Whitepaper

Datenintegrität bei Veräußerungen oder Carve-outs

Einführung

Verantwortliche in der IT sind bei Veräußerungen von Unternehmensteilen vorübergehend in einer Doppelrolle: Sie müssen die Ausgliederung so vorbereiten, dass weder der Betrieb des Verkäufers (RemainCo) noch die Geschäftsabläufe beim abgespaltenen Firmenteil (SpinCo) ins Stocken geraten. Über das TSA (Transition Service Agreement) regeln die Transaktionsparteien, dass der IT-Support so lange über den Verkäufer weiterläuft, bis SpinCo die Verwaltung der IT-Systeme alleine übernehmen kann oder die Integration in den neuen Mutterkonzern abgeschlossen ist. IT-Verantwortliche sind dabei vor eine besondere Herausforderung gestellt: Sie müssen den SpinCo-Usern und denen des neuen Mutterkonzerns einen sicheren Zugriff auf die Umgebung von RemainCo bereitstellen.

In der Regel beginnen die Vorbereitungen auf die Veräußerung beim Verkäufer einige Monate vor dem Versuch eines Verkaufs. Sobald auf geschäftlicher Ebene feststeht, welche Unternehmensteile inklusive Technologiekomponenten und Mitarbeitenden als SpinCo abgestoßen werden und welche als RemainCo fortbestehen sollen, wird klar, für welche Ressourcen ein TSA formuliert werden muss. Als entscheidendes Element einer solchen Transaktion regelt diese vertragliche Nebenvereinbarung die saubere Trennung und den Schutz der IT-Komponenten.

Der Verkäufer muss dann Pro-forma-Abschlüsse mit Zahlen zur herausgelösten Geschäftstätigkeit und zu den dazugehörigen Ausgaben aufschlüsseln, wie SpinCo nach der Transaktion als eigenständiger Betrieb voraussichtlich aufgestellt sein wird. Abschließend muss der Verkäufer eine IT-Architektur für die Übergangszeit aufsetzen, über die SpinCo-Beschäftigte sicher auf die einzelnen Technologiekomponenten zugreifen können.

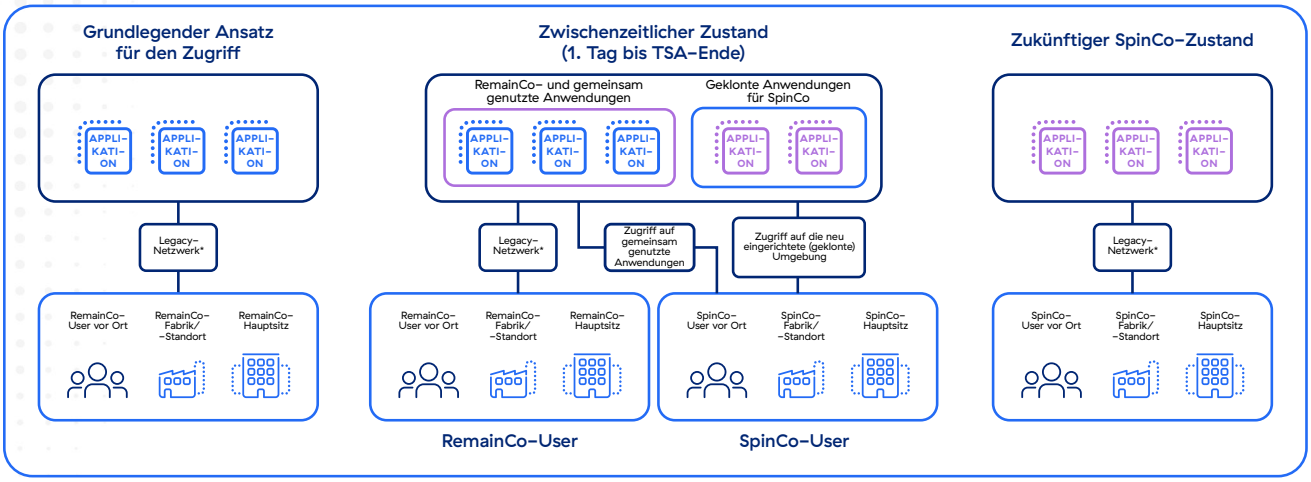
Herkömmlicher Ansatz mit Legacy-Tools

Der herkömmliche Ansatz für die Trennung der Ressourcen ist netzwerkbasiert. Der Verkäufer richtet für die Übergangszeit, in der das TSA gilt, den Zugriff auf Anwendungen ein. Dafür stehen ihm verschiedene Optionen zur Verfügung.

Beschreibung	Potenzielle Nachteile
Mit SpinCo-Usern geteilter Zugriff auf die aktuelle Umgebung des Verkäufers	Sehr hohes Risiko von Sicherheitsverletzungen, da User mit ungeklärtem Sicherheitsstatus Zugriff haben
Hybrider Ansatz, bei dem sowohl Anwendungen für SpinCo-User in einer separaten Umgebung eingerichtet werden als auch auf Anwendungen in der aktuellen Umgebung gemeinsam zugegriffen wird	Sehr hohes Risiko von Sicherheitsverletzungen, da User mit ungeklärtem Sicherheitsstatus Zugriff haben; außerdem hoher Planungsaufwand und Vorlauf des Verkäufers erforderlich, um eine eigene Umgebung einzurichten und den Traffic zu segmentieren.
Alle Anwendungen in separate Umgebung migrieren; auf SpinCo ausgelegte Anwendungen werden komplett ausgelagert, gemeinsam genutzte Anwendungen geklont und nur mit SpinCo-Daten übertragen	Umfassende Kenntnis aller in die neue Umgebung zu migrierenden Anwendungen und Daten erforderlich; mögliche Komplikationen durch voneinander abhängige Workflows, z. B. in Bezug auf Anwendungen, Daten, Hosting oder Netzwerke

Wie bereits erwähnt, erfordert dieser Ansatz einige Monate der Vorbereitung. Probleme mit der Lieferkette für Hardware und Komponenten der Netzwerkinfrastruktur müssen berücksichtigt werden. Noch vor der Trennung werden außerdem sichere Vermittlernetzwerke eingerichtet. Der Zeitrahmen für die einzelnen Schritte wird konservativ geplant. Weil das RemainCo-Netzwerk vorübergehend auch SpinCo-Usern zugänglich ist, besteht ferner das Risiko einer lateralen Bewegung und eines Datenverlusts.

Herkömmlicher Ansatz: geklontes SpinCo-Netzwerk mit Vermittlernetzwerk für den Zugriff von Usern verschiedener Entitäten



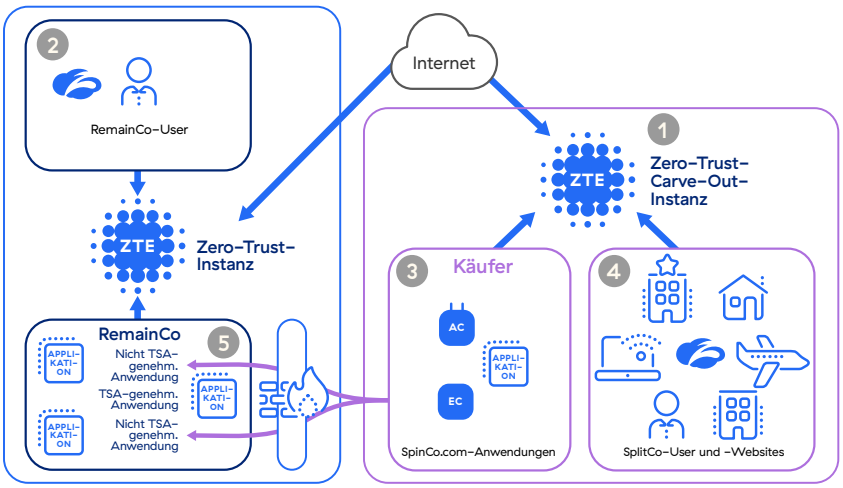
* Beim Legacy-Ansatz kommen u. a. MPLS, Firewalls und Load Balancer zum Einsatz.

Beispiel: Ein großer Fachhändler teilte das Unternehmen vor Kurzem in zwei getrennte Entitäten. Das TSA wurde auf zwei Jahre ausgelegt und umfasste gemeinsam genutzte Anwendungen. Auch auf die Infrastruktur und das Netzwerk wurde von beiden Unternehmensteilen zugegriffen. Um die Trennung zu vollziehen, mussten daher zwei separate IT-Umgebungen eingerichtet, Anwendungen dupliziert sowie ein komplex ineinandergreifendes Netzwerk segmentiert und auf zwei Entitäten aufgeteilt werden. Der Prozess ist für die Verantwortlichen in der IT und der Geschäftsführung gleichermaßen fordernd und birgt außerdem das Risiko eines Wertverlusts.

Moderner Ansatz mit der Cloud-Plattform von Zscaler

Die Zero-Trust-Plattform von Zscaler ist cloudbasiert. Eine herkömmliche Netzwerksegmentierung und hardwarebasierte Ansätze zur Konnektivität sind nicht mehr erforderlich. Über unsere Plattform lässt sich stattdessen die Segmentierung auf User- und Anwendungsebene durchführen. Dafür legt das IT-Team Richtlinien für den Zugriff fest, die dann über die Zscaler Cloud erzwungen werden. In der Regel wird bei Veräußerungen eine Instanz zwischengeschaltet, über die die Verbindung zu den gemeinsam genutzten Anwendungen in einer von beiden Entitäten geteilten Umgebung läuft. Mithilfe der Instanz lassen sich dann Richtlinien und betroffene User bestimmen und Zugriffsberechtigungen festlegen.

Zscaler-Ansatz: Zero-Trust-Zugriff auf SpinCo über eine Carve-out-Instanz



1. ZTE-Instanz, IdP und Domains für ausgegliedertes Unternehmen (SplitCo) einrichten
2. Umgebung erstellen, um User, Anwendungen und Richtlinien zu definieren
3. SplitCo-User zu SplitCo-ZTE umleiten
4. SplitCo-Anwendungen der SplitCo-ZTE zuweisen
5. Kontrollen für zurückbleibende TSA-Anwendungen einrichten

Vor Kurzem arbeitete Zscaler mit einem großen Mischkonzern zusammen. Für einen veräußerten Unternehmensteil hatte das Industriekonglomerat eine separate Instanz eingerichtet. Der Zugriff auf die gemeinsam genutzten Anwendungen wurde über konfigurierte Richtlinien eingeschränkt. Letztendlich wurden alle User der veräußerten Entität auf die neue Instanz migriert. Bei Veräußerungen dieser Art lässt sich mithilfe von Zscaler der User-Zugriff auf eigens auf das SplitCo ausgelegte sowie auf gemeinsam genutzte Umgebungen einrichten — standortunabhängig und für unterschiedliche Rollen.

Häufige Anwendungsfälle für Zscaler-Lösungen bei Veräußerungen

1. **Zugriff auf ausgewählte Anwendungen:** Mit Zscaler Private Access (ZPA) können IT-Verantwortliche einen sicheren Zugriff auf ausgewählte Anwendungen zur Verfügung stellen. Der Ansatz funktioniert für alle Applikationen, egal ob über das On-Premise-Rechenzentrum oder eine öffentliche Cloud gehostet, ob über die IT-Infrastruktur des Verkäufers oder in der SpinCo-Umgebung bereitgestellt, ob gemeinsam genutzt oder speziell auf das SplitCo ausgerichtet.
Ganz ohne zusätzliche Hardware lässt sich mit Zscaler über die Konfiguration der Cloud schnell ein sicherer Zugriff für User einrichten — standortunabhängig für alle Mitarbeiter im Büro, im Homeoffice oder unterwegs.

2. **Geschützter Internet-Traffic:** Über Zscaler Internet Access (ZIA) ist ein sicherer Zugriff auf SaaS-Applikationen und Websites im öffentlichen Internet möglich. Organisationen profitieren von Funktionen zum Schutz vor komplexen Bedrohungen und können die Sicherheitsmechanismen mit nur einem Klick aktivieren. In der Übergangszeit kann sich der Verkäufer so ganz einfach vor potenziellen Cyberangriffen und Sicherheitsverletzungen absichern.

3. **Anwendungserkennung:** Nach der vollständigen Bereitstellung von Zscaler erhalten IT-Teams über die Plattform Statistiken zu den Anwendungen, die SpinCo-User verwenden. Aus den Analysen lässt sich ablesen, welche Tools am häufigsten genutzt werden und wie User die Anwendungen einsetzen.
Mithilfe dieser Informationen kann das IT-Team in der TSA-Phase ableiten, wie die Trennung erfolgen sollte.

4. **Performance-Monitoring:** Mit Zscaler Digital Experience (ZDX) lässt sich der IT-Aufwand reduzieren. Über das zentrale Verwaltungsportal von Zscaler Zero Trust Exchange (ZTE) haben die RemainCo- und SpinCo-Supportteams Netzwerkausfälle und Performanceprobleme im Blick. Gleichzeitig sehen sie sofort alle erforderlichen Telemetriedaten in beiden Umgebungen und haben so bei Support-Tickets zeitnah alle Informationen zur Hand, um die von den Problemen betroffenen Eigentümer ausfindig zu machen. Die Arbeit des Supports wird auf diese Weise erleichtert.

Die Vorteile des Zscaler-Ansatzes

 **Kürzere Zeit zur Umsetzung**	• Schnelle Bestandsaufnahme der benötigten Anwendungen • Sichere Verbindung zwischen Usern und Anwendungen in wenigen Wochen • Verkürzte TSA-Dauer
 **Einfachheit**	• IT entfällt als kritisches Element der Vorbereitungsphase für sofortige Bereitschaft • Vollständig cloudbasierter Ansatz für die Konnektivität • Sicherer Zugriffspfad und geschützter Internet-Traffic durch Zero-Trust-Lösung
 **Finanzielles**	• Geringere einmalige und wiederkehrende Trennungskosten • Niedrigere TSA-Kosten und weniger verlorene Vermögenswerte / technische Schulden • Kostensenkung durch weniger IT-Verzögerungen dank der Übertragbarkeit der Zscaler-Plattform
 **Datenintegrität**	• Minimiertes Risiko von Datenverlusten • Geringere Bedrohung durch Insider oder unautorisierten Zugriff von Dritten • Überprüfbare Kontrollen in Vorbereitung auf Day-1

Fazit

Bei Veräußerungen ist die Trennung der IT-Systeme häufig kompliziert. Eine besonders herausfordernde Aufgabe dabei ist, den Beschäftigten einen sicheren Zugriff zum richtigen Zeitpunkt zur Verfügung zu stellen, damit sie produktiv weiterarbeiten können. Herkömmliche Ansätze bergen Cyberrisiken, denn der Betrieb von zwei parallelen Netzwerken bietet zahlreiche Angriffsstellen. Mit Zscaler hingegen haben Unternehmen die Möglichkeit, Usern im Rahmen der Transaktion einen klar begrenzten sicheren Zugriff auf wichtige Anwendungen bereitzustellen, ob bei der Aufspaltung eines großen Konzerns oder bei der Veräußerung kleinerer Unternehmensteile. Dank Zscaler lässt sich das Risiko von Cyberbedrohungen deutlich senken und der Trennungsprozess vereinfachen.

zscaler™ | Experience your world, secured.™

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 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.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