Storage Architects BV
Westerbracht 16, 7821 CH Emmen
Postbus 2234, 7801 CE Emmen
Nederland
T. +31 591 67 03 40
KvK 04073246

INFORMATIEBEVEILIGING EN DATABESCHIKBAARHEID

1. Inleiding

De eisen aan informatiebeveiliging en databeschikbaarheid nemen toe. Oorzaken liggen onder andere in de continu groeiende hoeveelheden digitale data en strengere wetgeving omtrent veiligheidseisen en bewaartermijnen. Aan de andere kant wordt de beschikbare tijd voor het maken van een back-up steeds korter als gevolg van onder andere internationalisering en langere werktijden.

Traditionele back-upmethodes blijken hiervoor in toenemende mate onvoldoende veiligheid te bieden of niet betrouwbaar genoeg te werken. Praktijkvoorbeelden hiervan zijn lange restore tijden, niet actuele back-ups of het niet terug kunnen zetten van data vanaf een back-uptape in verband met ruimtegebrek of corrupte tapes. Daarnaast biedt een traditionele back-upmethode meestal ook geen oplossing voor uitval van een server aangezien de gehele server (OS, applicaties en data) teruggezet dient te worden. Niet altijd is er de juiste server hardware of een disk image beschikbaar die snel terug te zetten is.

De noodzaak voor een andere benadering van informatiebeveiliging en databeschikbaarheid is derhalve van groeiend belang. In dit document wordt vanuit de ICT een methodiek hiervoor uiteengezet.

2. Continuous Data Protection (CDP)

Een concept die op deze problematiek inspeelt is het concept van Continuous Data Protection (CDP). Centraal binnen deze methodiek staat het principe dat data continu veilig gesteld wordt, zodat te allen tijde een actuele versie van de data beschikbaar is en er daarnaast uitwijkmogelijkheden zijn.

Een belangrijke eerste stap binnen CDP is om allereerst de verschillende data en de bijbehorende applicaties in te delen in mate van afhankelijkheid en belangrijkheid voor de bedrijfsvoering. Immers kan de bedrijfseconomische waarde per applicatie of systeem verschillend zijn. In figuur 1 zijn enkele voorbeeldvragen opgenomen die kunnen helpen om deze bedrijfseconomische waarde vast te stellen:

Figuur 1: Vraagstelling

Vraagstelling:	**Grote invloed**	**Middel-matige invloed**	**Geringe invloed**
1. Wat is de invloed op de omzet van de applicatie of het systeem?			
2. Hoeveel interne gebruikers zijn afhankelijk van de applicatie of het systeem?			
3. Hoe hoog zijn de kosten van deze interne gebruikers?			
4. Welke invloed heeft de applicatie/het systeem op het voldoen aan wet- en regelgeving ('compliancy')?			
5. In welke mate zijn klanten en partners afhankelijk van de applicatie/het systeem?			
6. Welke bedrijfsprocessen werken met de applicatie/het systeem samen?			

Met de antwoorden op deze vragen kunnen helpen om vervolgens de bedrijfsmatige eisen te classificeren in mate van belangrijkheid. In figuur 2 is uitgegaan van drie classificatieniveaus, maar dat kunnen er ook meer zijn.

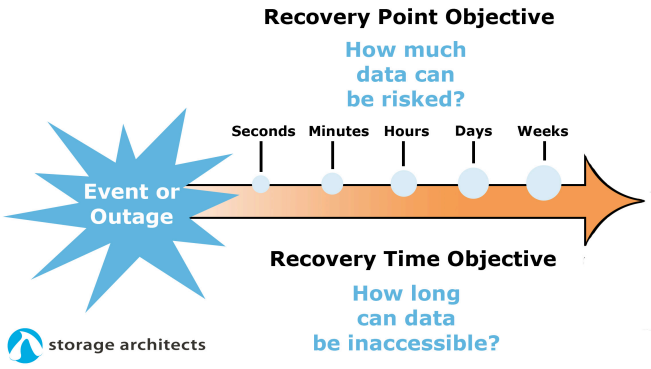
Figuur 2: Classificeren van bedrijfsmatige eisen

	Niveau 3 (kritisch)	Niveau 2 (belangrijk)	Niveau 1 (niet-belangrijk)
Bedrijfseisen	• Downtijd heeft onmiddellijk effect op het bedrijf • Onmogelijk om zaken te doen zonder het bedrijfsproces	• Downtijd beïnvloed nadelig het bedrijf na verloop van tijd • Kan nog zaken doen zonder het bedrijfsproces, maar niet heel lang	• Downtijd heeft op korte of lange termijn geen effect op het bedrijf • Kan nog langere tijd zaken doen zonder het bedrijfsproces

De nadruk in het concept van Continuous Data Protection komt te liggen op restore en recovery die dus zijn afgestemd op de organisatie en de bedrijfsmatige doelstellingen. Een belangrijk hulpmiddel hierbij is om de zogenaamde Recovery Time Objective (RTO) en de Recovery Point Objective (RPO) vast te stellen.

Recovery Time Objective (RTO):
De RTO is de beoogde tijdsperiode waarbinnen eindgebruikers na een calamiteit weer toegang tot hun zakelijke applicaties dienen te hebben: 1 dag, 4 uur, 1 uur, 5 minuten of nog korter?

Recovery Point Objective (RPO):
De RPO is de maximale tijdsperiode waarover in geval van een calamiteit data verloren mag zijn gegaan, ofwel hoe actueel dient een veiligheidskopie te zijn: 1 dag, 4 uur, 1 uur, 5 minuten of nog korter?



Per applicatie en per datatype worden deze Recovery Time en Recovery Point Objectives bepaald. In figuur 3 worden typische Recovery Time en Recovery Point Objectives genoemd:

Figuur 3: Typische Recovery Time- en Point Objectives

	Niveau 3 (kritisch)	Niveau 2 (belangrijk)	Niveau 1 (niet-belangrijk)
Primary Site			
RTO	5-30 minutes	30 minutes – 8 hours	> 8 hours
RPO	< 1 minute before event	1 minute – 24 hours	< 24 hours (last backup)
Secondary Site			
RTO	> 8 hours	8 hours – 72 hours	72 hours – 1 week
RPO	< 15 minutes before event	Last backup (< 24 hours)	Last full backup (1 week)

3. Matchen van bedrijfsdoelstellingen met technologie:
Er bestaat een direct verband tussen het niveau aan veiligheid en beschikbaarheid en de hiervoor benodigde investeringen. Technische oplossingen om uit te kiezen zijn er vele waaronder replicatie, SAN, mirroring, hot back-up, snap shots, backup-to-disk, redundant storage, remote backup, etc. In figuur 4 staan enkele van deze mogelijke technieken per niveau ingevuld.

Figuur 4: Mogelijke technieken ten behoeve van Continuous Data Protection:

	Niveau 3 (kritisch)	**Niveau 2 (belangrijk)**	**Niveau 1 (niet-belangrijk)**
Hoofdvestiging	• Automatische fail-over mogelijkheden • Snapshots van de database volumes • Geen 'single point of failure'	• Handmatige fail-over mogelijkheden • Bedrijfsback-up en hersteloplossingen • Backup van database d.m.v. split mirror • Backup van de online database	• Ad hoc backup en herstelmogelijkheden • Backup van de statische database • Geen failover mogelijkheden
Nevenvestiging	• Real-time of bijna real-time data replicatie • Hot failover servers (OS, online applicaties en dedicated servers voor support) • Geen 'single point of failure'	• Remote tape vaulting • Warm Standby servers, beschikbaar voor handmatige reconfiguratie (OS en geladen applicaties, die gebruikt worden voor niet-productie werk	• Cold Standby servers, opgebouwd bij een andere vestiging • Tape opslag op afstand

Gestreefd wordt naar een oplossing die optimaal evenwicht biedt tussen dataveiligheid, databeschikbaarheid, bedrijfsmatige eisen en benodigde investeringen. In de bijlage staat een werkdocument die gebruikt kan worden om de verschillende applicaties en de waardes in een matrix weer te geven. Deze matrix vormt, samen met aanvullende informatie, voor Storage Architects belangrijke input voor het samenstellen van een oplossing.