Business continuity

LAURENS VAN AGGELEN

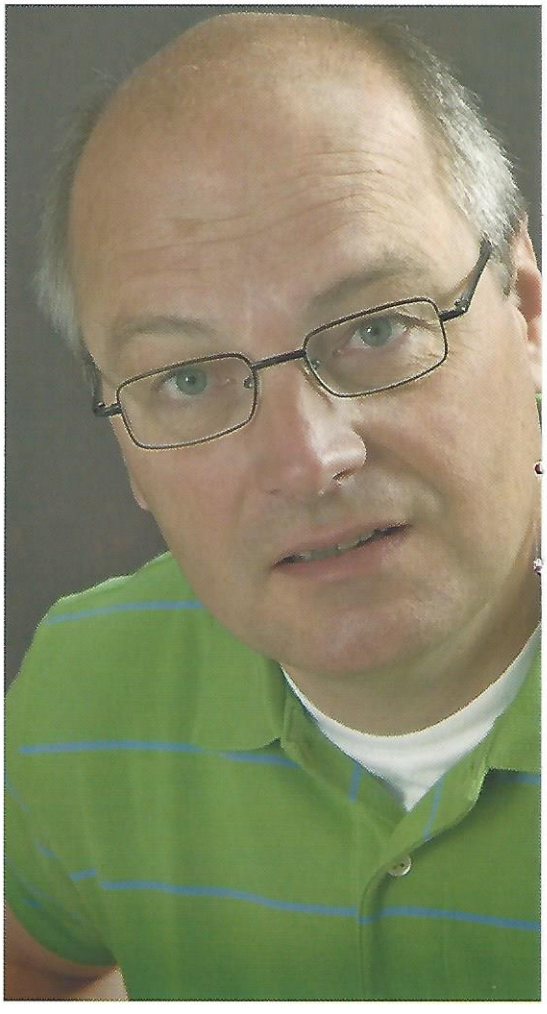
Aangezien bedrijven steeds afhankelijker zijn van IT-systemen, zou je mogen veronderstellen dat iedereen zich er wel voldoende bewust van is dat dit ons ook steeds kwetsbaarder maakt. Alle reden om voorzorgsmaatregelen te nemen zodat de gevolgen van een systeemuitval of calamiteiten de continuïteit van het bedrijf niet in gevaar kunnen brengen. Wie dit onderschat, opereert als bedrijf voortdurend op de rand van de afgrond.

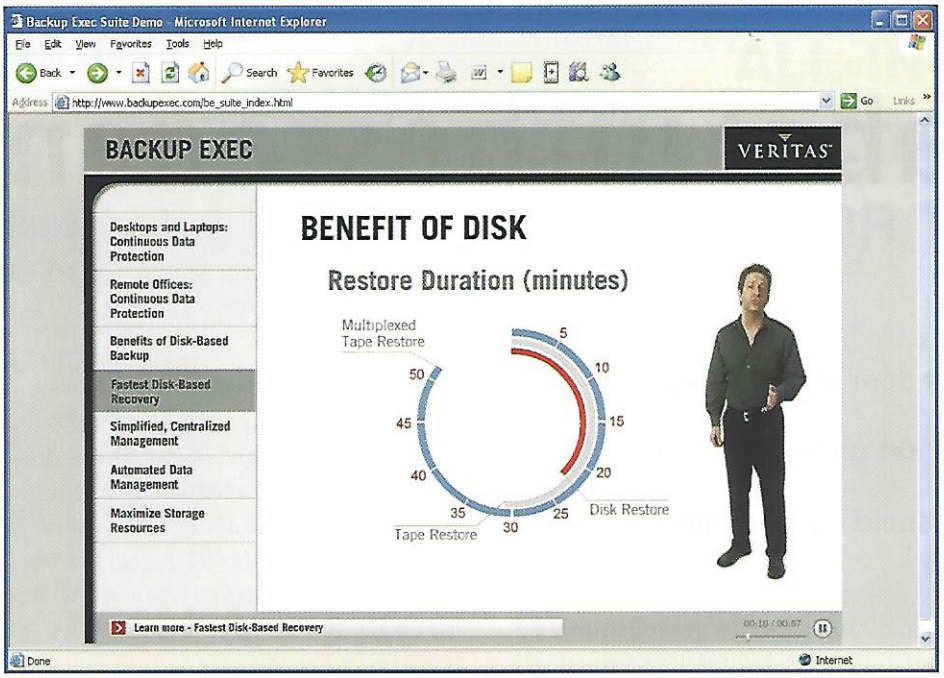
Goed bedoelde pogingen om calamiteitenplannen op te stellen zijn er absoluut maar de effectiviteit van dit soort plannen wordt meestal zwaar overschat. Het probleem is dat bij veel bedrijven ten onrecht wordt verondersteld dat men door de genomen maatregelen sneller operationeel is dan de praktijk uitwijst. Daarnaast blijkt dat werknemers bij calamiteiten onvoldoende op de hoogte zijn over hoe er gehandeld moet worden.
Door goede backup-procedures die garanderen dat er snel kan worden teruggevallen op een recente, betrouwbare kopie van waardevolle data, zou veel ellende voorkomen kunnen worden. Maar daarmee is de kous nog niet af. In de praktijk blijkt namelijk dat het bij het herstellen vaak gebeurt dat weggeschreven informatie niet of slechts gedeeltelijk teruggehaald kan worden. "Een belangrijke oorzaak is dat men nalaat om met enige regelmaar het 'restoren' van backups te testen", vertelt Erik van Veen, product marketing manager Benelux bij Symantec. Uit onderzoek van Veritas, sinds juni opgegaan in Symantec, bleek in 2004 echter nog dat 66 procent van de bedrijven hun disaster-recovery-plan niet test. Maar liefst 38 procent van de bedrijven (EMEA) zou bovendien geen enkel idee hebben hoe lang het hen bijvoorbeeld na een brand zou duren om weer volledig operationeel te zijn.
Dat het testen van gemaakte backups bittere noodzaak is, blijkt alleen al uit het feit dat na een disaster recovery 43 procent van de bedrijven toch nog last heeft van dataverlies. De gevolgen daarvan worden nog altijd onderschat. Volgens onderzoeksbureau Gartner gaat 40 procent van de bedrijven die te maken krijgt met dataverlies binnen vijf jaar op de fles.

Procedures

"Bij het maken van backups gaat het niet alleen om de techniek, maar ook op processen en mensen. Bij een goed disaster-recoveryplan is het testen van backups dan ook absoluut noodzakelijk gaat Van Veen verder. "Daarbij is het zaak om data eerst te classificeren, want hoe lang wil je bepaalde data bewaren en voldoe je daarmee wel aan de nieuwe verscherpte regelgeving. Deze is in Europa weliswaar minder streng dan in Amerika maar het feit dat deze 'principle based' is, geeft niet meer vrijheden." Het essentiële verschil tussen de regelgeving tussen Europa en Amerika wat Van Veen hiermee wil aanduiden, is dat de wetgeving in Amerika ten aanzien van

Herman Doorn van Bakbone: "Er wordt te vaak blindelings op de logfiles vertrouwd".





archivering dwingend is terwijl in Europa 'slechts' voor de rechter aangetoond moet kunnen worden dat men de uiterste inspanningen heeft verricht om alles volgens de regels te doen. Deze vrijheid legt dus een grotere claim op het verantwoordelijkheidsgevoel van bedrijven.
Bij het opstellen van backup-procedures is het verder van belang te kijken naar het zogenaamde 'Recovery Point Objective (RPO) en de Recovery Time Objective (RTO). Bij de RPO gaat het om het bepalen van het punt waarop data teruggezet moet kunnen worden. Daarbij speelt de vraag hoeveel data je als bedrijf zeker wilt stellen en dus hoe actueel data moet zijn. Verder moet er bij het terugzetten van data (RTO) bekend zijn hoeveel tijd je je als bedrijf kunt permitteren om alles terug te zetten. Het lijkt erop dat men daar in het bedrijfsleven een beter beeld over heeft. Maar liefst 57 procent van de bedrijven uit het onderzoek van Veritas gaf aan het onacceptabel te vinden wanneer zij vier uur of langer geen e-mail zouden kunnen gebruiken. Hoe kleiner het verschil tussen een calamiteit en dat wat binnen een RPO en RTO is vastgelegd, hoe duurder de oplossing. "Het bepalen van de juiste objectives voor een organisatie is volgens Van Veen specialistenwerk. Binnen bedrijven in het MKB is er nauwelijks voldoende expertise in huis om die inschatting goed te kunnen maken."

Testen

Dat het ondanks de gebruikersvriendelijkheid en de kwaliteiten van de backupsoftware toch nog vaak misgaat, wijt ook Herman Doorn, Senior Channel Manager Benelux bij BakBone, aan het onvoldoende testen van gemaakte backups. Bakbone is leverancier van databeschermingsoplossingen en ontwikkelt en distribueert software voor backup, restore en disaster recovery voor omgevingen met netwerkstorage en open systemen.
"Recovery mag dan geen dagelijks activiteit zijn, er wordt te vaak blindelings op de logfiles vertrouwd. Sommige bedrijven hebben echter wel degelijk behoefte aan testdata en testen de gemaakte backups zelfs dagelijks. Ook kleinere bedrijven zouden er goed aan doen dit in ieder geval maandelijks te doen. Maar niet voor slechts één bestand terug te halen, zoals we vaak zien. Dit biedt geen enkele zekerheid dat de rest van de backup geheel terug te halen is."

Doorn raadt gebruikers aan in ieder geval altijd duplicaten te maken van tapes en dan bij voorkeur naar andere type media zoals discs. Ook adviseert hij te waken voor foute instellingen en policy's ten aanzien van expiratiedata. "Is er ook ingesteld dat bepaalde data na een x-aantal maanden of jaren gewist kan worden en wordt daar nooit meer naar omgezien, dan zou belangrijke data verloren kunnen gaan."

Coördinatie

"Menselijke fouten en het te snel willen handelen bij een calamiteit, zorgt er vaak voor dat de problemen zich verergeren. Zo zien we nog wel eens dat er meteen wordt doorgewerkt op een schaduwserver, maar men realiseert zich niet dat dit veel risico's met zich meebrengt wanneer ook daarmee wat mis zou gaan", zegt Robbert Brans, datarecoveryspecialist bij Norman.
"Bij een brand, inbraak of andere calamiteiten wordt vaak onderschat dat er meer moet gebeuren dan het terugzetten van een backup. Op zo'n moment ziet een bedrijf zich voor tal van problemen geplaatst. Hoe moet een pand opnieuw van apparatuur worden voorzien, wat kan er nog gereconditioneerd worden, wie gaat de uitwijk coördineren? Door snel handelen worden er vaak verkeerde beslissingen genomen waardoor het langer duurt dan noodzakelijk om weer volledig 'in de lucht' te zijn."
Om bedrijven een aanspreekpunt te bieden waar men terecht kan voor datarecovery, IT continuity en calamiteitenplanning werkt Norman sinds een jaar samen met Revital Consulting en Livingston. Bij calamiteiten kan er 24 uur per dag een beroep worden gedaan op dit centrale aanspreekpunt en wordt er meteen iemand gestuurd die de coördinatie regelt om alles te regelen en aan te sturen.

Top 5 van de gevolgen van een ramp

Verminderde productiviteit van werknemers (62%)
Verlies van data (43%)
Teruglopende winst (40%)
Imagoschade (38%)
Teruglopende omzet (27%)

Bron: Veritas 2004