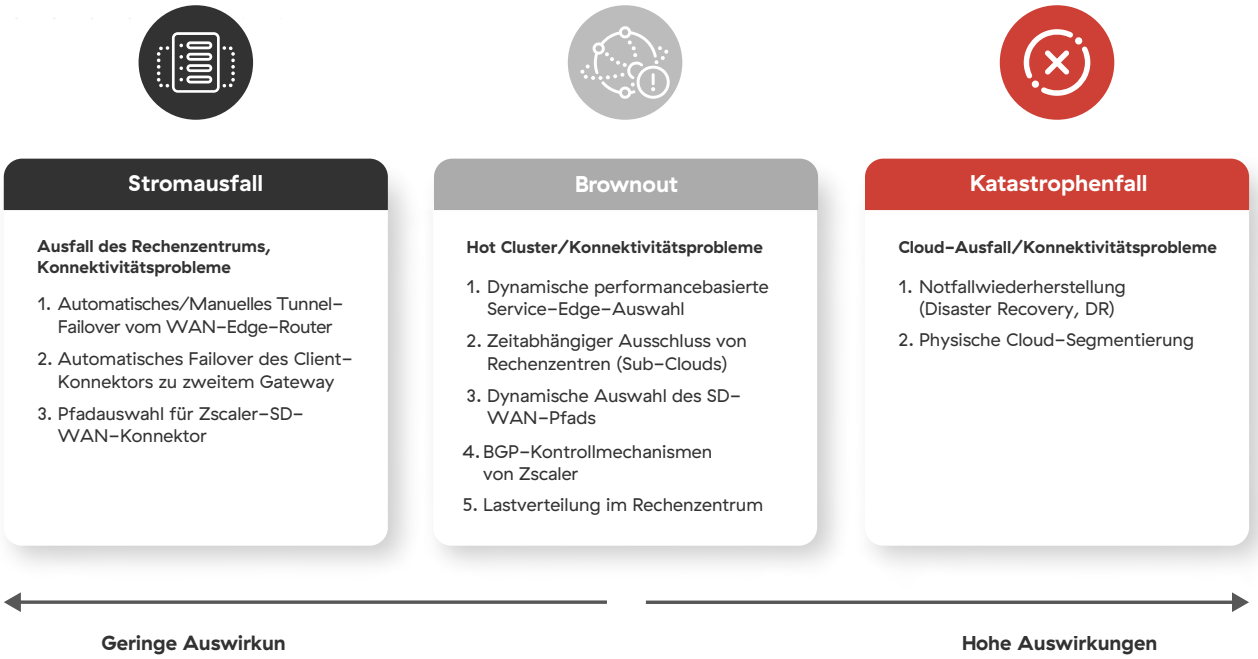

Abb. 1: Mehrere Optionen zur Reaktion auf Ausfallszenarien

Geringfügige Ausfälle

Geringfügige Ausfälle umfassen Performanceschwankungen, Kompatibilitätsprobleme und Betriebs- oder Qualitätsstörungen, die keine schwerwiegenden oder kritischen Auswirkungen haben. Knotenausfälle oder Festplattenprobleme sind oft die Ursache solcher isolierten Ausfälle, die zwar besonders häufig auftreten, aber meist unbemerkt bleiben und Verzögerungen, betriebliche Störungen und Frustration der User zur Folge haben. Mithilfe der robusten Architektur und operativen Exzellenz der Zscaler Cloud lassen sich solche Auswirkungen jedoch vermeiden. Geringfügige Ausfälle werden im Hintergrund mit minimaler Mitwirkung der Kunden behoben, während die Produktivität aufrechterhalten wird.

Entscheidende Vorteile von Zscaler Resilience

Business Continuity mit ununterbrochener Sicherheit

Wenden Sie kritische Sicherheitsrichtlinien an und stellen Sie Zero-Trust-Zugriff auf Internet, SaaS und private Anwendungen bereit, selbst im Fall unvorhergesehener Katastrophen.

Reibungslose Erfahrungen bei allen Vorfällen

Mit der erstklassigen Architektur und der operativen Exzellenz der Zscaler Zero Trust Exchange lassen sich Stromausfälle, Brownouts und katastrophenbedingte Ausfälle problemlos bewältigen.

Reduzierte Kosten und Komplexität

Vermeiden Sie Betriebsunterbrechungen und Produktivitätsverluste durch Probleme beim Zugriff auf kritische Anwendungen und verzichten Sie auf kostspielige Legacy-Infrastrukturen sowie On-Premise-VPNs.

Stromausfälle

Rechenzentrumsausfälle (z. B. der Ausfall der Interxion-Rechenzentren in London im Januar 2022) oder schwerwiegende Konnektivitätsprobleme, wie etwa Ausfälle von Netzbetreibern oder Transitanbietern, sind meist auf Unterbrechungen der Stromversorgung zurückzuführen. Infolgedessen können Unternehmen ihren Traffic nicht mehr an das betroffene Zscaler-Rechenzentrum weiterleiten. Unsere redundante Architektur — betreiberunabhängige Rechenzentren mit mehreren Anbietern und Internet Exchange (IX) — verhindert Ausfälle effektiv, wenn Vorfälle bei einzelnen Netzbetreibern oder andere Konnektivitätsprobleme auftreten. Unabhängig von der Wiederherstellungszeit ist es unseren Kunden aber nicht möglich, die Services des betroffenen Rechenzentrums weiter zu nutzen.

Daher müssen sie den Traffic zu einem sekundären Zscaler-Rechenzentrum in der Nähe umleiten. Wir arbeiten mit verschiedenen Netzbetreibern und Rechenzentrumsanbietern zusammen, um Störungen bei einem bestimmten Anbieter effektiv auszugleichen und sicherzustellen, dass das sekundäre Rechenzentrum verfügbar ist. Zudem halten wir Reservekapazitäten im Rechenzentrum vor, um zusätzliche vorübergehende Lasten zu unterstützen.

Bei Business Continuity geht es darum, verschiedene mögliche Ausfallszenarien zu durchdenken und sich auf diese vorzubereiten. Die Infrastruktur von Zscaler ist genau für diese Szenarien konzipiert und darauf ausgelegt, eine 100-prozentige Verfügbarkeit zu gewährleisten.

Traffic aus einem Büro über ein SD-WAN-Gerät
Wenn Sie Traffic aus einem Büro über ein Routing-/SD-WAN-Gerät senden, benötigen Sie einen einsatzbereiten Backup-IPsec-/GRE-Tunnel, wenn der primäre Tunnel nicht erreichbar ist. Wie genau das Failover ausgelöst wird, hängt von den Funktionen des Geräts und dem Netzwerkdesign ab. Ein SD-WAN mit zwei Internetleitungen könnte beispielsweise automatisch auf den Backup-Tunnel auf einer zweiten Leitung umschalten, wenn der aktive Tunnel nicht mehr erreichbar ist oder eine Latenzschwelle überschreitet (bei aktivierten L7-Zustandsprüfungen). Bei technisch weniger komplexen Geräten muss der Backup-Tunnel manuell aktiviert werden. Sobald das primäre Rechenzentrum wieder in Betrieb ist, liegt es in der Verantwortung des Kunden, den Wechsel zurück vorzunehmen.

Traffic über Zscaler Client Connector
Beim Senden von Traffic über Zscaler Client Connector (ZCC) kontrolliert Zscaler beide Edges des Tunnels und führt automatisch ein Failover vom primären zum sekundären Gateway durch, wobei die Logik der App-Profile-PAC-Datei verwendet wird. Zscaler Client Connector leitet den Traffic wieder zum primären Gateway, sobald dieses erreichbar ist. In bestimmten Fällen haben Kunden die Möglichkeit, die PAC-Dateien manuell zu ändern, um ein Failover auszulösen.

Brownouts

Ein unbeabsichtigter oder unerwarteter Abfall der Netzwerkservicequalität weist in der Regel auf einen Brownout hin. Der falsche Umgang mit einem Brownout kann kostspielig sein, sowohl im Hinblick auf Umsatz- als auch auf Produktivitätsverluste. Wenn User einen Brownout melden, bevor das IT-Team ihn entdeckt und mit der Behebung beginnen kann, führt dies mitunter zu Verzögerungen und großer Frustration bei den Usern. Zusätzlich zu den Maßnahmen, die bei Stromausfällen ergriffen werden, bietet Zscaler wie unten beschrieben noch weitere spezielle Funktionen, um die Auswirkungen eines Brownouts zu mindern.

Dynamische performancebasierte Service-Edge-Auswahl von Zscaler
Zscaler Client Connector wählt den optimalen Pfad zwischen dem primären und dem sekundären ZIA Service Edge und berücksichtigt dabei nicht die geografische Nähe, sondern orientiert sich stattdessen am Zustand der jeweiligen ZIA Service Edge, wie in Abbildung 2 dargestellt. Die Latenz wird über eine durchgehende HTTP-Verbindung berechnet, indem kontinuierlich beide Gateways angepingt werden. Auf diese Weise werden Rechenzentren latenzbasiert ausgewählt und Ihr Unternehmen bleibt auch im Fall eines Brownouts leistungsfähig.

Kundengesteuerter Ausschluss von Rechenzentren
Eine weitere Möglichkeit, die Business Continuity während eines Brownouts aufrechtzuerhalten, ist der kundengesteuerte Ausschluss von Rechenzentren, wie in Abbildung 3 zu sehen. Sollten also Beeinträchtigungen bei einem Rechenzentrum auftreten, beispielsweise beim Peering einer SaaS-Anwendung in LAX (deren Behebung mitunter Stunden dauert), kann dieses Rechenzentrum über das Administrationsportal von der Sub-Cloud ausgeschlossen werden. Zscaler Client Connector ruft dann das neue primäre und sekundäre Gateway ab und stellt einen Z-Tunnel zu einem neuen Rechenzentrum her. Dieser kundengesteuerte Ausschluss von Rechenzentren gilt nur für einen bestimmten Zeitraum — nach dessen Ablauf wird automatisch wieder das ursprüngliche Rechenzentrum verwendet.

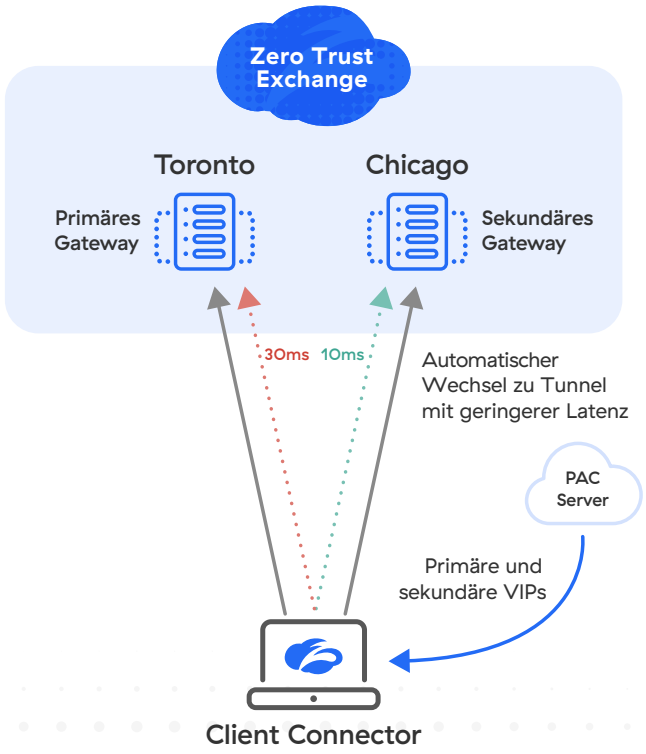

Abb. 2: Dynamische performancebasierte Service-Edge-Auswahl

Tunnel-Failover von Routing-Geräten mit Brownout-Erkennung
Wenn der Traffic aus einem Büro über ein Routing-/SD-WAN-Gerät gesendet wird, über das Zscaler keine direkte Kontrolle hat, beschränken sich die Optionen des Kunden auf die Funktionen des Edge-Geräts. Ein SD-WAN-Router kann beispielsweise eine Verschlechterung des Service mithilfe proprietärer Algorithmen erkennen, die auf L7-Zustandsprüfungen auf Testendgeräten von Zscaler basieren. Sobald ein potenzieller Brownout identifiziert wird, kann das SD-WAN-Gerät automatisch ein Failover auf einen Backup-Tunnel auf derselben oder auf einer sekundären Leitung durchführen. Das Gerät kehrt zum primären Tunnel zurück, sobald die Zustandsprüfungen bessere Ergebnisse liefern.

BGP-Kontrollmechanismen von Zscaler
Unsere redundante Architektur — betreiberunabhängige Rechenzentren mit mehreren Anbietern und Internet Exchange (IX) — minimiert die Auswirkungen von Brownouts, Überlastung oder anderen Problemen mit einzelnen Netzbetreibern erheblich. Sobald Zscaler CloudOps feststellt, dass ein Upstream-ISP den Traffic nicht optimal routet, leiten wir ihn über einen sekundären ISP um, während wir mit dem primären ISP an einer Lösung des Problems arbeiten.

Lastverteilung in Zscaler-Rechenzentren
Bei Netzwerküberlastung oder anderen Konnektivitätsproblemen mit einem bestimmten Rechenzentrum kann Zscaler Clients mithilfe von Zscaler Client Connector proaktiv auf sekundäre Rechenzentren in geografischer Nähe umleiten, ohne auf statistische Daten zurückgreifen zu müssen.

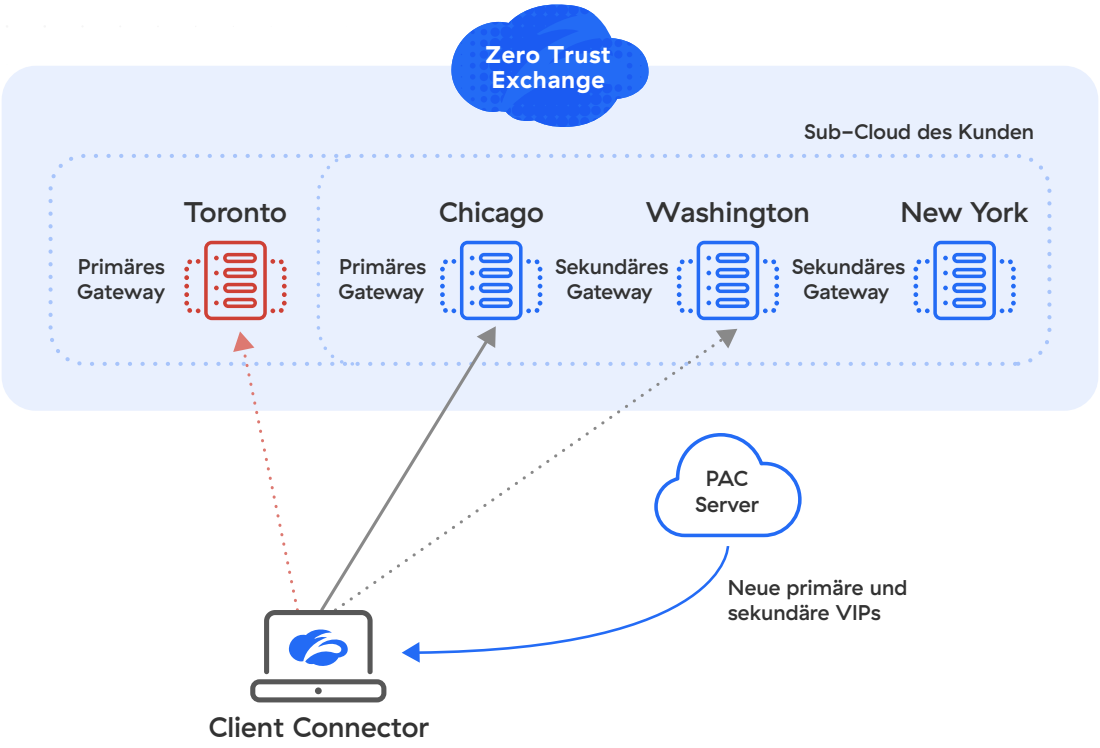

Abb. 3: Kundengesteuerter Ausschluss von Rechenzentren

Katastrophenfall

Notfallwiederherstellungsfunktion von Zscaler für ZIA/ZPA

Die Notfallwiederherstellung (Disaster Recovery, DR) von Zscaler für die Cloud bietet Usern unterbrechungsfreie Betriebsabläufe und gewährleistet selbst im Falle unvorhersehbarer Katastrophen nahtlosen Zugriff auf alle unternehmenskritischen Anwendungen.

Die Notfallwiederherstellung von Zscaler ist eine kundenseitig gesteuerte Business-Continuity-Lösung, mit der Organisationen ihre Funktionsfähigkeit selbst bei großflächigen Ausfällen, die die Zscaler Cloud beeinträchtigen, aufrechterhalten.

Diese Notfallwiederherstellung wird durch die Aktualisierung des DNS-TXT-Eintrags eingeleitet. Sobald ein DR-Failover initiiert wird, wird durch die Notfallwiederherstellung von Zscaler ein Pfad eingerichtet, über den User standortunabhängig auf unternehmenskritische private und SaaS-Anwendungen sowie das Internet zugreifen (siehe Abbildung 4). Dabei haben Kunden die volle Kontrolle darüber, welche Anwendungen während eines globalen Ausfalls der Zscaler Cloud verfügbar sein sollen.

Die Verbindung zu privaten Anwendungen wird über die Private Service Edge von Zscaler Private Access™ (ZPA™) — eine lokal bereitgestellte Version der Zscaler Cloud — hergestellt. Für den Zugriff auf kritische SaaS-Anwendungen und das Internet werden Richtlinien verwendet, die in der AWS S3-Instanz gespeichert sind. Jeder Kunde mit installiertem Zscaler Client Connector kann die Notfallwiederherstellung von Zscaler nutzen. Durch den selbst initiierten, DNS-basierten DR-Trigger haben Kunden die Option, individuell festzulegen, wann die Notfallwiederherstellung aktiviert werden soll.

Um sicheren Zugriff auf private Anwendungen zu gewährleisten, können Administratoren im Administrationsportal von Zscaler die Notfallwiederherstellung für kritische Anwendungssegmente, App-Connector-Gruppen und ZPA-Private-Service-Edge-Gruppen konfigurieren, um im Falle einer Katastrophe, die sich auf die globale ZPA-Cloud-Infrastruktur auswirkt, ununterbrochene Business Continuity zu bieten.

Zugriff auf individuell definierte kritische Anwendungen
Kunden haben die Möglichkeit, vorab im ZPA UI-Dashboard festzulegen, welche Anwendungen im Katastrophenfall für die Business Continuity entscheidend sind, damit User während eines DR-Ereignisses darauf zugreifen können.

Um sicheren Zugriff auf Internetanwendungen über Zscaler Internet Access™ (ZIA™) zu gewährleisten, stehen Administratoren die folgenden Optionen für die Notfallwiederherstellung zur Verfügung. Diese werden über Zscaler Client Connector bereitgestellt und im Zscaler-Portal konfiguriert:

- **Fail Open:** Bei einem unwahrscheinlichen Ausfall der Zscaler Cloud erhalten User direkten Zugang zum Internet. Dazu müssen Sie allerdings allen Usern uneingeschränkten Zugriff auf jede Website im Internet gewähren — ohne Sicherheitsbeschränkungen.
- **Controlled Fail Open — Zugriff auf eine von Zscaler definierte Liste von Internetzielen:** User haben Zugriff auf die gängigsten und wichtigsten Anwendungen im Internet (Office 365, Google Workspace, etc.). Zscaler verwaltet diese Liste, die auf AWS gehostet wird, sodass sie auch dann verfügbar ist, wenn die Zscaler Cloud von einem Ausfall betroffen sein sollte. Kunden können dieser Liste eigene Websites hinzufügen. Jede Website, die nicht enthalten ist, wird blockiert und der Zugriff auf dem Endgerät über Zscaler Client Connector entsprechend verhindert. Zscaler Client Connector lädt diese Liste zudem regelmäßig herunter, damit sie jederzeit auf dem neuesten Stand ist.
- **Fail Closed:** Sicherheitsbewusste Kunden, die nicht möchten, dass User ohne ZIA auf Ziele im Internet zugreifen, haben die Möglichkeit, den gesamten Zugriff zu unterbinden.

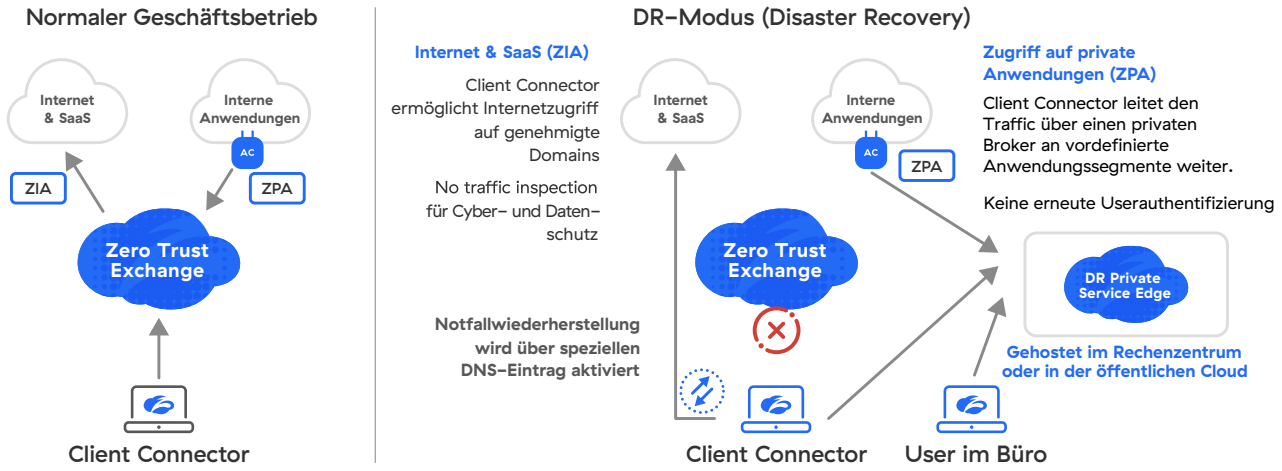

Abb. 4: Notfallwiederherstellung für unternehmenskritischen Zscaler-Service

Dank der Notfallwiederherstellung sorgen Sie selbst im Falle einer unvorhersehbaren Katastrophe, die die globale Infrastruktur der Zscaler Cloud beeinträchtigt, weiter für Business Continuity. Durch diese Implementierung können User von überall auf der Welt weiterhin nahtlos auf wichtige Anwendungen zugreifen.

Während des normalen Betriebs wird der Zugriff auf unternehmenskritische Anwendungen über die Zero Trust Exchange vermittelt. Kommt es zu großflächigen Ausfällen, erfolgt die Verbindung zu privaten Anwendungen über die ZPA Private Service Edge, die lokal im Rechenzentrum oder in der privaten Cloud des Kunden bereitgestellt wird. Alle Verbindungen zum Internet und zu SaaS-Anwendungen werden über im AWS S3-Bucket gespeicherte Richtlinien durchgesetzt. Auf diese Weise stellen wir selbst im Katastrophenfall eine nahtlose Anwendererfahrung bereit. Sobald die volle Funktionsfähigkeit der Zscaler Cloud wiederhergestellt ist, können Sie zum normalen Betrieb zurückkehren und die Vorteile der Zero Trust Exchange hinsichtlich Zero-Trust-Sicherheit und -Konnektivität wieder vollumfänglich nutzen. Zscaler Digital Experience erkennt geringfügige Störungen, Brownouts und Stromausfälle und unterstützt Sie bei deren Behebung, bevor es zu ernsthaften Beeinträchtigungen kommt. Durch die uneingeschränkte Flexibilität der Zscaler-Plattform erzielen Sie also nicht nur zuverlässige Business Continuity, sondern auch erstklassige Sicherheit und eine optimale User Experience.

Zscaler Resilience being part of the overall Zscaler Resilience ist Teil unserer umfassenden Plattform und bietet Ihnen inhärente Redundanz, sodass Sie auf keine zusätzlichen externen Services zurückgreifen müssen. Zscaler sieht es als seine Aufgabe, seine Resilienz-Lösungen kontinuierlich weiterzuentwickeln und zu optimieren, um sowohl Usern als auch IT-Teams jederzeit eine reibungslose Anwendererfahrung zu bieten.

Entscheidende Vorteile der Notfallwiederherstellung von Zscaler

- Minimale Betriebsunterbrechung auch bei großflächigen Ausfällen
- Zugriff auf unternehmenskritische Anwendungen selbst im Fall von unvorhergesehenen Katastrophen • Zuverlässigerer Anwendungszugriff dank Zscaler
- Kosteneinsparungen, da nur eine Plattform für den Anwendungszugriff im Normalbetrieb und der Notfallwiederherstellung verwaltet werden muss
- Potenzielle Einsparungen durch Vermeidung von Produktivitätsverlusten aufgrund von Unterbrechungen während eines Ausfalls

Weitere Informationen zu Zscaler Resilience finden Sie unter zscaler.de/resilience.

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter und sicherer arbeiten können. Die 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 auf über 150 Rechenzentren auf der ganzen Welt verteilt und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de