WHITEPAPER:

SentryOne

# Geschäftskontinuitätsplanung mit der Microsoft Data Platform

## EINFÜHRUNG

Geschäftskontinuität ist ein heißes Thema – es vergeht kaum ein Nachrichtenzyklus, ohne Berichte über einen ernsten technologischen Ausfall. Bis jetzt wurden für 2018 unterschiedliche Schweregrade an Ausfällen von Finanzunternehmen wie Chase Bank, TSB Bank und Visa berichtet. Diese Ausfälle haben eine enorme Auswirkung darauf, wie Unternehmen funktionieren – oder, was wichtiger ist, nicht funktionieren.

Außerdem verlagert sich eine zunehmende Anzahl an Unternehmen in die Cloud oder macht sich Cloud-Services zu Nutze, während Cloud-Anbieter ebenfalls von diesem Problem betroffen sind; Ausfallprobleme wurden von den drei größten Cloud-Anbietern berichtet: Google Cloud, Amazon AWS und Microsoft Azure. Amazons E-Commerce-Website war während ihres 2018 Prime Day 63 Minuten lang nicht aufrufbar, was zu einem Verlust von 99 Millionen USD in Verkäufen führte. Und Amazon ist nicht alleine: Ein IDC-Bericht schätzt die Kosten von unplanmäßigen Anwendungsausfällen von Fortune 1000 Unternehmen auf 2,5 Milliarden USD pro Jahr ein!

Heute müssen Unternehmen mehr als je zuvor die Risiken verstehen, die mit ihren täglichen Prozessen verbunden sind, und Änderungen vornehmen, um ihre Zukunft und die finanzielle Sicherheit ihrer Mitarbeiter und Teilhaber zu schützen. Dieses Whitepaper wird Sie bei der Planung Ihrer Geschäftskontinuitätsprozesse und der Nutzung der Microsoft Data Platform anleiten.

## Über den Autor

Richard ist ein Principal Solutions Engineer bei SentryOne, der sich auf die Angebote des SentryOne SQL Server-Portfolios im EMEA-Raum spezialisiert hat. Er hat in diversen Entwickler- und DBA-Rollen seit Version 7.0 mit SQL Server gearbeitet und verfügt über mehrere Microsoft-Zertifikate. Richard ist ein aktives Mitglied der SQL Server-Community; in der Vergangenheit leitete er eine PASS-Filiale im Vereinigten Königreich und war Mitglied des Organisationskomitees für SQLRelay.

## Über SentryOne

SentryOne ist ein Technologie-Unternehmen mit Sitz in Charlotte, dessen preisgekrönte Lösungen Microsoft-Datenspezialisten darin unterstützen, revolutionäre Durchbrüche in physischen, virtuellen und Cloud-Umfeldern zu erreichen. Das Team teilt seine Expertise unter blogs.sentryone.com und sqlperformance.com.

**Richard Douglas**
**PRINCIPAL SOLUTIONS ENGINEER**



SentryOne

# Geschäftskontinuitätsplanung mit der Microsoft Data Platform

VON RICHARD DOUGLAS

Die meisten Unternehmen, die über IT-Infrastruktur verfügen, sind sich im Klaren über die Notwendigkeit eines Disaster-Recovery-Plans (DR-Plans). Invenio ITs Bericht 2017 Disaster Recovery Statistics that Businesses Must Take Seriously (Disaster-Recovery-Statistiken für 2017, die Unternehmen ernst nehmen müssen) zeigt, wie extrem wichtig es ist, einen DR-Plan zu erstellen. Folgendes sind die wichtigsten Highlights des Berichts:

- 90 % aller Unternehmen ohne einen DR-Plan wurden nach einem großen Notfall aufgelöst
- 30 % aller untersuchten Unternehmen verfügten über keinen DR-Plan
- 30 % aller Unternehmen, die über einen Plan verfügten, waren bei Eintritt eines Notfalls nicht bereit zu handeln
- 45 % aller ungeplanten Ausfälle sind die Folge von Hardwareversagen
- 35 % aller unerwarteten Ausfälle sind die Folge von Stromausfällen
- 12 % aller Unternehmen waren nicht in der Lage, ihre Daten wiederherzustellen
- Die Kosten von ungeplanten Ausfallzeiten können sich auf 17.244 USD pro Minute belaufen

## Wenn DR so wichtig ist, wozu dann die Rede über Geschäftskontinuität?

Geschäftskontinuität (*Business Continuity*, BC) macht dort weiter, wo DR aufhört. Der Umfang von DR ist in der Regel auf bestimmte Situationen in der IT beschränkt, anstatt eine komplette Risikoeinschätzung (*Risk Assessment*, RA) aller kritischen Geschäftsanwendungen und Verfahren für jede einzelne Geschäftsfunktion innerhalb eines Unternehmens durchzuführen. Die Geschäftsauswirkungsanalyse (*Business Impact Analysis*, BIA) ist ausschlaggebend dafür, bei der Erstellung eines eigenen Geschäftskontinuitätsplans (*Business Continuity Plan*, BCP) die richtigen Prioritäten zu setzen.

### Eine Anmerkung zu hoher Verfügbarkeit

Funktionen für hohe Verfügbarkeit (*High Availability*, HA) in der IT werden oft als ein DR-Plan fehlinterpretiert. Eine HA-Funktion ist darauf ausgelegt, ein bestimmtes Szenario abzudämpfen. Ein DR-Plan kommt ins Spiel, wenn ein Notfall diese spezielle Funktion aushebelt. Wenn z. B. versehentlich Daten gelöscht wurden, werden sie auch auf sämtlichen sekundären Servern gelöscht sein, die eine Form von synchroner Replikation zum Ausfüllen ihrer Daten verwenden. Ein Ausfallsicherung zu einem der sekundären Server wird diese Daten nicht zurückbringen!

### Ein Beispiel, das HA, DR und BC einschließt

Ein häufiges Beispiel hierfür wäre ein Stromausfall. Denken Sie an unsere obige Statistik zurück, laut der 35 % aller unerwarteten Ausfallzeiten in Folge von Stromausfällen entstehen. Nehmen wir hypothetisch an, dass ein Unternehmen namens Acme Widgets in weiser Voraussicht einen DR-Standort eingerichtet hat. Es hat sogar einen Stromgenerator an seinem primären Standort installiert, um Stromausfällen entgegenzuwirken.

So kann die für die Implementierung des DR-Plans zuständige Person den Backup-Stromgenerator verwenden und den sekundären Standort als Ausfallsicherung bereithalten. Im Rahmen dieses Beispiels nehmen wir an, dass der DR-Plan nicht regelmäßig getestet wurde, sodass der Generator sich nicht aktiviert hat. Das bedeutet, dass der sekundäre Standort als einzige Option verblieben ist.

An diesem Punkt haben sich die HA-Funktionen als hilfreich erwiesen, die Datenbanken und Anwendungen haben ein Failover zum sekundären Standort vollzogen und die meisten Anwendungen scheinen ordnungsgemäß zu funktionieren.

Allerdings befinden sich alle Nutzer leider am primären Standort und haben keinen Strom, sodass sie sich nicht mit ihren Anwendungen verbinden und Aufträge annehmen können. Ohne den Stromgenerator müssen viele Nutzer nun einen Ort mit Strom aufsuchen. Der BCP kann Ausweichmaßnahmen enthalten, um einen Teil der Mitarbeiter an den sekundären Standort zu schicken, während andere von Zuhause aus arbeiten oder ein spezielles gemeinsames Büro verwenden, das von einem anderen Unternehmen gemietet wurde.

## Prüfung

Wie bereits erwähnt, ist die BIA ein grundlegender Bestandteil des BCP eines jeden Unternehmens. Diese sollte mehrere zentrale Komponenten enthalten, darunter:

- Eine Entdeckungsphase, um die Anfälligkeiten aller Geschäftsprozesse offenzulegen.
- Eine Finanzprüfung der Kosten für das Unternehmen, falls eines dieser Risiken eintreten sollte.
- Eine strategische Phase, um die Wahrscheinlichkeit des Eintretens dieser Risiken zu verringern oder zu eliminieren.
- Eine Berichterstattungsphase, um all das für das leitende Management zusammenzufassen, sodass es diese Informationen überprüfen und das erforderliche Budget zuweisen kann.

Den Umfang der BIA zu definieren ist ausschlaggebend. Auch wenn Ihre morgendliche Tasse Kaffee am Arbeitsplatz für Sie extrem wichtig erscheinen könnte, handelt es sich hierbei nicht um einen Geschäftsprozess. Die Installationen mehrerer Kaffeemaschinen mit zweifacher Wasserversorgung und einem eigenen Generator vorzuschlagen, könnte ziemlich übertrieben klingen.

Allerdings sollten Sie nicht vergessen, dass Mitarbeiter ebenso eine Ressource sind wie Ihre IT-Infrastruktur. Bereiche wie Sicherheit und Gesundheit werden oft übersehen. Über wie viele medizinisch geschulte Mitarbeiter verfügen Sie für den Fall einer Naturkatastrophe? Können sie alle zur gleichen Zeit ihren jährlichen Urlaub antreten? Verfügen Sie über ausreichend medizinische Versorgungsgüter? Der Verlust eines menschlichen Lebens ist immer tragisch. Wenn Sie es von einer geschäftlichen Perspektive betrachten, ist der Verlust eines Lebens auch immer mit den zusätzlichen Kosten eines Wissensverlusts für das Unternehmen verbunden. Aus diesem Grund verbieten einige Unternehmen wichtigen Angestellten sogar, gemeinsam zu reisen, damit im Falle eines extrem unwahrscheinlichen Unfalls nicht zu viel Wissen auf einen Schlag verloren geht.

## SLAs festlegen

Wenn es um BCPs geht, müssen diverse Service-Level-Vereinbarungen (*Service Level Agreements*, SLAs) einbezogen werden. Die drei häufigsten sind:

- **Recovery Point Objective (RPO)** – Die Menge an Daten, deren Verlust ein Unternehmen im Falle eines Ausfall-Ereignisses hinnehmen kann.
- **Recovery Time Objective (RTO)** – Die angestrebte Zeit für die Wiederaufnahme einer kritischen Aktivität nach einem Ereignis.
- **Maximum Tolerable Period of Disruption (MTPD)** – Der Punkt an dem die Überlebensfähigkeit eines Unternehmens in Gefahr ist, wenn kritische Aktivitäten nicht wiederaufgenommen werden können.

Es ist äußerst wichtig, diese Faktoren in Ihren BCP einzubeziehen. Beachten Sie dabei, dass das kein universeller Einheitsansatz ist. Es gibt immer bestimmte Anwendungen und Prozesse, die mehr oder weniger widerstandsfähig gegenüber Datenverlusten sind als andere. Sobald die RA durchgeführt und Ihre BIA abgeschlossen wurde, können Sie diesen Prozessen die entsprechenden SLAs zuordnen.

Finanzielle Einschränkungen geben in der Regel die Technologien und Prozesse vor, die implementiert werden können, um gute RTO- und RPO-Zeiten zu erreichen. Es ist eine bewährte Praxis, BCP-Konversationen durchzuführen, bevor neue Anwendungen integriert und bereitgestellt werden, um die wahren Kosten dieser Anwendung in Erfahrung zu bringen.

## Geschäftsprozesse überwachen, nicht nur die Infrastruktur

Aktivitätsstatus-Überwachung ist die elementarste Form der Überwachung, die ein Unternehmen einsetzen kann. Es handelt sich dabei meist um eine Reihe einfacher Skripts oder um eine Freeware-Anwendung, die Sie in irgendeiner Art benachrichtigt, wenn ein Server offline geht. Um Ihren internen und externen Kunden ein hochwertiges Service-Niveau bieten zu können, benötigen Sie allerdings viel mehr Informationen. Noch wichtiger ist es, dass Sie bereit und in der Lage sein sollten, anhand dieser Informationen Maßnahmen zu ergreifen, um eine alternative Lösung bereitzustellen und diesen speziellen Geschäftsprozess am Laufen zu halten.

Überwachung ist Ihre erste Verteidigungslinie, wenn es um DR-, HA- und BC-Planung geht. Erweiterte Überwachungslösungen bieten die Möglichkeit, bestimmte Ereignisse einzuleiten, wenn ein Szenario eintritt. Die besten Überwachungslösungen erlauben es Ihnen, diese Szenarios selbst zu erstellen, anstatt eine Option aus einer vordefinierten Liste von Ereignissen auszuwählen. Das ermöglicht Ihnen, Ihre eigenen Geschäftskontinuitätsprozesse innerhalb einer solchen Lösung zu implementieren und zu automatisieren.

### Überwachung für DR

Eine Überwachung für DR auf Basis-Niveau ist sehr einfach. Sicherzustellen, dass Sie über ausreichende Informationen verfügen, um die korrekten Verfahren zur Wiederherstellung nach einem Notfall zu implementieren, ist hingegen etwas schwieriger. Einen proaktiven Ansatz für die DR zu verfolgen ist noch schwieriger, aber es gibt Warnsignale, über die gute Überwachungslösungen Sie benachrichtigen können, darunter:

- Sehen Sie verdächtige Seiten in Ihren Datenbanken?
- Sehen Sie Fehler 825 in Ihren Fehlerprotokollen?

Beides davon kann darauf deuten, dass die zugrundeliegende Speicherebene anfängt, Daten zu korrumpieren. Eine Wiederherstellung der Daten von letzter Nacht kann in diesem Fall auch die Korruption wiederherstellen. Sie müssen wissen, wann das Problem eingetreten ist und Maßnahmen ergreifen, um es zu beheben.

## Überwachung für HA

Im Rahmen der Microsoft Data Platform gibt es diverse Technologien, die eingesetzt werden können, um Ausfallrisiken zu reduzieren. Beachten Sie, dass nur die synchrone Replikation von Daten eine Garantie gegen Datenverlust darstellt. Nur weil Sie bestimmte HA-Technologien implementiert haben, bedeutet das nicht, dass Sie vor Datenverlust geschützt sind. Sie müssen dafür sorgen, dass der erlittene Datenverlust nicht ihren RPO überschreitet.

Mit einer guten Überwachungslösung können Sie Ihre HA-Technologien überwachen, z. B. mit Microsoft SQL Servers AlwaysOn Availability Groups. Sie sollten sowohl in der Lage sein zu sehen, wie viele Daten an Ihren sekundären Standort übertragen werden als auch wie viele Daten an den sekundären Standorten noch verarbeitet werden müssen.

Wenn dieser Prozess zu weit zurückliegt, könnten Sie Ihre RPO SLAs überschreiten. Ein gutes Überwachungstool wird Sie warnen können, wenn diese Art von Ereignissen eintritt.

*Überwachung von potentiellem Datenverlust in AlwaysOn Availability Groups*

**Überwachung für BC**

Da Überwachung für BC ein derart benutzerdefinierter Prozess ist, kann er nur schwer vorkonfiguriert bereitgestellt werden. Deshalb erlauben Ihnen die besten Überwachungslösungen ihr Warnungs-Framework zu benutzen, um viele unterschiedliche Datenquellen zu erfassen und zusammenzuführen, um ein szenariobasiertes Warnsystem zu erstellen. Wir bei SentryOne bevorzugen den Begriff „Bedingung“ anstelle von „Warnung“, um zwischen den unterschiedlichen Methodiken der Überprüfung einfacher Schwellenwerte und aussagekräftigeren szenariobasierten Situationen zu unterscheiden.

Dies sind einige der häufigen Fragen, die Sie mit Hilfe der besten Überwachungslösungen beantworten können:

- Wissen Sie, wann die letzten Backups der vollständigen und differentiellen Protokolle und der Transaktionsprotokolle Ihrer Datenbankserver erstellt wurden?
- Wurden einige Ihrer Backup-Aufträge nicht durchgeführt?
- Wird Ihr RPO durch das Fehlen eines Backups überschritten?

## Kommunikationsprobleme

Die richtigen Personen zur richtigen Zeit mit den richtigen Informationen zu benachrichtigen, um die nächsten Schritte zu implementieren, ist ausschlaggebend für den Erfolg eines BCP. Die besten Überwachungslösungen ermöglichen Ihnen, Benachrichtigungen über unterschiedliche Plattformen zu verschicken, z. B. Slack, Skype, E-Mail und Pager.

Ein häufig übersehener Aspekt von BC ist Lärm. Sowohl extremer Lärm als auch komplette Stille stellen äußerst unterschiedliche Probleme dar, die adressiert werden müssen. Die Abwesenheit von Benachrichtigungen als solche kann als etwas Gutes angesehen werden. Doch haben Sie auch daran gedacht, dass eine Trennung der Internet-Verbindung oder ein Ausfall Ihres E-Mail-Servers verhindern könnten, dass Sie Benachrichtigungen erhalten? Eine bewährte Praxis, sich vor diesen Situationen zu schützen, ist es, zu bestimmten Zeiten False Positives zu erstellen, um zu überprüfen, dass der Empfang von Benachrichtigungen ordnungsgemäß funktioniert.

Extremer Lärm kann zu Konzentrationsstörungen führen. Es ist menschlich, nach Mustern in Dingen zu suchen; sobald Lärm ein Muster annimmt, besteht das Risiko, dass keine Maßnahmen ergriffen werden, wenn ein wirklich kritisches Ereignis vom Hintergrundlärm getarnt ist. Stellen Sie sicher, dass Sie Ihre Benachrichtigungen bei der Erstellung Ihrer Bedingungen sorgfältig kalibrieren, um ungewünschten Lärm herauszufiltern, indem Sie die korrekten Szenarien für jede Bedingung einstellen.

## Prozesse automatisieren

Im vorherigen Bereich habe ich erwähnt, dass die Benachrichtigung der korrekten Personen ausschlaggebend für Ihre Geschäftskontinuität ist. Doch was wäre, wenn Sie sie nicht benachrichtigen müssten? Was wäre, wenn es einen Weg gäbe, automatisch mehrere Probleme zu adressieren, die zur Unterbrechung Ihrer Geschäftskontinuität führen könnten? Die besten Überwachungstools verfügen über Funktionen, mit denen Sie Skripts automatisieren können, um bestimmte Probleme zu beheben, die in der Regel mit Ihrer IT-Infrastruktur verbunden sind. Die Hauptvorteile dieser Funktion sind ein verringertes RTO und die Gewissheit, dass keine Fehler unter Druck entstehen.

In der Lage zu sein, die Menge repetitiver Arbeit zu verringern, die Mitarbeiter erledigen müssen, verringert ihre Gehaltskosten. Team-Mitglieder können auf diese Weise einen größeren Mehrwert erzeugen, indem Sie sich dringenderen Aufgaben widmen, die den Profit Ihres Unternehmens beeinflussen.

Nachdem die Risiken im Rahmen der BIA identifiziert wurden, müssen Sie Methoden entwickeln, um diese Risiken zu mindern.  Wenn es in dieser strategischen Phase einen Weg gibt, diesen Prozess zu automatisieren, werden die besten Überwachungslösungen Ihnen dabei helfen. Stellen Sie sich zum Beispiel vor, dass Server 1 an Standort A als offline gemeldet wurde. Das System könnte automatisch ein Skript oder einen Auftrag für Server 2 an Standort B auslösen, ein manuelles Failover durchzuführen / Datenbanken wiederherzustellen, sodass Nutzer auf diese Datenquellen zugreifen könnten.

## FAZIT

Einen BCP zu erstellen und fortlaufend weiterzuentwickeln ist extrem schwierig. Es gibt viele bewegliche Teile, die sich ständig verändern. Jedes dieser Teile verfügt über einen unterschiedlichen Wert für unterschiedliche Personen und Abteilungen innerhalb Ihres Unternehmens. Deshalb ist es ausschlaggebend dafür zu sorgen, dass wichtige Teilhaber des Unternehmens in den Planungs- und Überwachungsphasen involviert sind. Ohne ihren Input, könnte der BCP unzureichend sein, um sicherzustellen, dass der maximal tolerierbare Störungszeitraum (Maximum Tolerable Period of Disruption) nicht eintritt. Denn das wäre eine wahre Katastrophe!

# Geschäftskontinuitäts-planung mit der Microsoft Data Platform

VON RICHARD DOUGLAS


### Kontaktinformationen

+1-704-895-6241
+1-855-775-7733 gebührenfrei
sales@sentryone.com

### Corporate Office

8936 NorthPointe Executive Park Dr
Suite 200
Huntersville, NC 28078, Vereinigte Staaten


SentryOne