CLOUD COMPUTING

de cloud in theorie en de praktijk

JEROEN HORLINGS

uitgeverij
SYCORAX

INKIJKEXEMPLAAR

ISBN:	978-94-92404-04-6
NUR:	980
Titel:	Cloud computing
Ondertitel:	De cloud in theorie en de praktijk
Trefwoorden:	cloud, cloud computing, security, sla, saas, paas, iaas, hosting, storage
Auteur:	Jeroen Horlings
Druk:	2e druk (heruitgave), mei 2016
Opmaak:	Uitgeverij Sycorax
Omslagontwerp:	Uitgeverij Sycorax

Dit is een uitgave van Uitgeverij Sycorax - www.sycorax.nl

Inhoudsopgave

1
Inleiding

Cloud computing. Wat het is en vooral niet is, is lastig in een paar zinnen uit te leggen. Dat de meeste bedrijven ermee bezig zijn, staat echter buiten kijf.

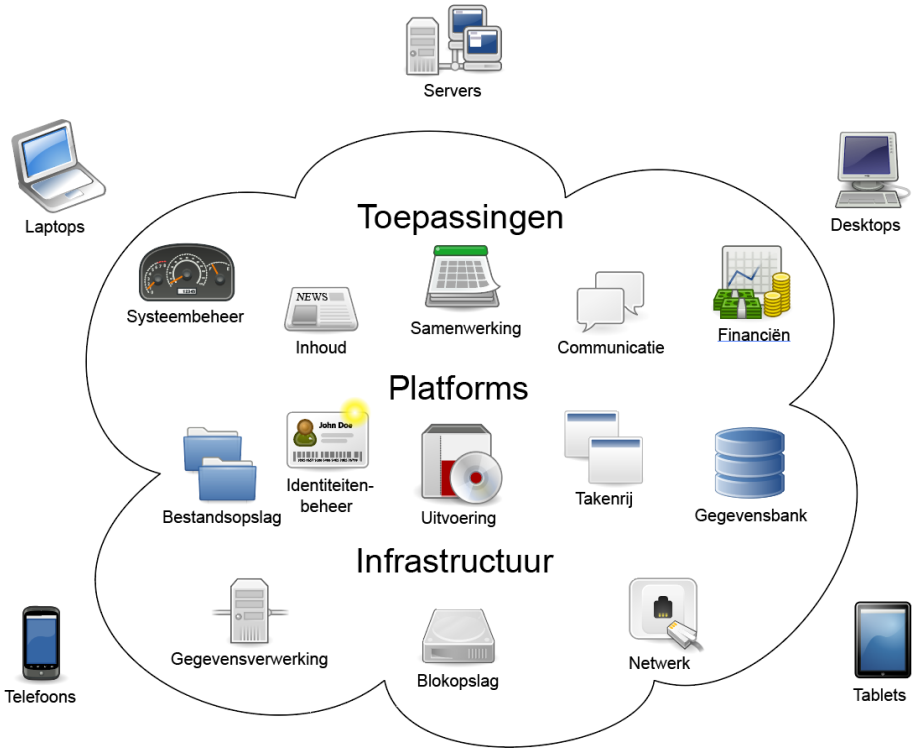
Het woord 'cloud' staat synoniem voor het internet en dankt zijn afkomst aan een wolkensymbool waarmee 'het netwerk' werd afgebeeld. Hoewel cloud dus min of meer synoniem is aan 'netwerk' en 'internet', wil dat niet zeggen dat alles wat zich via het internet afspeelt automatisch als clouddienst gekenmerkt kan worden, hoewel sommige bedrijven wel op die manier op de hype inspelen (door simpelweg het hippe woord 'cloud' aan hun portfolio toe te voegen).

Cloud computing slaat op het gebruik van online resources en niet op het hele internet. Het gaat om specifieke diensten die via het internet worden aangeboden, in plaats van traditionele oplossingen. Zoals we in de komende hoofdstukken in het boek zullen bespreken, zijn er verschillende soorten clouddiensten en ook verschillende vormen om deze te realiseren.

Inleiding

Het traditionele uitgangspunt

Een traditionele infrastructuur binnen een bedrijf gaat uit van een aantal vaste uitgangspunten. Het web wordt gebruikt om te surfen, voor e-mail en uitwisseling van bestanden en daar houdt het zo ongeveer wel mee op. De applicaties, data en rekenkracht worden geleverd vanuit de eigen datacenters. Kenmerkend voor deze infrastructuur is dat in het datacenter verschillende servers staan met ieder een eigen functie. Bijvoorbeeld een mailserver (voor het interne en externe mailverkeer), servers voor bestandsopslag



(op honderden harde schijven), tapes voor back-ups (Virtual Tape Library), databaseservers (met gegevens), webservers (voor websites), applicatieservers (voor bepaalde software) en een ftp-server (voor bestandsuitwisseling). In een traditionele omgeving werken de individuele servers van verschillende soorten applicaties en databases niet als een groep samen (en maken dus bijvoorbeeld geen gebruik van dynamische workload-verdeling). Eigenlijk heel onlogisch, want daardoor ontstaan allerlei problemen, zoals hotspots (oververhitting op bepaalde plekken) in de serverruimte doordat de ene server staat te stomen vanwege druk verkeer, terwijl andere servers praktisch niets te doen hebben (en dus voor niets energie verbruiken). In deze setting is het datacenter het kloppende hart van een onderneming; vanuit daar worden allerlei diensten aangeboden (e-mail, applicaties, opslag, data, rekenkracht, websites, intranet).

Verder heeft iedere werknemer z'n eigen werkplek met een eigen desktop pc. Deze pc maakt gebruik van het netwerk en de bijbehorende diensten, maar los daarvan bevat deze ook eigen opslagcapaciteit en lokaal geïnstalleerde software. Vreemd, want lokale opslag is eigenlijk achterhaald: het datacenter biedt immers via het interne netwerk ook opslagcapaciteit aan, die – in tegenstelling tot lokale pc's – regelmatig wordt gebackupt. Wanneer de lokale harde schijf er de brui aangeeft, wat vroeg of laat gebeurt, dan zijn alle gegevens die lokaal waren opgeslagen (zoals op het bureaublad) dus verloren gegaan. Verre van efficiënt en een schrikbeeld van menig werknemer, manager én IT-beheerder. En het kan een beveiligingsrisico opleveren omdat iedereen zo'n pc kan aanzetten (en dan dus bij de lokale gegevens kan). Bij goed gebruik wordt de lokale opslag van een pc dus niet echt gebruikt, evenals de rekenkracht van die computer. Uitzonderingen daargelaten natuurlijk, want voor bepaalde werkzaamheden – zoals 3D ontwerpen, foto- en videobewerking en animaties – is lokale rekenkracht en opslag wel noodzakelijk. Bijvoorbeeld voor tijdelijke werkruimte (opslag bestanden wel op het netwerk, maar daarnaast tijdelijke lokale opslag en rekencapaciteit lokaal voor efficiency). Maar de opsomming hierboven geeft eigenlijk aan dat we jarenlang op een manier gewerkt hebben die in feite erg onlogisch is. Een andere aanpak, zou efficiënter, betrouwbaarder en voor-

al ook goedkoper zijn. Daar komt de cloud om de hoek kijken.

De drie hoofdelementen uit de voorgaande alinea (datacenter, werk-pc en internet) bestaan nog steeds in een moderne IT -infrastructuur, maar de uitvoering is compleet anders. Het datacenter bestaat voornamelijk uit gevirtualiseerde servers. Deze opereren niet meer individueel, maar vormen samen een 'wolk' met rekenkracht, opslagcapaciteit en diensten. Op één fysieke server draaien verschillende virtuele platformen (bijvoorbeeld meerdere Windows- en Linux-omgevingen). Een vorm van consolidatie, waardoor er uiteindelijk minder fysieke servers nodig zullen zijn en het beheer ervan daardoor ook vermindert. Wanneer er voldoende capaciteit is, worden machines vanzelf uitgeschakeld en wanneer de vraag naar capaciteit toeneemt, schakelen andere systemen bij, waardoor een zeer schaalbaar en efficiënte infrastructuur ontstaat. Iedere machine wordt zo optimaal benut en omdat de rekenkracht onderling verdeeld wordt, zal het aantal hotspots in een datacenter afnemen. Virtuele systemen zijn bovendien veel eenvoudiger te beheren. Een virtuele machine kan met een paar klikken naar een andere fysieke machine gekopieerd worden. Ook hoeft het beheer niet meer in het datacenter plaats te vinden, maar kan het ook daarbuiten – desnoods vanuit huis via een webinterface. Dat is zo een aantal opsommingen van de impact van virtualisatie in een bestaand datacenter, maar het is ook mogelijk om bepaalde of alle diensten voortaan extern te betrekken. Een gevirtualiseerd datacenter wordt ook wel een 'private cloud' genoemd. Kant- en klare diensten betrekken uit een datacenter van derden heet een 'public cloud'. In dat laatste geval wordt de hele datacenterinfrastructuur uitbesteed.

Maar het plaatje is nog niet compleet. Los van een gevirtualiseerd datacenter of diensten uit een public cloud zijn ook de werkplekken en de manier waarop het internet gebruikt wordt compleet anders in een cloudinfrastructuur. Het internet wordt niet alleen meer gebruikt voor basiszaken zoals e-mail en surfen, maar feitelijk voor vrijwel alle werkzaamheden. Applicaties, opslag, e-mail, digitale agenda's en managementsystemen (zoals CRM) komen rechtstreeks uit de cloud. Dat betekent ook dat de desktop eens goed onder handen kan worden genomen. Een complete pc is – zoals eerder al gesteld – onnodig (want: inefficiënt, lastig te beheren en de capaciteit van het apparaat zelf wordt niet benut). Het

Mainframes

Cloud computing is niets nieuws onder de zon, zo menen sommigen. Immers, de mainframes uit de jaren zeventig en tachtig hadden een vergelijkbare functie: een centrale (super)computer waar honderden tot duizenden gebruikers tegelijkertijd op konden werken. Ook het client-servermodel bestond toen al, met 'domme' terminals (de thin clients van nu) die toegang gaven tot een bepaald applicatie die gehost werd op een mainframe in het datacenter. Door de opkomst van de pc (en pc servers) in de jaren negentig nam de vraag naar mainframes af, maar aan het begin van de 21ste eeuw nam dat weer langzaam toe (mede door de opkomst van groeimarkten als China en India). IBM is de belangrijkste speler in de mainframe-markt met een marktaandeel van rond de 90 procent.

betekent dat de desktop wordt opgevolgd door een 'domme computer', een zogenaamde 'thin client'. Deze is dom in de zin dat het slechts een doorgeefluik is en niet zelfstandig kan opereren. In feite is het een virtuele desktop. Het besturingssysteem en de werkomgeving met applicaties komt rechtstreeks uit het datacenter (of de cloud). Het enige wat er nodig is, is een vorm van authenticatie (bijvoorbeeld met naam en wachtwoord of met een token; een speciaal apparaat). Na het inloggen verschijnt het bureaublad zoals deze de laatste keer is achtergelaten. De desktop is niet persoonsgebonden, dus iedereen kan hem gebruiken – wat ideaal is in een omgeving met flexplekken. Bovendien, als de werkomgeving webgebaseerd is, kan deze vanaf ieder apparaat met een webbrowser benaderd worden. Dat kan een thin client zijn, maar ook een zelf meegebrachte laptop of zelfs een tablet, zoals een iPad. Ook is werken vanaf huis hiermee zeer eenvoudig te realiseren; het enige dat er nodig is, is een webbrowser en het fysieke systeem en de werkomgeving worden door een goede beveiliging meestal van elkaar gescheiden (zodat een virus op de pc niet op het bedrijfsnetwerk kan komen).

Het Nieuwe Werken

Een cloudinfrastructuur speelt volledig in op 'Het Nieuwe Werken' (in het Engels: the new world of work). Sterker nog, het is bijna een vereiste om een dergelijke werkomgeving te realiseren. Bij

‘het nieuwe werken’ maakt het in principe niet meer uit waar u werkt; op kantoor, thuis of vanuit het buitenland op zakenreis. U kunt overal uw e-mail ophalen en beantwoorden, bent mobiel bereikbaar en kunt inloggen op het bedrijfsnetwerk. De scheiding tussen werk en privé verdwijnt daardoor zo langzamerhand ook op het gebied van apparatuur. Restricties op laptops, waarop tot voor kort van de systeembeheerder niets anders dan bedrijfssoftware gebruikt mocht worden, zijn steeds minder noodzakelijk. Dat biedt keuzevrijheid voor het personeel, dat daardoor zelf kan kiezen welk type laptop en smartphone men wil en maakt het inzetten van diverse apparatuur, zoals een tablet of telefoon, eenvoudiger. Ook het beheer wordt een stuk simpeler omdat de virtuele werkmachines centraal te onderhouden zijn en niet meer fysiek zoals dat normaal het geval was. Een probleem kan veelal op afstand worden opgelost.

Omdat werk niet meer gekoppeld is aan een fysieke machine ontstaan er steeds meer flexplekken. Waarom zou een bedrijf nog 100 pc's voor 100 werknemers hebben staan, terwijl gemiddeld niet meer slechts 65 daarvan gebruikt wordt? Steeds meer bedrijven gaan dan ook over naar flexplekken; geen vaste bureaus meer, maar flexibele werkplekken waar iedereen kan gaan zitten. Wie wil overleggen of op zoek is naar gezelligheid, gaat in een grote ruimte bij een groep collega's zitten en wie een idee wil uitwerken of informatie moet bestuderen gaat naar een stilteplek zonder afleiding. Ook telepresence – videovergaderen – begint steeds meer gemeengoed te worden. Enkele jaren geleden nog vlogen zakenmensen soms wekelijks een dag naar New York om een overleg op het hoofdkantoor bij te wonen. Anno 2011 is dat echt niet meer verantwoord. Niet alleen vanuit kostenperspectief, maar ook wat betreft een efficiënte werkbesteding en natuurlijk het milieuoogpunt. Videoconferencing via de cloud is een beter alternatief. Met bestaande apparatuur, zoals een webcam in een notebook en slimme software, kan een vergadering worden opgezet. Zie ook het hoofdstuk over het nieuwe werken.

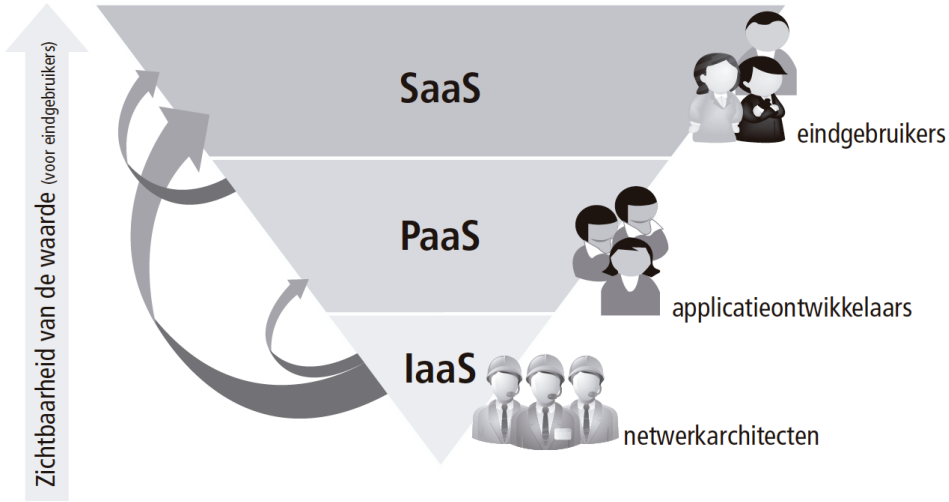
Samenwerken in de cloud

Door documenten in de cloud op te slaan wordt het bovendien een stuk makkelijker om samen te werken. Jaren geleden kondigde Microsoft een nieuwe revolutionaire Office-versie aan waarmee verschillende auteurs samen konden werken aan documenten. Wijzigingen

werden per auteur bijgehouden en commentaar werd netjes gescheiden. Maar de documenten werden wel ‘ouderwets’ per e-mail doorgestuurd. Het gevolgd daarvan was dat er uiteindelijk meerdere versies van de documenten in omloop kwamen, wat tot problemen leidde. Ook waren mensen op elkaar aan het wachten, wat het proces niet bespoedigde. Via de cloud is realtime samenwerking mogelijk. Een document wordt in de cloud opgeslagen en gedeeld met andere personen. Deze personen kunnen gelijktijdig aan het document werken, wat veel efficiënter is dan het doorsturen van een document (en dus op elkaar wachten). Online is bovendien te zien wie er op dat moment aan het werk is én wat ze doen. En zoals gezegd is opslag in de cloud ook veilig. Het bestand wordt geback-upt door de softwareleverancier (zoals Google, Microsoft of Oracle). Het enige onveilige deel is het menselijke handelen. Door bestanden (met volledige toegang) te delen met de verkeerde personen, of wachtwoorden uit handen te geven, kunnen serieuze problemen ontstaan.

Software via het web (SaaS)

De simpelste en meest gebruikte cloudvorm is SaaS, wat staat voor Software-as-a-Service. Deze dienst is vooral gericht op eindgebruikers. Een voorbeeld is Google Docs. Een online softwaresuite die in de basis hetzelfde kan als een



lokaal geïnstalleerde versie van Microsoft Office. Met als grote verschil dat de bestanden ‘in de cloud’ staan (oftewel op het internet). Lokale opslag is dus niet nodig en het voordeel is bovendien dat er heel makkelijk kan worden samengewerkt met anderen. In plaats van documenten via e-mail heen en weer te sturen, kunt u gewoon een bestand aanmaken of aanpassen en deze delen met anderen (die dit kunnen inzien en – indien gewenst – wijzigen). U hoeft zich niet meer druk te maken over back-ups, want dat is het pakkie-an van de leverancier, in dit geval Google. Als uw harde schijf crasht of uw computer gestolen wordt, blijven uw documenten in de cloud gewoon behouden. In vergelijking met traditionele software is het betaalmodel het grote verschil. Waar bij software eenmalig een licentie wordt aangeschaft, eventueel aangevuld met (betaalde) updates, werkt online software met een abonnementensysteem. Bijvoorbeeld een maandelijkse of jaarlijkse betaling per gebruiker. SaaS kan een individueel softwarepakket zijn, maar ook een complete suite met applicaties.

Een ander belangrijk kenmerk van SaaS is dat de software over het algemeen systeemonafhankelijk werkt, omdat de software meestal via een webbrowser draait. Daardoor is niet het besturingssysteem bepalend (zoals Microsoft Windows, Apple OS X of Linux), maar de webbrowser. Omdat bij een webbrowser gebruik wordt gemaakt van standaarden, werkt SaaS vaak op alle platformen met een fatsoenlijke webbrowser (inclusief nieuwe apparaten zoals de Apple iPad of Samsung Galaxy Tab). Voorbeelden van SaaS-diensten zijn onder andere webmail, Google Apps en Skype.

PaaS en IaaS

SaaS heeft dus betrekking op software. Maar er zijn ook hardwarematige clouddiensten beschikbaar, zoals PaaS en IaaS. IaaS staat voor Infrastructure-as-a-Service en richt zich op netwerkarchitecten. In dat geval wordt de infrastructuur, oftewel de hardware, als een dienst aangeboden. Deze laag bestaat bijvoorbeeld uit servers, netwerken en opslagcapaciteit. De klant hoeft hier zelf niet in te investeren, maar ‘huurt’ deze van een leverancier, veelal een grote partij met meerdere datacenters. De leverancier koopt deze hardware groot in, waardoor schaalvoordeel ontstaat en de investeringen lager zijn – veel lager dan wanneer een kleine partij dit zou doen. De hardware wordt vervolgens verhuurd aan derden. Voor klanten scheelt dit forse inves-

teringen en beheer. Ook is er geen bijzondere expertise nodig voor het beheer en onderhoud, want dit wordt allemaal door de leverancier verzorgd. Een bedrijf kan zich daardoor op z'n core business richten en besteedt de IT-infrastructuur als het ware uit. De dienst is zowel beschikbaar als private clouddienst (volledige controle over de hardware) en als public cloud (waarbij de hardware en locatie volledig door de leverancier wordt bepaald). Voorbeelden zijn Amazon's EC2, GoGrid, Uniserver UniStructure en Windows Azure.

De PaaS-laag, wat staat voor Platform-as-a-Service, gaat uit van een aantal diensten bovenop de infrastructuur – en is vooral bedoeld voor applicatieontwikkelaars. Bijvoorbeeld een bepaald platform dat SaaS-toepassingen mogelijk maakt. Een PaaS-laag biedt toegang tot een bepaald platform waarop applicaties kunnen draaien, zoals Python, .NET of Java. Voorbeelden zijn de Google App Engine, Amazon S3, Rackspace Cloud Sites, Paypal en Microsoft BPOS (Office 365).

Het 'as-a-service' toevoegsel kan op meer diensten worden toegepast, bijvoorbeeld storage en rekenkracht. Er wordt soms ook wel gesproken over XaaS, oftewel alles als een service.

Public, Private en Hybrid

Er zijn grofweg drie manieren om clouddiensten te betrekken. Public clouds zijn publieke diensten in een gedeelde infrastructuur, zoals bijvoorbeeld Google Docs, Amazon en Salesforce. De klant hoeft geen investeringen te doen in apparatuur, want die staat bij de leverancier en wordt als het ware verhuurd – veelal via een pay-per-use-concept (betalen naar gebruik). De diensten zijn kant-en-klaar en zeer schaalbaar. Een public cloud wordt echter vaak als potentieel onveilig gezien omdat de infrastructuur gedeeld wordt. Daarnaast is er weinig ruimte voor maatwerk.

Bij een private cloud is dat wel het geval. De klant maakt dan gebruik van een eigen infrastructuur die te finetunen is; hiervoor moeten echter wel investeringen worden gedaan en is de klant zelf verantwoordelijk voor het onderhoud. In principe staan de gevirtualiseerde servers in het eigen datacenter, maar het is ook mogelijk om alles bij een derde partij onder te brengen die desgewenst ook het beheer kan doen. Een private cloud is meestal duurder dan een public

cloud, maar er is wel veel meer controle en ruimte voor maatwerk. Public clouddiensten zijn bovendien door wet- en regelgeving vaak niet toegestaan voor bepaalde gegevens vanwege de bescherming van persoonsgegevens. Ook wordt de data van publieke clouds vaak in het buitenland bewaard, waar andere regels gelden (zoals de Patriot Act in de VS). Een private cloud is dan de enige optie. Hoewel… Een combinatie van beide is de zogenaamde hybride cloud, waarbij bijvoorbeeld bedrijfskritische data via een private cloud te gebruiken zijn en handige webapplicaties (zoals CRM) via een public cloud worden afgenomen.

Pieken en dalen

Een belangrijk argument voor een flexibele infrastructuur zijn de constante pieken en dalen waar datacenters (en websites) mee te maken hebben. Denk bijvoorbeeld aan structurele pieken en dalen, zoals overdag en ‘s avonds. Tijdens kantoortijd zijn de servers continu in gebruik en worden dus flink belast. ‘s Avonds en met name ‘s nachts daarentegen gebeurt er vrijwel niets. Hetzelfde geldt voor websites, zoals een e-commerce-shop of een online krant. Gedurende de dag en in iets mindere mate ‘s avond is er flink wat activiteit, maar ‘s nachts is er amper bezoek. De servers staan dus in feite urenlang voor niets aan en kosten alleen maar energie. Sommige beheerders lossen dat op door bepaalde systemen (automatisch) uit te schakelen na werktijd, maar dat is niet bevorderlijk voor de flexibiliteit. Er zijn immers ook onberekenbare pieken en dalen. Stel er moet overgewerkt worden en het personeel werkt ‘s avonds en zelfs een deel ‘s nachts door vanwege een naderende deadline van een project. Wanneer een deel van de machines buiten kantoortijden uitgeschakeld wordt, leidt dat tot een acuut probleem.

Het bekendste publieke voorbeeld is een (onverwachte) piek bij websites. In het huidige internettijdperk gebeurt het regelmatig dat een website plotseling veel bezoekers trekt. Vaak gaat het om bijzonder nieuws, speciale content of bijvoorbeeld een spectaculaire aanbieding. Weblogs, twitteraars en andere websites pikken het nieuws razendsnel op en verwijzen de lezer naar de bron. Een website krijgt dan plotseling zoveel verkeer te verwerken dat de server waarop deze gehost wordt, onderuit dreigt te gaan. Dat komt vaak doordat de server, of het hosting account, niet berekend en gedimensioneerd is op deze hoeveelheid verkeer. Ofwel door een fysieke limiet of door

een beveiligingsmaatregel die een (virtuele) server automatisch uitschakelt wanneer deze een bepaalde limiet overschrijdt (bijvoorbeeld om de andere accounts op dezelfde server te beschermen). Dit komt vrij regelmatig voor en wordt ook wel een 'ondergang van het eigen succes' genoemd. Toch is het probleem zeer schadelijk. Immers, een website wil bezoekers. Als de site niet bereikbaar is, gaat dat ten koste van potentiële lezers, of erger nog... klanten. Ook is de imagoschade zeer groot.

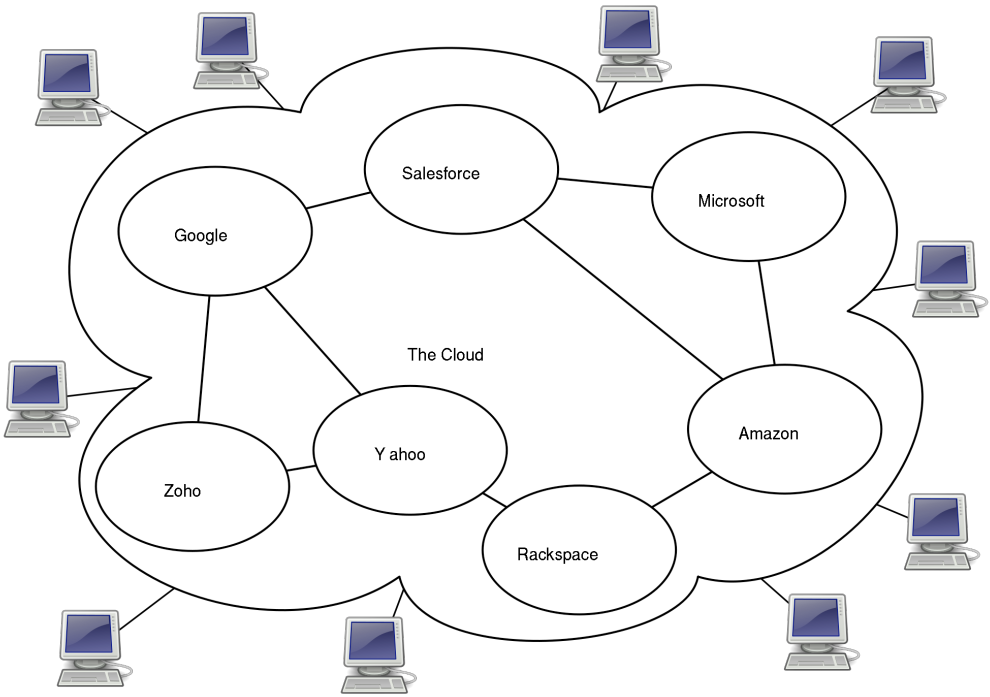
Een schaalbare architectuur voorkomt dit probleem. Uitgaande van het ideale scenario is er een onbeperkt aantal servers beschikbaar, die zich realtime aanpassen aan de behoefte. Tijdens een drukke werkdag schalen er extra servers bij en 's nachts schakelen ze zichzelf grotendeels uit – tenzij er onverwacht een beroep op de capaciteit wordt gedaan. In de praktijk is dit scenario niet altijd haalbaar omdat veel leveranciers verschillende bundels bieden, met bijbehorende (al dan niet theoretische) limieten. Schaalbaarheid buiten de bundel is mogelijk mits dat specifiek wordt afgesproken. Uiteraard staat hier een prijskaartje tegenover: de klant neemt een duurdere bundel af en betaalt daar bovenop de rekening voor het extra gebruik (als daarvan sprake is). Toch zijn volledig schaalbare servers wel mogelijk. Dat was een van de redenen waarom Wikileaks er eind 2010 voor koos om haar servers bij Amazon's AWS-dienst onder te brengen. Allereerst verwachtte het bedrijf een groot aantal bezoekers voor 'cablegate' (uit uitlekken van zogeheten 'cables' met correspondentie tussen Amerikaanse ambassades). Maar het rekende op ook vijandige aanvallen door middel van dDoS (dedicated Denial of Service), waarbij besmette zombie pc's honderden keren per seconde toegang tot een bepaalde site vragen met als doel deze plat te leggen. Dankzij de gigantische schaalbaarheid van Amazon's servers en bandbreedte capaciteit heeft een dergelijke aanval in dat geval geen zin.

Betalen voor gebruik

Een typisch kenmerk voor clouddiensten is het bijzondere betaalmodel. Bij software is het traditioneel gebruikelijk om eenmalig een licentie voor een pakket te kopen en deze na verloop van tijd, meestal enkele jaren, te upgraden. Eventuele updates zijn gratis, maar voor een nieuwe versie moet opnieuw een (upgrade)licentie worden aangeschaft. Bij cloud computing gaat dat anders, ongeacht het product (een dienst, software of

De herkomst van ‘cloud’

Het woord ‘cloud’ staat voor het internet en dankt zijn afkomst aan een wolkensymbool waarmee het netwerk werd afgebeeld. Vroeger liep een verbinding fysiek van A naar B, oftewel met een vaste route van een begin- tot een eindpunt. Met de opkomst van grote netwerken, zowel intern bij bedrijven als via het wereldwijde web, verdween de vaste route. Data werden opgedeeld in verschillende pakketjes die via ‘packet switching’ hun doel bereikten. Het netwerk werd niet meer weergegeven als een set kabels, maar als een wolk waaruit bepaalde data kwamen. Of een applicatie. Of een dienst. De weg die de pakketjes volgen is niet meer interessant. Het gaat niet om de verbindingswegen, maar om de infrastructuur. Omdat hetzelfde geldt voor diensten via het internet, werd al snel ‘het internet’ als een wolk afgebeeld. Toen steeds meer diensten via dit medium werden aangeboden werd ook wel gesproken over ‘cloud computing’.



hardware). Simpel gezegd: er wordt betaald voor het gebruik. In het geval van software is dat bijvoorbeeld een jaarlijks bedrag via een abonnement (bijvoorbeeld Google Apps Premiere dat € 40 per gebruiker kost). Voor een PaaS- of IaaS-dienst wordt betaald voor het daadwerkelijke gebruik, bijvoorbeeld voor verbruikte rekencapaciteit of bandbreedte. De 'pay-for-use'-methode is een van de grootste voordelen van cloud computing en tevens een van hoofdredenen om hiervoor te kiezen. Allereerst voorkomt het grote investeringen in apparatuur en software, ten tweede is het zeer flexibel (wat betreft gebruik en bijvoorbeeld het aantal werknemers) en ten derde is het simpelweg een eerlijke betaalmethode; niet betalen voor wat u denkt nodig te hebben (wat meestal minder is dan verwacht), maar gewoon voor wat u daadwerkelijk verbruikt. Voor grote multinationals is cloud computing een significante kostenbesparing, voor jonge entrepreneurs maakt het de start van een nieuw bedrijf mogelijk (start-ups), zonder dat er eerst een flinke zak geld nodig is voor de klassieke basisinvesteringen.

Toekomst

Het is de vraag of we over tien jaar nog wel spreken van 'de cloud' of 'cloud computing'. Het is dan naar alle waarschijnlijkheid gewoon de manier waarop ICT gefaciliteerd wordt.

De overige pagina's in dit voorbeeld bestaat uit een willekeurige selectie van twee naast elkaar liggende pagina's uit het boek.

Public, Private en Hybrid clouds

Over public versus private clouds is altijd veel discussie geweest. Simpel gezegd levert publieke cloud een kant-en-klare infrastructuur, die gedeeld wordt door meerdere klanten. Een zogenaamde 'shared' omgeving, zoals we die ook kennen van webhosters (waarbij er meerdere sites draaien op dezelfde fysieke server). Denk bijvoorbeeld aan Gmail, Windows Live Mail, Google Docs of een CRM-dienst van Salesforce. De hele infrastructuur, het plaftorm of de software is in het bezit van de leverancier, die deze verhuurt aan verschillende klanten. De klant hoeft dus zelf geen investeringen te doen in software of apparatuur maar betaalt simpelweg voor het gebruik – bijvoorbeeld per gebruiker of per periode (uur of maand). Omdat de dienst kant-en-klaar is, is er weinig ruimte voor maatwerk. De leverancier bepaalt welke hardware en welke virtualisatiesoftware er gebruikt worden en in principe ook waar de data wordt opgeslagen.

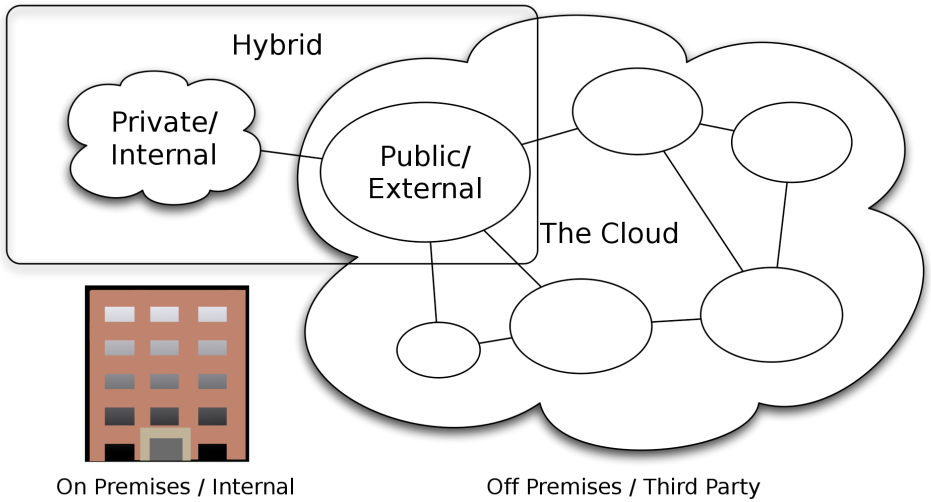
Bij een private cloud heeft de klant veel meer zeggenschap over de onderliggende infrastructuur. In feite is het een schaalbare gevirtualiseerde omgeving zoals een public cloud, maar dan exclusief voor een bepaald bedrijf. Een 'dedicated' omgeving, zoals in het geval van een webhost met eigen webservers in een rack en datacenter van de hoster. Of gewoon in het eigen datacenter, waar een private cloud is opgebouwd met een cluster gevirtualiseerde servers. Een private cloud is kostbaarder dan een public cloud, maar het biedt ook veel meer vrijheid. Voor een private cloud zijn investeringen nodig omdat de apparatuur door de klant zelf moet worden aangeschaft. Ook moet de apparatuur worden beheerd, al kan dat ook worden uitbesteed aan een derde partij. Op het gebied van dataopslag en beveiliging is maatwerk mogelijk, maar de expertise daarvan moet wel zelf worden verzorgd of ingehuurd.

Wat kosten betreft is een publieke cloud vrijwel altijd goedkoper dan een private cloud, omdat de leverancier daarvan een zeer grote infrastructuur (en dus schaalvoordeel) heeft. Vergelijk bijvoorbeeld maar eens wat een uur reken-

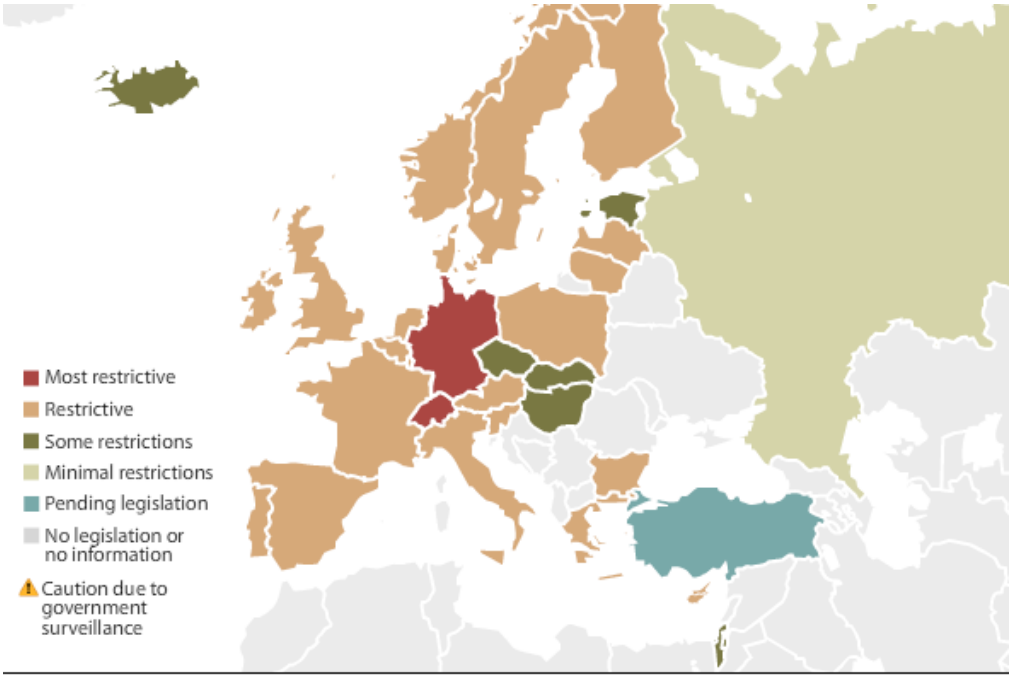
kracht of een TB opslag kost bij Amazon in vergelijking met het eigen datacenter. Vooral voor start-ups is een publieke cloud voor de hand liggen, omdat dit amper startkapitaal vergt. Ook voor het MKB ligt een publieke cloud meestal meer voor de hand vanwege de kosten. Ook is een publieke cloud beter schaalbaar, omdat de capaciteit vrijwel onbeperkt naar boven of beneden kan worden bijgeschroefd. Voor Enterprises is dat een ander verhaal omdat er een punt komt waarop de kosten voor investeringen niet meer interessant zijn. Wanneer je investeert in een paar duizend servers, raakt de hefboom uitgewerkt. De prijs van extra servers is dan niet meer interessant. Wanneer dat wordt vergeleken met de kosten voor een public cloud, dan is het verschil op lange termijn niet schrikbarend groot.

Marktsituatie

Cloud computing heeft enorme groei doorgemaakt die vooral aan public cloudleveranciers, zoals Google en Amazon, te danken is. Desondanks lijkt de private cloud de komende tijd de meeste groei door te maken. In een recent onderzoek van Gartner bleek dat driekwart van de IT-managers van plan is om de komende twee jaar meer te investeren in

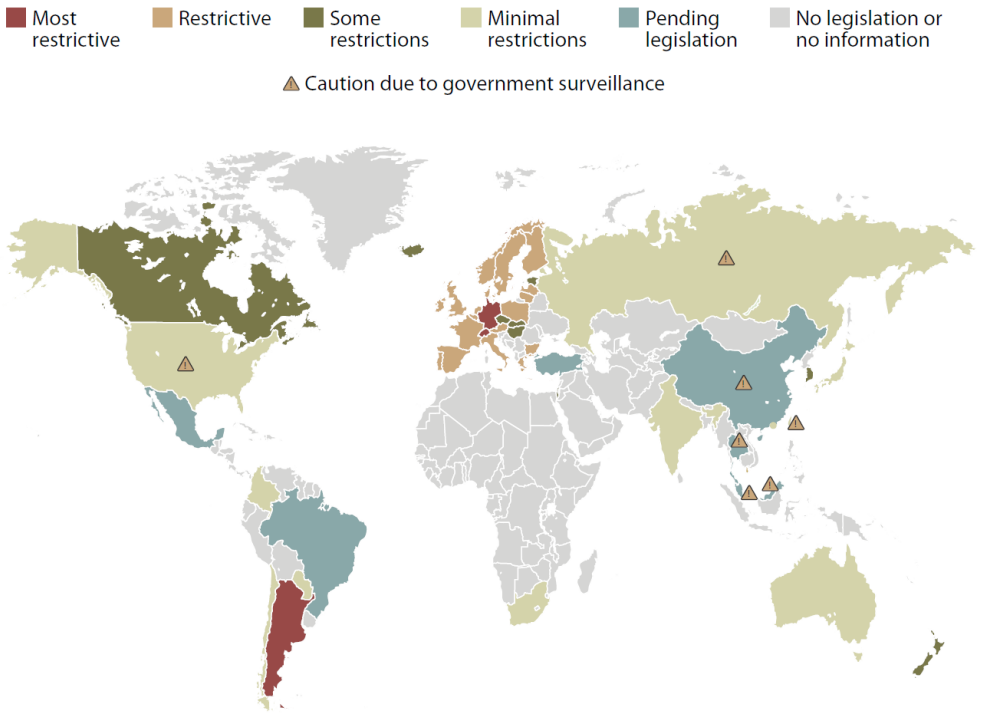


Cloud Computing Types



Source: Forrester Research, Inc.

datacenters en infrastructuur zo in te richten dat gegarandeerd kan worden dat de data niet buiten de landsgrenzen van de EU komen. Google garandeert dat tot op heden niet, hoewel het wel heeft gesteld dat een 'Europese cloud' overwogen wordt. Het schijnt dat de architectuur van Google niet is ingesteld om data te beperken tot bepaalde locaties, omdat ze letterlijk de hele wereld over gaan. Daar staat – in zwaar contrast – tegenover dat Google (sinds juli 2010) de Amerikaanse overheid wel de garantie biedt dat hun data in de VS blijven. Google zegt hierover het volgende: "Onze klanten zijn tevreden met de bescherming die wij hun kunnen bieden. De in Europa door Google Apps gegenereerde data van klanten worden in de EU en de VS bewaard en voldoem volledig aan de zogeheten 'Safe Harbour'-overeenkomst. Dit betekent dat Europese bedrijven of organisaties voldoende adequate bescherming krijgen, in lijn met wat de Europese Dataprotectierichtlijn voorschrijft. We bekijken continu op welke manier we ervoor kunnen zorgen dat we onze klanten vandaag en in de



toekomst maximaal blijven beschermen." Overigens pleiten grote cloudproviders als Amazon, Google en Microsoft al langer voor een soort ‘datavrijhaven’, die gevrijwaard is van juridische en geografische beperkingen.

Op de vorige pagina staat de geografische kaart van Europa waarop de verschillende restricties in de lidstaten worden aangegeven, waarbij Duitsland en Zwitserland de strengste wetten hebben en Tsjechië, Slowakije en Hongarije de minst strenge (bron: Forrester).

En bovenaan deze pagina staat hetzelfde kaartje, maar dan wereldwijd. Opvallend is de markering voor ‘government surveillance’, wat er op duidt dat aan de privacywaarborg van data getwijfeld kan worden. Dat geldt bijvoorbeeld voor landen als Rusland en China, maar ook voor de VS (vanwege de Patriot Act). China heeft eind 2015 een decryptieplicht ingevoerd voor bedrijven.

Security

Bij ieder onderzoek naar cloud computing wordt ‘security’ vrijwel altijd als voornaamste punt voor terughoudendheid genoemd. En dat is ook wel logisch. Wanneer immers diensten vanuit het eigen datacenter worden gefaciliteerd, is er sprake van directe controle. Bij een cloudleverancier is die controle echter indirect en bij publieke clouddiensten is er meestal ook geen ruimte voor specifiek maatwerk (dat afwijkt van andere klanten). Bovendien wordt een multi-tenantomgeving, waarbij de infrastructuur door meerdere klanten – soms zelf wereldwijd – gedeeld wordt, gevoelsmatig als onveilig ervaren. Immers, de concurrent zou theoretisch wel eens gebruik kunnen maken van dezelfde harde schijf. Ook het gevaar van mogelijke bugs en kwetsbaarheden in de beveiliging van de leverancier, of bij een klant daarvan (op dezelfde infrastructuur), kan onbehaaglijk voelen. Maar is dat gevoel wel op feiten gebaseerd?

Beveiliging

Ook publieke clouddiensten zijn goed te beveiligen. Dat vereist wel een specialistische aanpak, waar grote publieke providers als Google, Amazon of Microsoft inmiddels veel expertise in hebben opgebouwd. Het aanbieden van publieke diensten is hun core business, dus beveiliging heeft de hoogste prioriteit. Immers, de imagoschade zou enorm zijn als er iets misgaat en dat zou weer tot klantenverlies en terughoudende nieuwe klanten leiden.

De beveiligingsmaatregelen bij publieke clouddiensten zijn doorgaans een stuk beter dan de meeste bedrijven zelf kunnen leveren, zo stelde Gartner-analist Neil MacDonald recentelijk. Door hun enorme schaalgrootte hebben cloud providers vaak een speciaal securityteam dat dag en nacht de diensten op veiligheidslekken controleert en het verkeer in de gaten houdt. De datacenters zijn bovendien veelal state-of-the-art en geoptimaliseerd voor efficiënte beveiligingsmaatregelen. Er zijn bijvoorbeeld geen

Zorgen rondom de cloud

Security & privacy	169
Prestaties	58
Onvolwassenheid	56
Wet- en regelgeving	53
Integratie	43
Vendor lock-in	32
Kosten	26
Uptime	13
Expertise	7

(Bron: Gartner; n=94, 1e prioriteit = 3, 2e prioriteit = 2, 3e prioriteit = 1)

legacy-systemen met een verouderde architectuur die een potentieel veiligheidsrisico vormen. En doordat alles is gevirtualiseerd, is het beheer en het management minder complex een makkelijker in de gaten te houden.

Ook in fysieke beveiliging rondom de datacenters is voorzien; buiten en binnen is bewaking en zonder toegangspas en/of biometrische controle komt iemand niet binnen. Er zijn bovendien diverse technische veiligheidsmaatregelen mogelijk, zoals unieke encryptiesleutels per klant, strategisch verdeelde opslag en specifieke authenticatiemethoden op verschillende niveaus (rangorde).

Virtuele netwerken

Virtualisatie vereist extra aandacht voor de beveiliging in het netwerk. Wanneer twee virtuele machines op dezelfde fysieke pc met elkaar communiceren, wordt dat door traditionele firewalls soms niet goed gedetecteerd. Volgens marktonderzoeker Gartner blijkt dat 60 procent van de virtuele servers minder goed beveiligd is dan de fysieke servers die zij vervangen. Volgens analist Neil MacDonald is virtualisatie op zich niet onveilig, maar worden veel gevirtualiseerde workloads onveilig uitgerold. MacDonald wijt dat aan de onvolwassenheid van de hulpmiddelen en processen en de beperkte training en expertise van de IT-staf. Tegelijkertijd verwacht Gartner dat tegen 2012 circa de helft van alle workloads gevirtualiseerd zal zijn en dat het percentage dat slecht beveiligd is dan zal zijn afgenomen tot 30 procent. Een aantal punten waarop de beveiliging tekort schiet worden genoemd. Zo stelt men dat Informatie Security-teams vaak niet worden betrokken bij de planning en het ontwerp van de architectuur, doordat het operationele team stelt dat er niets wezenlijks zal veranderen. Vaak wordt ten onrechte gedacht dat men reeds beschikt over vaardigheden om workloads veilig te stellen, evenals de besturings-

CLOUD COMPUTING

Clouddiensten zijn niet meer weg te denken uit het bedrijfsleven. Toch zijn er nog steeds veel vraagtekens. Wat is cloud computing nu precies? Welke soorten en vormen zijn er (met hun specifieke voor- en nadelen) en op welke manier kan het een positieve bijdrage leveren aan de bedrijfsvoering van grote en kleine bedrijven? De 'cloud' belooft kostenbesparingen (betalen voor gebruik), eenvoudiger beheer en vrijwel onbeperkte capaciteit (zoals rekenkracht en opslag). Maar er zijn ook diverse schaduwzijden zoals beveiligingsrisico's, juridische kwesties en het gevaar van een zogenaamde 'vendor lock-in' door gebrek aan open standaarden.

Alles wat te maken heeft met cloud computing wordt op begrijpelijke en objectieve manier besproken in dit boek, inclusief basisterminologie als SaaS, PaaS, IaaS, Private-, Public en Hybride-clouds, virtualisatie en SLA's. Daarnaast komen ook aanverwante thema's als hosting, security, connectivity, storage en wet- en regelgeving uitgebreid aan de orde. Het boek sluit af met een reeks cases waarbij clouddiensten in de praktijk werden gebracht.

"Jeroen Horlings is er in geslaagd om vanuit de gebruiker te denken en heeft alleen daar waar functioneel noodzakelijk meer technische teksten toegevoegd - die overigens eveneens goed leesbaar zijn voor een leek."

ISBN 9789492404046

OVER DE AUTEUR

Jeroen Horlings (1974) is zelfstandig IT journalist en voormalig hoofdredacteur van het vakblad CloudWorks. Hij schrijft veel over technologie en heeft in verleden artikelen geschreven voor Computable, IT Executive, High Tech Analysis en Computerworld over cloud computing, virtualisatie en datacenters.