

HET VEILIGSTELLEN VAN GEGEVENS IS EEN HALSZAAK

Backuppen moet, maar hoe moet het?

Vorig jaar ging er iets goed mis vlak voor Kerstmis. Door een crashende harde schijf in de server lag de organisatie even stil. Wat een rust in een drukke tijd. Snel de backup van de dag ervoor terugzetten. Hoe groot was de schrik om het hart echter, toen bleek dat er niets op de backup-tape stond. En die van de dag daarvoor was ook leeg, net als alle andere (inclusief de week-backup). Helaas is het een waar gebeurd verhaal en het is niet voor het eerst dat het voorkomt.

U zou niet de eerste zijn die te maken krijgt met computerproblemen waarbij al uw gegevens verloren gaan. Een defecte harde schijf of een geheel niet meer functionerende server: het kan u overkomen! In dit artikel benadrukken we daarom het belang van een backup van uw kostbare of persoonlijke gegevens. Al vanaf het eerste moment dat er

wekelijks – is het minstens zo belangrijk te testen wat er daadwerkelijk gebackupt is. Probeer zo nu en dan eens een bestand of map uit een backup terug te halen, zodat u zeker weet dat u in noodgevallen ergens op terug kunt vallen. Dit is vooral belangrijk als de backup unattended – dus zonder dat er iemand aan te pas komt – plaatsvindt, bijvoorbeeld midden in de nacht. Het medium waarop wordt gebackupt, speelt ook een rol: op een dvd met gekopieerde bestanden is de test makkelijker dan het terughalen van een bestand uit een image of vanaf een gecompriëerde tape.

Gelukkig is dit besef bij velen van u ondertussen wel aanwezig. In de meeste organisaties is al nagedacht over hoe en vooral ook wat er gebackupt moet worden. Want u hoeft niet altijd alles veilig te stellen zoals we verderop zullen zien. Er zijn diverse manieren waarop u een backup kunt maken, laten we er eens enkele onder de loep nemen. Een onderscheid daarbij is of u dat hardware- of softwarematig doet. Maar de belangrijkste overweging in

de keuze voor backup-methode is de maximale tijd dat het mag duren voordat de organisatie weer up-and-running is na een calamiteit. Daarbij speelt mee hoeveel tijd het terugzetten van een backup in beslag neemt en hoeveel dataverlies nog acceptabel is bij een ramp. U zult begrijpen: hoe sneller en vollediger, des te duurder.

Calamiteit

De meest eenvoudige vorm van backup is een kopie van een bestand. Stel u heeft met uw tekstverwerker op uw pc een handleiding geschreven en dit is als een bestand opgeslagen op de harde schijf. We raden u aan om dit bestand op een floppy disk of cd/dvd te kopiëren, zodat u de documentatie bij een voorkomende calamiteit nog heeft. Het grootste voordeel van een kopie

Haal eens een bestand terug uit de backup

gegevens op een computer werden opgeslagen heeft men bezig gehouden met het verschijnsel backup, omdat een ongeluk nu eenmaal in een klein hoekje kan zitten.

Testen

Behalve het maken van backups –bijvoorbeeld dagelijks en ook nog eens

Kopiëren is in feite al backuppen

opslaan op een extern geheugenmedium dat zich niet in uw pc bevindt, is wel dat u die backup mee kunt nemen naar een andere locatie dan waar zich de computer bevindt. U moet er namelijk ook rekening mee houden dat de calamiteit wel eens heel fysiek van aard zou kunnen zijn: er kan bijvoorbeeld brand uitbreken of uw spullen kunnen gestolen worden.

Backup-media

Voor een standaard backup-procedure met behulp van tapes, zip-disks of cd/dvd's heeft u per jaar 21 backup-media nodig. In onderstaand overzicht nemen we als voorbeeld het jaar 2005:

- 4 media voor de wekdagen maandag t/m donderdag voor de dagelijkse backup, met labels maandag2005, dinsdag2005, etc. Gebruik deze media elke week opnieuw (dit overschrijft de dag-backup van vorige week, maar die gegevens zijn ook nog aanwezig op de wekelijkse backup), maar vervang ze door verse media bij aanvang van het nieuwe jaar.
- 3 media voor de wekelijkse backup op vrijdag, met labels vrijdag1-2005, vrijdag2-2005 en vrijdag3-2005. Ook deze media kunnen hergebruikt worden.
- 13 media voor de vierwekelijkse backup (is beter dan per maand, tenzij u daar een reden voor heeft, zoals met een gebroken boekjaar of afsluiting

van gegevens per maand), gelabeld week04-2005, week08-2005 t/m week52-2005. Deze backup maakt u elke vierde vrijdag op een nieuw medium. Na afsluiten van het jaar 2005 bewaart u deze periodieke backups naast de jaar-backup. Dat is handig voor terugzoeken en als reserve als er iets mis mocht zijn met de jaar-backup.

- 1 medium voor de jaarlijkse backup met label backup2005. Deze bewaart u vanzelfsprekend ook. Let ook op de comptabiliteit van de media: soms is voor een medium van 5 jaar geleden geen geschikte apparatuur meer aanwezig.

Bezuinig niet op media: gebruik goede, betrouwbare merken die goed uit de tests komen en begin elk jaar met allemaal nieuwe media. Niets is vervelender dan wanneer een backup in een noodgeval niet leesbaar blijkt te zijn. En: vergeet de test om te restoren niet!

Andere methoden

In feite is een backup altijd een kopie. Zolang het te backuppen materiaal een bestand is met een voor u herkenbare uitgang zoals .DOC voor een document of .AVI voor een video, zult u de kopie ook als bestand kunnen herkennen. Maar anders wordt het wanneer u bijvoorbeeld programma's of het besturingssysteem van uw computer wilt backuppen: als u alle bestanden in de map C:\Windows zou kopiëren naar cd/dvd en die vervolgens op een nieuwe computer weer zou terugzetten, dan werkt dat systeem niet! Dat komt omdat programma's vaak hele andere methoden gebruiken om bepaalde zaken op de harde schijf te bewaren. Een programma – dus ook het besturingssysteem – moet u meestal installeren, omdat er allerlei zaken zijn die voor het programma van belang zijn, maar die niet in een bestand staan. Denk aan stuurpro-

gramma's voor bepaalde hardware, de samenwerking met bepaalde software of het bestaan van randapparatuur, besturingssysteem of andere programma's.

Omdat u software meestal koopt op een cd/dvd of downloadt van Internet, kan die na een calamiteit weer opnieuw worden geïnstalleerd. Dus meestal is het niet nodig om de (standaard) programma's zelf te backuppen. Maar wél de gegevens, teksten en tekeningen, die u maakt met die programma's natuurlijk! Algemene vuistregel hierbij is: alles wat u in de winkel kunt kopen, hoeft u in principe niet te backuppen.

Images

Toch kan het wel handig zijn om hele programma's te backuppen. Stel, u gebruikt vele tientallen programma's op uw computer. In al die programma's heeft u bepaalde voorkeursinstellingen gemaakt, bijvoorbeeld het auto-

matisch kiezen van uw internetverbinding of de lay-out en functionaliteit van uw Office-toepassingen. Bepaalde programma's zijn ingesteld op de specifieke hardware die zich in uw pc bevindt met allemaal hun eigen stuurprogramma's en instellingen. Om dat alles weer opnieuw te installeren en in te stellen op een harde schijf (nadat uw vorige schijf bijvoorbeeld is beschadigd door een virus) is een hele klus! Een alternatief kan dan een image-programma zijn: daarmee maakt u een complete kopie van alles dat zich op de schijf bevindt, dus inclusief alle instellingen en werkende aanpassingen die u tijdens uw werkzaamheden heeft gedaan tot het moment dat u zo'n image maakt. De programma's Norton Ghost of PowerQuest Drive Image kunnen dit tegen relatief geringe kosten voor u verzorgen. Door het terugzetten van een image (restore) keert u in feite terug naar een situatie dat alles volledig werkend op de schijf stond.

Restjes

Images – maar ook programma's zoals QuickEx of Norton SystemWorks – zijn handig als de gebruiker veel nieuwe programma's installeert. Er vinden bij de installatie van een programma diverse aanpassingen plaats op de computer en na verwijdering van een programma kunnen er nogal wat restjes achterblijven. Dan is het terugzetten van een 'schoon systeem' in veel gevallen beter dan het oninstalleren (uninstall – dat is niet het simpelweg verwijderen van mappen en bestanden) van nieuwe toevoegingen.

Organisaties die 24/7 werken (continuu) kunnen geen offline backups maken, want er is geen periodieke downtime voor. Bij dergelijke organisaties, zoals bedrijven met een volcontinu dienst of ziekenhuizen zijn de data nooit exclusief beschikbaar voor een backup. Van zulke systemen maakt

men regelmatig snapshots (momentopnamen) van de gegevens. Alle mutaties na een snapshot houdt men dan niet alleen in de actuele database bij, maar ook in log-bestanden. De snapshots kunnen dan tezamen met de logs een kopie van het systeem vormen tot het moment van de calamiteit.

Backup op fysiek andere locatie bewaren

Spiegeling

Voor het kopiëren van bestanden kunt u de normale hardware (diskteststation of cd/dvd-brander) van een pc gebruiken. Voor het maken van backups van grote systemen, zoals servers, is meer nodig. Zo zijn er bijvoorbeeld backup-procedures waarbij de gehele inhoud van de centrale harde schijf in een netwerk wordt gekopieerd op een andere harde schijf ergens anders in de organisatie, bij voorkeur ook op een andere fysieke locatie (denk aan brand of dief-

stal). Men noemt dit 'mirroring', ofwel spiegeling, van een schijf. Men doet dit bij voorkeur op een systeem dat ook de taken van de probleem-server kan overnemen. Een wat ouder – maar nog altijd veel gebruikt – systeem is de backup met een tapestreamer, een soort recorder met een – meestal magnetische – opslagmogelijkheid (vergelijk een videoband) die alles van een harde schijf kopieert.

Planning

In veel organisaties gebruikt men een backup-procedure zoals in bijgaand kader. Het systeem maakt bijvoorbeeld elke nacht unattended (automatisch gestuurd, dus als iedereen weg is) een backup op een tape, zodat er bij calamiteiten nooit méér dan één dag werken verloren kan gaan.

Een planning maken of een routine bedenken waarmee u uw gegevens zo veilig mogelijk backupt is belangrijk en kan van diverse zaken afhankelijk zijn:

- Hoe groot is het nieuwe aantal gegevens dat moet worden gekopieerd? Als het erg veel is maar eigenlijk weinig nieuwe bestanden zijn, kan de frequentie lager zijn.

Mobiele apparatuur

Veel aandacht is er traditioneel voor de backup binnen de muren van de organisatie. Hiervoor zijn vele middelen – zowel computertechneisch als financieel – beschikbaar. Maar in deze tijd dat mobiele apparaten zoals laptops en personal digital assistants (pda's) erg populair zijn, ziet men vaak enorme hoeveelheden kostbare bedrijfsgegevens over het hoofd. Dat komt omdat dergelijke apparatuur zich het grootste deel van de tijd buiten het bereik van de backup bevindt. Als ze überhaupt al ooit binnen dat bereik komen.

Telewerkers

Werknemers in uw organisatie die zich veel buitenshuis bevinden, zijn vaak niet ingecalculiseerd in de backup-planning. Denk daarbij niet alleen aan de buitendienstmedewerkers met hun laptop,

maar ook aan de directeur met zijn pda en de telewerkers met hun pc op de zolderkamer. Hun gegevens staan vrijwel altijd allemaal op één plaats: de harde schijf van hun apparaat. Op de doorsnee laptop van tegenwoordig is een harde schijf van 20 GB of nog groter heel gewoon. Vaak staat de helft vol met evenzo goed belangrijke gegevens. Een stroomstoot, een afgebroken handvat van de laptoptas, diefstal of een omgevallen kop koffie betekent dan meestal net zo goed een ramp van ongekend formaat. Neem uw externe medewerkers op in de backup-planning, door hen bijvoorbeeld regelmatig de belangrijkste zaken uit hun mobiele apparatuur te laten overhevelen naar het centrale netwerk. Tip: gebruik werkmappen die automatisch worden gesynchroniseerd zodra ze in contact komen met het (bedrijfs)netwerk.

- Wat is het onheil dat kan toeslaan? In een gevaarlijke omgeving kan een frequentere backup nodig zijn dan in een ongevaarlijke omgeving. Dat geldt ook voor diefstalgevoelige situaties: ga nooit zonder een backup gemaakt te hebben met al uw gegevens op een laptop op reis!

Maak een planning en test de procedure

- Waar staan de gegevens die moeten worden gebakupt? In een netwerk worden bijvoorbeeld vaak alleen de gebruikersmappen gekopieerd, niet de programma's.

Nuttige tips

Tot slot nog enkele nuttige tips voor u omtrent backups:

- Bewaar de backup altijd op een veilige plaats, maar vooral (ver) weg van het origineel. De ramp kan altijd volledig zijn.
- Mocht u images gebruiken, maak dan voordat u op (zaken)reis gaat twee image-kopieën en laat er één achter op de thuisbasis.
- Sla op mobiele apparatuur alleen de hoogstnoodzakelijke gegevens en bestanden op. In geval van een calamiteit hoeft u dan niet alleen veel minder te herstellen, maar u voorkomt daarmee ook dat echt álles op straat komt te liggen in geval van diefstal.
- Let op de maximaal aanbevolen gebruiksduur van de gebruikte media, met name tapes mogen niet te oud en/of teveel gebruikt zijn om daarmee niet de betrouwbaarheid negatief te beïnvloeden.

Hoe u het ook plant of regelt: er kan altijd iets fout gaan. Daar moet u op proberen te anticiperen, zodat u niets kwijtraakt in een noodsituatie. Zelfs een gebrekkige backup is altijd nog beter dan geen backup. Maar dat wist u al.