

**VERITAS Disaster-Recovery-Studie 2004**



**UNABHÄNGIGER MARKTFORSCHUNGSBERICHT  
IM AUFTRAG VON VERITAS SOFTWARE**

**SEPTEMBER 2004**

## INHALT

|   |          |
|---|----------|
| <b>WIE STABIL IST IHR DISASTER-RECOVERY-PLAN? .....</b>                               | <b>3</b> |
| Szenario Brandkatastrophe: [3.23].....  | 3        |
| Business Continuity oder nur technische Wiederherstellung? [3.3] .....                | 3        |
| Maßnahmen ergreifen – Vorhandene DR-Technologie und -Prozesse: [3.25].....            | 3        |
| Wie effektiv sind DR-Pläne bei der Unterstützung der Business Continuity: [3.24]..... | 3        |
| Potenzial für grundlegende Verbesserungen: [3.9].....                                 | 4        |
| Testen des Plans: [3.4 & 3.5].....  | 4        |
| Reale Totalausfälle: [3.21] .....   | 4        |
| <b>PROBLEMBEREICH ÄNDERUNGSMANAGEMENT (CHANGE CONTROL):.....</b>                      | <b>5</b> |
| Das IT-System: eine dynamische Umgebung? [3.27 & 3.29].....                           | 5        |
| Lösen Veränderungen auch Überprüfungen aus? [3.7 & 3.8].....                          | 5        |
| Bedeutung des Änderungsmanagements für DR [verschiedene Fragestellungen].....         | 5        |
| <b>DIE VORSTANDSETAGE – EIN FALSCHES SICHERHEITSGEFÜHL? .....</b>                     | <b>5</b> |
| Wer trifft beim Disaster Recovery tatsächlich die Entscheidungen? [3.12] .....        | 5        |
| Abnahme des DR-Plans: [3.13].....   | 6        |
| Zukünftige Investitionen in das Disaster Recovery: [3.14 & 3.15] .....                | 6        |
| Was wird vom DR-Plan abgedeckt: [3.10, 3.16 & 3.12] .....                             | 6        |
| Gehört Ihr Desktop zu den Prioritäten? [3.26].....                                    | 7        |
| Die Lieferanten – eine Achillesferse? [3.30].....                                     | 7        |

## ZUSAMMENFASSUNG

### WIE STABIL IST IHR DISASTER-RECOVERY-PLAN?

#### Szenario Brandkatastrophe: [3.23]

- Den befragten Unternehmen wurde ein Szenario präsentiert, bei dem das gesamte Hauptrechenzentrum durch einen Brand zerstört wird. Alarmierende 43% der Unternehmen, die über einen DR-Plan verfügen, gaben an, dass sie nicht wüssten, wie viel Zeit sie benötigen würden, um zumindest die wesentlichsten Betriebsprozesse nach einem solchen Vorfall wieder aufzunehmen.
- In der Asien/Pazifik-Region (56%) und den USA (55%) ist diese Unkenntnis stärker verbreitet als in der Region EMEA (Europa und Naher Osten) mit 38%.
- Einige Unternehmen gaben von sich aus Wiederherstellungszeiten an, und nur 3% nehmen an, dass sie den Geschäftsbetrieb nach einer kompletten Zerstörung ihres Hauptrechenzentrums normal weiterführen könnten.
- Darüber hinaus könnten nur 28% der Unternehmen die wesentlichsten Betriebsprozesse in weniger als 12 Stunden nach einer Brandkatastrophe wieder aufnehmen, darunter mehr EMEA-Unternehmen (31%) als US-Unternehmen (17%).
- Der durchschnittlich dafür benötigte Zeitraum liegt bei 3,23 Tagen. Dabei reicht die Spanne von sofort bis zu einem Monat.
- Die nächste Stufe ist das Recovery, also die Wiederherstellung. Hier wären nur 19% der Unternehmen in der Lage, den Betrieb in weniger als 12 Stunden nach einem derart großen Katastrophenfall wieder aufzunehmen. Aber auch hierbei geben 45% der Unternehmen an, dass sie nicht wüssten, wie schnell sie in der Lage wären, den Betrieb in einer solchen Situation nahezu vollständig wieder aufzunehmen.
- Zur vollständigen Wiederherstellung des normalen Betriebs nach einem Großbrand in weniger als 12 Stunden wären nur 12% fähig; 40% geben jedoch auch zu, dass sie nicht wüssten, wie lange sie dafür bräuchten.

#### Business Continuity oder nur technische Wiederherstellung? [3.3]

- Plausibler werden die obigen Ergebnisse wenn man weiß, dass nur 38% der Unternehmen über einen Disaster-Recovery-Plan (DR-Plan) verfügen, der in den Business-Continuity-Plan (BC-Plan) integriert ist. Dies ist häufiger in den EMEA-Unternehmen (42%) als in der Asien/Pazifik-Region (27%) der Fall.
- Weitere 15% verfügen über einen DR-Plan, haben aber keinen BC-Plan. Besonders häufig tritt dieser Fall – im Vergleich zu US- (6%) und EMEA- (11%) Unternehmen – bei Unternehmen aus der Asien/Pazifik-Region (33%) auf.
- 40% verfügen über einen DR-Plan und einen BC-Plan, wobei es sich allerdings um zwei voneinander getrennte Pläne handelt. Dies ist im Vergleich zur EMEA- (40%) und der Asien/Pazifik-Region (36%) vor allem in US-Unternehmen (50%) verbreitet.
- Besorgnis erregend ist hierbei auch, dass 7% der befragten IT-Mitarbeiter, in deren Verantwortungsbereich der DR-Plan ihres Unternehmens liegt, gar nicht wissen, dass zwischen DR- und BC-Plan eine Verbindung besteht oder ob überhaupt ein Plan existiert. Dies geben insbesondere US- (9%) und EMEA-Unternehmen (8%) und zu einem geringeren Prozentsatz (3%) Unternehmen aus dem Gebiet Asien/Pazifik an.

#### Maßnahmen ergreifen – Vorhandene DR-Technologie und -Prozesse: [3.25]

- Die Unternehmen nutzen bereits eine Vielzahl von Technologien und Prozessen für ihre DR-Pläne. 96% verfügen über mindestens eine Lösung, die sie dabei unterstützen soll, ihre Handlungsfähigkeit nach den unterschiedlichsten Ausfallformen so schnell wie möglich wiederherzustellen.
- 87% setzen einfache Backup-Systeme ein. An zweiter Stelle stehen feuersichere Backup-Speichereinrichtungen. Jedoch verfügen nur 54% der globalen Unternehmen über diese elementare Ausstattung für die Sicherung ihrer wertvollen Backup-Daten.
- Software zur Wiederherstellung nutzen 44%, und 39% setzen Verifikationssoftware ein. Nur 9% verwenden Replikationstechniken und lediglich 5% Clustering-Technologien.
- Verträge mit Anbietern, die beinhalten, dass nach einer Katastrophe Hardware und/oder Software ausgetauscht wird, liegen bei 11% vor. Weitere 11% nehmen für das Disaster Recovery die Dienste eines Outsourcing-Unternehmens in Anspruch, welches einen Ausweichstandort zur Verfügung stellt. Bei 11% werden die IT-Systeme durch ein DR-Outsourcing-Unternehmen innerhalb eines vorgegebenen Zeitrahmens wiederhergestellt. Solche Drittanbieterlösungen sind im Vergleich zum Asien/Pazifik-Gebiet eher in den EMEA- und US-Unternehmen verbreitet.

#### Wie effektiv sind DR-Pläne bei der Unterstützung der Business Continuity: [3.24]

- Doch obwohl diese verschiedenen Technologien und Prozesse bereits vorhanden sind, meinen 92% der Unternehmen weltweit, dass es trotzdem schwerwiegende Konsequenzen für sie hätte, wenn sie ihre DR-Pläne vollständig umsetzen müssten.
- Die fünf meistgenannten möglichen Auswirkungen nach einem Totalausfall mit den vorhandenen DR-Plänen sind:
  1. Abnahme der Mitarbeiterproduktivität (62%)
  2. Datenverlust (43%)

- 3. Geringere Erträge (40%)
- 4. Schädigung der Kundenbeziehungen (38%)
- 5. Geringere Umsätze (27%)
- 18% gehen sogar soweit zu sagen, dass bei einem möglichen Totalausfall und mit der darauf folgenden Umsetzung des DR-Plans das Fortbestehen ihres Unternehmens gefährdet sein würde. Dieser Meinung sind vor allem die Unternehmen der Asien/Pazifik-Region (29%) sowie die US-Unternehmen (27%). Geringer ist der Prozentsatz in der EMEA-Region (14%).

#### **Potenzial für grundlegende Verbesserungen: [3.9]**

- Viele DR-Pläne sind schon aufgrund ihres Speicherortes gefährdet, denn bei 67% der Unternehmen befindet sich der DR-Plan im Hauptrechenzentrum. 53% bewahren ihren DR-Plan sogar AUSSCHLIESSLICH im Hauptrechenzentrum des Unternehmens auf.
- Nur 26% bewahren ihren DR-Plan in einem anderen Unternehmensgebäude auf, welches sich in einiger Entfernung zum Hauptrechenzentrum befindet, wobei die Distanz meistens nur 10 km beträgt. So wird vor allem in den EMEA-Unternehmen (28%) und weniger im Asien/Pazifik-Gebiet (16%) verfahren.
- 18% lagern den DR-Plan außerhalb ihres Standorts an einem sicheren Ort bei einem Drittanbieter, jedoch beträgt die Entfernung zum Hauptrechenzentrum hier wiederum häufig nur 35 km.
- Allerdings bewahren 81% der Unternehmen ihren DR-Plan nur an einem dieser Orte auf.
- Es hat sich jedoch seit 2003 eine leichte Verbesserung gezeigt: 26% der 2004 befragten Unternehmen gaben an, dass der DR-Plan sich in einem anderen Gebäude des Unternehmens und vom Hauptrechenzentrum entfernt befindet. Im Jahr 2003 sagten dies nur 20%.

#### **Testen des Plans: [3.4 & 3.5]**

- 91% der Befragten testen ihre DR-Pläne, wobei aber ein Großteil (34%) solche Tests nur einmal pro Jahr durchführt. Nur 17% testen die Pläne monatlich.
- Dass die Tests so selten durchgeführt werden ist eventuell dadurch begründet, dass 81% der Unternehmen weltweit der Meinung sind, dass ihnen bei der Testdurchführung Grenzen gesetzt sind.
- Die drei meistgenannten Hindernisse sind:
  1. Ressourcen, hinsichtlich der verfügbaren Zeit (49%)
  2. Ressourcen, hinsichtlich des Budgets (32%)
  3. Beeinträchtigung der Mitarbeiter (29%)
- Die Beeinträchtigung der Kunden geben 19% als Hindernis für die Testdurchführung an. 13% meinen, dass die Beeinträchtigung von Vertrieb und Einnahmen hinderlich ist.
- 13% sind der Meinung, dass andere IT-Projekte wichtiger sind als das Testen des DR-Plans.
- Es geben jedoch nur 7% an, dass DR-Tests von der Unternehmensleitung als nicht dringlich angesehen werden.
- Im Vergleich zu den US- und EMEA-Unternehmen geben Asien/Pazifik-Unternehmen mehr Gründe an, die sie daran hindern, DR-Pläne zu testen. Trotzdem schaffen es diese Unternehmen häufiger, diese Tests durchzuführen als US- und EMEA-Unternehmen.

#### **Reale Totalausfälle: [3.21]**

- Insgesamt mussten 51% der Unternehmen ihre DR-Pläne tatsächlich in die Praxis umsetzen – entweder komplett oder nur teilweise.
- Dagegen mussten 46% ihren DR-Plan noch nie anwenden. Dies trifft im Vergleich zur Asien/Pazifik-Region (36%) und den USA (33%) häufiger auf EMEA-Unternehmen (50%) zu.
- Die häufigste Ursache für die Umsetzung des DR-Plans waren Ausfälle von Computersystemen, d.h. Ausfälle von Hardware und Software (37%).
- Gefolgt wird dies von 26%, die ihren Plan aufgrund von externen Computer-bezogenen Bedrohungen wie Viren- oder Hackerangriffe eingesetzt haben. Solche Bedrohungen scheinen bei Asien/Pazifik- (47%) und US-Unternehmen (35%) häufiger aufzutreten als in der EMEA-Region (20%).
- 14% der Unternehmen weltweit haben ihren DR-Plan aufgrund von Naturkatastrophen, wie Bränden oder einer Flut, eingesetzt. Ebenso viele Unternehmen (13%) mussten ihren DR-Plan infolge interner Computer-Gefährdungen, wie unbeabsichtigtem oder vorsätzlichem Fehlverhalten ihrer Mitarbeiter, in die Praxis umsetzen.
- Beträchtlich ist der Anteil der Unternehmen, welche ihre Pläne bei Katastrophen ausführen mussten, die von Menschen verursacht wurden, wie etwa Krieg oder Terrorismus (10%). Der Anteil liegt dabei in der Region Asien/Pazifik (21%) sowie in den USA (15%) höher als in den EMEA-Ländern (7%).
- Im Vergleich zum letzten Jahr ist der Anteil der implementierten DR-Pläne gestiegen: Im Jahr 2003 gaben noch 65% der Unternehmen an, dass sie noch nie einen DR-Plan anwenden mussten. In diesem Jahr waren es nur noch 46% ohne Erfahrung.

- Während des letzten Jahres sind folgende Katastrophenfälle häufiger eingetreten: Naturkatastrophen wie Feuer oder Flut (vorher 33%, jetzt 51%); durch Menschen verursachte Gefahrensituationen wie Krieg und Terrorismus (vorher 2%, jetzt 10%); externe Computer-Gefährdungen wie Viren und Hacker (vorher 12%, jetzt 26%); interne Computer-Gefährdungen wie unabsichtliches oder vorsätzliches Mitarbeiter-Fehlverhalten (vorher 6%, jetzt 13%).

## PROBLEMBEREICH ÄNDERUNGSMANAGEMENT (CHANGE CONTROL):

### Das IT-System: eine dynamische Umgebung? [3.27 & 3.29]

- Insgesamt installieren 94% der Unternehmen Patches – und 59% verwenden sie mindestens einmal pro Monat oder öfter, darunter 17% täglich, 25% einmal pro Woche und 21% einmal monatlich.
- US- und EMEA-Unternehmen verwenden häufiger Patches als Unternehmen aus dem Raum Asien/Pazifik.
- Etwa ebenso hoch ist der Anteil der Unternehmen, die Hardware- und/oder Software-Änderungen vornehmen. Er liegt bei 98%. Dabei nehmen 31% die Veränderungen mindestens einmal pro Monat oder häufiger vor, davon 7% täglich, 9% einmal pro Woche und 15% einmal pro Monat.

### Lösen Veränderungen auch Überprüfungen aus? [3.7 & 3.8]

- Bei solch dynamischen IT-Umgebungen könnte man annehmen, dass der DR-Plan sehr häufig aktualisiert wird – und tatsächlich überarbeiten 93% der Unternehmen ihren DR-Plan mehr oder weniger regelmäßig.
- Jedoch überprüft ein Großteil der Unternehmen (34%) ihren DR-Plan und die DR-Strategie nur einmal pro Jahr, 11% sogar noch seltener und 4% überhaupt nicht.
- Nur 14% überarbeiten ihre DR-Strategie sowie den Plan monatlich, wohingegen sehr viel mehr Unternehmen ebenso häufig oder noch öfter Patches (59%) verwenden und Hardware- und Software-Veränderungen (31%) vornehmen.
- Zudem testen nur 17% ihren DR-Plan monatlich.
- Technologische Veränderungen gaben 35% als Anlass für eine Überarbeitung ihrer DR-Strategie an. Bei nur 5% war der häufigere Einsatz von Patches der Auslöser. Letzteres war vor allem in den US-Unternehmen (18%) der Fall. Geringer ist hierbei der Anteil der Unternehmen aus den Regionen Asien/Pazifik (2%) sowie EMEA (4%).
- Die Unternehmen überarbeiten ihre DR-Pläne jedoch insgesamt häufiger als in den Jahren zuvor: In diesem Jahr gaben 14% an, dass sie ihren DR-Plan monatlich überarbeiten, während es im Jahr 2002 nur 2% und im Jahr 2003 nur 7% waren.
- Darüber hinaus gaben mehr der 2004 befragten Unternehmen (35%) an, dass Technologie-Veränderungen sie zu einer Überarbeitung der DR-Strategie veranlasst hätten. Im Jahr 2003 waren dies nur 15%.

### Bedeutung des Änderungsmanagements für DR [verschiedene Fragestellungen]

- Das Änderungsmanagement scheint ein zunehmend wichtigeres Thema zu werden:
  - 40% der Unternehmen geben an, dass Technologie-Veränderungen der Auslöser für die Erstellung eines DR-Plans waren. Diese Aussage trafen im Vergleich mehr Unternehmen aus den USA (49%) und dem Raum Asien/Pazifik (51%) als aus der EMEA-Region (36%).
  - Bei 8% wurde die Erstellung eines DR-Plans durch die häufigere Verwendung von Patches motiviert. Dabei liegen die US-Unternehmen (22%) weit vor den Unternehmen der EMEA-Region (7%) sowie der Asien/Pazifik-Region (5%).
  - 49% sind der Meinung, dass sie sich ohne ihre Pläne möglichen Problemen bei der Änderungskontrolle, z.B. bei Patches, zu sehr ausgesetzt fühlen würden. Dies sagen insbesondere EMEA-Unternehmen (52%) und zu einem geringeren Anteil Unternehmen aus der Region Asien/Pazifik (40%).
  - 7% mussten ihre Pläne aufgrund von Problemen beim Änderungsmanagement, z.B. mit Patches, ausführen. Dies trifft vermehrt auf Unternehmen aus der Region Asien/Pazifik (10%) und aus den USA zu (22%), weniger auf die Unternehmen der EMEA-Region (5%).
- Obwohl 66% der Unternehmen Probleme beim Änderungsmanagement, z.B. mit Patches, befürchten, haben sie die möglichen Kosten dieser Gefahren nicht kalkuliert.

## DIE VORSTANDSETAGE – EIN FALSCHES SICHERHEITSGEFÜHL?

### Wer trifft beim Disaster Recovery tatsächlich die Entscheidungen? [3.12]

- Die Entscheidungen bei der Definition einer DR-Strategie werden meistens vom IT-Manager der Abteilung (52%) getroffen.
- Nur bei 21% liegt die Verantwortung für den DR-Entscheidungsprozess beim Vorstand. In noch weniger Unternehmen übernehmen die Geschäftsführer (8%), andere Führungskräfte aus dem nicht IT-bezogenen Bereich (3%) oder Manager aus IT-fremden Bereichen auf einer niedrigeren Ebene (2%) die Entscheidungsfindung.
- Jedoch sind die Vorstände seit 2003 häufiger involviert (2002 zu 12%, 2003 zu 11% und jetzt zu 21%). Im Vergleich zu den US-Vorständen (11%) ist die Beteiligung in den Unternehmen der Asien/Pazifik-Region (25%) und der EMEA-Region (21%) höher.
- Zudem scheint sich die Einbindung des leitenden Sicherheitsbeauftragten in diesem Bereich ebenfalls erhöht zu haben, und zwar von 2% im Jahr 2002 auf 4% im Jahr 2003 und auf 9% in diesem Jahr.

- Jedoch ist der Anteil der Unternehmen, bei denen nur die IT-Mitarbeiter in den Entscheidungsprozess zur Festlegung einer DR-Strategie für ihr Unternehmen involviert sind, mit 71% noch sehr hoch.

#### **Abnahme des DR-Plans: [3.13]**

- Obwohl sich die Vorstände und Geschäftsführer offensichtlich weitestgehend aus diesem Thema heraushalten, haben 75% der Unternehmen angegeben, dass der Vorstand ihren DR-Plan bereits abgenommen hat.
- Nur 8% gaben an, dass der Vorstand den DR-Plan noch abzeichnen muss. Dies ist insbesondere bei Unternehmen aus der Asien/Pazifik-Region (15%) und den USA der Fall, jedoch eher weniger bei den EMEA-Unternehmen (5%).
- Besorgnis erregend ist jedoch, dass 17% der IT-Manager, die für die DR-Pläne zuständig sind, nicht wissen, ob der Vorstand den DR-Plan für das Unternehmens genehmigt oder nicht.
- Problematisch ist in Anbetracht der zunehmenden Bedeutung von Problemen im Bereich Änderungsmanagement auch, dass 35% angeben, der DR-Plan werde bei seiner Erstellung nur durch den Vorstand abgezeichnet. Vorgegangen wird so vor allem in der Asien/Pazifik-Region (37%) sowie in EMEA-Unternehmen (36%). Der Anteil der US-Unternehmen ist mit 22% niedriger.
- Nur 11% der Unternehmen weltweit geben an, dass der Vorstand den DR-Plan immer abzeichnet, wenn er überarbeitet wird und Veränderungen vorgenommen werden. So wird vor allem in EMEA-Unternehmen (14%) verfahren, während Asien/Pazifik- und US-Unternehmen (beide 4%) hierbei weit zurückliegen.

#### **Zukünftige Investitionen in das Disaster Recovery: [3.14 & 3.15]**

- Während 39% der Unternehmensvorstände weitere Investitionen im Bereich Disaster Recovery für notwendig halten (insbesondere in der EMEA- und der Asien/Pazifik-Region), ist der Anteil derer, die dies nicht für erforderlich halten, genauso groß (39%).
- Außerdem sind 22% der IT-Manager, die für den DR-Plan zuständig sind, sich nicht einmal sicher, ob der Vorstand überhaupt einen Bedarf dafür sieht, dass mehr darin investiert werden muss. Diese Aussage wurde häufiger in den EMEA-Unternehmen (24%) als in den Unternehmen der Asien/Pazifik-Region (15%) getroffen.
- Unter den Unternehmen, die meinen, dass weiter in DR investiert werden sollte, geben 33%, an, dass die Investitionen in wirtschaftlich schweren Zeiten zwar reduziert, aber dennoch fortgeführt werden würden.
- 16% geben an, dass die fortlaufenden Investitionen in schwierigen Zeiten und alle dahingehenden Aktivitäten ausgesetzt werden würden. Im Vergleich zu den US-Unternehmen (4%) ist diese Vorgehensweise speziell in Unternehmen aus der Asien/Pazifik- (22%) als auch aus der EMEA-Region (15%) verbreitet.
- Nur 22% geben an, dass die fortlaufenden Investitionen weitergeführt und gesichert werden würden.
- Sogar nur 6% der Unternehmen meinen, dass die Investitionen in wirtschaftlich schwierigen Zeiten erhöht werden könnten, wenn dies erforderlich wäre. Das gilt besonders für US-Unternehmen (17%), während es bei Unternehmen aus den Regionen Asien/Pazifik und EMEA weniger häufig (jeweils 5%) angegeben wurde.
- Jedoch waren 24% der IT-Manager sich nicht sicher, was in wirtschaftlich schlechten Zeiten mit den IT-Investitionen passieren würde.

#### **Was wird vom DR-Plan abgedeckt: [3.10, 3.16 & 3.12]**

- Die meisten DR-Pläne umfassen Datenbankserver, Anwendungen, E-Mails, Außenstellen und Webserver, sofern ein Unternehmen darüber verfügt.
- Weniger häufig sind in den DR-Plan die Desktop-Umgebung, Laptops, Mobiltechnologie und Home-Office-PCs integriert.
- Nur 22% der Unternehmen beziehen die Mobiltechnologien mit ein und nur 36% die Laptop-Umgebung.
- US-Unternehmen integrieren insgesamt mehr dieser Technologien in ihre DR-Pläne als Unternehmen aus der Region Asien/Pazifik. Dabei handelt es sich insbesondere um E-Mails, Webserver, die Desktop-Umgebung, die Laptop-Umgebung, Mobiltechnologie wie Handhelds, Außenstellen und Home-Office-PCs.
- Im Vergleich zu 2003 decken wesentlich mehr Unternehmen nun den E-Mail-Bereich (vorher 39%, jetzt 78%), die Desktop-Umgebung (vorher 20%, jetzt 53%) sowie die Laptop-Umgebung (vorher 14%, jetzt 36%) mit ab.
- Die IT-Manager scheinen sich recht sicher zu sein, dass der Vorstand gut darüber informiert ist, welche Bereiche vom DR-Plan abgedeckt werden, denn 74% sind der Meinung, dass der Vorstand umfassend informiert ist. Diese Meinung herrscht im Vergleich zu der EMEA-Region (72%) und den US-Unternehmen (65%) vor allem in den Asien/Pazifik-Unternehmen (81%) vor.
- Nur 11% meinen, dass ihr Vorstand nicht ausreichend informiert ist, und die meisten derer, die dies angegeben haben, sind auch der Meinung, dass dies gar nicht nötig ist. Dies ist am häufigsten bei den US-Unternehmen (19%) der Fall und eher weniger in den Unternehmen der Asien/Pazifik- (7%) sowie der EMEA-Region (11%).
- Weitere 15% sind sich nicht sicher darüber, ob ihr Vorstand weiß, was der DR-Plan umfasst und was nicht.

### **Gehört Ihr Desktop zu den Prioritäten? [3.26]**

- Darüber, welche Anwendungen nach einem Totalausfall am schnellsten wieder einsatzbereit sein müssen, gibt es viele unterschiedliche Meinungen. Jedoch stehen drei ganz oben auf der Liste: Telekommunikations- (53%), Finanz- und Buchhaltungs- (53%) sowie Sicherheitssysteme (50%).
- Gefolgt werden diese Anwendungsbereiche von den E-Mails. Viele Unternehmen bewerten die Priorität der Wiederherstellung von E-Mails (34%) sogar höher als die der grundlegenden Büroanwendungen (29%).
- 29% messen dem Bereich Vertrieb und Marketing (29%) eine hohe Priorität bei, während dies bei den HR-Systemen nur 19% tun.
- Insgesamt stehen diese Anwendungen eher bei US-Unternehmen an vorderster Stelle als bei den Unternehmen aus der Region Asien/Pazifik.

### **Die Lieferanten – eine Achillesferse? [3.30]**

- Die Unternehmen achten zwar auf die Daten, die sich innerhalb ihres Unternehmens befinden, allerdings vernachlässigen die meisten die Unternehmensdaten, die durch die unterschiedlichen Lieferanten verwaltet werden.
- 28% der Unternehmen lassen sich die DR- und BC-Pläne ihrer Geschäftspartner gar nicht zeigen. Sie nehmen einfach an, dass solche Pläne existieren und adäquat gestaltet sind. Hierbei scheinen die EMEA-Unternehmen ein höheres Vertrauen in ihre Lieferanten zu haben (33%) als die Unternehmen aus dem Raum Asien/Pazifik (18%) und den USA (16%).
- Weitere 12% sind sich nicht sicher, ob ihr Unternehmen die BC- und DR-Pläne der Lieferanten für wichtig hält.
- Im Gegensatz dazu geben 32% an, dass sie sich immer, bevor sie mit dem Technologie-Lieferanten zusammenarbeiten, die BC- und DR-Pläne zeigen lassen. Verglichen mit den Unternehmen aus den Regionen Asien/Pazifik (36%) und EMEA (27%) ist dies in den USA (62%) üblicher.
- Noch sehr viel weniger Unternehmen sehen sich jedoch die DR- und BC-Pläne ihrer DR-Outsourcing-Partner an. Die Unternehmen aus der Region Asien/Pazifik (22%) und den USA scheinen dahingehend umsichtiger zu sein als die EMEA-Unternehmen (11%).