Disaster Recovery: Die nötigen Schritte

Viele Unternehmen würden einen unvorhergesehenen Ausfall ihrer entscheidenden Systeme von mehr als vier Tagen nicht überleben. Das sollte einem schon zu denken geben.

Der Computer-Alltag beweist es immer wieder: Technik ist nicht unfehlbar. Sei es ein schlichter Lesefehler von der Festplatte oder eine Katastrophe, die Ihre Firma in Schutt und Asche legt - ein Zusammenbruch der Computersysteme kann Ihr gesamtes Unternehmen ruinieren. Ein vernünftiges Recovery-Konzept auf der anderen Seite könnte es am Leben erhalten. Hier sind die grundlegenden Schritte dafür, wie man ein solches Konzept erstellt und gewährleistet, dass es im Ernstfall auch funktioniert.

Prioritäten setzen

Sie sollten Disaster Recovery zu einem integralen Bestandteil aller Unternehmensabläufe machen. Jemand aus dem obersten Management muss ausdrücklich für die Umsetzung des Konzepts verantwortlich sein, da man in schwierigen Zeiten allzu leicht Entscheidungen nur mit Blick auf die Kosten trifft, was gefährlich sein kann.

Legen Sie fest, welche Daten und Systeme zuerst wiederhergestellt werden müssen. Jede Abteilung nimmt natürlich an, dass dies die eigenen sind, aber diese Entscheidung muss getroffen werden. Am Ende landet das Ganze sonst immer in der IT-Abteilung, die nicht unbedingt den notwendigen Überblick über die Geschäftsabläufe besitzt. Und vergessen Sie nicht, sich auch außerhalb des Datenzentrums nach schützenswerten Daten umzusehen. Was, wenn die Mitarbeiter ihre PCs in hohem Grade individuell eingerichtet haben und auf einmal wieder ganz von vorn beginnen müssen? Auch Aufzeichnungen in Papierform sind immer wichtig.

Stellen Sie sicher, dass alle entscheidenden Systeme redundant vorhanden sind, sei es mithilfe eines RAID Speicher-Systems, Server-Spiegelung oder sogar einem vollständig duplizierten Datenzentrum. Es sollte keinen Single Point of Failure geben, weder bei der Stromversorgung noch bei der Telekommunikation oder dem Bürogebäude selbst, der eine längere Unterbrechung des Geschäftsablaufs verursachen könnte. Die meisten Unternehmen würden einen unvorhergesehenen Ausfall ihrer entscheidenden Systeme von mehr als vier Tagen nicht überleben. Und selbst wesentlich kürzere Ausfallzeiten können überproportional viel Schaden anrichten.

Die Bedeutung von Backups

Neben der Redundanz sind Backups der wichtigste Bestandteil von Disaster Recovery. Wenn man weiß, von welchen Daten man Backups erstellen muss, kann man festlegen, wann und wie diese Backups durchgeführt werden. Eine übliche Vorgehensweise ist ein vollständiges Backup am Anfang jeder Woche mit täglichen (oder häufigeren) Backups der aktuellen Änderungen. Das können kumulativ inkrementelle Backups sein, wo alle Änderungen im Vergleich zum Ausgangsstatus jedes Mal komplett gespeichert werden, oder differenziell inkrementelle Backups, wo die Änderungen seit dem letztem Backup gespeichert werden. Differenzielle Backups erfordern weniger Zeit, erzeugen aber mehr einzelne Backups, die in der richtigen Reihenfolge wieder hergestellt werden müssen. Bei kumulativen Backups sind nur zwei solche Vorgänge erforderlich.

Offsite-Backups sind wichtig, aber schwierig zu verwalten, besonders für kleinere Firmen. In Unternehmen, in denen es sowieso Mitarbeiter an entfernten Orten gibt, lässt sich eventuell die Aufbewahrung von entfernten Kopien in die Standardprozesse integrieren. Aber man sollte sicherstellen, dass nicht nur eine einzige Person Zugriff auf die Offsite-Backups hat. Üblich ist es, die wöchentlichen Backups zu duplizieren und außerdem monatliche Backups aufzubewahren.

Diebstahlprävention

Wenn man Backups von sensiblen Daten macht, sind diese dann angemessen gegen Übergriffe geschützt, falls jemand Zugang zu den Backups erhält oder diese stiehlt? Und umgekehrt: Wenn Sie ein sicheres Backup haben, das durch Verschlüsselung oder strenge Zugriffskontrollen geschützt ist, ist es dann möglich, an die Informationen zu gelangen, auch wenn die zuständigen Mitarbeiter nicht da sind? Sie sollten regelmäßig Tests durchführen, um Fehlern des Konzepts auf die Schliche zu kommen. Tests, die keine Fehler produzieren, sind nicht streng genug. Man testet nicht um sicherzustellen, dass alles funktioniert, sondern um herauszufinden, wann es nicht funktioniert. Damit wird man auch feststellen, ob die Recovery-Prozeduren zwar funktionieren, aber zu langsam oder umständlich sind.

Halten Sie die Pläne immer auf dem laufenden Stand
Wenn Geschäftsprozesse sich ändern, sollten Sie Ihre Pläne neu bewerten. Eine Firmenübernahme, die Installation eines neuen Betriebssystems oder eine Umstrukturierung können Auslöser hierfür sein. Auch wenn Sie ein grundlegendes System wechseln und die Daten dorthin migrieren, sollten Sie sicherstellen, dass Sie das alte System so lange wie erforderlich wiederherstellen können. Es nutzt nicht viel, wenn Sie alte Daten haben, die Sie dringend benötigen, aber kein System mehr, das diese Daten lesen kann.

Sie sollten außerdem sicherstellen, dass auch Ihre wichtigen Zulieferer über genaue Pläne für Disaster Recovery verfügen. Es macht keinen Sinn, seine Daten einer Firma zu überlassen, die im Notfall selbst damit zu kämpfen hat, wieder auf die Beine zu kommen. Und man sollte auch elementare Informationen wie Adresslisten der Mitarbeiter samt Handynummer oder Ansprechpartner bei Lieferanten immer auf dem laufenden Stand halten. Außerdem sollte jeder Mitarbeiter über seine Rolle im Recovery-Konzept ausreichend informiert und geschult sein.