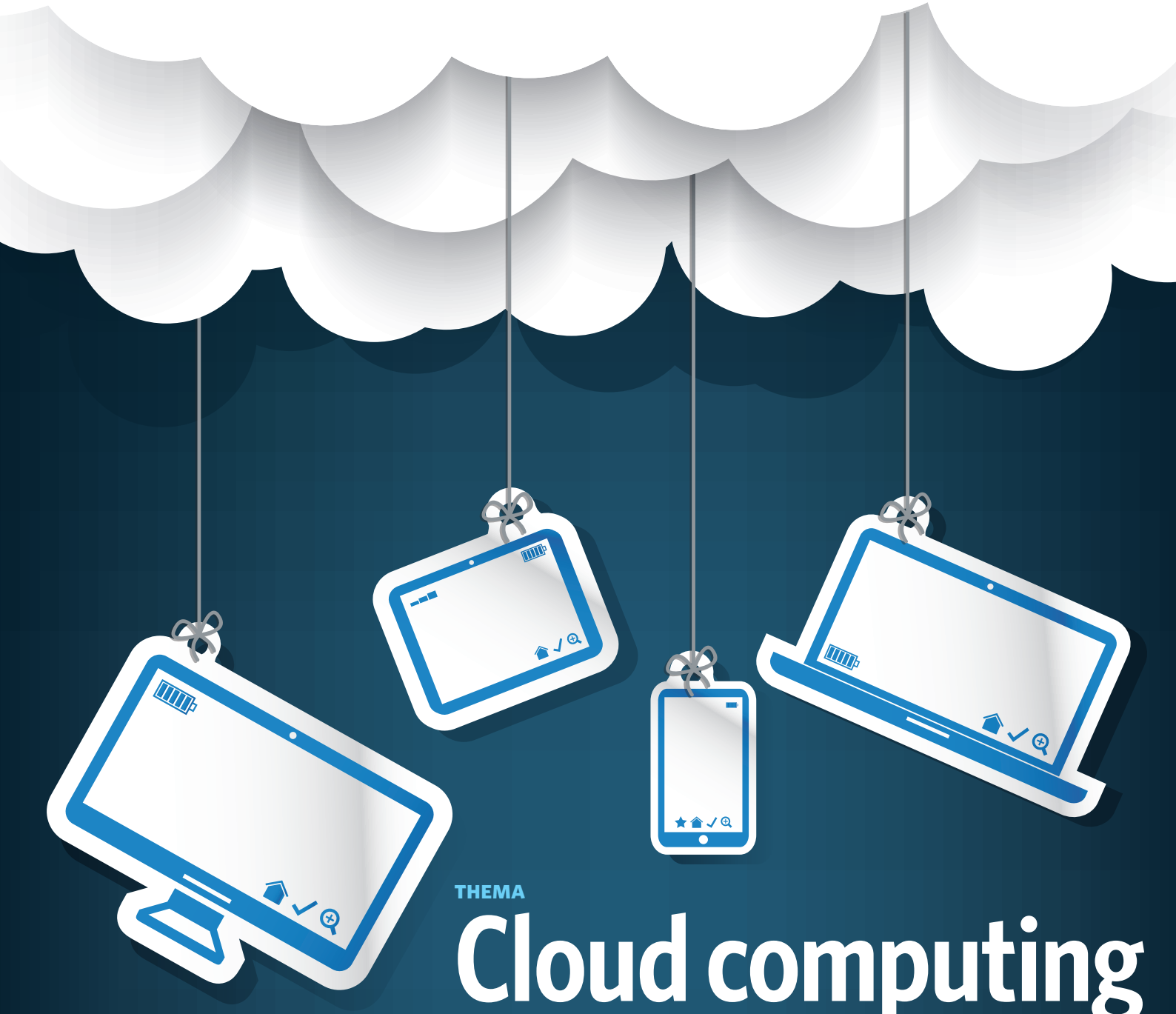
COMPUTABLE

WHITEPAPER - NOVEMBER 2014

ONDERZOEK



THEMA

Cloud computing

ONDERZOEK

Beveiliging krijgt met cloud verdiende aandacht

INTERVIEW

Hans Bos, Microsoft

INTERVIEW

Gijsbert Janssen van Doorn, Nexenta Systems

COMPUTABLE

INHOUD

ONDERZOEK

Beveiliging krijgt met cloud verdiende aandacht

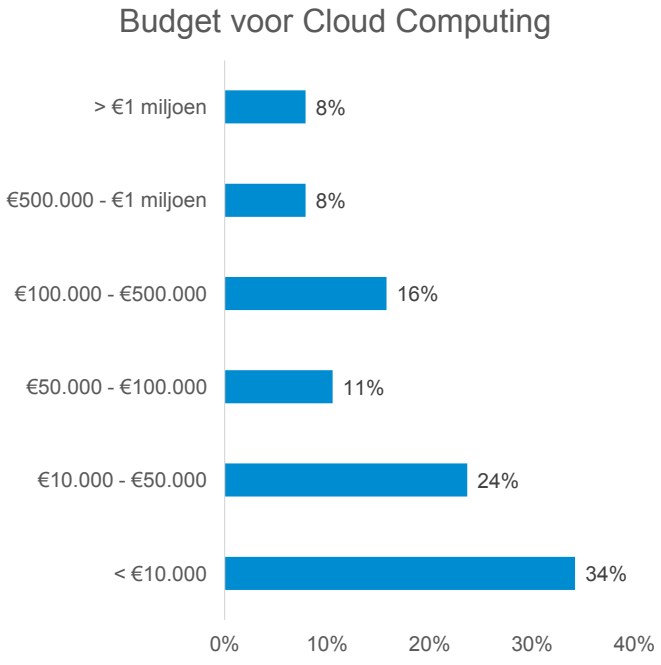
Beveiliging van geautomatiseerde systemen staat hoog op de agenda bij zowel it- als algemeen management. De bedrijfsbrede toename van mobiliteit en het gebruik van cloud-toepassingen dragen hier zeker aan bij. Daarbij komt dat tegenwoordig verlies van gegevens niet alleen direct financiële consequenties heeft, maar ook imagoschade. Desondanks neemt het gebruik van clouddiensten nog steeds toe. Evenals de nadruk op beveiliging.

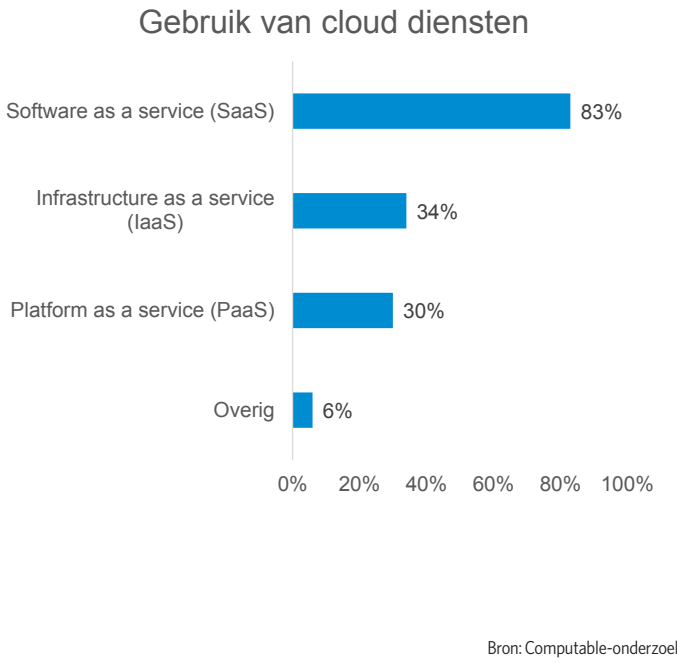
Tekst: Teus Molenaar

Februari 2014 maakte Rightscale, een Amerikaanse leverancier van een cloud portfolio managementsysteem, het derde onderzoek naar cloud-ontwikkelingen bekend. Jaarlijks doet dit bedrijf onderzoek naar hoe organisaties clouddiensten gebruiken. In 2014 bracht de onderneming haar derde 'State of the Cloud Report' uit. Hieruit blijkt dat 94 procent van de ondervraagde organisaties actief clouddiensten gebruikt of experimenteert met een infrastructure-as-a-service (IaaS). 87 Procent gebruikt een public cloud, terwijl de meesten naar een hybride cloud willen. 74 procent van de ondernemingen heeft een hybride cloud-strategie, en meer dan de helft gebruikt al zowel de publieke als de private cloud.

Tegelijk blijkt dat een gebrek aan regelgeving rond het gebruik van clouddiensten de acceptatie ervan hindert. Minder dan een derde van de organisaties heeft zwart op wit staan welke clouds gebruikt mogen worden, hoe om te gaan met disaster recovery en het beheer van de kosten. Dat zijn essentiële aspecten van een goed cloud-beheer.

De beveiligingsvraagstukken rond cloudgebruik achten de ondervraagden van minder belang dan voorheen. Dat geldt zowel voor de beginnende cloud-gebruikers als voor de ondernemingen die hier al langer ervaring mee hebben.





Bron: Computable-onderzoek

Het is een Amerikaans onderzoek. In het land van Amazon, Salesforce.com, HP, IBM, Microsoft en andere cloud-aanbieders loopt de acceptatie van cloud computing voor op bijvoorbeeld Nederland. Niettemin zijn de uitkomsten van de studie ook indicatief voor de Nederlandse situatie.

STEVIGE UITDAGING

Uit het onderzoek van Computable/Jaarbeurs blijkt evenwel dat 65 procent van de Nederlandse ondervraagden informatiebeveiliging als een stevige uitdaging beschouwt. Gevolgd door de bescherming van persoonsgegevens (48 procent). Eigenlijk zijn dit twee kanten van dezelfde medaille: het zorgvuldig omgaan met gegevens. Niettemin zit ook in Nederland het cloud-gebruik in de lift.

Na alle onthullingen rond NSA, dataverlies bij bijvoorbeeld eBay, is het logisch dat dit onderwerp op de agenda staat van it-beslissers. Uit het Risk Based Security's Data Breach QuickView blijkt dat de ernst van dataverlies toeneemt en dat bepaalde organisaties vaker met incidenten te maken hebben dan andere (kijk op www.riskbasedsecurity.com).

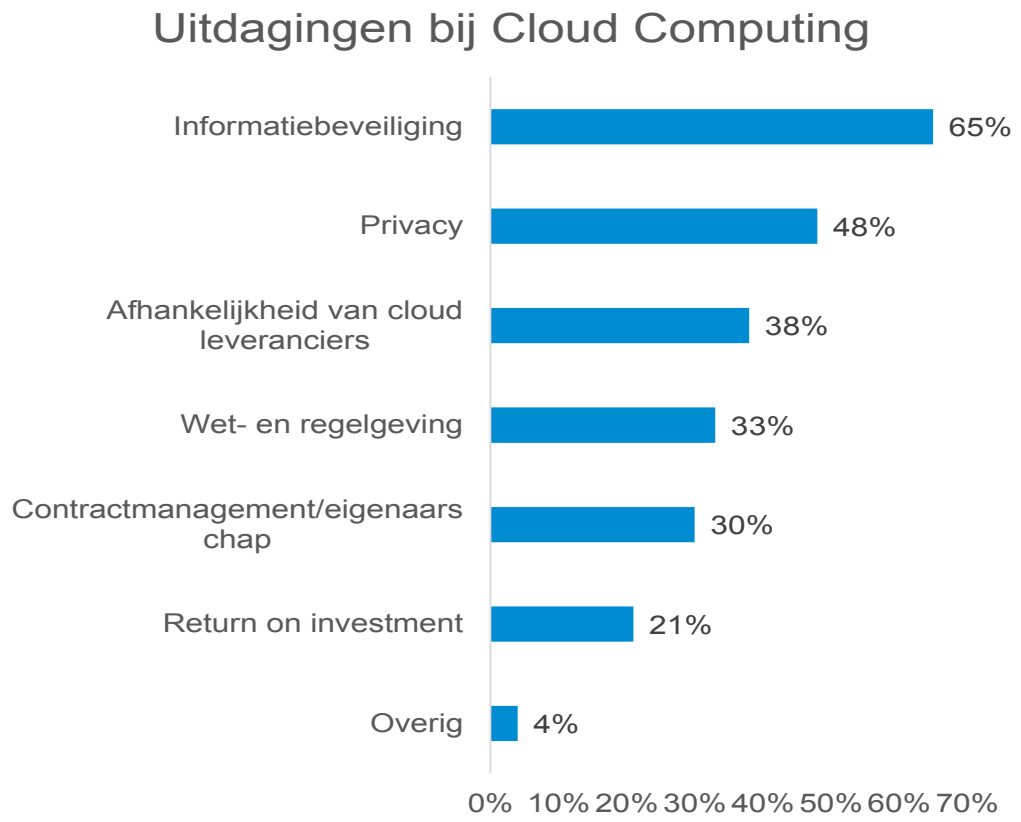
Wat maar aantoont dat beveiliging on premise net zo'n grote zorg is als bij het gebruik van cloud diensten. Velen vrezen dat het uit handen geven van bedrijfsgegevens of (een deel van) een bedrijfsproces extra risico's met zich meebrengt. Dat valt echter nog te bezien, want zeg nou zelf: is het in de eigen computerruimte of datacenter nou zoveel beter geregeld dan bij een cloud-provider?

Vooral kleinere en middelgrote bedrijven zullen menen dat de dienstverlener het beter heeft geregeld dan zij dat zelf kunnen doen en tegen lagere kosten. De bedreigingen worden steeds complexer; je hebt schaars, gespecialiseerd personeel nodig om ze te weerstaan. Een concentratie van it-diensten bij cloud-leveranciers adresseert minstens dit schaarsteprobleem.

Maar er is meer: de cloud-providers zijn zich ervan bewust dat zij een naam hoog te houden hebben. Ook al blijft de organisatie altijd zelf verantwoordelijk voor haar gegevens - waar ze ook zijn opgeslagen of worden gemanipuleerd - de cloud-dienstverlener zal er alles aan doen dataverlies tegen te gaan. Tenslotte is dat hun core business. Een dienstverlener die er onzorgvuldig mee omspringt en in het nieuws komt met incidenten, krijgt het moeilijk zijn klanten te behouden, laat staan nieuwe te werven.

AUDITS NALEZEN

Hun kantoren hangen vol met certificaten van ISO, NEN, Europa (de aanstaande EU General Data Protection Regulation) en dergelijke. Sterker nog: zij hebben afspraken gemaakt met onafhankelijke accountancykantoren om te controleren of zij wel alle regels naleven die opgenomen zijn in die certificaten. Klanten kunnen die rapporten maandelijks inzien.



Bron: Computable-onderzoek

Toezichthouders op de financiële sector staan het gebruik van clouddiensten toe, mits zij te allen tijde toegang hebben tot de gegevens om hun controletaken te kunnen uitoefenen. Hiertoe hebben zij afspraken gemaakt met de cloud-dienstverleners.

Over het algemeen hebben de cloud-providers op beveiligingsgebied hun zaakjes goed voor elkaar. Dat neemt niet weg dat het goed is te constateren dat security een belangrijk aspect is bij het uitbesteden van bedrijfsgegeven en bedrijfsprocessen (zoals personeelszaken). Dat moet je 'de cloud' nageven: beveiliging is een belangrijk onderwerp geworden. Dat had het natuurlijk al lang moeten zijn - tot op board-niveau - maar nu de gegevens de deur uit gaan, staat het ineens wel op de agenda.

GEEN IT-FEESTJE

Toch is de neiging bij het algemeen management dan nog groot om beveiliging af te doen als een it-onderwerp. Laat de cio of de it-manager zich maar hierover buigen. Agendapunt afgehamerd: it zorgt voor een goede beveiliging. Maar dan begaat de directie een grote fout, want beveiliging is een zaak van bestuurders. De business immers weet welke data welke beveiliging nodig hebben. De business weet welke recovery time objective (rto) acceptabel is, want in één adem hoort bij security een disaster recovery plan. Daar moet je afspraken over maken met de cloud-dienstverlener. Hoe lang duurt het voordat - in geval van een brand, overstroming of iets dergelijks - het bedrijf zijn complete omgeving weer beschikbaar heeft? Dat is inclusief alle gebruikersrechten.

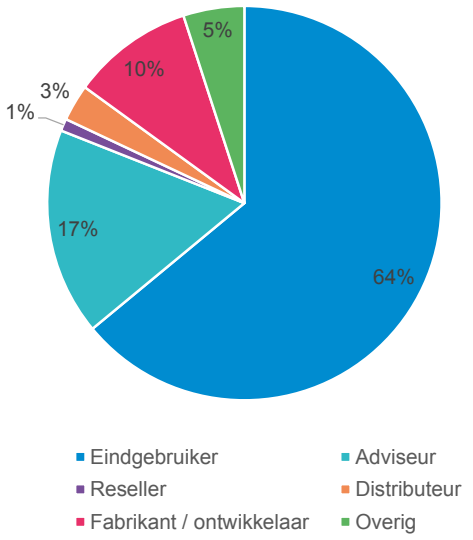
EXIT-STRATEGIE

Dan gaat het om bedrijfsprocessen. Daar dient het algemeen management uitspraken over te doen. Trouwens ook over een exit strategy. Want de providers hebben het altijd wel over pay per use en flexibel computeren; alles per maand opzegbaar, maar is dat wel zo? Is de complete dataset, inclusief de metadata, geschikt om bij een andere provider onder te brengen zonder dat de bedrijfsvoering daar iets van merkt? Vendor lock in, die wij zo goed kenden uit de software-industrie, ligt nu op de loer bij cloud computing. Hoe lang doet de provider erover om alle bedrijfsgegevens bruikbaar beschikbaar te hebben in geval het contract afloopt en niet wordt verlengd? Daar zou het gesprek over moeten gaan, nadat eerst is gecontroleerd dat de provider zijn beveiligings/privacy-certificaten heeft en laat controleren

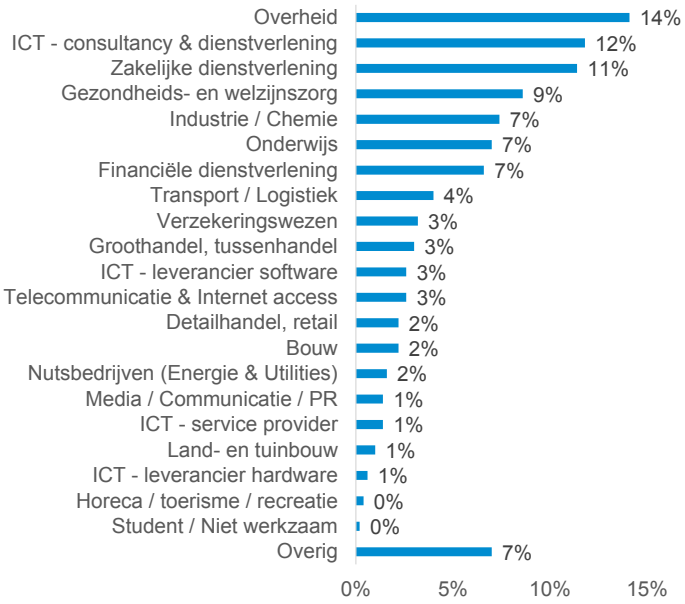
OVER HET ONDERZOEK

Aan het onderzoek van Jaarbeurs en Computable over cloud computing deden begin september 2014 502 personen mee. De focus lag op eindgebruikers en adviseurs, waarbij leveranciers zoveel als mogelijk buiten beschouwing zijn gelaten. Van het profiel van de respondenten zijn sector, functie, rol, bedrijfsgrootte en beslisniveau bekend.

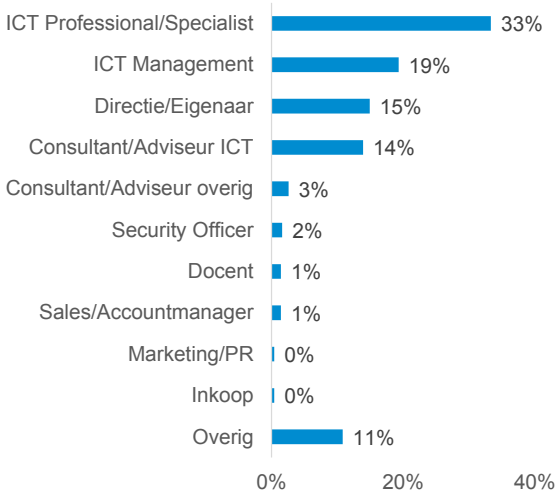
Rol bedrijf



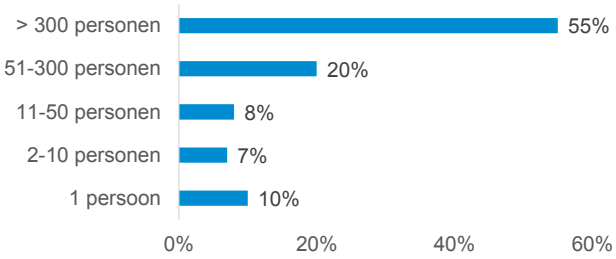
Sector



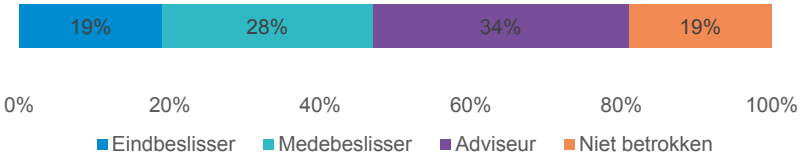
Functie



Bedrijfsgrootte



Beslisniveau



INTERVIEW

Hans Bos, national technology officer bij Microsoft Nederland

Cloud is vooral flexibiliteit

Voor cloud computing zijn verschillende definities te geven. Die van de International Organization for Standardization (ISO) kom je het vaakst tegen. Maar bij Microsoft gaat het er niet zozeer om wat cloud computing is, maar wat het de organisaties te bieden heeft. Dan gaat het vooral om flexibiliteit in een beveiligde omgeving. De cloud helpt bedrijven zich op een kostenefficiënte manier snel aan te passen aan veranderingen in de bedrijfsvoering.

De ISO en International Electrotechnical Commission (IEC) trekken samen op als het gaat om de beschrijving van cloud computing. In 2014 hebben ze de ISO/IEC 17788 gepubliceerd. Deze norm beschrijft wat wij onder het begrip dienen te verstaan. Het geeft onder meer de architectuur weer van het computernetwerk dat de diensten levert. Maar veel afnemers van die diensten zal het niet veel uitmaken hoe een en ander technisch in elkaar steekt. Zij willen weten welke voordelen zij kunnen hebben bij cloud computing. Dat is ook de visie van Microsoft: wat brengt cloud computing.

In de eerste plaats flexibiliteit. Het gaat bij deze vorm van automatisering om de verbindingen tussen systemen onderling en tussen mensen. Het belangrijkst is dat je overal toegang hebt tot de gegevens waarmee je wilt werken. Het maakt niet uit waar je bent en wat voor apparaat je gebruikt (een desktop, notebook, tablet of smartphone), de gegevens zijn altijd beschikbaar, 24 uur per dag en zeven dagen per week. De enige voorwaarde is dat je een werkende internetverbinding hebt.

De flexibiliteit zien we ook terug in het gebruik van de rekenkracht bij de cloud-aanbieder. Je benut alleen wat je nodig hebt, op het moment dat je dat nodig hebt. Dat maakt het kostenaspect van automatisering flexibel: betalen voor wat je gebruikt en op- en afschalen wanneer dat nodig is. Bijvoorbeeld wanneer een bedrijf een intensieve consumentencampagne voert en wil analyseren hoe dat verloopt. In dat geval kun je alleen voor die periode rekenkracht inhuren. Het kapitaliseringsmodel van automatisering gaat van Capex naar Opex.

Over het algemeen is cloud computing de goedkoopste manier van het inzetten van informatietechnologie.

KWALITEIT

Microsoft ziet cloud computing eveneens als een middel tot kwaliteitsverbetering van de geautomatiseerde systemen bij organisaties. Vaak hebben bedrijven binnen hun eigen datacenters of computerruimtes nog oudere infrastructuren en/of oudere computerapparatuur. Veelal is het een mengsel van 'oud en nieuw'. Dat kan performance problemen opleveren. Of storingen waardoor de beschikbaarheid van de systemen voor de eindgebruikers afneemt.

Microsoft heeft de afgelopen jaren miljarden euro's besteed aan de bouw van moderne datacenters; en zal dat blijven doen. Het motto van het softwarehuis is: 'cloud first, mobile first'. Bij alle inspanningen van het bedrijf geldt dat de uitkomst in eerste instantie geschikt moet zijn voor cloud en mobile computing.

HANS BOS

‘Eigenlijk moet elke onderneming de beveiliging van zijn gegevens ter discussie stellen. In het verleden is dit te weinig gebeurd. Maar het afnemen van cloud-diensten is een mooie gelegenheid om dit onderwerp onder de loep te nemen’

DATACLASSIFICATIE

De kwaliteit op het gebied van privacy en beveiliging neemt ook toe bij het gebruik van de cloud diensten van Microsoft. De toename van beveiligings- en privacykwaliteit heeft onder meer te maken met dataclassificatie. Het gebruik van cloud computing zal meestal in een hybride-omgeving plaats vinden. Een deel van de gegevens wil de eigenaar in het eigen datacenter houden, een deel in de public-cloud (zoals de Azure-diensten van Microsoft) of in de private-cloud, waarbij een deel binnen het datacenter van Microsoft specifiek voor die klant is gereserveerd.

Om te weten welk platform je wilt gebruiken voor welke data, is het nodig die gegevens de classificeren. Ook hiervoor kun je een beroep doen op de it-dienstverlener en zijn partners.

Het gaat overigens niet alleen om de gegevens (verwerking), maar ook om de processen. Welke processen wil je waar afhandelen? Bij de classificatie kun je aangeven welke gebruikers toegang hebben tot welk platform. Met dit alles neemt de kwaliteit van de bescherming van persoonsgegevens en beveiliging toe.

DISCUSSIE

Beveiliging neemt een aparte positie in. Over dit onderwerp heeft Microsoft diverse white papers beschikbaar gesteld. Op diverse niveaus is security geregeld. Natuurlijk op het vlak van de infrastructuur met firewalls, geharde servers, ids- en ips-systemen, toegangscontrolesystemen in het datacenter, tot aan het controleren van de achtergrond van het personeel dat in het datacenter werkt.

Voor klanten heeft Microsoft rapportages beschikbaar over beveiliging tot op het diepste niveau. Natuurlijk voldoet de onderneming aan de Safe Harbor-principes en heeft zij een ISO 27001 certificaat. Deze norm legt de regels vast voor beveiliging van informatiesystemen.

Het bedrijf gaat nog een stap verder en voldoet aan de ISAE3402, een norm voor rapportages die wettelijk verplicht is gesteld voor banken en andere financiële instellingen. Het rapport geeft inzicht in welke processen er zijn binnen het datacenter, de beheersing ervan en de beveiliging ervan. Klanten krijgen inzage in deze rapportages. Daarbij komt dat Microsoft de ISAE3402-rapportages laat controleren door een onafhankelijke, derde partij: Deloitte. Ook die bevindingen zijn beschikbaar voor klanten.

Eigenlijk moet elke onderneming de beveiliging van zijn gegevens ter discussie stellen. In het verleden is dit te weinig gebeurd. Maar het afnemen van cloud-diensten is een mooie gelegenheid om dit onderwerp onder de loep te nemen.

VERTROUWEN

Ook al brengt een organisatie (een deel van) haar gegevens onder bij een cloud-dienstverlener, zij blijft altijd eigenaar van de data en is dus wettelijk gezien verantwoordelijk voor die gegevens. Gezien de voordelen die cloud computing biedt (flexibiliteit, kostenbeheersing en kwaliteitsverbetering) gaan toch veel bedrijven over op deze vorm van automatisering. Het is dan een kwestie van vertrouwen dat Microsoft zich als een goed beheerder opstelt. De Nederlandsche Bank heeft, zoals hij het zelf formuleert, ‘samen met Microsoft’een barrière voor de adoptie van cloud weggenomen. Dit gebeurt door een contractformulering op te stellen waarmee DNB zijn recht op toezicht onbeperkt kan effectueren; ook bij/in Microsofts cloud.

Financiële instellingen zijn/blijven zelf verantwoordelijk om voor hen geldende risico’s te adresseren.

Het is een veelgehoorde misvatting dat alle gegevens Nederland niet mogen verlaten. Dit is echter niet in wet- en regelgeving terug te vinden. Alleen bestanden die het stempel ‘staatsgeheim’ dragen moeten in ons land blijven.

Microsoft heeft een datacenter in Dublin, met een mirror-site in Amsterdam voor back-up & recovery. Over het algemeen - gelet op het voorgaande over data-, proces- en gebruikerclassificaties - kan een organisatie zonder belemmeringen gebruik maken van de cloud-diensten van dit softwarehuis. Dat neemt niet weg dat elke organisatie pas aan cloud-computing moet gaan denken als zij een risico-managementplan heeft opgesteld en ingericht. Toezichthoudende instanties als CBP en DNB willen dat de cloud-gebruiker goed heeft nagedacht over eventuele risico’s, die risico’s heeft benoemd en kan adresseren (beperken, oplossen of acceptreren).

INTERVIEW

Gijsbert Janssen van Doorn, sales engineer bij Nexenta Systems

Cloud vraagt om software defined storage

Cloud computing heeft veel voordelen, zoals veelal lagere kosten, flexibiliteit en geen gebrek aan deskundig personeel. De kurk waarop deze vorm van automatisering drijft neemt in toenemende mate de vorm aan van software defined storage (sds). Netflix, Google, Amazon, noem maar op. Ondernemingen overwegen nu ook sds toe te passen om de betaalbare flexibiliteit te verkrijgen.

Cloud computing (een paraplubegrip) is feitelijk niets meer dan een nieuw leveringsmodel van informatietechnologie. De 'grote jongens' (denk aan Spotify en Netflix) zouden hun diensten niet kunnen aanbieden zonder de cloud-eigenschappen: ongebreidelde schaalbaarheid, self service, pay per use. Die eigenschappen zijn ook voor bedrijven en (overheids) organisaties uiterst nuttig, vandaar dat vele met een schuin oog naar deze architectuur kijken, omdat zij snel willen kunnen inspelen op veranderingen in de markt of politieke besluitvorming.

Maar er komt nog wel wat bij kijken om de organisatie zo ver te krijgen. Allereerst moet het personeel worden bij/omgeschoold om alle mogelijkheden te benutten van een 'open' cloud structuur; veelal in een hybride vorm (deels on premise en deels bij een cloud provider). Maar ook de applicaties moeten 'cloud bewust' zijn. Vooral bij de public cloud moeten zij kunnen omgaan met onzekerheden. Want in de eerste plaats weten zij niet wat de performance van het systeem zal zijn; noch weten zij wat de beschikbaarheid is van het systeem. In de private cloud is het systeem af te stemmen op de wensen van de gebruiker.

AVAILIBILITY-ZONES

De cloud-providers, zoals Amazon, werken met zogenoemde availibility zones. De software zorgt ervoor dat altijd storage and compute beschikbaar is, ook al is het aanbod niet bekend. Een voorbeeld maakt dit duidelijk. Enige tijd geleden heeft Amazon, de grootste cloud provider ter wereld, zijn hypervisors opgewaardeerd. Ook bij een gigant - of misschien: juist – als dit Amerikaanse bedrijf gaat dat niet zonder slag of stoot. Er waren op een gegeven moment 218 database servers niet beschikbaar. Netflix, de online video-dienst, gebruikt het Amazon-platform, maar heeft er niets van gemerkt dat de cloud provider problemen had met een aantal van zijn servers.

Ook Microsoft zoekt het in deze richting met zijn beschikbaarheidsmodel door van databases meerdere kopieën te hebben op meerdere, verschillende plaatsen. Voorheen werd dit gedaan met clustering software, maar de kostendaling van hardware, brengt availibility zones als eenvoudiger te beheren alternatief naar voren.

Cloud-providers gebruiken deze architectuur, maar het sijpelt nu ook door naar grote en zelfs kleinere ondernemingen.

GIJSBERT JANSSEN VAN DOORN

‘Het gebruik van open standaarden - ook op het gebied van storage - betekent dat geen ‘cloud lock-in’ dreigt. Het betekent ook dat eenvoudiger gebruik is te maken van een hybride situatie met eigen datacenter en meerdere cloud providers.’

ALS EEN VLAN

Voor een veilige cloud-oplossing is een parallel te trekken met lan’s (local area network) die evolueerde in vlan’s (virtual lan) om ervoor te zorgen dat data hun weg vervolgen binnen een afgeschermde omgeving. Sds werkt op een zelfde manier en maakt het mogelijk opslagruimte naar behoefte toe te voegen onafhankelijk van het hardwareplatform.

Het uitbreiden van legacy opslagsystemen vergt veel installatie- en configuratiewerk. Tevens is het vaak nodig weken, soms maanden te wachten tot ‘het ijzer’ wordt geleverd. Je praat al gauw over honderdduizenden euro’s om de opslagcapaciteit uit te breiden. Bij sdds gaat het om duizenden euro’s.

Je moet natuurlijk nog wel steeds het vloerplan opstellen, koeling en elektriciteit regelen, maar je kunt al wel tevoren de netwerkbekabeling, de stroomkabels en de fysieke racks installeren. Als extra opslag nodig is, is het gewoon een kwestie van een nieuwe server inschuiven.

OBJECTEN

De trend is dat applicaties het beste weten wat zij met de data moeten doen. Vooral het analyseren van die data. Dat betekent dat de metadata steeds belangrijker zijn; die geven immers aan wat die gegevens voorstellen. Door de enorme en wisselende omvang van gegevens die moeten worden opgeslagen, is het handiger te werken met objecten in plaats van file systems. Google Drive, Dropbox en dergelijke werken alle met objecten. Een file system is immers van nature gelimiteerd. Als er meer opslag nodig is, moet je een tweede file system aanmaken. Dat betekent dat je het in de gaten moet houden en handelingen moet verrichten. Dat kost tijd en geld.

Met objecten is dat niet nodig. Sds werkt dan ook veelal met objecten die met metadata (waar ze zijn opgeslagen, welk bestandstype, en dergelijke) worden opgeslagen. Het voordeel is dat het analyseren bij wijze van spreken meteen al kan beginnen; en dat ze sneller zijn op te vragen.

Wel is het dan nodig de juiste api’s te gebruiken. Want een applicatie heeft geen idee hoeveel ruimte beschikbaar is op een schijf of flash-geheugen. Dat zit allemaal verwerkt in de api’s. Die beschikken over de definities die nodig zijn voor de juiste system calls of service routines die toegang verschaffen tot de lees/schrijf schijven, het versturen van berichtjes naar andere applicaties, enzovoorts. Overigens werkt sda niet per definitie met ‘object’, maar ook met tradiotionele file/block systemen. Eigenlijk is sds een paraplubegrip en omschrijft het meer het ‘leveringmodel’ dan de technologie die het gebruikt.

VRIJHEID

Amazon werkt ook met object-storage. Dit doet het bedrijf met zijn webservice S3 (Simple Storage Service), die het bedrijf publiek heeft vrijgegeven. Het is belangrijk na te gaan of de opslagstructuur open standaarden ondersteunt. Net zoals het belangrijk is na te gaan welke api’s beschikbaar zijn (zie eerder in dit artikel).

Sds betekent de vrijheid om systemen kostenefficiënt op- en af te schalen. En vrijheid gaat gepaard met het gebruik van open standaarden op elk niveau van de opslagstructuur.

In toenemende mate tonen organisaties belangstelling voor het werken met object-storage, omdat zij de voordelen ervan inzien. Het betekent wel dat een plan moet worden opgesteld om naar de nieuwe situatie te komen. Zo moet in kaart worden gebracht welke applicaties hier geschikt voor zijn en welke niet.

EXIT-STRATEGIE

Het gebruik van open standaarden - ook op het gebied van storage - betekent dat geen ‘cloud lock-in’ dreigt. Het betekent ook dat eenvoudiger gebruik is te maken van een hybride situatie met eigen datacenter en meerdere cloud-providers.

Daarom is het altijd belangrijk bij de gesprekken met een cloud dienstverlener meteen een exit strategie af te spreken. Dat voelt soms lastig, omdat je net bezig bent een relatie aan te gaan, maar het kan heel wat ellende in de toekomst voorkomen. Dan is het nuttig vast te leggen binnen hoeveel uur de complete omgeving (data en eventueel digitale werkprocessen) beschikbaar is om terug te nemen in het eigen datacenter of onder te brengen bij een andere dienstverlener.

Het gebruik van een sds-systeem vergemakkelijkt de overgang naar een andere provider. Ook hier biedt deze architectuur vrijheid.

COLOFON

Deze whitepaper over cloud computing is een uitgave van Computable, www.computable.nl

Marqit BV
Stille Veerkade 27
2512 BE Den Haag

Reacties kunt u mailen naar:
redactie@computable.nl

Hoofdredactie: Sander Hulsman
Eindredactie: Henk Boot
Vormgeving: Wonderworks, Heemstede
Teksten: Teus Molenaar
Onderzoek: Manfred Moret, Jaarbeurs
Uitgever: Roderick Wijsmuller
Marketing: Marlijn Griesheimer

Dit Computable-onderzoek over het thema cloud computing wordt mede mogelijk gemaakt door:

nexenta™ Global Leader in Software Defined Storage.

IBM®

Microsoft