# Sechs Fragen zu DRaaS, die Sie als KMU unbedingt stellen sollten

Eine Disaster-Recovery-Lösung darf auch in der Business-Continuity-Strategie von KMUs nicht fehlen, denn der Verlust von geschäftskritischen Daten hat auch für sie fatale Folgen. Ein entsprechender Service verhindert im Desaster-Fall nicht nur den Datenverlust, sondern ist auch dazu geeignet, erste Schritte in Richtung Cloud zu unternehmen.

Eine Zusammenarbeit mit einem DRaaS-Provider ist für viele KMUs unumgänglich, da meist das notwendige Kleingeld für eine eigene DR-Umgebung fehlt oder ein eigener DR-Plan weder erstellt, getestet noch ausgerollt werden kann. Cyberlink hat die wichtigsten Fragen und Antworten, die Sie im Auswahlprozess unterstützen sollen, für Sie zusammengestellt.

**1. Wie funktioniert eine DRaaS-Lösung auf Basis einer bestehenden Infrastruktur?**

Es gibt verschiedene technologische Disaster-Recovery-Ansätze. Einige funktionieren auf Infrastruktur-, andere auf Plattform- und manche auf Applikationsebene. Je höher die DR-Lösung im jeweiligen Technologie-Stack angesiedelt ist, desto höher auch die Komplexität und die Abhängigkeiten. Um eine möglichst grosse Anzahl an Anwendungsfällen abdecken zu können, bietet sich die von Cyberlink angebotene Replizierung auf Infrastrukturebene an. Diese repliziert ganze virtuelle Maschinen, unabhängig davon, welche Betriebssysteme oder Applikationen installiert sind. Im Self-Service können Sie selbst entscheiden, wann und wie repliziert werden soll und wann Sie auf die DR-Seite umschalten möchten.

**2. Steigen die Kosten, je individueller eine DRaaS-Lösung zugeschnitten ist?**

Ein gutes Disaster-Recovery-Konzept ist immer individuell zugeschnitten. So individuell es dann aber auch sein mag, die Umsetzung erfolgt meist mit standardisierten Lösungen und Tools. Entsprechend müssen die wiederkehrenden Kosten einer passgenauen Lösung nicht höher ausfallen. Hier ist vielmehr das Preismodell des jeweiligen Anbieters relevant. Die nutzungsbasierte Verrechnung von Cyberlink stellt sicher, dass Sie nur das bezahlen, was Sie auch nutzen. Für ausgeschaltete VMs entstehen keinerlei Computer-Kosten und im Desaster-Fall kommen für tatsächlich verbrauchte Ressourcen unsere normalen IaaS-Tarife zur Anwendung.

**3. Wie greifen Mitarbeitende auf interne Anwendungen zu?**

Da bei der Replizierung auf Infrastrukturebene ganze virtuelle Maschinen samt Inhalt repliziert werden, ändert sich an der Authentifizierung nichts. Nur das Management der DRaaS-Lösung findet über ein Cloud-Portal statt. In diesem können Sie VPN-Tunnel oder andere Zugriffsmöglichkeiten konfigurieren und wie gewohnt auf Ihre virtuellen Systeme und Applikationen zugreifen. Zusätzliche Konfigurationen sind notwendig, wenn zum Beispiel externe LDAP- oder ADFS-Authentifizierungen für Systeme und Applikationen genutzt werden. Im Normalfall reichen dafür aber einige Firewall- und VPN-Einstellungen aus, die vorgängig im Rahmen der Inbetriebnahme konfiguriert werden können.

**4. Wie lange können wir nach einer Katastrophe das Provider-Rechenzentrum nutzen?**

Eine zeitliche Beschränkung ist in den meisten Fällen nicht gegeben. Allerdings fallen höhere Kosten an, wenn die Desaster-Seite produktiv genutzt wird. Achten Sie daher auf faire Kostenmodelle.

**5. Wie läuft der Testprozess?**

Um überprüfen zu können, ob die Disaster-Site im Ernstfall auch funktioniert, müssen eigenständige Test-Failovers jederzeit möglich sein. Zudem sollte bei einem Test-Failover ausschliesslich mit Klonen der Produktionsumgebung gearbeitet werden. Dann sind Ihre produktiven Umgebungen von Tests nicht betroffen und die Replikation im Hintergrund kann problemlos weiterarbeiten. Wie häufig und zu welchem Zeitpunkt Sie solch einen Testprozess durchführen möchten, kann von Ihnen selbst bestimmt werden. Im Rahmen des Self-Service sind bei Cyberlink Test-Failovers jederzeit möglich.

**6. Wie skaliert die Lösung?**

Ein intelligent angelegtes Kapazitätsmanagement sollte langfristig sicherstellen, dass Cloud-Plattformen immer über genügend freie Kapazitäten verfügen. Cyberlink wächst mit Kundenanforderungen mit und erweitert fortlaufend die physischen Kapazitäten. Somit steht Ihren Skalierungswünschen nichts im Wege. Genauso flexibel können Sie auch Leistungen reduzieren, falls Ihr Bedarf sinkt.

**CYBERLINK AG**

**Gehostet in der Schweiz:** Wir betreiben unsere Infrastruktur in unserem ISO-27001-zertifizierten Datacenter. Ihre Daten liegen ausschliesslich in der Schweiz und können dank zweier Rechenzentrumsstandorte georedundant gespeichert werden.

**Nahtlose Integration:** Durch die Anbindung von VMware Cloud Director Availability erreichen Sie eine nahtlose Integration in Ihre bestehende VMware-Umgebung ohne Drittprodukte.

**Externe Replikation:** Durch die Replikation virtueller Maschinen zu Cyberlink nutzen Sie ein geografisch von Ihrem Standort getrenntes Hochsicherheits-Rechenzentrum in der Schweiz.

**VMware Cloud Verified:** Cyberlink setzt seit mehr als 10 Jahren auf VMware-Technologien. Unsere Kompetenz ist geprüft – wir sind «VMware Cloud Verified».

**Angepasste RPO & RTO:** Realisieren Sie in Zusammenarbeit mit uns, die RPO und RTO anhand Ihrer spezifischen Anforderungen.

**Testen Sie unsere DRaaS-Lösung jetzt kostenlos.**

cyberlink

**Cyberlink AG**

Bellerivestrasse 241
8008 Zürich
Tel. 044 287 29 92
www.cyberlink.ch