

# Netwerk of 'Net niet werkend netwerk'?

## *Nieuwe benaderingen voor het succesvol koppelen van uw bedrijf in de cloud*

Terwijl de technische security kan worden gerealiseerd met de juiste inspanning, levert de nationale wet- en regelgeving vaak een probleem op. "Private cloud" is een alternatief waarbij cloud- diensten aan specifieke veiligheidseisen kunnen voldoen. De uitdaging ligt hier eerder bij de bestaande infrastructuur van het bedrijf dat vaak niet aan de nieuwe eisen voldoet. Er moet een oplossing worden gekozen, die over een extra niveau intelligentie beschikt, namelijk de SMART MPLS.

### 1. Security bij cloud computing

Al geruime tijd is Cloud Computing een veelbesproken onderwerp. Regelmatig verschijnt dit nieuw "paradigma" bijna als een wondermiddel voor alle IT-problemen; van de toenemende complexiteit van de systemen, het energieverbruik van datacenters, de ruimte ingenomen door de servers tot de aanhoudende kostenbesparingen binnen de IT-afdeling. Bij cloud computing gaat het niet om een revolutionaire technologie, maar om een alternatief model voor het toepassen van IT-oplossingen. De voordelen voor het bedrijfsleven zijn in ieder geval duidelijk: De concentratie van middelen en het locatie-onafhankelijk, gevirtualiseerd bereik van IT-oplossingen leiden tot schaalvoordelen en synergie

Aangezien meer bandbreedte beschikbaar is, kan deze methode voor standaardapplicaties, zoals e-mail, social media platforms, maar ook voor zoekmachines worden gebruikt. Een privé-gebruiker hoeft geen eigen e-mailserver meer te implementeren en beheren; via cloud kan hij in zijn eigen omgeving de applicaties gebruiken. Het voldoet misschien niet aan alle technische eisen, maar over het algemeen is het vaak economisch interessanter als er geen tussen-of pre-investeringen moeten worden gemaakt. Ondertussen is voor bedrijven een uitgebreid portfolio van Cloud applicaties beschikbaar. Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) en Infrastructure-as-a-Service (IaaS) zijn daar voorbeelden van. De offertes van cloud leveranciers omvatten onder meer de beschikbaarheid van ruimtes tot de uitwerking van volledige ERP-toepassingen.

Bedrijven hebben echter, in vergelijking met de residentiële sector, veel strengere eisen. De vraag rond security in het bijzonder is naar voren gekomen als een kritisch punt. Blijkbaar is voor veel IT-managers het idee om hun eigen gegevens in een "cloud" over te dragen veel te riskant. Dat men in het bedrijfsleven voorzichtig omgaat met een mediahype is gemakkelijk te begrijpen. In een digitale wereld hangt het welzijn van elk bedrijf af van de integriteit en geheimhouding van zijn gegevens.

Bij de vraag rond security moet men een onderscheid maken tussen technische en juridische aspecten. Puur technisch gezien is er duidelijk een risico, aangezien het om een extern kanaal gaat, waarbij verscheidene processen interacteren. Een geïsoleerde verbinding is onaantastbaar maar volkomen onpraktisch. Geen enkel bedrijf kan met een eigen verbinding het contact met de buitenwereld controleren of communiceren met klanten. Uiteraard kunnen verbindingen nu effectief worden beveiligd. Het tegenhouden van ongeautoriseerde toegang maakt deel uit van de dagelijkse IT-

beveiliging en is geen innovatie in de “Cloud” omgeving. Het feit dat cloud providers gegevens van meerdere bedrijven tegelijk verwerken, verandert niets aan de fundamentele veiligheidssituatie. Bovendien gaat het extreem beperken van risico’s gepaard met zeer hoge kosten. IT-beveiliging is uitgegroeid tot een zeer complex thema dat veel know-how en ervaring eist. Grote bedrijven hebben meestal de juiste experts in huis. Echter, de snel veranderende technologieën zijn voor de mid-market-gebruikers moeilijk bij te houden. Voor hen is het veiliger de IT-infrastructuur toe te wijden aan gespecialiseerde providers.

## **2. Het structureel probleem bij Cloud Computing**

Bij cloud computing is de technische beveiliging niet echt het centrale probleem. Gevallen van ongeautoriseerde toegang zijn uiterst zeldzaam. Bovendien kan daadwerkelijk misbruik getraceerd worden. Deze problemen zijn niet gebonden aan de cloud, maar aan IT in het algemeen.

Het echte probleem is de aanhoudende rechtsonzekerheid die wordt veroorzaakt door het bestaan van verschillende nationale regelgeving bij het leveren van internationale oplossingen. Cloud Computing is feitelijk locatie-onafhankelijk. Cloud providers verlagen hun kosten op basis van efficiëntie criteria, waarbij zij in het kader van “Disaster Recovery” een zo breed mogelijk distributienetwerk beschikbaar moeten hebben. Daardoor zijn de resources onderworpen aan verschillende nationale of regionale wet- en regelgeving, waarbij de Cloud een structureel probleem kent.

Dit wil niet zeggen dat gegevens buiten Europa niet sterk beveiligd kunnen worden, maar er kunnen plaatselijk regelingen bestaan, die van de dienstverlener eisen om voor de lokale autoriteiten de gegevens toegankelijk te maken (bijvoorbeeld in de Verenigde Staten), terwijl dit in het land waar de klant gebaseerd is, niet is toegestaan. In dit geval hebben beide partners - leverancier en klant - een probleem. Zo is de overdracht van persoonsgegevens naar landen buiten de EU alleen met grote restricties toegestaan of soms zelfs helemaal niet. Ook de Zwitserse bankenwet bepaalt dat bepaalde gegevens het land niet mogen verlaten. Dergelijke voorschriften zijn slechts een voorwendsel om de nationale gevoeligheden op vlak van privacy niet te schaden, want hierachter staan meer tastbare belangen. Zelfs Amerikaanse bedrijven kunnen moeilijk aanvaarden dat bijvoorbeeld Chinese autoriteiten hun gegevens publiceren, ook al gebeurt dit volledig in overeenstemming met de lokale wet- en regelgeving.

Zolang er geen internationale wet- en regelgeving voor handen is, kan dit structurele probleem niet worden opgelost. Speciaal voor bedrijfskritische toepassingen is cloud computing daarom geen prioriteit, althans, zolang het als “Public Cloud” geïnterpreteerd wordt. Andere vragen rond cloud computing, zoals het verwijderen van gegevens na contractafloop of de procedure in geval van faillissement van een leverancier, kunnen daarentegen wel opgelost worden. Ondanks dit dilemma, blijven de technische en economische voordelen van dit model bestaan. Het hangt allemaal af van wat men wil bereiken met cloud computing.

### 3. Private versus Public Cloud

Via Private Cloud kunnen de voordelen van een eigen bedrijfsnetwerk met de voordelen van cloud computing gecombineerd worden omdat de provider specifieke resources ter beschikking stelt. De term "private cloud" kan bovendien wel tot misverstanden leiden, aangezien het privé-gegevens en toepassingen suggereert. Het is meer opportuun om te spreken van "dedicated Clouds" of "Enterprise Cloud Services". Hierbij bestaat een fysieke scheiding tussen de resources van de verschillende klant-gegevens. Applicaties van meerdere klanten worden niet op eenzelfde server bewaard. Klanten weten altijd waar hun data opgeslagen is en kunnen gemakkelijk hun individuele behoeften invullen.

Aangezien Security bij private cloud voor bedrijven transparant is, kunnen klanten en providers samen een securityniveau afspreken. Bij publieke cloud is dit onmogelijk, aangezien in dit geval de provider een standaard security model bepaalt, dat voor alle gebruikers geldt.

Het volgende voorbeeld illustreert dit probleem. Om toegang te krijgen tot de uitbestede diensten, dient men normaalgezien beveiligde codes aan te geven. Indien de klant bij het implementeren van een publieke cloud service geen technische of organisatorische controles vereist, kunnen deze codes door hackers gekraakt worden. Zelfs als de service complexe wachtwoorden vereist en een beveiligde verbinding ter beschikking stelt, loopt de volledige veiligheidsketen risico en komen de gegevens van andere gebruikers ook in gevaar. Het risico neemt toe naar gelang het aantal gebruikers van publieke cloud services toeneemt.

Private of Enterprise cloud bieden hier een veel hoger beveiligingsniveau aan, maar kunnen het kostenvoordeel van de publieke cloud niet evenaren. Voor veel gebruikers gaat het meer om de winst in flexibiliteit en schaalbaarheid, dan om de kosten. Het beveiligingsniveau wordt hier aangepast aan de respectievelijke eisen van de klant. De cloud-klanten moeten wel een duidelijk beeld hebben van het gewenste resultaat met de systemen en de risico's die hieraan verbonden zijn. Op grond hiervan kunnen bijhorende controles en rapportages geïmplementeerd worden en de juiste certificeringen gerealiseerd worden. Bij Enterprise Cloud Computing gaat het om een individuele oplossing, die sterk afhangt van de nauwe samenwerking tussen de klant en de dienstverlener en waarbij van de dienstverlener verwacht wordt dat ze de bedrijfsprocessen van de klant op de juiste wijze beheert.

Diverse dienstverleners, zoals Easynet bijvoorbeeld, zijn gecertificeerd volgens de internationale informatiebeveiliging ISO 27001 en ISO 9001 op het gebied van kwaliteitsmanagement, samenwerking met de klant en het uitvoeren van audits. Andere certificeringen die van toepassing zijn in de cloud omgeving zijn bijvoorbeeld: ISAE3402 of SSAE16. Deze certificeringen zijn essentieel als het gaat om zeer bedrijfskritische gegevens, zoals het verwerken van creditcardgegevens. Wat de private cloud toelaat bedrijfskritische opdrachten uit te voeren is dus de fysieke scheiding tussen de resources van de verschillende klanten.

#### 4. Het belang van het netwerk

Uit een eerder dit jaar gehouden onderzoek onder CIO's bleek dat, terwijl de helft van plan was om hun investeringen in cloud computing te verhogen, amper een op de vijf hun netwerk ziet als een cruciaal element bij het formuleren van de Cloud-strategie. Dit impliceert dat bedrijven niet voldoende in detail nadenken wat de implicaties van Cloud inhouden en welk effect deze hebben op het netwerk. Aangezien de data die eerder was beperkt tot de LAN (Local Area Network) plotseling het bedrijfsnetwerk doorkruist, en zelfs het openbare internet, zullen er grote spanningen ontstaan op het netwerk. Dit zal ertoe leiden dat eindgebruikers grote prestatie problemen kunnen ervaren voor relatief alledaagse taken.

Justin Fielder, CTO bij Easynet Global Services: "Ik ben ervan overtuigd dat netwerkexperts een belangrijke rol spelen in het laten zien hoe noodplanning en een 'intelligent' netwerk design kunnen bijdragen aan het beperken van een aantal van deze problemen".

De Cloud lost, dankzij de zeer gedistribueerde en gevirtualiseerde structuur, een groot aantal continuïteitsproblemen op. Echter, de afhankelijkheid van het netwerk speelt nog een te grote rol als single point of failure; dat wil zeggen dat er niet veel nodig is om een regionaal kantoor volledig van diensten af te sluiten. In de meeste gevallen zou een redundante verbinding (op basis van ADSL of ISDN) een voor de hand liggend antwoord zijn om de connectiviteit te garanderen, maar zou het kunnen omgaan met de Cloud en alles wat over het netwerk loopt, zoals telefonie?

Met de wijd verspreide toepassing van cloud-gebaseerde diensten zien we een stijging in de vraag naar nieuwe producten die een aanvulling zijn op de bestaande business, niet alleen in de onderliggende netwerktechnologie (zoals overgaan naar goedkopere glasvezelverbindingen), maar ook op de manier waarop dubbel uitgevoerde bandbreedte wordt gebruikt.

Een benadering die veel bedrijven kiezen om deze uitdaging op te lossen, is wat we noemen 'active-active'. Het grootste voordeel van deze nieuwe oplossing is dat het gebaseerd is op twee afzonderlijke access lijnen die samenwerken onder normale omstandigheden; een lijn die prioriteit geeft aan spraak-, intranet, ERP etc. en een tweede lijn die niet-bedrijf kritisch verkeer zoals surfen op het web, sociale media, extranet etc. afhandelt. Het belangrijkste is dat wanneer een primaire of secundaire lijn uitvalt, het bedrijf over een MPLS-netwerk dient te beschikken dat slim genoeg is om het bedrijf kritische verkeer voorrang te geven.

Dit vereist niet alleen een oplettende dienstverlener die beschikt over de juiste controle-instrumenten om te bepalen wanneer een lijn uitvalt, maar ook een MPLS-netwerk dat slim genoeg is om dataverkeer voorrang te geven. Deze mate van verfijning dient zorgvuldig te worden afgewogen, omdat niet alle 'communicatie' gelijk is.

Echter, dit wil niet zeggen dat business continuïteitsmanagement de sleutel tot de oplossing is voor bedrijven die zich bezighouden met de Cloud problematiek. Cloud computing vraagt nieuwe eisen aan het netwerk en in veel gevallen zal de bestaande infrastructuur van het bedrijf niet in staat zijn om aan deze nieuwe eisen te voldoen. Gezien de verschuiving van een lokaal gehoste data omgeving naar

hosting bij externe datacenters, is het redelijkerwijze te veronderstellen dat de service levels, de prestaties en de bandbreedte van een bedrijfsnetwerk wellicht niet in staat zijn om aan de gewenste eisen te voldoen.

We weten dat het ontwerpen van een MPLS netwerk dat moet voldoen aan de prestatie criteria met betrekking tot de belangrijkste zakelijke toepassingen van een bedrijf, terwijl het ondertussen de dagelijkse behoeften van de eindgebruikers moet ondersteunen, geen sinecure is. Men kan zeker geen beslissingen nemen op basis van de top-line claims van service providers. Het is cruciaal dat de dienstverlener de tijd en moeite neemt en krijgt om te begrijpen waar uw data zich fysiek bevindt en hoe het beweegt over het netwerk, alvorens een geschikt netwerk design te adviseren. De markt wordt overspoeld met aanbieders die MPLS-oplossingen aanbieden die ogenschijnlijk eenvoudig zijn. Geen van beide is waar als u een Cloud-strategie wenst die u een voordeel oplevert.

De tijd van de 'fit and forget' MPLS-netwerken is nu voorbij. Er moet een oplossing worden gekozen, die over een extra niveau intelligentie beschikt; wat wij noemen SMART MPLS. Wanneer er een storing optreedt zal het netwerk automatisch de bron van het probleem opsporen en corrigerende maatregelen nemen. Dit zorgt voor stabiele verbindingen, services kunnen snel omgeschakeld worden en eindgebruikers worden niet beïnvloed.

Bovenop deze SMART MPLS zijn eenvoudige configuraties te maken voor optimale prestaties, met de extra voordelen van de lage investeringen en het gemak van het managen hiervan. Het belangrijkste verschil tussen MPLS en SMART MPLS is dat in plaats van het MPLS-netwerk, dat IP-verkeer begrijpt en prioritiseert, het in staat is om te begrijpen, rapporteren en, belangrijker nog, het in staat is om te allen tijde te reageren op de toepassingen die over door het netwerk lopen.

Justin Fielder vervolgt: "De Cloud vraagt steeds hogere eisen van het bedrijfsnetwerk en bedrijven verwachten dat hun netwerk deze uitdaging aankan. Zonder de ingebouwde flexibiliteit van de 'active-active' diensten, of de intelligentie van SMART MPLS, is er een reëel risico dat de eerste ervaringen van bedrijven met Cloud een negatieve is. Ik hoop dat ik ongelijk krijg".

### **Over Easynet Global Services**

Easynet Global Services is een wereldwijde aanbieder van managed network-, hosting- en integratiediensten, waaronder [Telepresence](#), voor grootzakelijke klanten. Het bedrijf heeft klanten in vijftig landen, waaronder Via Michelin, Newscorp, Transport for London, EDF, SAGE, Q-Park en Bridgestone. LDC (Lloyds TSB Development Capital) is de privé-investeerderstak van Lloyds Banking Group en samen met het managementteam honderd procent eigenaar van Easynet. Meer informatie is te vinden op [www.easynet.com](http://www.easynet.com) en Easynet is ook te volgen via [@easynet](#) en [Easynet | LinkedIn](#).

### **PR Contact**

Laurence Van Doosselaere

Tel: +32 (0)2 402 37 58

E-mail: [Laurence.VanDoosselaere@easynet.com](mailto:Laurence.VanDoosselaere@easynet.com)