Dataverlies en erger

LAURENS VAN AGGELEN

De impact van 9/11 heeft ook in Nederland zijn sporen achtergelaten. Het maakte opeens duidelijk hoe kwetsbaar bedrijven zijn wanneer niet voldoende is nagedacht over risico's en het op de rails houden van een bedrijf bij calamiteiten. Hoe snel ben je weer up- en running wanneer het misgaat? Hoe lang kun je het je als bedrijf permitteren uit de lucht te zijn?

Tijdens de Business Continuity Management Summit 2006 van IDC, liet het vermaarde onderzoeksbureau zien wat een steekproef onder 220 IT-ers en zakelijke beslissers bij bedrijven met meer dan 100 werknemers aan het licht had gebracht. De conclusies bieden stof tot nadenken. Zo kwam naar voren dat de strategie van veel bedrijven nog altijd sterk bepaald wordt door incidenten die een organisatie hebben getroffen of incidenten van andere organisaties die de aandacht van het management trekken. Zo zorgen vooral verloren memorysticks, gestolen laptops en dataverlies in 2006 ervoor dat er veel aandacht is voor de bescherming van data. Directies nemen bovendien vaak te weinig verantwoordelijkheid. Vaak is *business continuity* iets waarover men pas gaat nadenken na aanschaf en implementatie van allerlei hard- en software terwijl *business continuity* dient te worden geïntegreerd met de business en IT architectuur en de bijbehorende *governance* structuren. Bestuurders en managers zijn zich over het algemeen wel bewust van de noodzaak van een continue bedrijfsvoering, alleen worden plannen en intenties te vaak versnipperd en blijken verantwoordelijkheden onduidelijk te zijn. IDC is van mening dat bedrijven hun *business continuity*-plannen beter op elkaar moeten afstemmen. Alleen dan kan een bedrijf adequaat reageren op bedreigingen die een gevaar opleveren voor de continuïteit.

"De aandacht van het Nederlandse bedrijfsleven voor *business continuity* blijft toenemen. In 2005 werd de noodzaak vooral gedreven door risico's van natuurgeweld als orkaan Katrina of de bomaanslagen in Londen", aldus Peter Vermeulen, Research Director bij IDC Benelux. "In 2006 zien we

dat de organisaties de risico's dichter bij huis zoeken."

Maatregelen

Ook in de media zou er volgens Vermeulen te eenzijdig over *business continuity* worden bericht. Alsof bedrijven alleen het verlies van data boven het hoofd hangt terwijl er voor zoveel meer zaken aandacht zou moeten zijn. "Naast de angst voor dataverlies laten veel bedrijven zich bij hun interesse en investeringen in *business continuity* ook leiden door scherpere wet- en regelgeving, bijvoorbeeld op het gebied van privacy, bewaarplicht en financiële risicobeheersing binnen bedrijven. Een andere reden voor de toegenomen aandacht voor *business continuity* is dat steeds meer bedrijven zich ervan bewust zijn dat verlies van data een negatief effect heeft op de productiviteit van werknemers.
Om gevaren het hoofd te bieden, is het bedrijfsleven zich er veelal van bewust dat goede continuïteitsplannen belangrijk zijn. Zo'n 80 procent van de door IDC ondervraagde bedrijven geeft aan uitgewerkte plannen te hebben voor databeveiliging, data back-up en -recovery. Daarnaast heeft bijna 70 procent van de bedrijven ook een uitgewerkt plan voor de fysieke beveiliging van gebouwen en medewerkers. Hieruit blijkt dat beveiliging niet alleen draait om technologie, maar onderdeel uitmaakt van de algemene bedrijfsvoering. Verder beschikt ruim 70 procent van de onderzochte organisaties over een crisismanagementteam dat alle continuïteitsplannen coördineert en beheert. Wat betreft verantwoordelijkheden blijkt dat bij de meeste bedrijven op papier de directie verantwoordelijk is, maar in de praktijk wordt deze verantwoordelijkheid vaak gedelegeerd.
De voornemens kunnen echter nog zo goed zijn, wanneer technologie faalt, liggen belangrijke processen stil. Bij een derde van de onderzochte bedrijven komt het minstens een keer per maand voor dat bedrijfskritische applicaties niet beschikbaar zijn. Bij twaalf procent van de organisaties gebeurt dit minimaal eens in de week.
Hoewel de betrouwbaarheid van IT gedurende het afgelopen jaar is toegenomen, is het aantal schadelijke incidenten die als cybercrime kunnen worden aangerekend, ook toegenomen. Uit het onderzoek blijkt dat organisaties als gevolg van cybercrime gemiddeld vier keer per jaar direct omzet mislopen en dat dit ook de oorzaak is dat de productiviteit van de organisatie vier keer per jaar nadelig wordt beïnvloed.

Peter Vermeulen: "Aandacht voor business continuity in de media is te eenzijdig."

Dataverlies

De angst dat data verloren gaat of in verkeerde handen terecht zou kunnen komen, zijn alle redenen om backups te maken en het restoren daarvan met enige regelmaat te testen. Toch blijkt uit onderzoek van Contingency Planning Research dat bijna 96 procent van alle business pc's niet gebackupt worden. Een schrikbarend aantal. Dat volgens Gartner zes procent van alle pc's te maken krijgt met dataverlies, is een gegeven dat veel lijkt op het topje van een ijsberg. Na het maken van backups verzuimen veel bedrijven overigens om ook een kopie van het betreffende opslagmedium buiten het pand op te bergen. Maar ook als dit wel gebeurt zijn goede procedures van groot belang. Zo kwam een tape met gegevens van miljoenen creditcardhouders niet zo lang geleden in Amerika nog in verkeerde handen doordat deze bij een medewerker uit de auto werd gestolen.
De primaire insteek van een goed bedrijfscontinuïteitsplan zou er op gericht moeten zijn om primair risico's weg te nemen. Te vaak ligt de focus op alleen de *recovery* van data en niet het voorkomen van dataverlies. Belangrijke valkuilen bij het opstellen van een goede policy is dat problemen niet onderkend of begrepen worden, maatregelen niet realistisch genoeg zijn of te ingewikkeld. Dat laatste komt vaak doordat IT-omgevingen te complex en weinig efficiënt zijn ingericht en er sprake is van slecht gestructureerde bedrijfsprocessen.

Bedrijfscontinuïteitsplan? Enkele tips:

1. Ga met de juiste insteek en motivatie te werk;
2. Inventariseer wat de impact van bepaalde calamiteiten zou zijn op de bedrijfsvoering;
3. Kijk goed naar de relatie met toeleveranciers;
4. Kijk kritisch naar je eigen business infrastructuur;
5. Analyseer risico's en vraag je af welke risico's je wel en niet kunt lopen en wat de schade zou kunnen zijn die daaruit uit voort zou kunnen komen. Dat kan bijvoorbeeld ook imagoschade zijn;
6. Zorg dat datarecovery uiteindelijk het laatste is wat je zou moeten doen;
7. Wijk wanneer alles door welke oorzaak dan ook plat gaat niet te snel uit naar een andere locatie omdat dit ook extra risico's met zich meebrengt. Wanneer er meteen doorgewerkt wordt op een schaduwserver zou de schade niet te overzien zijn wanneer ook die onderuit gaat;
8. Focus op die onderdelen van de bedrijfsvoering die in ieder geval altijd beschikbaar zouden moeten zijn.