EEN BIJZONDERE CONFERENTIE OVER EEN BEKEND THEMA

Begin april vond in Amsterdam de tweedaagse conferentie Secure Cloud plaats. Deze bijeenkomst, georganiseerd door CSA [1], Enisa [2] en Fraunhofer [3] besteedde aandacht aan tal van aspecten die uiteindelijk ervoor moeten zorgen dat wij allemaal meer gebruik van cloud gaan maken, allemaal op basis van een veilig aanbod. Cloud en veiligheid zijn inmiddels al zo lang onlosmakelijk met elkaar verbonden begrippen en thema van menig congres dat de vraag rijst of deze conferentie nog wel nodig was.

Om antwoord te geven op die vraag kan worden verwezen naar het programma [4]. Dit maakte op voorhand duidelijk dat de sprekers verschillende disciplines vertegenwoordigden en daarmee ook uiteenlopende invullingen zouden geven aan het begrip secure cloud. De diversiteit was ook zichtbaar bij de ruim 150 aanwezigen, dit was duidelijk geen conferentie uitsluitend bedoeld voor één beroepsgroep. Doordat de groep zo gemêleerd was, werd tijdens de presentaties en discussies veelvuldig teruggegrepen op nadrukkelijk niet-cloud gerelateerde issues en voorvallen. Dit was geen zwakte bod, het hielp juist de probleemstelling vanuit meerdere invalshoeken te bekijken. Deze wisseling van perspectief zal het voor non-insiders overigens lastig gemaakt hebben delen van het programma te volgen. In tegenstelling tot andere bijeenkomsten was hier het hebben van parate kennis van afkortingen minder een pre dan het signaleren van een gewijzigde invalshoek. Het was verder een bijeenkomst waar het tempo hoog lag. Sprekers en zaal reageerden zeer snel op elkaar en dat gaf de conferentie al vanaf de start een opvallende dynamiek. Het is daarom ook minder eenvoudig puntsgewijs weer te geven wie waar over sprak.

Rashid Niamat is journalist en werkzaam bij ISPam.
Rashid is te bereiken via rashid@niamatmediagroup.nl

De bondige keynotes van onder andere Neelie Kroes over de doelstellingen van de EC op het vlak van uitgebreidere cloud adoptie, omdat het een banenmotor is en Richard Clarke over de werkwijze van de NSA en de veranderingen die deze organisatie moet doorvoeren, staken in dat opzicht schril af tegen de rest van het programma. Kroes gaf aan dat meer cloud in de EU tot 400.000 nieuwe bedrijven kan leiden en het EU BNP met 1000 miljard kan vergroten. Clarke deed zijn uiterste best de balans te beschrijven tussen de noodzaak tot incidenteel zeer vergaande surveillance en de nog grotere noodzaak te voorkomen dat er wordt doorgeschoten naar een 24/7 surveillance staat. Verder was dit een conferentie waar in

het plenaire gedeelte nadrukkelijk geen ruimte was voor salespitches en marketing activiteiten. De sprekers en de zaal hielden zich daar voorbeeldig aan en het gevolg was dat de aandacht niet onnodig werd afgeleid. Nadeel kan zijn geweest dat bij bepaalde thema's aan de beoogde gebruiker van secure cloud diensten – namelijk de klant – te weinig aandacht is besteed. De rest van het programma was, zoals al aangegeven, minder simpel samen te vatten. Wat wel mogelijk kan is het aantal termen of begrippen dat deze twee dagen steeds terugkwam te beschouwen als een rode draad, dat levert een lijst op met de volgende zeven begrippen:

1. **Taal**
2. **Telco's**
3. **Snowden en NSA**
4. **EU**
5. **Standaarden, welke Standaarden?**
6. **Juridische issues en cloud techniek**
7. **Security in de cloud - de praktijk**

Taal

Het klinkt als een open deur, maar zeker bij een thema als secure cloud is het nodig dat partijen opletten dezelfde taal te spreken. Hiermee wordt niet bedoeld taal , bijvoorbeeld Engels, als de voertaal tijdens een debat, maar taal als essentieel instrument bij het streven naar duidelijkheid en transparantie. Gedurende deze conferentie werd diverse keren duidelijk dat

Dit was duidelijk geen conferentie uitsluitend bedoeld voor een beroepsgroep

een woord of begrip door sprekers en zaal verschillend werd gebruikt of soms echt niet door allen werd begrepen. Om met dat laatste te beginnen, door meerdere sprekers werd gewezen op de noodzaak van een eigen Europese of nationale cloud omgeving. Landen als Frankrijk en Griekenland gaan hier vrij ver in, omdat wetgeving verhindert dat bepaalde data (denk aan archieven) buiten de nationale landsgrenzen wordt opgeslagen. De Amerikaanse sprekers zijn uiteraard niet gecharmeerd van een dergelijk ontwikkeling en pleitten voor open grenzen en internationalisering van de cloud. Het begrip dat daarbij werd gehanteerd is "balkanisering van de cloud". Het is zonder meer een beladen term en achteraf bleek dat echt niet iedereen in de zaal begreep wat er mee bedoeld werd.

Een ander voorbeeld van taalgebruik in relatie tot cloud werd genoteerd bij de presentatie van Evangelos Floros van GrNET, de IaaS oplossing voor de academische sector toepassing [5]. Een van de randvoorwaarden die daarvoor gold was dat die cloud secure en sustainable moest zijn. In Nederland associëren we het begrip subliminale vooral met groen of duurzaam. In Griekenland heeft het uitsluitend te maken met het rond krijgen van de businesscase. Peleus Uhley van Adobe, gaf in zijn presentatie een praktijk voorbeeld van onjuiste taal- en beeldgebruik. Hij merkte op dat we heel vaak cloud afbeelden als een wolk en daarin de servers aan de frontend en de backend als twee losse serverkasten. Dat beeld is herkenbaar en laat zich makkelijk uitleggen, maar het is inmiddels te vaak onjuist. Tegenwoordig zijn backend en frontend steeds vaker geen separate fysieke machines meer maar elk weer onderdeel van een virtuele omgeving. Dat legt moeilijker uit, gaf de spreker direct toe, het kan verwarring geven door 3 wolken in een afbeelding te stoppen. Maar het is wel nodig want anders leggen we de zaak niet goed uit en ontstaat onvermijdelijk spraakverwarring op enig moment.

Telco's

De eerste panelsessie waren gewijd aan de rol die telco's nu en op termijn spelen op het vlak van secure cloud. Telco's zijn allemaal gewend te denken in grote aantallen en perfect in

Telco's kunnen complexe billingstraten runnen, daarom zijn zij cloud leverancier geworden

staat complexe billingstraten te runnen. Dat laatste werd door enkele sprekers uit die sector aangegeven als een belangrijke zo niet de belangrijkste reden waarom ook zij allemaal cloud leverancier gaan worden. Opvallend was verder dat in deze groep de link werd gelegd tussen het begrip critical infrastructure, de core business telefonie en datatransport en secure cloud. Tegelijkertijd werd duidelijk dat telco's hier een positie claimen omwille van new-business maar nog niet helemaal klaar zijn met de invulling van de case. Gaat de focus uit naar enterprise cloud, MKB cloud diensten of juist voor de grote aantallen, de SoHo en consumenten markt. Cloud is voor elk van deze segmenten een ander aanbod (achter de schermen hoeft dat trouwens niet) en elk segment vraagt ook weer een aparte benadering. Gaan telco's dit allemaal zelf uitvoeren of worden ze in toenemende mate reseller van white-label cloudoplossingen die elders worden ingekocht. Voorbeeld van dat laatste is een cloud oplossing dat Belgacom haar klanten biedt. Dit is een dienst van F-Secure dat relabelled is. Ander voorbeeld is de wijze waarop Britse telco's en internetproviders mail leveren, dat is voor bijna alle grote spelers een van de bekende Amerikaanse SaaS oplossingen. De wijze waarop telco's die inkoopslag combineren met focus op security zal nog wel vaker aan de orde komen. Ook voor partijen die niet de consumentenmarkt (B2C) als speerpunt hebben of zich positioneren als leverancier van telco's vormt dit al een ontwikkeling die de moeite van het volgen waard is.

Snowden en NSA

Onvermijdelijk waren deze twee begrippen en zeer prominent aanwezig tijdens de conferentie. Waar Richard Clarke zijn best deed de vernieuwde NSA te beschrijven was dit bij alle andere sprekers keer op keer aanleiding voor kritische noten. Duidelijk was dat de onrust die de Snowden affaire heeft veroorzaakt, nog lang niet voorbij is. Amerikaanse aanbieders maar ook Britse sprekers worstelden hier mee en in elke zaal was er wel iemand die daar lastige vragen over wist te stellen. De impact in de dagelijkse praktijk werd door meerdere sprekers geïllustreerd. Aernout Reymer van BT gaf aan dat de affaire direct leidde tot een ander type vragen van klanten. Het is niet meer 'are you safe?', maar 'show me you're safe!' De spreker van Verizon, Lee Miller, ging hierin mee en wees erop dat aantonen waar data staat relatief eenvoudig is. Door de onrust

van de laatste maanden verlangen klanten nu ook vooral dat wordt aangetoond dat data ergens niet staat. Dat is in een fysieke omgeving al lastig, maar hoe toon je dat aan in de context van cloud. Beide sprekers sloegen hiermee een brug naar een permanent terugkomend onderwerp tijdens de conferentie: audits. Audits om vertrouwen te verkrijgen of om het afkalvende vertrouwen te herstellen. De spreker van Google, Peter Dickman, plaatste een terechte opmerking toen het begrip "right to audit", dat sinds de Snowden onthullingen schijnbaar nog vaker wordt gebezigd, werd besproken. 5 miljoen klanten en het "right to audit"? Dat is het grootst mogelijke security risico dat je je maar kunt voorstellen. Die relativering kwam komisch over, maar had een uiterst serieuze ondertoon. Een pasklare oplossing voor bedrijven met veel klanten die steeds vaker met audits eisen was op deze conferentie niet beschikbaar.
Desondanks zal iedere bezoeker aan deze conferentie in antwoord op de vraag wat rond het onderwerp Snowden en NSA de meeste indruk heeft gemaakt een antwoord geven dat geen betrekking heeft op bovenstaande. Zoals ook elders is beschreven hebben twee aspecten van de keynote van Richard Clarke veel indruk gemaakt. De eerste was de – wellicht cynisch bedoelde – opmerking dat iedereen die zich zorgde maakte om het aftappen van zijn cloud of data door de NSA gewoon zijn spullen op Amerikaanse bodem moet zetten. Daar heeft de NSA namelijk veel minder bevoegdheden en mogelijkheden. In het buitenland daarentegen, dat hoefde de zaal amper te worden uitgelegd. Haaks op die opmerking stond zijn slotwoord: het was de oprechte bezorgdheid dat we veel te weinig doen om 'the police surveillance state' tegen te houden.

EU

De keynote van Neelie Kroes is al aan het begin genoemd, maar ook gedurende de gewone sessies was de EU een van de centrale thema's. EU werd gehanteerd als motief voor een lokalisering van cloud, als een factor die uitwisseling van data in het algemeen bepaalt en natuurlijk als handelsblok dat gewoon kwaliteitseisen kan stellen.
Een interessante opmerking hierover werd gemaakt door Udo Helmbrecht, de executive director van Enisa. Hij wees op het EU verplichte logo voor veilig speelgoed. Waarom, vroeg hij zich hardop af, hebben we EU breed nog geen label systeem dat zowel SME's als burgers helpt de kwaliteit van het cloud aanbod te bepalen. Elders werd verwezen naar de energie labels, zou dat niet een manier zijn om specificaties van cloud zoals veiligheid eenduidiger weer te geven. De vertegenwoordigster van de Zweedse Piratenpartij, Amelia Andersdotter, had een variatie op het thema EU labels. Prijzen voor consumenten in de EU moeten altijd inclusief BTW zijn. Kunnen we van cloudaanbieders ook niet eisen dat bepaalde privacy en security componenten altijd verplicht inclusief zijn?
De EU bezorgdheid over labels was nadrukkelijk aanwezig. Op de vraag waar die zorg vandaan komt zijn meerdere antwoorden mogelijk. De EU-sceptici vrezen dat dit de voorbode is voor een zoveelste EU-loket en toename van de administratieve lasten voor ondernemers. Anderen, in ieder geval Kroes en de medewerkers van EU instellingen, zullen wijzen op de achterblijvende vraag in de EU naar clouddiensten. Met in het achterhoofd de rapporten die wijzen op een maximale bijdrage aan de EU economie tot 2020 in de vorm van 400.000 nieuwe SME bedrijven en 4.000.000 nieuwe banen is het begrijpelijk dat die laatste groep vooral op zoek is naar manieren cloud te stimuleren. Wat geen van de partijen hardop zei is dat alle argwaan en twijfel die er bestaat rond de veiligheid en betrouwbaarheid van IT nu wordt gefocust op cloud. Cloud als zondebok of bliksemafleider? De EU medewerkers en natuurlijk alle aanbieders van deze en gene zijde van de grote plas hebben daar duidelijk geen behoefte aan. Cloud als multifunctionele toolbox om de stagnatie dan wel recessie te bestrijden: daar heeft men duidelijk wel behoefte aan.

Standaarden – welke standaarden?

Voor een buitenstaander is het vreemd te horen dat cloud geen echte standaarden kent. IaaS, SaaS, PaaS, die termen lijken te verwijzen naar in beton gegoten industriestandaarden, maar zijn het niet. Na twee dagen was tevens duidelijk dat begrippen als veiligheid en beschikbaarheid door partijen verschillend worden geïnterpreteerd. Daar is niets mis mee, zolang de beoogde gebruiker van de diensten in kwestie dit maar vooraf op een eenduidige en heldere wijze is medegedeeld. Op dat punt trok menig spreker de volle aandacht van de zaal. Professionals en insiders weten het al lang, maar ISO certificering is slechts een point in time. Bedrijven als SAP kunnen hier weinig mee. Dit soort partijen voorspelden dan ook dat continuous auditing de oplossing zal zijn. Maar vooralsnog is het vooral een pittige uitdaging om zoiets intern van de grond te krijgen en extern verkocht en geaccepteerd te krijgen. De methodiek die CSA heeft ontwikkeld (STAR) kwam uiteraard ook uitgebreid ter sprake. Wie meer wil weten van de discussies over ISO tijdens de conferentie: Bart Veldhuis heeft daarover een goed verslag gemaakt dat op computable.nl [6] te lezen is.

Juridische issues en cloud techniek

Dat tijdens een bijeenkomst over cloud ook de juridische valkuilen ter sprake komen is onvermijdelijk. De secure cloud conferentie was in zoverre een uitzondering op die regel, dat het aantal besproken valkuilen meeviel. De vaak gehoorde opmerking dat legal en techniek niet te synchroniseren zijn is deels terecht, maar Danielle Catteddu van CSA gaf aan dat we vooral moeten onthouden dat binnen bestaande contracten en wetgeving cloud niet meer is dan de variatie op een thema.

Dat cloud techniek aanleiding geeft voor nieuwe contractbepalingen werd eveneens duidelijk. Wellicht inhakend op de opmerking van Lee Miller, die opmerkte dat het voor cloud aanbieders lastig is aan te tonen dat data ergens niet staat, vestigde Catteddu de aandacht van de zaal op het verschijnsel cloud termination. Voor meer dan alleen security experts en informatie beveiligers is dit een onderwerp waar in bestaande en nieuwe contracten echt aandacht moet worden besteed. Catteddu noemde als andere dealbreakers: het ontbreken van goede contracten tussen de verschillende processors van data en de situatie waarin twee partijen als data controllers worden aangemerkt. Als laatste stelde hij nog de vraag: wat moet je doen als tijdens een contractperiode een van de partijen in de waardeketen (los van het gegeven of het een producent of bewerker is) wordt overgenomen? Het antwoord op de vraag kon hij zelf niet geven, wel de tip dat op dit punt de bestaande contracten nog eens goed moeten worden doorlopen.

Security in de cloud - de praktijk

Dat tijdens secure cloud heel vaak het begrip security werd gehanteerd zal niemand verwonderen. Het begon al bij de keynote van Kroes die de zaal om de oren sloeg met cijfers over data breaches en datalekken en de vraag stelde "why are we so vulnerable?" Het was weinig opmerkelijk dat zowel sprekers uit de profit sector zich terughoudend opstelden bij het geven van voorbeelden ter illustratie van veiligheid. Wat zonder twijfel het meest werd genoemd was encryptie. Of het nu gaat om encryptie van data, opslag of transport, iedereen leek van mening te zijn dat dit een eerste en zeer belangrijke stap is cloudgebruik op een hoger acceptatie- en veiligheidsniveau te brengen. Over de vormen van encryptie en het gebruiksgemak liepen de meningen sterk uiteen, dit kan deels komen omdat nogal wat partijen hier een eigen commercieel belang hebben.
Het beschrijven van risico's – die nadrukkelijk niet uitsluitend cloud only waren – ging de meesten makkelijker af. Voor de hand liggende constateringen als re-use van wachtwoorden passeerden de revue. Meerdere sprekers legden ook de link tussen het onderschatten van de waarde van data en de kans slachtoffer te worden van een security- of data breach. Brian Honan van Iriscert [7] had in het kader van monitoring van risico's de nodige tips. Een viel op omdat deze echt 100% cloud gerelateerd was. Medewerkers die tijdelijk iets in de cloud stallen en daarbij bestaande bedrijfspolicies omzeilen zijn een te traceren risico. Zorg dat de boekhouding bij de controle van betalingen met de bedrijfskredietkaart of de maandelijkse declaraties van medewerkers extra oplet bij posten die verwijzen naar cloudaanbieders. Dat veronderstelt samenwerking tussen boekhouding en IB'ers of de IT-security staff, iets dat in zijn optiek wel vaker voor verbetering vatbaar is.

Oordeel over Secure Cloud

Aan de hand van zeven verschillende begrippen is een beeld geschetst van de complexiteit die onlosmakelijk verbonden is met het gebruik van clouddiensten. Waar de meeste events voor een beperkte invalshoek kiezen, heeft Secure Cloud nadrukkelijk voor een brede kijk op de materie gekozen. Dat maakte de tweedaagse bijeenkomst soms lastig te volgen, maar het bood zowel plenair als in de marge van de bijeenkomst heel wat ruimte de samenhang tussen de verschillende factoren te analyseren. Zoals te verwachten viel: voor geen van de genoemde problemen was na de twee dagen een kant en klaar antwoord beschikbaar.
Misschien is dat ook het best mogelijke resultaat. Iedereen die hoopte direct toepasbare oplossingen gepresenteerd te krijgen keerde wat dat betreft met lege handen naar huis. Hij of zij heeft wel geleerd dat het inzien van de samenhang tussen de verschillende factoren meer dan eens nodig is om te begrijpen waarom cloud – as we know it – in de perceptie van vooral gebruikers niet veilig genoeg kan zijn. De balans vinden tussen emotie en ratio, tussen verwachtingen en realiteit, weten dat het geen of-of keuzes betreft, dit alles veronderstelt inzicht in de factoren die inhoud geven aan het begrip cloud. Wat dat betreft is de opzet van deze conferentie zonder meer geslaagd.

Links

[1] https://cloudsecurityalliance.org/

[2] https://www.enisa.europa.eu/?

[3] https://www.fokus.fraunhofer.de

[4] https://cloudsecurityalliance.org/events/securecloud2014/#_agenda

[5] https://www.grnet.gr/

[6] http://www.computable.nl/artikel/opinie/cloud_computing/5049473/2333364/iso-27001-is-geen-garantie-voor-veilige-cloud.html

[7] http://www.iriss.ie