Zscaler Resilience™

Ununterbrochene Business Continuity bei Blackouts, Brownouts und unvorhersehbaren Katastrophen

Lösungsprofil

Business Continuity steht für IT-Führungskräfte an erster Stelle

Wir arbeiten heute anders als früher. Durch diesen Wandel bedingt ist Geschäftskontinuität für IT-Verantwortliche zur obersten Priorität geworden. Dazu zählt insbesondere, Unterbrechungen unternehmenskritischer Dienste zu verhindern und die Produktivität jederzeit aufrechtzuerhalten. Mit den richtigen Tools, Prozessen und Technologien können IT-Verantwortliche auch bei Ausfallszenarien schnell und einfach die volle Funktionsfähigkeit des Unternehmens wiederherstellen.

Durch die Umstellung auf cloudbasierte Services für Storage, Computing und Sicherheit profitieren Unternehmen 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 ist ein komplettes Set an Resilience-Funktionen, das eine unterbrechungsfreie Geschäftskontinuität für Kunden bei Blackouts, Brownouts and katastrophalen Ausfallszenarien gewährleistet. Die Lösung basiert auf der Architektur der Zscaler Zero Trust Exchange™ und wird durch operative Exzellenz erweitert, um Kunden jederzeit hohe Verfügbarkeit und Wartungsfreundlichkeit zu bieten. Die kundengesteuerten Disaster-Recovery-Funktionen von Zscaler unterstützen in Kombination mit einem robusten Satz an Failover-Optionen die Business-Continuity-Planung der Kunden bei allen Ausfallszenarien. Diese umfassenden Funktionen machen die Zscaler Security Cloud zur branchenweit sichersten und resilientesten Cloud.

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

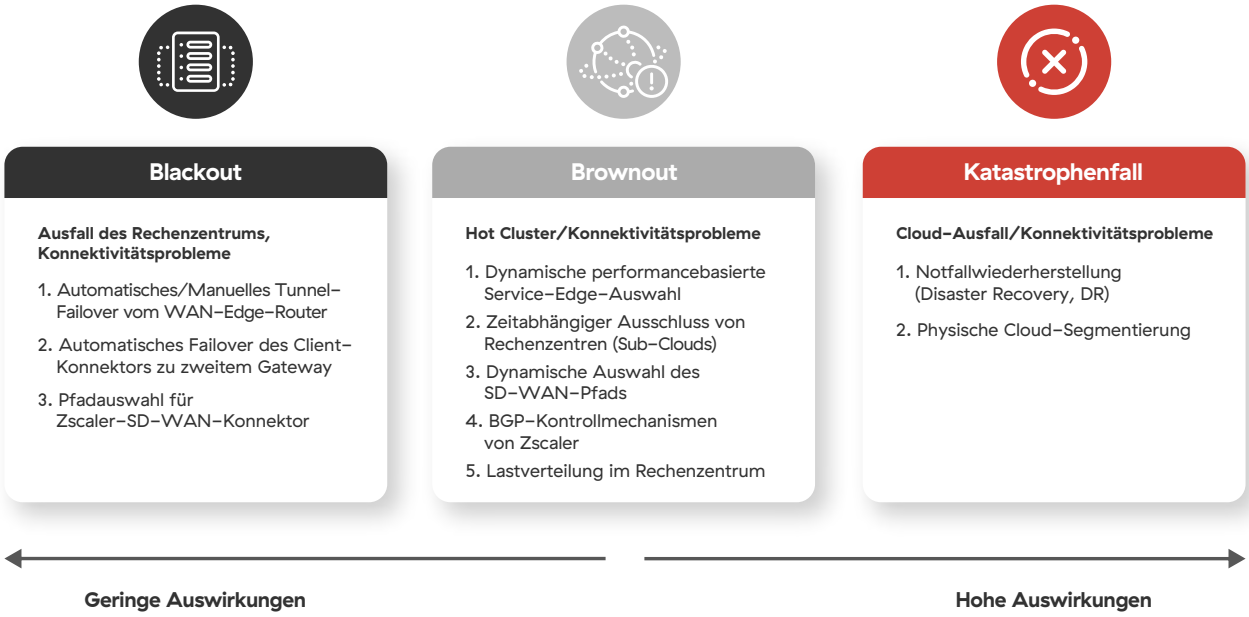

Abb. 1: Mehrere Optionen zur Reaktion auf Ausfallszenarien

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

Setzen Sie zentrale Sicherheitsrichtlinien um und gewähren Sie auch in Notfallszenarien Zero-Trust-Zugriff auf Internet, SaaS und private Unternehmensanwendungen.

Eine reibungslose User Experience in allen Szenarien

Blackouts, Brownouts und katastrophale Ausfallszenarien lassen sich mit der branchenführenden Architektur und operativen Exzellenz der Zero Trust Exchange problemlos bewältigen.

Weniger Kosten und Komplexität

Vermeiden Sie Geschäftsunterbrechungen und Produktivitätseinbußen durch fehlenden Zugriff auf wichtige Anwendungen. Und eliminieren Sie zugleich die Kosten für veraltete Backup-Infrastrukturen und lokale VPNs.

Blackouts

Rechenzentrumsausfälle (z. B. der Ausfall des Interxion-Rechenzentrums 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 Unternehmensstandort über ein SD-WAN-Gerät

Beim Senden von Traffic aus einem Unternehmensstandort über ein Routing-/SD-WAN-Gerät müssen Kunden die Best Practices für die Bereitstellung von Zscaler befolgen, indem sie einen IPsec/GRE-Tunnel als Backup für Fälle einrichten, in denen der primäre Tunnel nicht erreichbar ist. Wie das Failover konkret ausgelöst wird, hängt von den Funktionen des Geräts sowie dem Netzwerkdesign ab. Beispielsweise könnte ein SD-WAN mit dualen Internetverbindungen automatisch auf den Backup-Tunnel einer sekundären Verbindung umschalten, wenn der aktive Tunnel nicht erreichbar ist oder einen Latenzschwellenwert überschreitet (bei aktivierten L7-Integritätsprüfungen). Bei einfacheren Geräten müssten Kunden den Backup-Tunnel manuell aktivieren. Sobald das primäre Rechenzentrum wieder verfügbar ist, liegt die Verantwortung für die Rückschaltung beim Kunden.

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. Die falsche Handhabung eines Brownouts kann kostspielig sein, sowohl im Hinblick auf Umsatzeinbußen als auch auf Produktivitätsverluste. Wenn User einen Brownout melden, bevor die IT-Verantwortlichen ihn entdeckt und mit der Behebung begonnen haben, kann dies zu großer Frustration führen. Zusätzlich zu den Möglichkeiten zur Behebung von Blackouts hilft Zscaler bei der Minderung ihrer Folgen, wie nachstehend erläutert.

Dynamische Performance-basierte Service-Edge-Auswahl durch 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 Geschäftskontinuität bei Blackouts aufrechtzuerhalten, ist die kundengesteuerte Auswahl von Rechenzentren, wie in Abbildung 3 dargestellt. Wenn ein Kunde Kapazitätsprobleme in einem Rechenzentrum hat, beispielsweise ein Peering-Problem mit einer SaaS-Anwendung in LAX (dessen Behebung Stunden dauern kann), kann dieses Rechenzentrum im Admin-Portal von der Subcloud ausgeschlossen werden. Der Zscaler Client Connector ruft dann das neue primäre und sekundäre Gateway ab und richtet einen Z-Tunnel zu einem neuen Rechenzentrum ein. Dieser kundengesteuerte Ausschluss von Rechenzentren ist zeitlich begrenzt und kehrt nach einer festgelegten Zeit zur ursprünglichen Auswahl des Rechenzentrums zurück.

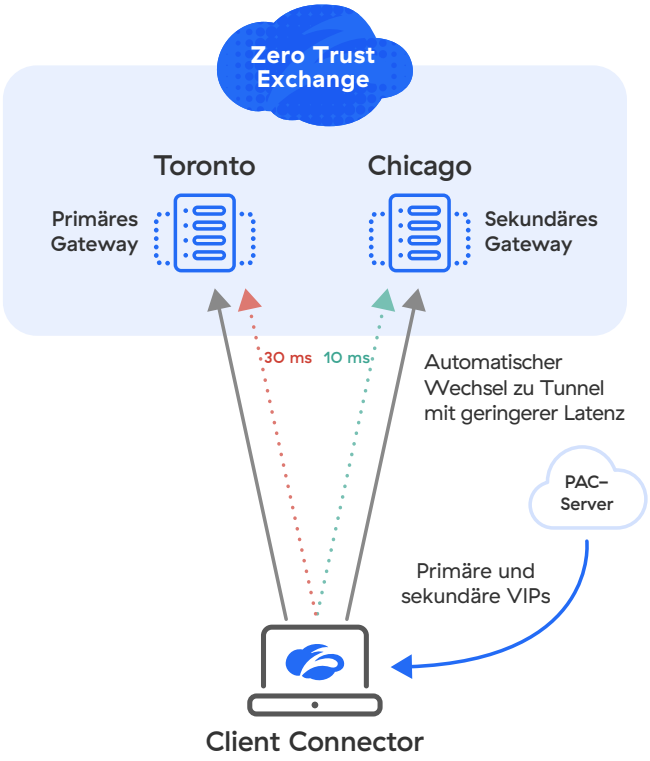

Abb. 2: Dynamische performancebasierte Service-Edge-Auswahl

Tunnel-Failover von Routing-Geräten bei 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.

Zscaler BGP-Steuerungen
Unsere redundante Architektur — betreiberneutrale Rechenzentren mit mehreren Anbietern und Internet-Exchange (IX) — minimiert effektiv Brownouts, Überlastungen oder andere Probleme mit einzelnen Anbietern. Wenn Zscaler CloudOps feststellt, dass ein Upstream-ISP kein optimales Routing bietet, können wir den Datenverkehr über einen sekundären ISP umleiten, während wir mit dem primären ISP an der Lösung des Problems arbeiten.

Lastverteilung in Zscaler-Rechenzentren
Im Falle einer Netzwerküberlastung oder von Verbindungsproblemen in einem bestimmten Rechenzentrum kann Zscaler Clients mithilfe des Zscaler Client Connector proaktiv zu nahegelegenen sekundären Rechenzentren umleiten und so einen nahtlosen Service gewährleisten, ohne auf statistische Methoden angewiesen zu sein.

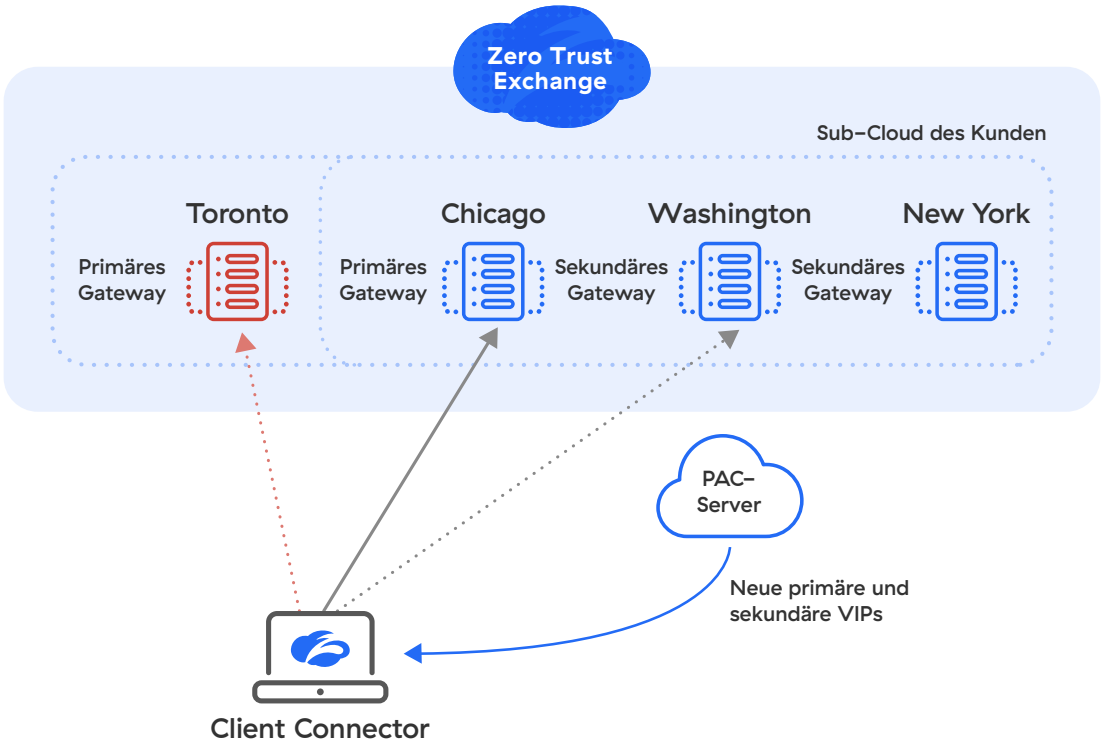

Abb. 3: Kundengesteuerter Ausschluss von Rechenzentren

Katastrophenfall

Zscaler Business Continuity für ZIA/ZPA

Zscaler Business Continuity für die Cloud bietet Usern unterbrechungsfreie Betriebsabläufe und gewährleistet selbst im Falle unvorhersehbarer Ausfallszenarien nahtlosen Zugriff auf alle unternehmenskritischen Anwendungen.

Unternehmen sind auf einen unterbrechungsfreien Zugriff auf Anwendungen angewiesen, ohne die Zero-Trust-Sicherheit bei Ausfallszenarien oder in Zeiten mit eingeschränktem Zugriff auf die Infrastruktur zu beeinträchtigen. Darüber hinaus müssen in vielen Branchen Compliance- und aufsichtsrechtliche Standards für die Geschäftskontinuität eingehalten werden.

Um diesen Anforderungen gerecht zu werden, bietet Zscaler die Option einer privaten Business-Continuity-Cloud, um den Betrieb von Unternehmen auch während eines katastrophalen Ausfallszenarios aufrechtzuerhalten, das die öffentliche Cloud von Zscaler beeinträchtigen könnte.

Wenn die öffentliche Cloud von Zscaler nicht erreichbar oder nicht verfügbar ist, können Kunden in den Business-Continuity-Modus wechseln. In diesem Zustand werden Richtlinien und Userauthentifizierung weiterhin von Zscaler-Services erzwungen, die auf einer vom Kunden gehosteten virtuellen Maschine ausgeführt werden.

Business Continuity für ZIA

Um einen unterbrechungsfreien Zugriff auf das Internet und SaaS-Anwendungen zu gewährleisten und die Konformität aufrechtzuerhalten, bietet Zscaler die Möglichkeit eines Failovers auf eine private Business-Continuity-Cloud, die aus vom Kunden gehosteten privaten ZIA-Service-Edges und einem privaten Richtlinien-Cache besteht.

Die PSEs bieten eine konsistente Trafficverarbeitung und unterstützen Funktionen wie Traffic-Überprüfung und Firewall für User, die den Client Connector von Zscaler ausführen. Bei einem Ausfall werden diese privaten Service-Edges durch einen privaten Richtlinien-Cache unterstützt, der eine zwischengespeicherte Kopie der Kundenkonfiguration enthält.

Kunden, die keine selbst gehosteten Funktionen bereitstellen möchten, ermöglicht die Business-Continuity-Lösung von Zscaler im Falle eines Ausfalls den fortlaufenden Zugriff auf die Web- und SaaS-Anwendungen. Kunden können in diesem Szenario eine von drei Optionen wählen:
Fail Open: Uneingeschränkter Internetzugang ohne Sicherheitsbeschränkungen
Vordefinierte AllowList: Uneingeschränkter Zugriff auf eine begrenzte Anzahl gängiger Anwendungen
Fail Closed: Der gesamte Internetzugang ist für die Dauer des Ausfalls gesperrt

Business Continuity für ZPA

Um während eines Ausfalls einen unterbrechungsfreien Zugriff auf private Unternehmensanwendungen zu gewährleisten, haben Kunden die Option, eine eigene private Business-Continuity-Cloud bereitstellen. Dabei handelt es sich um logische Gruppierungen der folgenden Komponenten, die jeweils in einer Gruppe bereitgestellt werden können, um zusätzliche Redundanz zu gewährleisten:
Private Cloud Controller, die Konfiguration und Richtlinien kontinuierlich mit der Zscaler-Cloud synchronisieren,
ZPA Private Service Edges, die öffentliche ZPA-Funktionen in der Umgebung des Unternehmens bereitstellen
App Connectors für den sicheren Zugriff auf private Services
Protokollempfänger zum Erfassen von Protokollausgaben anderer Komponenten

Im Falle eines katastrophalen Ausfalls oder wenn die Zscaler-Cloud nicht erreichbar ist, stellen User zur Authentifizierung und Umleitung an die privaten Service-Edges von ZPA automatisch eine Verbindung zu den Private Cloud Controllern her. Sobald eine Verbindung mit der PSE besteht, liegt der Steuer- und Datenkanal bei der ZPA-PSE.

Die als virtuelle Maschine bereitgestellten Private Cloud Controller gewährleisten bei einem Ausfall kritische Funktionen:

- Authentifizierungsumleitung
- Userumleitung
- Protokoll Streaming-Service
- Synchronisierung der Kundenkonfiguration
- Synchronisierung der Kundenrichtlinien

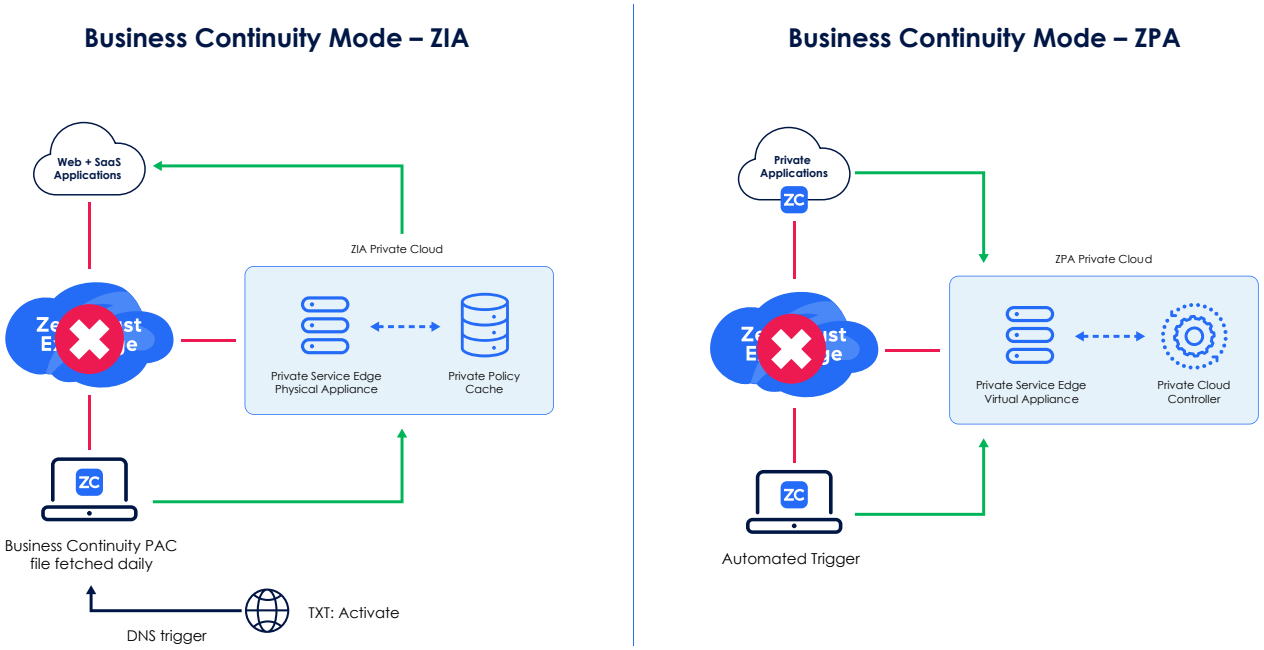

Abb. 4: Private Business-Continuity-Clouds gewährleisten Zugriff auf alle Anwendungen mit umfassendem Sicherheitsstatus

Geschäftskontinuität für Endgeräte

Ein weiteres Problem, das für ein Unternehmen verheerende Folgen haben kann, ist die Unfähigkeit, seine regulären Endgeräte (Laptops, Computer usw.) zu verwenden, wenn diese aus irgendeinem Grund nicht verfügbar sind: aufgrund einer Fehlfunktion, weil sie nicht vorhanden oder kompromittiert sind. Um dieses Szenario zu bewältigen, kann Zscaler Cloud Browser Isolation eingesetzt werden, um einen sicheren browserbasierten Zugriff auf private, Web- oder SaaS-Anwendungen von nicht verwalteten Endgeräten (wie BYOD) ohne Risiko eines Datenverlusts bereitzustellen.

Zscaler Business Continuity — Fazit

Nachdem die Funktionalität der Zscaler Cloud wiederhergestellt wird, kann das Produkt zum Normalbetrieb zurückkehren, um alle Vorteile der Zero-Trust-basierten Sicherheit und -Konnektivität der Zero Trust Exchange voll auszunutzen. Zscaler Digital Experience erkennt kleinere Störungen, Brownouts und Blackouts und hilft Kunden, diese zu beheben, bevor sie drastische Auswirkungen auf die User haben. Die Zscaler-Plattform sorgt für volle Flexibilität für Geschäftskontinuität mit unübertroffener Sicherheit und einer nahtlosen User Experience.

Zscaler Business Continuity als Modul der Zscaler-Plattform gewährleistet Redundanz innerhalb der Plattform, ohne dass zusätzliche Lösungen von Drittanbietern erforderlich sind. Die Resilienz-Lösungen von Zscaler werden kontinuierlich weiterentwickelt und optimiert, um sowohl Usern als auch IT-Teams jederzeit eine reibungslose Anwendererfahrung zu bieten.

Hauptvorteile der Business-Continuity-Lösungen von Zscaler

- Minimale Betriebsunterbrechung für Kunden auch bei katastrophalen Ausfallszenarien
- Zugriff auf unternehmenskritische Anwendungen auch während eines Black-Swan-Ereignisses
- Erhöhte Lösungszuverlässigkeit für den Anwendungszugriff mit 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

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

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler 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 SSE-basierte Zero Trust Exchange ist auf über 150 Rechenzentren der ganzen Welt verteilt und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.com/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.com/de