# DNS-Ausfallsicherheit

## Duale Anbieter- und duale Infrastruktur-Strategie – worauf es bei DNS-Redundanz ankommt

# DNS-Ausfallsicherheit

## Duale Anbieter- und duale Infrastruktur-Strategie – worauf es bei DNS-Redundanz ankommt

Viele Unternehmen betrachten eine duale Anbieter-Strategie als die Lösung für DNS-Ausfallsicherheit. Das klingt zunächst überzeugend, lässt aber die eigentliche Problemstellung außer Acht. Es geht nicht um die Anzahl der Anbieter, sondern um die Ausfallsicherheit der Infrastruktur.

Das zentrale Ziel bleibt das gleiche: Das DNS darf kein Single Point of Failure sein. Um dieses Ziel zu erreichen, braucht es zwei voneinander unabhängige Infrastrukturen.

Ob diese von zwei verschiedenen Anbietern bereitgestellt werden oder von einem Anbieter in vollständig getrennten Umgebungen betrieben werden, ist zunächst zweitrangig. Viel wichtiger sind die Architektur, die technische Umsetzung und die Qualität des laufenden Betriebs.

Daraus ergibt sich auch die strategischere Frage: „Brauchen wir zwei Anbieter oder brauchen wir zwei Infrastrukturen?“

**Die eigentliche Entscheidung besteht also darin, eine dieser Optionen zu wählen:**

1. **Zwei Anbieter mit interoperablen Architekturen in Primär-Sekundär-Modellen**
2. **Ein Anbieter mit zwei unabhängigen Infrastrukturen**

Die eigentliche Herausforderung besteht darin, die Lösung zu finden, die die gewünschte Ausfallsicherheit bietet – bei möglichst geringem Betriebsaufwand und hoher langfristiger Zuverlässigkeit. Dabei gilt es zu beachten, dass nicht alle DNS-Anbieter nahtlos zusammenarbeiten. Einige Cloud-Plattformen, darunter AWS und Google Cloud, unterstützen beispielsweise keine klassischen Primär-/Sekundär-Szenarien. Dadurch sind bestimmte Anbieterkombinationen von vornherein ausgeschlossen.

# Duale Anbieter-Strategie

Zwei verschiedene DNS-Anbieter (z. B. CSC + AWS)

## Vorteile

- Höchstmögliche Unabhängigkeit – Schutz vor Ausfällen, Softwarefehlern oder geschäftlichen Rückschlägen eines einzelnen Anbieters.
- Geringeres systemisches Risiko – fällt ein Anbieter global aus, bleibt der zweite weiterhin verfügbar.
- Stärkere Resilienz – lässt sich der Führungsebene und den Prüfern leicht vermitteln.
- Potenzielle Leistungssteigerungen – unterschiedliche Netzwerke können die globalen Lösungszeiten verbessern.

## Nachteile

- Die betriebliche Komplexität nimmt deutlich zu – zwei Portale, zwei APIs, zwei Sicherheitsmodelle, zwei Monitoring-Stacks.
- Das Änderungsmanagement wird anspruchsvoller – jede DNS-Änderung muss repliziert, validiert und synchronisiert werden.
- Nicht alle Anbieter sind interoperabel – einige Cloud-DNS-Plattformen (AWS, Google) unterstützen keine klassischen Primär-/Sekundär-Modelle.
- Höhere Kosten – zwei Verträge, zwei Supportvereinbarungen, zwei Abrechnungsstrukturen.
- Risiko von Konfigurationsabweichungen – die häufigste Ursache für DNS-Ausfälle in Multi-Vendor-Umgebungen.
- Erweiterte Funktionen wie Apex Alias, Geolokalisierung oder Failover erfordern zusätzliche technische Komplexität.

# Duale Infrastruktur-Strategie

Ein Anbieter, aber zwei vollständig isolierte Infrastrukturen (z. B. separate Cluster, Regionen oder Konten)

## Vorteile

- Geringerer Betriebsaufwand – Tools, APIs und Prozesse eines Anbieters.
- Bessere Risikominimierung – eine zentrale Ansprechstelle ermöglicht eine schnellere Fehleranalyse und -behebung.
- Konsistenter Funktionsumfang – gleiche Datensatztypen, identische Automatisierung und einheitliche Sicherheitskontrollen.
- Einfachere Sicherstellung der Konfigurationsgleichheit – reduziert menschliche Fehler.
- Oft günstiger – ein Lieferantenvertrag, skalierte Infrastruktur.
- Eliminiert weiterhin Single Points of Failure – sofern die Architektur korrekt umgesetzt wird (getrennte Regionen, Netzwerke und Steuerungsebenen).
- Zugriff auf erweiterte Funktionen – Apex-Alias, Geolokalisierung, Failover usw., die nahtlos synchronisiert werden.

## Nachteile

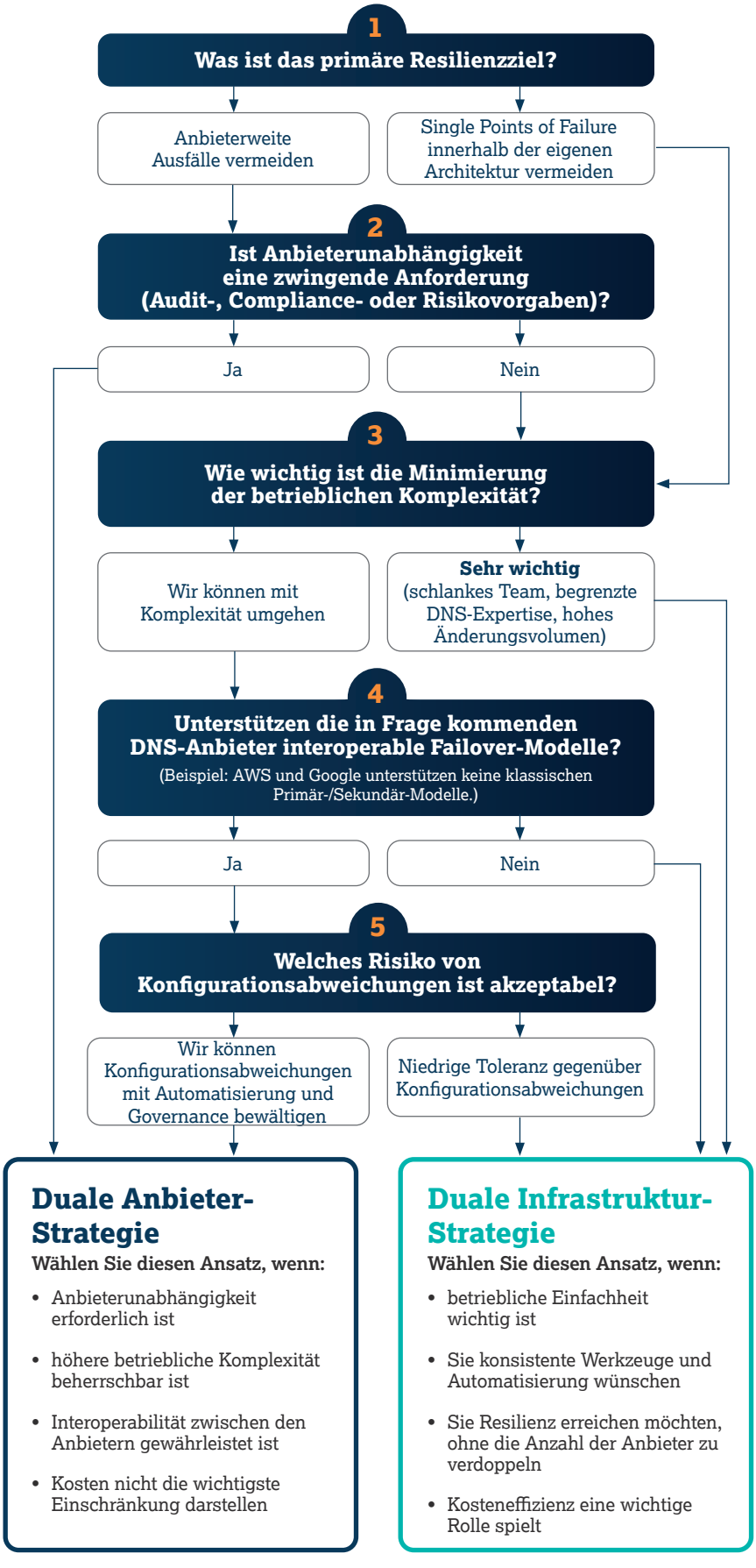
- Anbieterabhängigkeit bleibt bestehen – bei einem systemischen Problem des Anbieters können beide Infrastrukturen betroffen sein.
- Die Ausfallsicherheit hängt von der Architektur des Anbieters ab – nicht alle Anbieter trennen ihre Umgebungen tatsächlich vollständig.
- Wahrnehmungsrisiko – manche Stakeholder setzen „ein Anbieter“ mit „Single Point of Failure“ gleich, auch wenn dies technisch nicht zutrifft.

# Entscheidungsbaum für DNS-Ausfallsicherheit

**Eine duale Anbieter-Strategie** bietet das höchste Maß an Anbieterunabhängigkeit und reduziert die Abhängigkeit von einem einzelnen Anbieter. Sie führt jedoch zu größerer betrieblicher Komplexität, erhöhtem Integrations- und Verwaltungsaufwand.

**Eine duale Infrastruktur-Strategie** bietet eine starke Ausfallsicherheit bei geringerer Komplexität, indem Redundanz innerhalb desselben Betriebsmodells geschaffen wird. Diese Option ermöglicht eine zentrale Gesamtübersicht und ist einfacher zu verwalten als eine duale Anbieter-Strategie, bleibt jedoch vom Ökosystem eines einzelnen Anbieters abhängig.

Die richtige Wahl hängt von Ihren Prioritäten ab.



# Unabhängig davon, welchen Ansatz Sie bevorzugen – wir bieten die passende Lösung.

## Die duale Anbieterlösung von CSC – mit 100 % Verfügbarkeit

Die DNS-Services der Enterprise-Klasse von CSC basieren auf einem autoritativen Netzwerk, das Border Gateway Protocol (BGP) und IP-Anycast-Routing nutzt, um täglich Milliarden von DNS-Anfragen über 48 Points of Presence (PoPs) auf sechs Kontinenten zu verarbeiten. Es verfügt über die längste nachweisbare 100-prozentige Verfügbarkeit. Darüber hinaus stehen erweiterte Funktionen wie DNSSEC, Failover, Geolokalisierung und gewichteter Lastausgleich zur Verfügung, um Sicherheit und Kontrolle zusätzlich zu erhöhen.

## Die duale Infrastrukturlösung von CSC – eine zentrale Benutzeroberfläche in Aktiv-Aktiv-Konfiguration

CSC Ultimate DNS bietet sämtliche Funktionen, die ein Unternehmen für das DNS-Management benötigt, ergänzt um die zusätzliche Redundanz eines zweiten unabhängigen globalen DNS-Anycast-Netzwerks – verwaltet über eine einzige Benutzeroberfläche in einer Aktiv-Aktiv-Konfiguration. Anbieterrisiken werden durch tatsächlich isolierte Umgebungen sowie die Nutzung unterschiedlicher Rechenzentren und Netzbetreiber reduziert. Das sorgt für ein ausgezeichnetes Preis-Leistungs-Verhältnis mit einem zentralen Ansprechpartner für die Verwaltung Ihres DNS-Netzwerks.

CSC ist der vertrauenswürdige Anbieter von Sicherheit und Threat Intelligence der Wahl für Unternehmen im Forbes Global 2000 und für die 100 Best Global Brands (Interbrand®) mit Schwerpunkten in den Bereichen Domain-Sicherheit und -Management sowie digitalem Markenschutz und Betrugssicherung. Angesichts der erheblichen Investitionen, die globale Unternehmen in ihre Sicherheitsposition tätigen, kann unsere Plattform DomainSec℠ ihnen helfen, bestehende Versäumnisse in puncto Cybersicherheit zu verstehen und ihre digitalen Online-Vermögenswerte und -Marken zu schützen. Durch den Einsatz der firmeneigenen Technologie von CSC können Unternehmen ihren Sicherheitsstatus verbessern, um sich vor Cyberbedrohungen zu schützen, die auf ihre Online-Assets und den Ruf ihrer Marke abzielen. So können sie verheerende Umsatzeinbußen vermeiden. CSC bietet darüber hinaus Online-Markenschutz – eine Kombination aus Online-Markenüberwachung und Durchsetzungsmaßnahmen – einschließlich einer mehrdimensionalen Übersicht über verschiedene Bedrohungen außerhalb der Firewall, die bestimmte Domains ins Visier nehmen. Unsere Lösungen werden ergänzt durch Betrugspräventionsdienste, die Phishing bereits in der Frühphase des Angriffs bekämpfen. CSC hat seinen Hauptsitz seit 1899 in Wilmington, Delaware, USA, und verfügt über Niederlassungen in den Vereinigten Staaten, Kanada, Europa und im asiatisch-pazifischen Raum. CSC ist ein globales Unternehmen, das überall dort tätig werden kann, wo unsere Kunden sind – und das erreichen wir, indem wir Experten in jedem Geschäftsbereich beschäftigen, den wir bedienen.

**Kontaktieren Sie uns**

**cscdbs.com**

*CSC ist eine Dienstleistungsgesellschaft und bietet keinerlei rechtliche oder finanzielle Beratung an. Die hier aufgeführten Materialien dienen ausschließlich Informationszwecken. Wenden Sie sich an Ihren Rechts- oder Finanzberater, um zu ermitteln, inwiefern diese Informationen auf Sie zutreffen.*



DBS052626