

Pressemitteilung

642drs, 3. September 2008

Virtualisierung erfordert neuen Ansatz beim Disaster Recovery

Studie von Symantec: Jeder dritte Disaster Recovery-Test nicht erfolgreich, mehr Automatisierung nötig

München, 3. September 2008 - Virtualisierung stellt neue Anforderungen an die Disaster Recovery (DR)-Strategie von Unternehmen – weshalb viele IT-Verantwortliche aktuell ihre Notfall-Pläne überarbeiten. Da immer mehr Applikationen und Daten in einer virtuellen Umgebung verwaltet werden, suchen Unternehmen nach neuen Methoden und Technologien, die sich für die Datenwiederherstellung in virtuellen Umgebungen besonders eignen. Außerdem sind Notfälle nicht so selten wie gemeinhin vermutet: Rund ein Drittel der befragten Unternehmen gab zudem an, dass vorliegende Notfall-Pläne im vergangenen Jahr wenigstens teilweise zum Einsatz kamen. Das sind die Ergebnisse des jährlichen Disaster Recovery Reports von Symantec, für den im Juni und Juli 2008 mehr als 1.000 IT-Manager in großen Unternehmen aus mehr als 15 Ländern befragt wurden.

Auch wenn Disaster Recovery-Tests sich im letzten Jahr häufiger als erfolgreich erwiesen haben als in der Vergangenheit, sind einige grundlegende Probleme noch nicht gelöst: ein Drittel der Befragten gab an, dass DR-Tests sich negativ auf ihre Kundenbeziehungen auswirken würden, 20 Prozent befürchten eine generelle Beeinträchtigung des Geschäftsbetriebs durch solche Tests. Durch den Zuwachs bei der Zahl der geschäftskritischen Applikationen und der gespeicherten Daten in Unternehmen steigt gleichzeitig die Bedeutung von regelmäßig geprüften Disaster Recovery-Plänen erheblich.

Rasanten Wachstum geschäftskritischer Applikationen

Auch wenn 56 Prozent der Applikationen von den Befragten als geschäftskritisch eingeschätzt wurden – ein deutlicher Anstieg gegenüber 36 Prozent aus dem Jahr 2007 – werden nur 54 Prozent aller Applikationen in die DR-Pläne der befragten Unternehmen mit einbezogen. Durch den schnellen Anstieg der als geschäftskritisch eingeschätzten Applikationen entwickelt sich die Applikationsverfügbarkeit gerade für Unternehmen mit kleinerem IT-Budget zu einer Herausforderung. Daher sind immer mehr Unternehmen auf der Suche nach kosteneffizienten Methoden für den Schutz ihrer Applikationen. Hohe Priorität haben hier die

Reduzierung doppelter Server, die Erhöhung der Server-Kapazität, oder der Einsatz von Virtualisierung.

Kritische IT-Vorfälle keine Seltenheit

Disaster Recovery-Pläne gehen normalerweise von ernsthaften Vorfällen aus, die den Betrieb der IT gefährden. Solche Vorfälle sind in der Unternehmenspraxis nach den Ergebnissen der Studie gar nicht selten: Ein Drittel der Befragten gab an, ihre DR-Pläne im letzten Jahr durchgeführt zu haben. Die Gründe für den Einsatz sind vielfältig: Ausfall bei Hard- und Software (36 Prozent), externe Sicherheitsbedrohungen (28 Prozent), Stromausfall oder Störungen bei der Stromversorgung (26 Prozent), Naturkatastrophen (23 Prozent), IT-Problemmanagement (23 Prozent), Datenverlust (22 Prozent) oder versehentlich oder absichtlich schädigendes Verhalten durch Mitarbeiter (21 Prozent). Da solche Ereignisse regelmäßig auftreten, müssen IT-Abteilungen davon ausgehen, dass die Qualität ihrer DR-Pläne irgendwann in der Praxis überprüft wird.

Virtualisierung treibt Re-Evaluierung und Automatisierung

Der zunehmende Einsatz von Virtualisierung bringt Unternehmen mehr und mehr dazu, ihre DR-Pläne neu zu evaluieren – 55 Prozent gaben diese Technologie als Grund für diesen Schritt an. In einigen Fällen wird Virtualisierung auch gerade für einen leistungsfähigeren Schutz im Ernstfall implementiert, doch stoßen Unternehmen hier immer wieder auf Schwierigkeiten: Tools und Prozesse aus physischen Umgebungen lassen sich in virtuellen Umgebungen nicht einsetzen, und nicht alle Funktionen sind im Virtuellen verfügbar. So gaben beispielsweise 35 Prozent der Befragten an, dass ihre virtuellen Server momentan nicht in die DR-Pläne im Unternehmen integriert sind. Gleichzeitig sind nur bei 37 Prozent der befragten Unternehmen sämtliche virtuellen Systeme in die Backup-Strategie integriert. Bei mehr als der Hälfte der Unternehmen (54 Prozent) sind es vor allem Ressourcenprobleme, die sie von der vollständigen Integration virtueller Systeme in die Backup-Prozesse abhalten. Abhilfe schaffen könnten hier Vereinfachung und Automatisierung – nicht zuletzt deshalb, weil 35 Prozent der Befragten die große Anzahl verschiedener Tools als Hindernis beim Schutz geschäftskritischer Daten und Applikationen bezeichnen. Dadurch treten Schwierigkeiten wie höhere Schulungskosten, Ineffizienz bei den Operationen und höhere Software-Kosten auf. Jedes dritte Unternehmen bezeichnet außerdem den Mangel an Automatisierung bei der Wiederherstellung und nicht ausreichende Backup-Tools als ein Hindernis bei einer umfassenden Datensicherheitsstrategie.

Jeder dritte Disaster Recovery-Test problematisch

Die Studie zeigt deutlich, dass Unternehmen einen Disaster Recovery-Plan heute als essentiell ansehen. Genauso wichtig ist allerdings die Gewissheit, dass die Pläne im Ernstfall auch erfolgreich sind. 2007 gaben 88 Prozent der Befragten IT-Profis an, dass sie Wahrscheinlichkeits- und Wirkungs-Assessments für wenigstens eine Bedrohung ausgeführt haben. 2008 ist diese Zahl weiter auf 98 Prozent gestiegen. Dennoch erfüllt jeder dritte Test

(30 Prozent) nicht die Vorgaben des Recovery Time Objectives (RTO). Die Hauptgründe für Fehler in den Tests: menschliches Versagen (35 Prozent), technische Fehler (29 Prozent), nicht ausreichende IT-Infrastrukturen (25 Prozent), veraltete Pläne (24 Prozent), und nicht angemessene Prozesse (23 Prozent). Da von Menschen verursachte Fehler das Hauptproblem sind, sollten Unternehmen nach Automatisierung streben, da so die Wiederherstellung beschleunigt und gleichzeitig die Fehlerzahl verringert wird..

Stärkere Automatisierung von DR-Test notwendig – viele testen gar nicht

47 Prozent der befragten Unternehmen testen ihre DR-Pläne nur einmal im Jahr oder seltener, meist um die Auswirkungen auf das Geschäft gering zu halten, oder aufgrund nicht ausreichender Ressourcen in der IT-Abteilung. Die Gründe im Einzelnen: Personalknappheit (39 Prozent), Unterbrechungen für die Mitarbeiter (39 Prozent), Budgetknappheit (37 Prozent), Störungen für die Kunden (32 Prozent). 21 Prozent der Befragten gehen davon aus, dass sich DR-Tests auf Verkäufe und Umsatz auswirken. 12 Prozent der Unternehmen in Europa gaben auch in der aktuellen Umfrage an, ihre DR-Pläne überhaupt nicht zu testen, obwohl die Folgen signifikant sind:

Nur 31 Prozent der befragten Unternehmen gingen davon aus, dass sie ihre IT nach einem schwerwiegenden Ausfall innerhalb von 24 Stunden wieder voll in Betrieb nehmen könnten; nur drei Prozent schätzen die Wiederherstellungszeit auf weniger als 12 Stunden. Beinahe die Hälfte (47 Prozent) der befragten Unternehmen schätzt hingegen, dass sie eine komplette Woche benötigen würden, um wieder einen vollständig normalen Betrieb erreichen zu können.

„Das Bewußtsein für die Notwendigkeit von geprüften Disaster Recovery-Plänen ist seit dem letzten Jahr gewachsen“, sagt Andreas Zeitler, Vice President und Regional Manager Zentraleuropa bei Symantec. „Dennoch besteht ein Nachholbedarf bei Praxistests, einmal im Jahr oder seltener reicht in vielen Fällen nicht aus. Unternehmen befürchten Störungen in ihrem Geschäftsbetrieb, da sie zu wenige automatisierte Test-Tools einsetzen, um den Einfluss der Assessments auf den Geschäftsbetrieb zu reduzieren. Disaster Recovery-Lösungen, die außerdem auf Virtualisierung zurückgreifen und sich nahtlos in virtuelle Umgebungen einfügen, können eine Lösung dafür sein. Unsere Studie zeigt, dass viele Unternehmen das ähnlich sehen und ihre Pläne dementsprechend neu evaluieren.“

Über den 2008 Symantec Disaster Recovery Research Report

Der Disaster Recovery Research Report, der 2008 zum vierten Mal veröffentlicht wurde, ist eine weltweite Studie, die jährlich von Symantec in Auftrag gegeben wird, um Trends bei Planung und Tests von Disaster Recovery zu identifizieren. Die Untersuchung wurde vom unabhängigen Marktforschungsunternehmen Applied Research West zwischen Juni und Juli 2008 ausgeführt. Mehr als 1.000 IT-Manager in großen Unternehmen aus mehr als 15 Ländern wurden befragt.

Textumfang: 8.083 Zeichen

Über Symantec

Symantec ist ein weltweit führender Anbieter von Sicherheits-, Storage- und Systemmanagement-Software, mit der Unternehmen und Privatpersonen ihre Informationen sichern und verwalten können. Symantec hat seinen Hauptsitz in Cupertino, Kalifornien und betreibt Niederlassungen in mehr als 40 Ländern. Mehr Informationen unter www.symantec.de.

Hinweis für Redakteure:

Wenn Sie mehr über Symantec und seine Produkte erfahren möchten, dann besuchen Sie unser Online-Presseszentrum unter www.symantec.com/presse
Dort liegt auch Bildmaterial von Personen und Produkten für Sie bereit.

Symantec und das Symantec Logo sind Warenzeichen oder eingetragene Warenzeichen der Symantec Corporation in den USA und ihrer Tochtergesellschaften in einigen anderen Ländern. Andere Firmen- und Produktnamen können Warenzeichen oder eingetragene Warenzeichen der jeweiligen Firmen sein und werden hiermit anerkannt.

*Symantec (Deutschland) GmbH, Humboldtstraße 6, 85609 Aschheim
Telefon: +49 (0) 89 / 94302 - 100
Telefax: +49 (0) 89 / 94302 - 950*

Ihr Ansprechpartner (NUR PRESSE!) für Rückfragen:

*Sabine Kuch
Corporate PR Manager*

*Symantec (Deutschland) GmbH
Telefon: +49 (0) 2102-745-3878
Mobil: +49 (0)151-149.39.123*

E-Mail: Sabine_Kuch@symantec.com

*Stefan Epler
PR Consultant*

*Trimedia Communications Deutschland GmbH
Telefon: +49 (0) 211-96485-55
Fax: +49 (0) 211-96485-45*

E-Mail: stefanepler@dus.trimedia.de