Acronis

Die **7 goldenen Regeln** für **Business Continuity** in der **IT**

Wie Sie Ihr Unternehmen, Ihre Kunden und sich selbst mit BCDR schützen

Während das Konzept „Business Continuity und Disaster Recovery“ (hier kurz BCDR genannt) bereits seit einiger Zeit etabliert ist, variiert die tatsächliche Implementierung je nach Lösung, Anbieter und Branche. Oberflächlich betrachtet sieht es oft unkompliziert aus: Sichern, replizieren, vorausplanen und testen. Und Sie möchten vermutlich nicht derjenige sein, der die Sache verbockt – besteht der einzige Zweck von BCDR doch darin, nur ein einziges Mal zu funktionieren, oder? Falsch! Denn der Teufel liegt bekanntlich im Detail. Betrachten wir zuerst doch einmal das Gesamtbild:

> “
> **80% aller Unternehmen,** die eine höhere Betriebsbereitschaft erreichen wollen, werden diese ohne Implementierung angemessener Management-Tools für BCDR nicht schaffen.[1]
>
> *Gartner* ”

BCDR im Überblick

Lassen Sie uns zuerst einmal die Zielsetzung von BCDR verstehen. Die wichtigsten Gründe für BCDR sind üblicherweise:

1. Ungeplante Ereignisse „überleben“

Viele Ereignisse können dazu führen, dass ein IT-Service ausfällt oder in seiner Leistung stark absinkt: natürliche Katastrophen, technische Ausfälle, Anwenderfehler, etc. Während Desaster, Terroranschläge oder bösartiger Datendiebstahl für gewöhnlich ein hohes Maß an Aufmerksamkeit bekommen, sind es jedoch betriebsbedingte Ereignisse (und keine Desaster), die für die meisten IT-Ausfälle verantwortlich sind. Laut Forrester Research[2] sind die Hauptursache einfache Stromausfälle, gefolgt von Fehlfunktionen bei Hardware, Software und Netzwerk. Es ist wichtig, die unterschiedlichen Konsequenzen zu verstehen: Während natürliche Desaster und Feuer einen kompletten Standort für längere Zeit außer Betrieb setzen können, sind die Auswirkungen technischer oder menschlicher Fehler in der Regel begrenzt und können meist relativ schnell behoben werden.

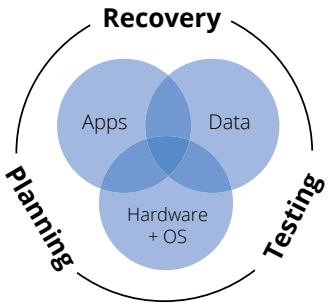
> “
> Immer noch sind alltägliche Ereignisse (wie **Stromausfall, Fehler in der IT oder menschlicher Irrtum**) die **Hauptursachen** für Störungen.[2]
>
> *Forrester* ”

2. Business Continuity für den regulären Betrieb sicherstellen

Zusätzlich zu ungeplanten IT-Ausfällen nimmt die Bedeutung moderner BCDR-Lösungen auch deswegen zu, weil die Ansprüche an Stabilität und Agilität von IT-Diensten immer höher werden. Geplante betriebliche Prozesse wie Soft- und Hardware-Upgrades, Wartung von Anlagen und Migration von Datenzentren oder auch Änderungen der Unternehmensstruktur wie Firmenfusionen/Übernahmen verlangen von der IT hohe Anpassungsfähigkeit und Unabhängigkeit in Bezug auf die physische Infrastruktur und den Standort. Da die Kontinuität des IT-Services für Unternehmen von entscheidender Bedeutung ist, betrachten diese BCDR zunehmend unter dem Aspekt, damit auch bei allen geplanten betrieblichen Ereignissen einen kontinuierlichen IT-Betrieb aufrechtzuerhalten.

Die zugrundeliegende Technologie

DR-Lösungen (Disaster Recovery) müssen – unabhängig von der zugrundeliegenden Technologie – folgende Kernkomponenten wiederherstellen können:



1. Daten
2. Infrastruktur (Hardware und Betriebssystem)
3. Applikationen

Durch dateibasierte Sicherung werden im Prinzip Kopien von Dateien und Ordnern lokal oder offsite erstellt. Über die Jahre wurden Backup-Technologien weiterentwickelt, um die Größe des Backup Storages zu minimieren (Deduplizierung), den Datenverkehr übers Netzwerk zu reduzieren (Datenkomprimierung), die Sicherheit der Daten bei Übertragung und Speicherung zu gewährleisten (Verschlüsselung) und das benötigte Backup-Fenster zu verkleinern. Die Backup-Vorgänge wurden durch all diese Verbesserungen mittlerweile soweit optimiert, dass normales Backup zum ganz alltäglichen IT-Betrieb eines Datenzentrums gehört.

> “
> Da man für eine On-Demand-Wiederherstellung von Daten und Servern keine besonderen Anlagen oder Räumlichkeiten bereitstellen muss, können Kunden ihre Recovery-Pläne regelmäßig testen.[3]
>
> *Gartner* ”

Durch Systemreplizierung wird im Prinzip eine Kopie der geschäftskritischen IT-Umgebung erstellt: von Servern, Datenbanken und Netzwerken, egal ob sie physisch oder virtuell sind. Wenn das primäre Datenzentrum ausfällt, kann diese Kopie gestartet und solange verwendet werden, bis die ursprüngliche Umgebung wieder verfügbar ist. Es gibt viele mögliche Architekturen und Verknüpfungen zwischen dem primären Datenzentrum und der Kopie – abhängig davon, wie geschäftskritisch eine Umgebung ist, sowie von der Verfügbarkeit von Räumlichkeiten für das zweite Datenzentrum und dem Budget. Mit der zunehmenden Verbreitung Cloud-basierter Services wird es zunehmend üblich, mandantenfähige Cloud-basierte Disaster Recovery Services namhafter DR-Anbieter einzusetzen – oder eine hybride Kombination von Services mit lokaler und externer Bereitstellung.

> “
> Nun, da herkömmliche DR-Ansätze zunehmend veraltet und uneffektiv sind, werden DRaaS-Anbieter mit einstellbarer Ausfallsicherheit, einer breiten Plattform-Unterstützung sowie attraktiven Vertragsbedingungen und Preisen die Führung übernehmen.[5]
>
> *Forrester Wave TM* ”

Virtualisierung ändert alles

In einer Umgebung mit physischen Servern können verschiedene Einzellösungen individuelle Funktionalität für Daten-Backup und Systemreplizierung ermöglichen. Durch die zunehmende Virtualisierung von IT-Umgebungen und die steigende Popularität Software-basierter Infrastrukturen (Daten, Netzwerke) können alle Komponenten jedoch auch in Form einer einzigen virtuellen Umgebung gesichert werden. Virtualisierung vereinfacht die Möglichkeiten für Disaster Recovery deutlich, reduziert die Kosten und verbessert die Gewissheit, dass zugesicherte RPOs (Recovery Point Objectives) und RTOs (Recovery Time Objectives), die über Service Level Agreements deutlich definiert sind, auch eingehalten werden können.

Der Teufel steckt im Detail

BCDR kann auf unterschiedliche Weise implementiert werden, und zwar mit unterschiedlichen Schutzniveaus bei unterschiedlichen Kosten. Dies könnte beträchtliche Investitionen erfordern – und das im Umfeld sinkender IT-Budgets und Personalressourcen. Den ROI (Return on Investment) von BCDR genauer zu berechnen, würde den Rahmen dieses Dokuments sprengen [lesen Sie dazu das Whitepaper „Der Return on Investment (ROI) von Disaster Recovery (DR)"]. Es ist jedoch entscheidend, dass eine BCDR-Lösung, die Ihre IT Services absichern soll, auch wirklich erfolgreich funktioniert.

> "Jedes dritte Unternehmen hatte innerhalb der letzten fünf Jahre ein Desaster zu verzeichnen.[2]"
>
> *Forrester*

Zum Entwerfen Ihrer BCDR-Lösung empfehlen wir bewährte Vorgehensweisen aus der Praxis:

1. Vorausplanen und Dokumentieren

Ihr IT-Personal benötigt sorgfältig dokumentierte Aktionspläne, um bei geplanten oder ungeplanten Service-Unterbrechungen effizient reagieren zu können. Diese Pläne sollten ausführliche Recovery-Prozesse sowie Einsatzregeln für den BCDR-Anbieter enthalten inkl. Kommunikationswege und Übertragungsmöglichkeiten. Wann tritt für Sie ein Desasterfall ein? Wo werden die entsprechenden Kopien der Daten, Programme und Lizenzen gespeichert? Welche Datenmenge darf schlimmstenfalls verloren gehen und wie schnell muss die Wiederherstellung erfolgen? Die detaillierten Pläne sollten zumindest auf Papier bzw. in gedruckter Form verfügbar sein. Noch besser ist es, wenn sie den Mitarbeitern auch digital vorliegen.

> "Cloud-basiertes Backup und Disaster Recovery ist der Top Cloud Service, dessen Nutzung IT Professionals innerhalb der nächsten 6 Monate planen – unabhängig von Region und Unternehmensgröße.[4]"
>
> *SpiceWorks*

2. Applikationen replizieren

Backup ist zwar fundamental für BCDR, aber dieser Faktor allein kann nicht für einen unterbrechungsfreien Geschäftsbetrieb sorgen. So sind Daten ohne funktionierende Server nutzlos. Hardware/Software neu aufzubauen und die entsprechenden Daten zu laden, kann einige Zeit dauern. Eine mögliche Lösung dafür ist ein zweiter Standort, an dem alle Applikationen und Daten repliziert vorliegen. Für kleine bis mittlere Unternehmen ist dies jedoch finanziell möglicherweise nicht umsetzbar. Dank der Leistungsfähigkeit cloudbasierter Technologien kann Disaster Recovery mittlerweile auch als Service angeboten werden (Disaster Recovery as a Service, kurz DRaaS), basierend auf einer mandantenfähigen Remote-Replizierung. Führende Anbieter können damit SLA-basierte Verfügbarkeit Ihrer Applikationen und Daten direkt aus DRaaS-Datenzentren heraus und über eine sichere Internetverbindung garantieren. Ihre wiederhergestellten IT Services können innerhalb eines vereinbarten Zeitfensters (von oftmals nur 15 Minuten) wieder verfügbar sein – und zwar solange, bis Ihr primärer Standort wieder online ist.

> "Cloud-basierte Recovery Services haben sich aus herkömmlichen Managed Services für DR entwickelt, wie sie von Enterprise-Unternehmen genutzt werden, und aus Online Backup Services, die überwiegend von kleinen und mittleren Unternehmen verwendet werden.[3]"
>
> *Gartner*

3. Onsite- und Offsite-Absicherung einrichten

Moderne BCDR-Technologien bieten sowohl eine Onsite- als auch eine Remote-Absicherung. Jede Option hat Vor- und Nachteile. Eine lokale Sicherung ermöglicht leichteren Zugriff auf Ihre Daten und ein grundsätzlich schnelleres Wiederherstellungstempo. Eine lokale Replizierung hilft nur, wenn Ihre primäre Umgebung noch verfügbar ist. Zum Schutz gegen schwere Desaster oder zur Langzeitaufbewahrung müssen Sie Ihre Daten und Applikationen jedoch offsite sichern – vorzugsweise an einem geografisch entfernten Ort, der von lokalen Vorfällen unberührt bleibt. Eine zeitgemäße, erstklassige BCDR-Technologie bietet Hybrid-Lösungen, damit Sie die Vorteile beider Optionen kombinieren können: eine lokale Appliance für schnellen Zugriff plus effiziente Replizierung Ihrer Umgebung in die Cloud für ultimativen Schutz.

4. Recovery-Prozesse automatisieren

Selbst wenn Ihre IT-Mitarbeiter die besten der Welt sind – im Notfall sollten Sie nicht auf deren fehlerfreie Ausführung komplexer Prozesse vertrauen. Denn die Wahrscheinlichkeit menschlicher Fehler nimmt unter Stress und den Unwägbarkeiten eines Desaster-Ereignisses deutlich zu. Stellen Sie sich vor, wie Ihre Mitarbeiter mehrere Server manuell starten, Daten wiederherstellen und validieren, Netzwerkverbindungen testen und diverse kritische Tasks ausführen, bei denen jeder Fehler zu Datenverlust oder verlängerter Ausfallzeit führen kann – und wie Sie die Wichtigkeit der Aufgaben gegen die Sicherheit ihrer Familien abwägen. Der Großteil Ihres Personals ist vielleicht noch nicht einmal greifbar, weil sie sich gerade um die Sicherheit ihrer Familien kümmern. Daher bietet ein DR-Ansatz, bei dem sich der Wiederherstellungsprozess „wie auf Knopfdruck" starten lässt, einen besseren ROI – besonders in Umgebungen mit nur begrenzten IT-Ressourcen und Know-How. Modernes, automatisiertes BCDR beinhaltet das Testen von Abhängigkeitsbedingungen, Parallelverarbeitung, manuelle Arbeitsabläufe mit Benachrichtigungen und andere Elemente, die Ihre Wiederherstellung zuverlässig, wiederholbar und testfähig machen.

> "Automatisieren, automatisieren, automatisieren. Die Komplexität heutiger Technologien übersteigt mittlerweile das, was Menschen handhaben können.[2]"
>
> *Forrester*

5. Regelmäßig testen

Die Erfahrung lehrt: Ausführlich und häufig testen! Eine Disaster Recovery-Lösung ist nur dann ihr Geld wert, wenn sie auch wirklich funktioniert. Ansonsten ist die Investition verschwendet. Selbst wenn Ihr Plan perfekt entworfen und durchgetestet ist, wird sich Ihre Umgebung mit der Zeit doch immer wieder ändern. Hard- und Software-Upgrades, Netzwerkoptimierung, Personalschulungen oder Übergabeprobleme können alle einen Einfluss auf den Erfolg Ihrer BCDR-Prozesse haben – selbst in vollautomatisierten Umgebungen. Aus diesem Grund ist es so wichtig, Ihre DR-Pläne so häufig wie noch sinnvoll möglich zu testen. Fortschrittliche BCDR-Lösungen bieten bereits integrierte Testmöglichkeiten, ein separates virtuelles Testnetzwerk und die Möglichkeit zur Zeitplanung.

> "Mit DRaaS erfolgen Testvorgänge üblicherweise automatisiert und ohne Störung anderer Betriebsabläufe. Sie können also häufiger testen.[5]"
>
> *Forrester Wave ™*

6. Datensicherungen schützen

Sicherheit ist immer ein wichtiger Aspekt und BCDR ist davon keine Ausnahme. Für lokal gehostete BCDR-Lösungen gilt dieselbe Sicherheit wie für Ihre primären Daten und Applikationen. Ihren Bedarf für BCDR einer Cloud anzuvertrauen ist jedoch eine Herausforderung. Insbesondere in stark regulierten Branchen ist eine entscheidende Voraussetzung, die Daten in der Cloud vertraulich und sicher zu halten. Viele Normen und Richtlinien verlangen, dass Unternehmen ihre Daten schützen und Abwehrmaßnahmen gegen Bedrohungen bereitstellen. Nicht zuletzt müssen insbesondere die von den DRaaS-Anbietern verwendeten Datenzentren selbst die Einhaltung höchster Sicherheitsstufen nachweisen. Zusätzlich sollte die Möglichkeit bestehen, Daten lokal, bei der Übertragung und bei der Ablage auf dem Remote-Storage verschlüsseln zu können, verbunden mit einer angemessenen Verwaltung und Handhabung der Schlüssel.

7. Wählen Sie Ihren BCDR-Partner sorgfältig

Die Erfahrung zeigt, dass man mit der Wahl eines Anbieters, dessen primärer Fokus auf BCDR liegt, am besten fährt. Bei größeren Anbietern ist BCDR zwar öfter als Komponente in vielen Lösungen enthalten, allerdings ist diese Funktionalität zu wichtig, um sie jemandem anzuvertrauen, der sie nur als nachträglichen Zusatz zu seiner breiten Palette von Hard- und Software-Produkten oder Professional Services betrachtet. Ein zweiter, entscheidender Punkt: Es ist wichtig, sich für jemanden zu entscheiden, der sich in Ihrer Branche auskennt und dort eine breit installierte Basis hat. Dadurch können Sie gewiss sein, dass der Anbieter mit Ihren Fragen und Problemen vertraut ist und bei brenzligen Situationen, die eine schnelle Reaktion erfordern, nicht erst aufwendige Untersuchungen durchführen muss. Die Wahl einer bewährten, überlegenen Technologie, die von unabhängigen Stellen validiert wurde, kann Ihnen intensive Nachforschungen und den Vergleich von Anbietern abnehmen. Es gibt eine Vielzahl von Analysten, die den BCDR-Bereich abdecken – erkundigen Sie sich dort, bevor Sie Ihre Wahl treffen!

Die nächsten Schritte

Zusammenfassend kann man also sagen, dass BCDR so etwas wie Ihre Versicherungspolice für die IT und Ihr Schutzmechanismus zur Risikominderung ist. Wir haben die wichtigsten Aspekte aufgezeigt, die dafür zu sorgen helfen, dass Ihre BCDR-Lösung im Bedarfsfall auch wirklich funktioniert, und Ihnen einen Überblick über die verfügbaren Möglichkeiten gegeben. Basteln Sie besser nicht selbst herum, sondern arbeiten Sie mit einem professionellen, erfahrenen Anbieter.

Quellen

1.) Witty, Roberta J./Morency, John P./Russell, Dave: Business Continuity and IT Disaster Recovery Management; In: Gartner: Predicts 2014; 2.) Balaouras, Stephanie: The State of Business Technology Resiliency; Forrester, Q2 2014; 3.) Morency, John P./Witty, Roberta J.: Hype Cycle for Business Continuity Management and IT Disaster Recovery Management; Gartner, 2014; 4.) Spiceworks Annual State of IT Report, 2014; 5.) Dines, Rachel A.: Disaster-Recovery-as-a-Service Providers; The Forrester Wave, Q1 2014

Über Acronis

Acronis setzt Standards für Data Protection der Neuen Generation. Mit seinen Lösungen für Backup, Disaster Recovery und sicheren Zugriff, basierend auf der AnyData Engine, und dem Vorsprung durch seine Imaging-Technologie, bietet Acronis einfaches, umfassendes und sicheres Backup für Dateien, Applikationen und Betriebssystem in beliebiger Umgebung – virtuell, physisch, Cloud oder mobil.

Acronis wurde 2002 gegründet und schützt Daten von über 5 Millionen Nutzern und 300.000 Unternehmen in über 130 Ländern. Acronis-Produkte beinhalten mehr als 100 Patente und wurden u.a. zum besten Produkt des Jahres gewählt von Network Computing, TechTarget und IT Professional. Die Produkte decken eine große Bandbreite von Funktionen ab wie z.B. Migration, Klonen und Replizierung.

Weitere Informationen erhalten Sie unter **www.acronis.de**; Folgen Sie Acronis auf Twitter unter **https://twitter.com/acronis_de** oder auf Facebook unter **https://www.facebook.com/acronis.germany**