plusserver

Disaster Recovery neu gedacht

DRaaS aus der Cloud als effizienter Rettungsschirm für businesskritische Anwendungen

Whitepaper

Inhalt

Vorteile von Disaster Recovery as a Service

- Schnelle Wiederherstellung des Geschäftsbetriebs
- Failover im Falle eines Hardware-, Software oder Komplettausfalls
- Kontrolliertes Failover von Workloads für Wartungsfenster
- Replikation in die Cloud als erster Schritt zur Cloud-Migration, um bei starkem Wachstum schnell skalieren zu können
- Einfache Tests möglich, ohne die Hauptumgebung zu beeinflussen
- Kein eigenes Know-how erforderlich
- Disaster-Recovery-Plan kann mit Cloud-Anbieter entwickelt werden
- Nutzungsbasierte Abrechnung von Cloud-Ressourcen

Executive Summary

Je wichtiger und geschäftskritischer Daten und digitale Angebote in Unternehmen sind, desto gravierender werden auch die Folgen eines möglichen IT-Ausfalls sein. Daher bilden Maßnahmen zur schnellen Wiederherstellung nach einem Katastrophenfall einen wichtigen Teil einer ganzheitlichen Business-Continuity-Strategie. Dank Disaster Recovery aus der Cloud rentieren sich diese heute für die meisten Unternehmen.

Der Schutz von IT-Ressourcen ist eine der wichtigsten Aufgaben innerhalb des Business Continuity Managements. Hierunter fallen alle Maßnahmen, die Unternehmen treffen müssen, um im Notfall handlungsfähig zu bleiben und Schaden zu minimieren. Das betrifft nicht nur die IT – aber wenn die IT-Systeme ausfallen, stehen viele wichtige Prozesse im Unternehmen still. Dabei sind die Auswirkungen umso höher, je mehr ein Geschäftsmodell auf digitalen Applikationen und Daten beruht.

Um die Risiken von Geschäftsausfällen oder Datenverlusten zu minimieren, benötigen Unternehmen unkomplizierte und zuverlässige Dienstleistungen, die keine zusätzlichen Investitionen in Infrastrukturen erfordern und umfangreiche Tests für den „Fall der Fälle“ erlauben. Daher kommen vermehrt einfache und wirtschaftliche DRaaS-Lösungen (Disaster Recovery as a Service) in der Cloud zum Einsatz. Diese bieten die Möglichkeit, die Daten und Anwendungen eines Unternehmens in mehreren Verfügbarkeitszonen vorzuhalten und so im Notfall den Geschäftsbetrieb schnell wiederherzustellen.

Warum überhaupt Disaster Recovery?

Naturkatastrophen wie Erdbeben, Orkane, Feuer, Tsunamis und Überflutungen sind hierzulande noch eher seltene Phänomene. Dennoch müssen wir uns angesichts des Klimawandels auch in Deutschland darauf einstellen, dass Überflutungen wie 2021 nur die Vorboten möglicher kommender Gefahren waren.

Rechenzentren zählen zu der am besten geschützten Infrastruktur. Redundanz in der Stromversorgung, bauliche Befestigungen und sichere Gebäudestandorte sind nur eine Auswahl der üblichen Schutzmaßnahmen. Dennoch gab es in der Vergangenheit einige große Ausfälle, auch in Europa. Die häufigsten Gefahren, die IT-Systeme von Unternehmen unterbrechen, sind aber nicht Wasser oder Feuer, sondern reichen von Fehlkonfigurationen und Hardwaredefekten über menschliches Versehen bis hin zu Ransomware-Angriffen. 34 Prozent der deutschen Unternehmen waren 2025 von Ransomware betroffen. 80 Prozent aller angezeigten Angriffe (inkl. Ransomware) betrafen KMU.[1]

Daher gehört zunächst eine saubere Backup-Strategie auf die To-do-Liste jedes Unternehmens. Diese sollte sich unter anderem an der 3-2-1-Regel orientieren, die mindestens drei Kopien der Daten (ein Original und zwei Sicherungen) auf mindestens zwei unterschiedlichen Medien vorsieht, wobei eine Sicherung extern aufbewahrt werden sollte. Dadurch ist sichergestellt, dass nicht auch das Backup zerstört oder gestohlen wird, wenn am Produktivstandort ein Datenausfall passiert.

Was aber tun, wenn nicht nur Daten betroffen sind, sondern die ganze Infrastruktur am Firmensitz ausfällt? Nun würde in vielen Fällen sogar ein externes Backup nicht mehr ausreichen, um den Geschäftsbetrieb aufrechtzuerhalten. Denn es wären in dem Fall keine lokalen Systeme mehr verfügbar, um die Daten zurückzuspielen.

Eine Ausnahme bilden hier Cloud-Backup-Lösungen wie zum Beispiel plusbackup. Bei diesen kannder Cloud Provider im Notfall kurzfristig eine IT-Umgebung für den Kunden in der Cloud bereitstellen, in der dieser mit seinen im Backup gesicherten Daten arbeiten kann. Jedoch ist dieses Verfahren zeitaufwendiger und deckt nicht die oft hochspezialisierten Anwendungen eines Unternehmens ab. Sind diese besonders geschäftskritisch und Ausfälle teuer, ist statt eines Backups eine konsistente Replikation (wie weiter unten beschrieben) ratsam.

[1] Bitkom „Wirtschaftsschutz 2025“;
BSI „Die Lage der IT-Sicherheit in Deutschland 2025“

Generell lässt sich aber sagen: Fällt die Unternehmens-IT für längere Zeit aus, kommt Disaster Recovery – oder auch Notfallwiederherstellung – ins Spiel. Darunter fallen alle Maßnahmen, die nach einem Ausfall von IT-Infrastrukturen dafür sorgen sollen, den ursprünglichen Zustand wiederherzustellen. Dies kann beispielsweise dadurch realisiert werden, dass Daten oder komplette Infrastrukturen an einem zweiten Standort oder in der Cloud vorgehalten werden. So kann der DR-Standort im Notfall komplett übernehmen und den Geschäftsbetrieb aufrechterhalten. Somit bildet Disaster Recovery einen wichtigen Teilaspekt des Business Continuity Managements, das unterbrechungsfreie Geschäftsabläufe durch eine Vielzahl von Maßnahmen ermöglichen soll.

Schließlich kann es sich kaum ein Unternehmen leisten, auf geschäftskritische digitale Anwendungen für einen längeren Zeitraum zu verzichten. Nicht nur im E-Commerce ist Verfügbarkeit ein entscheidender Faktor – wer offline ist, schickt seine Kund:innen direkt weiter zur Konkurrenz. Neben Umsatzausfällen drohen Unternehmen jeder Größe und Branche auch mögliche Regressanforderungen Dritter, wenn Termine oder andere geschäftliche Vereinbarungen nicht eingehalten werden. Zusätzlich können Reputationsverluste dauerhafte Auswirkungen auf den Geschäftserfolg haben. Ein Desaster im wahrsten Sinne sind Ausfallzeiten bei Unternehmen und Einrichtungen mit besonders hohen Sicherheits- und Verfügbarkeitsanforderungen wie beispielsweise Energieversorger, das Gesundheitswesen, Banken oder öffentliche Einrichtungen.

Es gilt also, für den Notfall gerüstet zu sein.

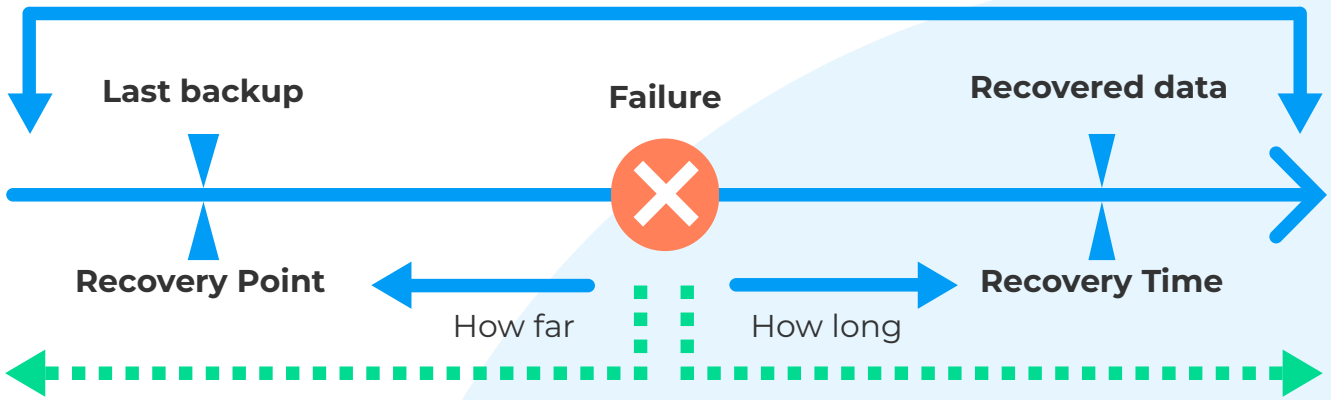
Datenreplikation in der Cloud

Längst haben sich Infrastruktur, Software und Plattformdienste „as a Service“ aus der Cloud als flexible und zuverlässige Alternative zu eigenen IT-Ressourcen bewährt. Zu den Vorteilen gehört die schnelle Verfügbarkeit nach Bedarf, ohne eigene Hardware betreiben und warten zu müssen. Zudem werden modernste Technologien zugänglich, ohne dass spezielles eigenes Know-how im Unternehmen aufgebaut werden muss. Die langfristigen Kosteneinsparungen im Vergleich zum Eigenbetrieb machen die Entscheidung noch einfacher. Auch für Storage- oder Backupzwecke gewinnen Cloud-Lösungen zunehmend an Bedeutung.

Selbst wenn geschäftskritische Applikationen eines Unternehmens nach wie vor „on Premises“ betrieben werden: Wer die Cloud als zusätzlichen Datenstandort nutzt, sorgt für eine höhere Verfügbarkeit. Während bei klassischer Disaster Recovery ganze Hardwarefuhrparks als Duplikate nur für den Notfall angeschafft und gewartet wurden, um die Produktivsysteme zu spiegeln, ist dies dank der Cloud nicht mehr nötig. Unternehmen, die bereits eine Cloud-basierte Backup-Lösung nutzen, haben schon einen ersten Schritt in Richtung Disaster Recovery unternommen. Denn wenn die lokale IT-Infrastruktur –

zum Beispiel infolge eines Hardwaredefekts – längerfristig nicht zur Verfügung steht, kann der Provider dabei helfen, in der Cloud eine virtuelle Maschine (VM) für den Kunden einzurichten und die Backup-Daten dort verfügbar zu machen. Damit wird der Kunde in einem gewissen Rahmen wieder arbeitsfähig. Das reicht aber nicht für jeden Anspruch: Je nachdem, wie stark das Geschäftsmodell eines Kunden auf der Verfügbarkeit bestimmter digitaler Applikationen beruht, empfiehlt sich vielmehr eine konsistente Replikation aller Daten sowie Applikationen in die Cloud. Dies spart kostbare Zeit im Desaster-Fall, denn der Kunde kann selbständig die Recovery-Maßnahme einleiten, und die Replikation ermöglicht im Gegensatz zum Backup die umgehende Wiederherstellung der geschäftskritischen Applikationslandschaft inklusive aller Daten. Je nach Konzeption und Zielen der Wiederherstellung gibt es unterschiedliche Vorgehensweisen, in welcher Form Daten repliziert werden und mit welchen Storage-Klassen die Daten gesichert werden. Eine Replikation kann in synchroner oder asynchroner Form erfolgen. Im ersten Fall können Daten in einer Umgebung nur dann geändert werden, wenn sie parallel auch in allen Replikaten geändert werden. Die synchrone Replikation wird häufig für Hot-Standby-Szenarien von Datenbanken angewendet, die sich im selben Rechenzentrum befinden, also keine Latenzen bei der Datenübertragung haben. Bei der asynchronen Replikation treten hingegen Latenzen auf. Je größer diese sind und je länger damit die Übertragung zwischen Standorten dauert, desto größer werden die Diskrepanzen zwischen Produktivdaten und den Replikationen.

Zwei wichtige Zielvorgaben bei DR-Plänen: RPO und RTO



Dementsprechend werden bei der Erstellung eines Disaster-Recovery-Plans zwei Zielvorgaben betrachtet: Recovery Time Objective (RTO) sowie Recovery Point Objective (RPO). Während das RTO vorgibt, wie viel Zeit zwischen einem Ausfall und der Wiederherstellung vergehen darf, legt das RPO unter anderem den maximalen zeitlichen Verlust an Daten fest und bestimmt damit die Mindesthäufigkeit der Sicherung. Mittels RPO definiert das Unternehmen somit die eigene Verlusttoleranz. Wie groß ist die maximale Datenlücke durch einen Ausfall und wie viele Daten dürfen maximal verloren gehen? Für kritische Daten kann ein RPO beispielsweise bei weniger als einer Stunde liegen, für selten geänderte oder weniger geschäftskritische Daten auch bei mehreren Stunden. Auch hier spielt die Cloud einen Trumpf aus, da viele Cloud-Dienste über mehrere vernetzte Rechenzentren verfügen und somit geringe Latenzen ermöglichen. Fällt also die Hauptumgebung aus, ist der Datenbestand in der Cloud idealerweise nur wenige Sekunden älter als der primäre Datenbestand.

DRaaS: Welche Modelle gibt es?

Die Anforderungen an RPO und RTO sind häufig ausschlaggebend dafür, welche Art von Cloud-basierter DR-Strategie ein Unternehmen wählt. Ein weiteres Kriterium können auch die Kosten der Lösung sein, die zur besseren Bewertung ins Verhältnis zu den erwarteten Auswirkungen eines Ausfalls gesetzt werden sollten. Um diese Auswirkungen einzuschätzen, eignet sich eine Business-Impact-Analyse.

In jedem Fall ist es empfehlenswert, gemeinsam mit dem Cloud Provider eine individuelle DRaaS-Strategie aufzusetzen, die genau auf die Anforderungen des Unternehmens zugeschnitten ist:

Datenbasierte DR

Diese Variante bietet ein relativ geringes Recovery-Niveau, da lediglich Datenbackups auf File-Servern in einer Cloud vorgehalten werden. Kommt es zu einem Ausfall, müssten zunächst alle Anwendungen wieder ans Laufen gebracht und anschließend die Daten zurückgespielt werden.

Voraussetzung dafür ist jedoch, dass die Hauptumgebung überhaupt wiederhergestellt werden kann und nicht etwa einer Naturkatastrophe zum Opfer gefallen ist – oder dass der Cloud Provider kurzfristig eine alternative Umgebung zur Verfügung stellt. Je nach Umfang der gesicherten Daten kann der Recovery-Vorgang eine längere Zeit in Anspruch nehmen. Der Vorteil: Datenbasierte DR lässt sich vergleichsweise einfach umsetzen, indem Unternehmen auf Cloud Backup Services setzen.

Applikationsbasierte DR

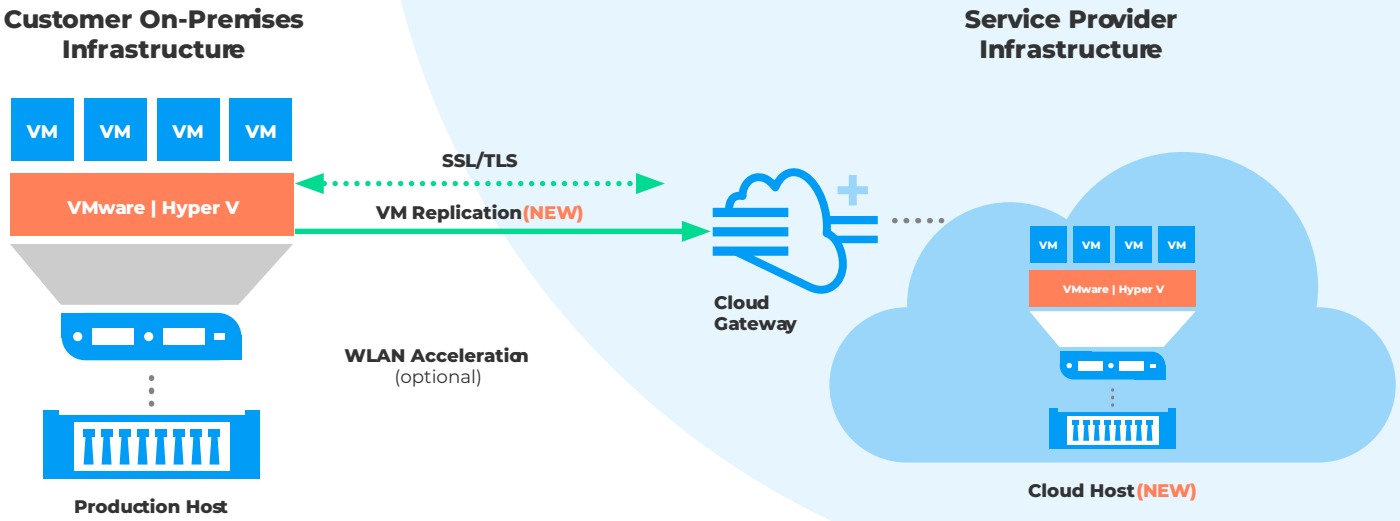
Bei dieser Methode besteht eine Zweitinstallation einer Applikation (beispielsweise einer Website) in der Cloud. Anwendungsdaten, die über die Hauptumgebung generiert werden, werden jeweils in die Cloud repliziert. Bei einem Ausfall der Hauptumgebung würden die Websitebesucher über einen geänderten DNS-Eintrag (Domain Name System) auf die Cloud-Applikation umgeleitet. Der Besucher merkt so nichts von dem Ausfall, außer dass womöglich sein Warenkorb plötzlich leer ist, weil die Daten nicht synchron gehalten sind.

Für die applikationsbasierte DR wird eine Ziel-VM (Virtual Machine) beim Cloud Provider erstellt und anschließend eine Replikation auf Anwendungsebene konfiguriert. Der Cloud Provider übernimmt nach Absprache die Pflege der DR-VM als Managed Service, etwa durch Patches und Upgrades, und unterstützt nach einem Failover die IT-Abteilung des Kunden dabei, die Daten wieder zurückzuholen.

VM-basierte DR

Hier werden komplette virtuelle Maschinen mit allen Daten, Anwendungen und Einstellungen konsistent in die Cloud repliziert. Dieses Modell eignet sich besonders gut für Umgebungen mit komplexen Abhängigkeiten und wenn das Businessmodell eines Unternehmens auf speziellen digitalen Applikationen beruht. Eine komplette Replikation einer Umgebung ermöglicht es auch, per Änderung des DNS-Eintrags im Notfall komplett auf die replizierte Umgebung in der Cloud umzuschwenken.

VM-basierte Disaster Recovery in der Cloud



Beispielhafte Darstellung einer VM-basierten DR beim Cloud Service Provider. (Quelle: Veeam)

Die wichtigste DR-Regel: testen, testen, testen

Wie bei allen Security-Methoden genügt es auch bei DRaaS nicht, sich blind auf die getroffenen Maßnahmen zu verlassen. Nur regelmäßige Tests geben die Gewissheit, dass im Notfall alle DR-Maßnahmen greifen. Dabei ist das Testing mit Hilfe der Cloud jedoch wesentlich einfacher als bei traditionellen Disaster-Recovery-Methoden. Beispielsweise ist es nicht erforderlich, eine zweite IT-Infrastruktur für den Kunden dauerhaft einzurichten. Für die Dauer der Tests kann der Cloud Provider dem Kunden eine entsprechende Failover-Umgebung zur Verfügung stellen und berechnet hierfür lediglich die während des Tests genutzten Compute-, Speicher- und Netzwerkressourcen.

Zudem ist Cloud-basierte Disaster Recovery in der Regel ein stark automatisierter Prozess, sodass der Aufwand auf Kundenseite enorm reduziert wird – bis hin zu wenigen Mausklicks. So muss ein Admin im besten Fall nur noch eine bestimmte VM oder ein Setup aus mehreren VMs sowie den gewünschten Recovery Point auswählen.

Des weiteren bringt das Testing bei klassischen Lösungen grundsätzlich Risiken für die Produktivumgebung mit sich, wenn ein Workload zunächst in ein zweites Rechenzentrum übertragen werden muss, um dort seine Funktion zu prüfen. Diese Risiken entfallen jedoch in einer DRaaS-Umgebung aufgrund der kontinuierlichen Datenreplikation. Das heißt, es besteht ohnehin eine Kopie des Workloads in der Cloud, sodass die Produktivumgebung von einem Test nicht beeinflusst wird.

DRaaS-Checkliste: Wo und mit wem?

Diese Kriterien helfen Unternehmen dabei, einen zuverlässigen DRaaS-Anbieter zu finden:

Service Level Agreements

Neben den zu vereinbarenden Recovery Point Objectives und Recovery Time Objectives der DRaaS-Lösung sind die generellen Service Level Agreements des Anbieters wichtig für den Kunden. Diese definieren beispielsweise garantierte Verfügbarkeiten und Wiederherstellungszeiten der Provider-Infrastrukturen. Bei Verstößen gegen diese Garantien muss der Provider entsprechende Entschädigungen leisten.

Infrastruktur

Relevante Fragen in diesem Zusammenhang sind: Verfügt das Netzwerk des DRaaS-Anbieters über eine ausreichende Bandbreite, um den Anforderungen an das RTO gerecht zu werden? Wie werden Traffic und Bandbreite abgerechnet? Zudem lohnt sich ein Blick auf die Möglichkeiten, das interne Netzwerk und das Netzwerk des Anbieters zu integrieren. Gibt es Tools und Prozesse, die sicherstellen, dass das Unternehmensnetzwerk von anderen Kunden isoliert ist?

Beratung und Security Services

Nicht jedes Unternehmen verfügt über eigene Sicherheitsexpert:innen sowie Expertise im Hinblick auf unterschiedliche Cloud-Lösungen. Es gilt also, zunächst durch ein Beratungsgespräch zu ermitteln, ob der Cloud-Anbieter auch eine nachvollziehbare Security-Strategie aufzeigen kann, die den Anforderungen des Unternehmens gerecht wird. Hat er neben DRaaS weitere Security-Maßnahmen im Angebot? Wie sieht der Schutz der DR-Rechenzentren vor Cyberangriffen aus?

Standort

Wo befindet sich die DRaaS-Lösung? Je weiter der Dienst entfernt ist, desto größer ist die Latenzzeit für die Übertragung von Daten in die und aus der Cloud. Dies hat vor allem Auswirkungen auf das gewünschte RTO. Auch Compliance-Anforderungen können eine Rolle bei der Wahl des Anbieters spielen. Sind die Daten in einer Region oder einem Land gespeichert, das andere Rechtsnormen anwendet und somit beispielsweise europäischen Datenschutzstandards nicht entspricht? Ein weiterer interessanter Punkt ist, ob der DRaaS-Anbieter selbst Disaster Recovery implementiert hat. Dies ist besonders für den Fall wichtig, wenn eine Failover-Lösung in der Cloud über einen längeren Zeitraum betrieben werden müsste.

DRaaS und Georedundanz in Deutschland

Provider wie plusserver, die mehrere Cloud-Standorte in Deutschland betreiben, bieten hierzulande eine interessante Alternative zu den großen, globalen Public-Cloud-Anbietern. In vier zertifizierten Rechenzentren in Köln, Düsseldorf und Hamburg (2x) sind wertvolle Unternehmensdaten nicht nur DSGVO-konform gelagert. Durch den eigenen Backbone und voll integrierte Netzwerkservices sind auch verschiedene Disaster-Recovery-Szenarien möglich – von geringsten Latenzen zwischen den Standorten zur hochsicheren Georedundanz für besonders kritische Anwendungen. plusserver berät seine Kunden individuell zu Art und Umfang des gewünschten DR-Services und setzt Lösungen führender Virtualisierungs- und Datensicherungsspezialisten wie VMware oder Veeam ein.

Fazit: DRaaS macht Disaster Recovery zum Mainstream

Disaster Recovery ist mittlerweile nicht mehr nur ein Thema für kritische Infrastrukturen wie Versorgungseinrichtungen, Banken oder den Gesundheitssektor. Glücklicherweise sind die Kosten und vormals hohen Hürden der Implementierung für vollständige Disaster Recovery dank modernen DRaaS-Lösungen aus der Cloud deutlich gesunken. Cloud-basierte Disaster Recovery ist auch für kleine und mittelständische Unternehmen besonders zugänglich, selbst wenn sie nicht über die nötige Erfahrung oder Ressourcen verfügen, einen Disaster-Recovery-Plan zu erstellen, zu testen und auszurollen.

Doch nicht nur der einfachere Zugang sollte Disaster Recovery auf das Radar kleinerer und mittlerer Unternehmen bringen. Denn auf der anderen Seite ist der Bedarf an Notfallabsicherung auch für KMU und öffentliche Organisationen in den vergangenen Jahren deutlich gestiegen. Zunehmende Bedrohungen durch Naturkatastrophen und gezielte Angriffe auf Unternehmen jeder Art haben die Anforderungen an den Schutz von IT-Systemen deutlich erhöht. Gleichzeitig sind Produktivität, Umsatz und das Image zunehmend von IT-Werkzeugen, digitalen Services und Vertriebswegen abhängig. IT-Verfügbarkeit ist auch in traditionellen Branchen ein essenzieller Baustein der Business Continuity geworden. Disaster Recovery ist also zu Recht mittlerweile ein Mainstream-Thema, das Unternehmen nicht ignorieren sollten. Mittels DRaaS aus der Cloud muss ein Unternehmen weder in eine eigene DR-Umgebung investieren noch diese betreiben und warten. All dies übernimmt der Provider – von der Hardware und Software über die Standorte bis hin zum Betrieb. Ein weiterer Vorteil ist das einfache Testing sowie die Vielzahl an Lösungen, die entsprechend den gewünschten Recovery Time Objectives und Recovery Point Objectives ausgewählt werden können.

DRaaS – made in Germany

Die Backup- und DR-Expert:innen von plusserver unterstützen Sie gern dabei, Ihr Unternehmen für den Notfall zu rüsten. Angefangen bei einem Offsite-Backup Ihrer Produktivdaten in zertifizierten und DSGVO-konformen Rechenzentren bis hin zu verschiedenen Disaster-Recovery-Lösungen Ihrer Primärumgebung. Egal ob diese in Ihrem Unternehmen oder bereits in einer Cloud betrieben wird.

Kostenfreies Beratungsgespräch