

Nieuws

[print](#)

20-04-2009

Richtlijnen voor een robuust datacenter

Barry Elliott

De [Amsterdam Internet Exchange](#) verbindt ruim driehonderd internetbedrijven via zes datacenters en het AMS-IX Network Operating Centre. Het Britse Capitoline is sinds kort als consulting partner verantwoordelijk voor de 'business continuity' van het internetknooppunt. Barry Elliott van [Capitoline](#) zet uiteen wat de richtlijnen en best practices zijn voor business continuity in datacenters.



Het leveren van een betrouwbare en succesvolle dienst is van een aantal zaken afhankelijk:

- Een productieomgeving die goed is ontworpen en degelijk is opgebouwd, en die de juiste standaarden en best practices in acht neemt om te komen tot efficiënte en betrouwbare bedrijfsvoering.

- Beheertechnieken die zorgen voor de procedures en protocollen om de efficiëntie en betrouwbaarheid van de onderneming blijvend te garanderen.
- Disaster recovery-plannen die een bewezen en geteste procedure omschrijven voor het afhandelen van incidenten die de activiteiten van de onderneming in gevaar brengen en laat zien wat er moet gebeuren om te herstellen na een ramp.

Deze benadering leent zich voor zowel het beheer van een olieraffinaderij als van een datacenter. Maar laten we ons hier richten op de specifieke eisen voor het datacenter, want dat is juist het gebied waar de verschillende achtergronden van de betrokkenen (IT, facilities, etc.) ervoor zorgen dat iedereen zich op zijn eigen gebied richt en het zicht op het algehele plaatje verloren raakt.

De hiërarchie van standaarden, codes, regels en wetgeving die zorgen voor de basisprincipes voor ontwerp en bedrijfsvoering, ziet er als volgt uit:

- 1. EU-richtlijnen.
- 2. CENELEC-standaarden
- 3. IEC/ISO-standaarden.
- 4. Nationale standaarden (alhoewel deze voorrang krijgen als er in lokale wetgeving naar wordt verwezen).
- 5. Andere internationale standaarden zoals van Ansi, Bicsi, Ashrae en BSI.
- 6. Richtlijnen van de fabrikanten.
- 7. De 'industry best practices'.

Technische standaarden

Technische standaarden geven de best practices-methodes voor het ontwerpen en implementeren van het datacenter, zowel vanuit een fysiek, elektrisch als een mechanisch oogpunt. Sommigen eisen met betrekking tot gezondheid en veiligheid en energiebeheer zijn gedekt door Europese richtlijnen en nationale normen. Er bestaan veel technische normen die betrekking hebben op de talloze technische disciplines in een datacenter. Twee stukken in het bijzonder hebben echter specifiek betrekking op de engineering-aspecten van het datacenter en de uiteindelijke robuustheid en redundantie van het ontwerp. Dat zijn:

- ANSI/TIA-942: 2005 Telecommunications Infrastructure Standards for Data Centers
- Tier Classifications define site infrastructure performance. The Uptime Institute, 2008

Het document van The Uptime Institute (TUI) deelt de bedrijfsvoering op in vier 'Tiers' die een inschatting geven van de verwachte jaarlijkse downtime van een datacenter, mits bepaalde ontwerproutes zijn genomen. De TIA 942-standaard trekt zwaar op de filosofie die in dit TUI-document uiteen is gezet en biedt in engineeringtermen meer over wat nodig is voor het bereiken van deze niveaus.

Een centraal onderdeel van de filosofie is de goedkeuring van de N, N + 1 en 2N methodologie. In het kort betekent 'N' dat er genoeg apparatuur aanwezig is om de klus te klaren. 'N + 1' betekent dat elk systeem een redundant component heeft. Bij '2N' zijn systemen volledig gerepliceerd. Een variant daarop is bijvoorbeeld 2N + 1 waarbij er sprake is van twee onafhankelijke systemen met elk zijn eigen redundante componenten. Uiteindelijk is het een afweging tussen risico en kosten: meer niveaus van redundantie en robuustheid zal altijd meer kosten. Voordat een besluit wordt genomen over de meest geschikte strategie is het aan de organisatie zelf om voor de eigen specifieke situatie te bepalen hoe duur een downtime is.

Beide bovengenoemde normen zijn Amerikaans. Er zijn geen direct vergelijkbare Europese (CENELEC) of internationale normen (ISO/IEC). De methoden beschreven in de twee Amerikaanse documenten zijn meestal universeel, maar voor gebruik in Europa moeten de technische verwijzingen in TIA 942 zo nodig worden vervangen door de EU-richtlijnen en CENELEC-normen.

Het TUI-model is niet het enige robuuste model dat momenteel in omloop is; in Duitsland heeft BEKOM een methode voor beschikbaarheid gepubliceerd en in de Verenigde Staten heeft Syska Hennesy zijn eigen 'beschikbaarheidssysteem' ontwikkeld. Het TUI-model blijft echter wel de meest geaccepteerde aanpak.

Andere normen zijn in productie, onder andere in Nederland (zie ook pagina 30). De enige Europese norm die zich ook richt op het datacenter is op dit moment EN 50173-5, hoewel dit in feite een bekabelingsstandaard voor datacenters is.

Business continuity-standaarden

Het bouwen van een datacenter dat voldoet aan de nieuwste normen en waarin de vereiste technieken zijn toegepast voor beschikbaarheid en redundantie, is slechts een eerste stap voor een succesvolle langdurige werking. De volgende fase is het beheer van het datacenter en ervoor zorgen dat je bent voorbereid op technische storingen of andere gebeurtenissen die van invloed zijn op de werking van het datacenter. Dit gebied valt onder de algemene titel van business continuity Management, BCM. BCM-standaarden zijn over het algemeen gericht op alle bedrijven en ondernemingen, waarbij opgemerkt dat sommige standaarden zich

meer richten op de informatie- en communicatietechnologie.

De volgende normen zijn vastgesteld met betrekking op dit gebied.

- NEN 7799-3:2006. Information security management systemen. Richtlijnen voor informatiebeveiliging risicobeheer.
- BS ISO/IEC 20000-1:2005. Informatietechnologie. Service management. Specificatie.
- BS ISO/IEC 27001:2005. Informatietechnologie. Beveiligingstechnieken. Information security managementsystemen. Eisen.
- BS ISO/IEC 27002:2005. Informatietechnologie. Beveiligingstechnieken. Code of practice voor informatiebeveiligingsbeheer.
- NEN 25999-1:2006. Business continuity management, deel 1: Code of practice.
- BS 25777:2008 Informatie- en communicatietechnologie – continuity management, Code of practice.
- BS ISO/IEC 17799:2005. Code of practice voor information security management.
- ISO/PAS 22399:2007. Maatschappelijke veiligheid – Richtlijn voor 'incidentparaatheid' en operationeel continuïteitsbeheer.
- NFPA 1600; 2007. Standaard voor disaster/emergency management en business continuity-programma's.

Daarnaast hebben we Itil. Itil bestaat uit een reeks boeken die een richtlijn bieden voor de bepaling van de kwaliteit van IT-diensten, en voor de huisvesting en installaties die nodig zijn voor de ondersteuning van IT. Itil is ontwikkeld met in het achterhoofd de groeiende afhankelijkheid van IT en belichaamt de best practices voor IT-servicemanagement.

We hebben ook Prince. Prince2 is een generieke, eenvoudig te volgen projectmanagementmethode. Het heeft betrekking op het organiseren, beheren en controleren van projecten. Het helpt bij het met succes kunnen leveren van de juiste producten, op tijd en binnen budget. Een projectmanager kan de beginselen van Prince2 en de bijbehorende opleiding voor elk type project toepassen. Het zal helpen bij het effectief beheren van risico's en veranderingen en bij het controleren van de kwaliteit.

Een Prince2-project heeft de volgende karakteristieken:

- Een beperkte en afgebakende levenscyclus.
- Omschreven en meetbare zakelijke producten.

- Een soortgelijke reeks activiteiten om de zakelijke producten te realiseren.
- Een vastgestelde hoeveelheid middelen.
- Een organisatiestructuur, met afgebakende verantwoordelijkheden, voor het beheer van het project.

BS25777

In een enquête van het magazine Continuity Central onder datacentermanagers in Noord-Amerika en Europa, werd BS 25999:2006 genoemd als zijnde de meest gebruikte. In 2008 is een aanvullende norm gepubliceerd, *BS 25777:2008 Information and Communications Technology – Continuity management, Code of Practice*. BS 25777 lijkt voor Europa zeer geschikt om de best practices voor business continuity management in de ICT-omgeving te omschrijven, in afwachting van een bredere ISO/IEC-norm.

BS 25777 definieert een ICT-dienst, zoals die bestaat uit mensen, gebouwen, technologie, gegevens, processen en leveranciers. Onder het kopje 'Technologie' zijn opgenomen de racks, bekabeling, servers en communicatieapparatuur. De beginselen van ICT-continuity management zijn gebaseerd rond zes centrale begrippen: Protect, Detect, React, Recover, Operate en Return.

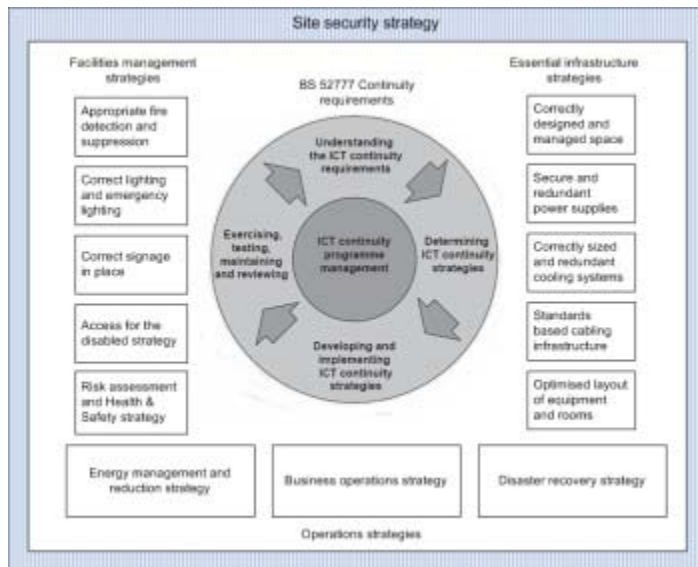
"Voor elke kritische ICT-dienst dient de continuity te worden bekeken vanuit een preventief oogpunt om zo het risico van een service-onderbreking op het spoor te komen, zoals bijvoorbeeld een single point of failure."

Conclusie

Het lijkt duidelijk dat een aantal strategieën moeten worden ingevoerd om te zorgen voor de succesvolle en aanhoudende exploitatie van een datacenter. Het begint bij het definiëren van wat het eigenlijke doel van het datacenter is. Nadat de vereiste software is omschreven kan de hardware worden gedefinieerd die nodig is voor de softwareverwerking, communicatie en opslag. Als dat bekend is, kan de omvang worden bepaald van het gebouw, stroomvoorziening en koeling. En parallel hieraan de hoeveelheid robuustheid en redundantie die door de klant wordt vereist. Energiemanagement en methoden voor het terugdringen van het energieverbruik moeten ook worden toegepast.

Wanneer het basisontwerp klaar is, dan moet de beveiliging van de site nog worden bepaald en geïmplementeerd. Als het een plaats is om te werken, net als alle andere, dan zal de wetgeving inzake gezondheid en veiligheid moeten worden opgevolgd. Als het best denkbare infrastructurele ontwerp klaar is, wordt het tijd om de 'best working practices' te implementeren en daar hoort uiteraard ook een

disaster recovery-plan bij.



Het diagram toont mijn interpretatie van een ontwerp gebaseerd op best practices en de beheerprincipes voor een datacenter gebaseerd op de Business Continuity Concepts van BS 25777.

Barry Elliott (RCDD) is werkzaam bij het Britse adviesbureau Capitoline (www.capitoline.eu)

[Terug](#)

copyright © 2009 FenceWorks BV
[disclaimer](#) | [sitemap](#) | [rss](#) 