

Was tun, wenn die IT nicht mehr läuft?

Fällt die IT aus, erbringt das Unternehmen keine Leistung mehr. Aus diesen Überlegungen entstanden das Business Continuity Planning und das Disaster Recovery. Doch wo liegen die Unterschiede, und was hat das ganze mit Hosting zu tun? *Kaspar Geiser*



Kaspar Geiser

ist Managing Director und Mitinhaber der Aspectra AG.

Mit dem «Business Continuity Planning» wird eine Vorgehensweise festgelegt, wie ein Geschäftsmodell in Krisen und unter erschwerten Bedingungen fortgesetzt wird. Also auf den ersten Blick eine reine Management-Problematik. Als «Disaster Recovery», also die Wiederherstellung von Daten und Systemen beispielsweise nach einem Ausfall des Rechenzentrums, bezeichnet man technische Wege, wie dieses Problem gelöst wird. Das Hosting beziehungsweise das Outsourcing ist wiederum eine mögliche Form, wie die eigene IT betrieben werden kann. In anderen Organisationsformen verfügt die jeweilige Geschäftseinheit über eigene IT-Ressourcen. Ein Hosting kann sowohl innerhalb des eigenen Unternehmens wie auch extern erfolgen.

Wer macht was?

Doch je einfacher die Erläuterung zu den einzelnen Begriffen ist, umso schwieriger wird es, Verantwortliche, Auftraggeber und Ausführende für die einzelnen Aufgaben innerhalb eines Unternehmens zu benennen. Typischerweise werden alle Aufgaben letztlich der IT selbst übertragen, die wiederum «nur» in den eigenen vier Wänden die möglichen Szenarien durchdenkt und entsprechende Massnahmen einleitet. Ein weiteres Risiko bei der Delegierung dieser Aufgaben an die IT besteht darin, dass die diese nur ein Unterstützungsprozess des Unternehmens ist. Oft geht die Möglichkeit eines Disasters in einer anderen Business Unit oder bei Lieferanten wie zum Beispiel von Börsenkursen, vergessen. Aus diesem Grund wäre das Business Continuity Planning Sache des Managements. Die Realität sieht jedoch anders aus,

das heisst, die Business-Owner und die IT sind die typischen Akteure.

Das Business

Die Business-Owner, die Prozess-Owner und das Operating sind als Erste gefordert, sich zu überlegen, welche Prozesse geschäftsnötig sind und auch nach einem IT-Zwischenfall sehr rasch wieder funktionieren beziehungsweise weitergeführt werden

müssen. Dabei gilt es, für jeden dieser Prozesse das «Disaster» zu bezeichnen. Typischerweise sind dies Aussagen wie: «Ohne Lohnbuchhaltung können wir vier Wochen leben», oder «Ohne Wertschriftenhandel können wir nicht leben».

«Der Betrieb, also möglicherweise das Hosting, Disaster Recovery sowie Business Continuity liegen sehr nahe beieinander und sind voneinander abhängig.»

Die Technik

Die Technik wiederum muss die Aussagen des Business verstehen und soll diese auch hinterfragen. Dabei sollten die bestehende Systemarchitektur, also die Aufteilung der Anwendungen, die Lagerung der Daten etc. nicht massgebend sein. Die Beurteilung sollte möglichst objektiv und auf das Geschäftsmodell des jeweiligen Unternehmens ausgerichtet sein. Am Ende müssen sich Business und IT auf eine Kategorisierung der Prozesse beispielsweise nach erster, zweiter und dritter Priorität geeinigt haben. Diesen Prioritäten wiederum ist jeweils eine maximale Ausfalldauer zuzuordnen. Eine weitere Aufgabe der Technik besteht darin, sämtliche involvierten Komponenten wie IT-Mitarbeiter, Server, Netzwerkanbindungen, PCs, Drucker sowie Anwendungen wie E-Mail, CRM, Handelsplattformen etc. zu kategorisieren sowie deren Verfügbarkeit und mögliche Stellvertreter respektive Ersatzsysteme festzulegen.



Was tun, wenn der Motor kaputt ist?

Bildquelle: AK-Photo Hannover / Fotolia.com

Aus dieser Analyse ergibt sich nun ein Katalog von Anwendungen und damit verbundenen Ressourcen. In diesem Katalog sollte zudem ersichtlich sein, wie und wo im Disaster-Fall gearbeitet und wie auf die Daten und Anwendungen zugegriffen wird. Dies beinhaltet ebenfalls die im Disaster-Fall nötigen Kommunikationsmassnahmen, und mögliche am Arbeitsplatz vorzunehmende Einstellungen.

Mögliche Konsequenzen und Lösungsansätze

Betrachtet man die Problemstellung etwas aus der Ferne, stellt man fest, dass der Betrieb, also möglicherweise das Hosting, Disaster Recovery sowie Business Continuity sehr nahe beieinander und von einander abhängig sind. Daraus resultiert, dass bereits die Konzeption der «normalen» Bedie-

nungen auf einen möglichen Zwischenfall ausgelegt werden muss. Dies wiederum hat zur Folge, dass eine mögliche Lösung auch weitere Synergien für die IT wie dezentrales Backup, redundante VPN-Terminierungen, Auslagerung von Teilen der IT nach sich ziehen. Dies aufgrund der Tatsache, dass unter Umständen eine Business Continuity Location umfangreicher ausgestattet ist, als das eigene Rechenzentrum. Zudem kann auf IT-Mitarbeiter Dritter zugegriffen werden, falls das Disaster zum Beispiel eine lokale Epidemie ist.

Anforderung an IT-Dienstleister

Was bedeutet dies nun für IT-Dienstleister? Können diese einfach Business Continuity, Disaster Recovery oder Hosting als einzelne Disziplin betrachten und als eigenständige Leistung anbieten? Wohl kaum. Was im Unternehmen, also die Verschmelzung der einzelnen Anforderungen, gemacht wird, muss auch auf der Seite der Anbieter geschehen. Nicht selten wird so ein Hostler zur Business Continuity Location. Dies wiederum bedeutet, dass neben Rechenzentrumsleistung auch Arbeitsplätze, Telefonleitungen sowie die PC-Infrastruktur angeboten werden müssen. ■