



CSO Interchange

Contact:
Theo Loth, Loth PR Writing
+31 652 322 210
theo@loth.nl

Nog veel onduidelijkheden over de veiligheid van Cloud Computing

Derde CSO Interchange Dinner in het teken van 'Security and the Cloud'

Haarlem, maart 2010 — De term Cloud Computing leeft heel nadrukkelijk in ICT. De voordelen van het via internet aanroepen van data, applicaties en rekenkracht zijn immens. Maar toch bestaat er nog veel bezorgdheid over de veiligheid van Cloud Computing. Is die zorg terecht? Deels. Cloud Computing heeft – ook op het vlak van security - implicaties die nog lang niet allemaal in kaart zijn gebracht. Tegelijkertijd biedt het extra mogelijkheden om de beveiliging van infrastructuren te verhogen. Dat was een van de conclusies tijdens het CSO Interchange Dinner, gehouden op 4 februari op de Euromast te Rotterdam. Ongeveer 25 CSO's en CISO's hebben deelgenomen.

CSO Interchange (www.csointerchange.org) is een exclusief ontmoetingsplatform voor CSO's en Chief Information Security Officers (CISO's) van toponderningen. Tijdens de CSO Interchange Dinners delen zij in beslotenheid hun zorgen en hun *best practices*. De diners worden regelmatig en op *invitation only* basis gehouden.

Keynote speaker van de bijeenkomst op 4 februari was de CISO van een internationale autofabrikant. De titel van zijn presentatie was *Cloud Computing How relaxed can we be?* Zijn bedrijf maakt al vele jaren gebruik van externe hosting, Cloud en SaaS. Zelfs voordat die termen algemeen ingang vonden. De CISO: "Als we de definitie van security evangelist Bruce Schneier aanhouden, dat Cloud Computing het runnen van software op de harde schijf van iemand anders is, dan is er niets nieuws onder de zon." Hij liet zien hoezeer ICT is verweven met de primaire bedrijfsprocessen van de autofabrikant. "Sterker nog, zonder ICT houdt alles op bij ons. Er rijdt geen auto de fabriek meer uit." Om de bedrijfscontinuïteit te beschermen, heeft de autofabrikant een effectief securitybeleid geformuleerd, gebaseerd op ISO/IEC 27000 normering. "Dat moet ons in staat stellen om op elk gewenst moment inzicht te krijgen in ons risicoprofiel, vanaf het hoogste aggregatieniveau tot, indien noodzakelijk, op het laatste detailniveau van het device." Deze geavanceerde vorm van risk management maakt het de autofabrikant mogelijk verantwoord SaaS en Cloud diensten in te zetten, indien nodig en wenselijk. Deze worden volledig geïntegreerd in de supplychain-risicoanalyse.

Volgens de CISO is de keuze van het al dan niet adopteren van Cloud Computing vooral een kwestie van het managen van het risico bij de toeleveranciers in de complete keten, ook bij leverancier verderop in de keten. Wat dat betreft wijkt Supply Chain Management voor IT in niets af van die van de productie. Het concept van een keten van opeenvolgende dienstverleners is algemeen bekend in de automobiellindustrie. "Meer dan 70% van de waarde van de door ons geproduceerde auto's wordt extern ingekocht".

Voer dit concept in van "Direct Line Feeding" (Just-in-Time bevoorrading van de productieketen)

rechtstreeks vanaf de leveranciers van het eerste niveau) en u begrijpt meteen dat de kleinste onachtzaamheid van een leverancier op niveau twee, drie en verder de hele assemblageketen kan stilleggen. Een dergelijke verstoring kan te wijten zijn aan technische problemen maar ook aan financiële (liquiditeitsproblemen die een invloed hebben op de bevoorrading) of menselijke factoren (stakingen). Om zich hiervan te vrijwaren, moet de opdrachtgever in staat zijn de betrouwbaarheid te evalueren van de belangrijkste dienstverleners in de hele keten van leveranciers die een impact kunnen hebben op het productieproces.

In welke mate houdt dit verband met Cloud Computing? Om te beginnen, is de notie van real-time in het verbruik van de gegevens en de verwerking in de wolk dezelfde, net zoals de verhoogde afhankelijkheid van IT. Ook, en vooral, is de leverancier van de Cloud dienst afhankelijk van een groot aantal andere leveranciers (netwerkapparatuur, besturingssystemen, virtualisatieplatform, hosting, stroomvoorziening, enz.).

Daarom kan de door de fabrikant gekozen aanpak om zich te beschermen tegen het risico van nalatigheid door een dienstverlener CSO's inspireren die zich aangetrokken voelen tot de Cloud. De spreker gaf uitgebreid uitleg bij vier essentiële punten van zijn strategie:

1. Vraag en krijg duidelijke antwoorden over certificering (bijv. ISO) en best practices die contractueel vastgelegd kunnen worden.
2. Eis transparantie ten opzichte van de andere uitbestedingcontracten die de leverancier heeft lopen.
3. Eis toestemming in elk nieuw uitbestedingcontract dat ondertekend wordt tijdens de relatie. Eis dat de leverancier niet overgenomen mag worden door de concurrent.
4. Formaliseer een exit-strategie die een goede afloop waarborgt in geval van beëindiging, misschien door een bonus in het vooruitzicht te stellen. Wat de zaak ietwat compliceert, is de noodzaak deze aanpak verder in de keten te repliceren.

In het ideale geval wordt de leverancier van de Cloud dienst aangemoedigd om dezelfde eisen toe te passen op zijn eigen belangrijkste leveranciers en zo verder de keten in, om zo aan de opdrachtgever (de eindklant) een algemeen beeld van het leveranciersrisico te kunnen voorleggen. Implementatie van ISO door de keten heen kan hierin van pas komen. Het wordt dan mogelijk om, volgens identieke criteria, elke leverancier van de leverancier die betrokken is in de servicesketen te evalueren. En ook om hen, naargelang hun mate van compliance (bijvoorbeeld in termen van transparantie over de uitbestedingcontracten van de leverancier of de weigering goed practices bijvoorbeeld op het gebied van passwords te bespreken), een status toe te kennen die de relatie met deze dienstverlener zal bepalen. Bij de fabrikant wordt de leveranciersrelatie beschreven in termen van actie: groeien, ontwikkelen, laten leven, "passief", beëindigen.

Deze aanpak is relatief makkelijk en tegen lage kosten te implementeren. Niet alle leveranciers hoeven even strak gemanaged te worden. "Je moet niet alles willen controleren, alleen die zaken waar je je zorgen over maakt. Als onze dieselleverancier bijvoorbeeld geen diesel kan leveren, is een andere leverancier zo gevonden. Deze hoeft je dus niet op te nemen in het controleframework." Risico's kunnen ook geaccepteerd worden indien er voldoende veiligheidsvoorraad aanwezig is.

De automobieliindustrie is uiteraard veel volwassener dan Cloud Computing. Maar de gepresenteerde aanpak geeft misschien de juiste richting aan.

Enisa

Onderzoeksjournalist Brenno de Winter ging vervolgens in op het in november verschenen ENISA Report *Cloud Computing Risk Assessment*. De voornaamste conclusie van het Report is dat de *economies of scale* en de flexibiliteit van de Cloud vanuit het oogpunt van veiligheid zowel een lust als een last zijn. De enorme concentratie van systemen en gegevens vormen een aantrekkelijk doelwit voor aanvallers, maar tegelijkertijd kan een op Cloud-gebaseerde verdediging meer robuust, schaalbaar en kosteneffectief worden opgezet. De Winter toetste vanuit zijn praktijk als security journalist en vanuit zijn eigen ervaringen met het onderhavige onderwerp een vijftal stellingen uit het Report.

Enisa waarschuwt voor “Loss of Governance” ten gevolge van Cloud Computing. Organisaties moeten ermee rekening houden dat hun werknemers Cloud services zoals Google Apps gaan gebruiken, of het nu wel of geen onderdeel is van het IT beleid van de onderneming. De Winter: “Welke *governance*? De meeste organisaties hebben helemaal geen IT policies. En als ze die al hebben, worden ze niet of nauwelijks nageleefd. Ik heb onthutsende staaltjes van naïveteit meegemaakt op het gebied van security. Met een goed verhaal kom je overal binnen.”

Enisa wijst op het gevaar van Vendor Lock-in. De Winter: “Dat is geen verschil met meer traditionele vormen van IT. Dit gevaar valt heel gemakkelijk te omzeilen: gebruik open standaarden.”

Een ander risico dat Enisa onderkent is de mogelijkheid dat er lekken ontstaan in de Cloud. ‘*multi-tenancy*’, het draaien van de infrastructures van meerdere klanten op een gevirtualiseerd systeem, en gedeelde resources zijn specifieke kenmerken van Cloud Computing. Dit brengt het risico met zich mee dat mechanismen falen om opslag, geheugen of routing van elkaar af te grendelen. Dit kan leiden tot zogeheten *guest-hopping attacks*: het door aanvallers gebruik maken van gaten in de virtualisatieinfrastructuur om van de ene *tenancy* naar de andere te gaan. De Winter: “Dit is technisch vooralsnog erg lastig. Maar het kan veel gemakkelijker. Het is mij meermalen gelukt datacenters binnen te lopen en tot de ruimtes door te dringen waar gedeelde server stonden opgesteld. Even inprikken, en je zit in de klantsystemen”.

Enisa waarschuwt verder voor Compliance risico’s. Het kan zijn dat de organisatie aanzienlijke investeringen heeft gedaan in certificering om te kunnen voldoen aan wet- en regelgeving. De overgang naar de Cloud kan deze investeringen in gevaar brengen als de Cloud service provider zelf niet in staat is zijn compliance aan te tonen, of als de provider de klant niet toestaat om zijn systemen aan een *audit* te onderwerpen. Het kan in sommige gevallen zelfs betekenen dat het gebruik van een publieke Cloud bijvoorbeeld PCI DSS certificering in de weg staat. PCI DSS zijn de eisen op het gebied van informatiebeveiliging die de Payment Card Industry stelt aan alle credit- of bankkaartaccepterende bedrijven. De Winter: “Dit is een serieus issue. Bedrijven zouden voor zichzelf de afweging moeten maken of de kosten van het niet-compliant zijn opwegen tegen de kosten om het wel te zijn of te blijven. *To be or not to be compliant, that’s the question.*”

Een laatste risico bestaat uit de compromittering van management interfaces. Management interfaces van systemen in de Cloud zijn toegankelijk via het Internet en ze zetten de deur open naar een grotere hoeveelheid aan systemen en resources dan de traditionele hosting providers doen. Om die reden betekenen ze een groter risico, speciaal bij een combinatie van *remote access* en *web browser vulnerabilities*. “Nu Microsoft de beveiliging van zijn client-producten steeds beter onder controle heeft, verleggen cybercriminals hun focus naar het web. Management interfaces en web applicaties gaan het zwaar te verduren krijgen.”

SecurityVibes

Tijdens het diner werd ook SecurityVibes gepresenteerd. De online community www.securityvibes.com is uitsluitend toegankelijk voor beslissers op het gebied van informatiebeveiliging op CSO/CISO niveau. Deelnemers kunnen hier in alle beslotenheid kennis en ervaringen uitwisselen, noodzakelijk om snel in te kunnen spelen op ontwikkelingen in security. SecurityVibes is in 2008 in Frankrijk gestart. Vorig jaar is de Britse community geopend. Naar verwachting zal na de zomer een Nederlandstalige community van start gaan, gericht op de Benelux. Belangstellenden kunnen zich nu al aanmelden voor ballotage bij de Engelse site.

De volgende CSO Interchange Dinner vindt plaats op xx yyy 2010 op een nog nader te bepalen locatie.

Kijk ook op www.csointerchange.org. Meldt u aan op SecurityVibes, de online community van CSO's/CISO's: www.securityvibes.com

Klik [hier](#) als u geen informatie meer wilt ontvangen van CSO Interchange.

CSO Interchange

The CSO Interchange is an intimate, invitation-only forum to discuss ideas and trends concerning all CSOs. There are no product pitches and no sales personnel, just frank talk on important security issues facing you and your peers.

CSO Interchange is a non profit, non-commercial organization, founded by Howard Schmidt, former Cyber Security advisor to the White House and Philippe Courtot, Chairman & CEO, Qualys Inc.