COMPUTERWORLD
Management special

CLOUD IS ZO VEILIG ALS de zwakste schakel

Door: Martijn Kregting

CLOUD IS ZO VEILIG ALS de zwakste schakel

Werken in de cloud, data opslaan in de cloud: het brengt voor organisaties grote voordelen met zich mee. De risico's en onzekerheden zijn net zo groot, maar welke risico's en gevaren zijn reëel? Hoe ontwikkel je goed beleid op het gebied van cloud-risico's, om op basis daarvan af te wegen of en zo ja wat er in de cloud gaat of mag?

De cloud is overal, het gebruik van clouddiensten groeit snel. Gmail, Dropbox, WhatsApp, zijn bekende publieke clouddiensten. Op zakelijk gebied worden de termen cloud en (X)aaS vaak door elkaar gegooid, wat de duidelijkheid niet altijd vergroot. Onderzoeksbureau Gartner stelt dat SaaS-diensten in 2012 mondiaal een omzet van 14,5 miljard dollar realiseerden. Voor 2015 wordt een omzet van 22,1 miljard dollar voorspeld. Toenemende bekendheid met SaaS-modellen, ICT-projecten die steeds buiten het budget gaan, de groei van PaaS (Platform-as-a-Service) en de belangstelling voor cloud computing jagen de adoptie van SaaS aan.

De voordelen van cloud en XaaS-diensten zijn duidelijk: flexibiliteit, schaalbaarheid, geen investeringen meer in licenties of hardware vooraf, maar betalen per gebruiker, per maand. Maar elk voordeel heeft een nadeel. Wie zijn data, toepassingen of infrastructuur deels of volledig uitbesteedt, dient daar rekening mee te houden. Hoe vind je een goede balans tussen de voor- en nadelen en wie kan daarmee behulpzaam zijn? Hoe krijg je inzicht in en grip op risico's? In deze tweede cloudspecial kijken we naar de noodzaak om goed beleid te ontwikkelen en de afwegingen die een organisatie moet maken bij een keuze voor een clouddienst.

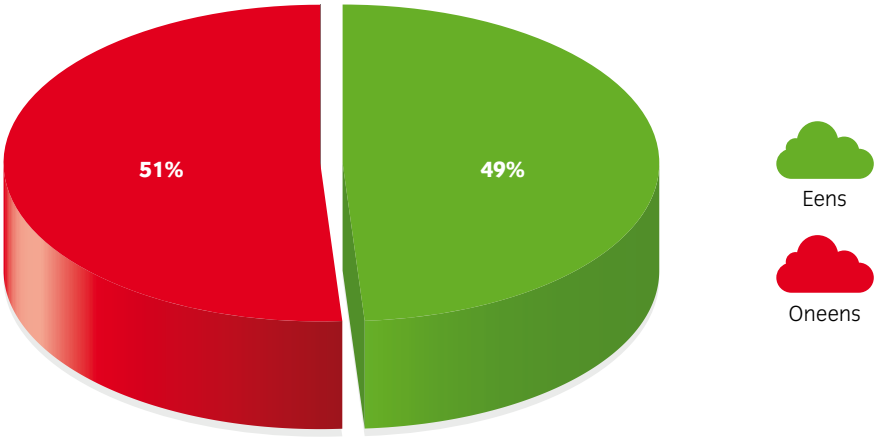
Beleid en risicoprofiel

Het is belangrijk om inzicht te hebben in en actief beheer te hebben over het zakelijk gebruik van alle apparaten die toegang hebben tot de cloud. Het blijft mensenwerk, dus je zult de personen die toegang hebben tot het netwerk ook bewust moeten maken van de gevaren. Het is belangrijk om voldoende

draagvlak te hebben voor de IT-beveiliging. Hoe zorg je ervoor dat je goed beleid ontwikkelt of hierin kan adviseren inzake security, veilig gebruik van cloud-diensten?

Security is vaak gericht op de IT van gisteren, niet op de IT van morgen – mobiele toepassingen en cloudgebruik. Kijk je naar beveiliging van dergelijke cloudapplicaties, dan blijkt dat het merendeel van de organisaties niet weet hoe zij hun netwerk en hun data goed moeten beveiligen tegen risico's van verlies of diefstal. Slechts negen procent zegt bereid te zijn wel in de opbouw van deze kennis te willen investeren, vertelt Peter Vermeulen, directeur van marktonderzoeksbureau PB7.

Figuur 1: "We hebben onvoldoende kennis in huis om te garanderen dat we cloudoplossingen veilig gebruiken" (Organisaties > 50 werknemers)



Bron: Nationale IT Security Monitor 2014, Pb7 Research

Omdat bedrijven niet goed weten hoe ze moeten omgaan met het steeds complexere, ondoorzichtige gebruik van mobiele en cloud-applicaties, wordt er vaak ingezet op repressie, op niet mogen gebruiken, maar dat is zinloos. Men vindt toch wel een manier om die repressie te omzeilen. Dit is in feite de eerste, vaak overgeslagen stap, die nog voor het toepassen van technische security-oplossingen komt. Langzaam lijkt het besef bij organisaties door te dringen dat men expliciet beleid moet ontwikkelen, ook op nieuwe vormen van IT-gebruik, om zo de menselijke risico's beter aan te pakken. Er is altijd een middenweg tussen alles verbieden en alles toestaan.

Het is wel moeilijk om zelf een goed beleid te ontwikkelen op het gebied van security wanneer de kennis op dat gebied deels of geheel ontbreekt. Voor een deel zal een organisatie die beleid hierop wil ontwikkelen deze kennis toch echt zelf moeten opbouwen. Maar groot of klein, geen enkele organisatie heeft zijn security volledig in eigen handen. Niemand schrijft nog zijn eigen antivirusprogramma's. Het maakt minder uit in hoeverre je advies over security en het beheer van security uitbesteedt, belangrijker is dat je zelf de regie in handen houdt.

Risicoprofiel

Beleid is net zo belangrijk als security zelf, stelt Gerard Klop, consultant cyberdreigingen en security management bij Motiv. "Dat was al zo voordat de cloud er was. Je moet weten wat je wil met je IT, wat mag en wat niet mag, wat mogelijke bedrijfsrisico's zijn en welke risico's acceptabel zijn, of juist niet. Pas met een duidelijk risicoprofiel kun je overwegen bepaalde diensten, infrastructuur of capaciteit op cloudbasis af te nemen. Biedt een cloudaanbieder afdoende zekerheiden om te voldoen aan je risicoprofiel? Zo niet, zijn er dan mogelijkheden om met eigen toevoegingen de risico's afdoende af te dekken?

Ook is het belangrijk dat de business goed beseft wat risico's zijn van het gebruik van cloud-diensten ten opzichte van het bedrijfsbeleid. Accepteert men die risico's? Nu is het vaak zo dat IT 'omzeild' wordt bij de keuze voor een cloud-dienst en pas wordt ingeschakeld bij de uitvoering. Dat doet men dan zonder te beseffen wat dit voor het risicoprofiel betekent. Een nieuwe rol van de IT-afdeling is om hierin te adviseren en te begeleiden, meent Klop. "Heel simpel is dat ook mede het bestaansrecht van de IT-afdeling wanneer men steeds meer de cloud in gaat: een andere vorm van ondersteuning van de business."

Technologie ondersteunt beleid

Op technologisch niveau kun je beleid flexibel inrichten via security-instrumenten, zoals op app-niveau of op gebruikersniveau. Daar zijn genoeg mogelijkheden voor. Zo kun je regelen dat voor bepaalde devices het doen van financiële transacties niet mogelijk is. Verder kun je encryptie toepassen, authenticatie of authorisatie-sleutels gebruiken.

Het is afhankelijk van de capaciteit van de IT-afdeling of dit ook haalbaar is. Uitbesteden van security is een optie, maar zeker bij kleinere bedrijven zullen de kosten vaak niet opwegen tegen de verwachte baten. Ook grotere organisaties moeten de risico's van het gebruik en het beveiligen van cloud-diensten goed afzetten tegen de verwachte voordelen. Dat moet eigenlijk per IT-segment (communicatie, werkomgeving, procesapplicaties), per soort data (e-mail, financiële gegevens, klantdata): is een cloud-dienst veilig genoeg, of beter gezegd: is het risico acceptabel?

IT en business: samen kijken

IT en business moeten samen kritisch kijken naar nut en risico's van cloudgebruik. Daar kan ook uit komen dat het beter is om met een hostingpartij in zee te gaan en zelf het beheer van de beveiliging in handen te houden, of deze beveiliging precies op maat te laten inregelen door een IT beveiligingsspecialist.

Kies je er voor om deels of geheel voor de cloud te gaan, dan wordt het een kwestie van kijken naar de SLA's en de mate van security die een cloudaanbieder heeft, meent Martijn van Lom, managing director Kaspersky Benelux & Nordic. "Is dat afdoende in relatie tot hoe bedrijfskritisch gegevens of applicaties zijn? Bij een werkplekomgeving kan het risicoprofiel op een lager niveau liggen dan bij een CRM-applicatie."

Cloud dringt door in bedrijfsleven

Ongeveer 35 procent van de Nederlandse ondernemingen met 50+ medewerkers gebruikte begin 2014 één of meer applicaties uit de cloud, 40 procent meer dan een jaar eerder. Vooral de uitrol van SaaS-dienst Microsoft 365 zorgde voor deze groei, stelt Computer Profile. Verder groeide het gebruik van HR-toepassingen en branchespecifieke oplossingen uit de cloud aanzienlijk.

De onderwijssector blijft veruit koploper in het gebruik van oplossingen die niet op de eigen locatie draaien. 79 procent van de ondervraagde onderwijsinstellingen geeft aan één of meer cloud/SaaS-applicaties te gebruiken. Dit komt voor een flink deel op het conto van branchespecifieke oplossingen zoals voor leerlingenadministratie, lessen en roosters. Bekeken per grootte van ondernemingen maken alleen organisaties met 100-200 werknemers bovengemiddeld gebruik te maken van cloud/SaaS-applicaties (43%).

De meest gebruikte SaaS-diensten zijn HR-oplossingen (28%). Verticale oplossingen (branchespecifiek) zijn goed voor 21 procent en office-applicaties voor 19 procent. Microsoft is in Nederland de grotoste leverancier van SaaS-oplossingen (vooral Office 365), met een penetratie in de markt van 17,8 procent. Schoolmaster (branchespecifiek voor het onderwijs) staat met 9,2 procent op 2 en Raet (HR) met negen procent penetratie op drie.

Bron: Computer Profile, april 2014

Afwegingen en overwegingen

Hoe goed je beleid ook is, hoe goed de beveiliging van clouddienst ook mag zijn, het is zeer de vraag of data 100 procent veilig kan worden opgeslagen in een cloud-omgeving. Peter Vermeulen is hier stellig over: “Dat is niet mogelijk. Je kunt proberen een netwerk dicht te timmeren, maar zelfs een stand alone pc kan besmet worden of data verliezen als iemand er een usb-stick in stopt.”

Martijn van Lom onderschrijft dit. “Dat betekent dat je moet gaan voor een andere vorm van security bij clouddiensten. Beveilig de data zelf, via encryptie, voordat gegevens via een server of een endpoint de cloud in gaan. Goede encryptiesoftware kan ook aantonen of er een poging is gedaan om gegevens te stelen of te bewerken onderweg. Eén tip: bewaar je encryptiesleutels niet in de cloud. Dat is hetzelfde als een kluissleutel op de kluis leggen.”

Veilig versus goedkoop

Wanneer 100 procent veilig niet bestaat, blijft de vraag over hoe het beste de afweging kan plaatsvinden tussen de businessvraag naar goedkopere clouddiensten, infra (netwerk- en computercapaciteit) en de wens dit zo veilig mogelijk te doen. Hoe regel je deze vorm van datastorage en verwerking zo goedkoop mogelijk voor zowel live-data als data-in-ruste?

Zo goedkoop mogelijk is natuurlijk een relatief begrip, meent Gemma Kerkhof, inside sales & marketing bij IT-aanbieder Lantech. “Ik denk dat het moet gaan om een goede kwaliteit-prijs verhouding. In verschillende prijscategorieën zijn er mogelijkheden. De afweging is dus: hoe belangrijk is de beveiliging van de cloud en wat heeft het bedrijf hiervoor over? Hoe willen we de cloud beveiligen? Alleen door de toegang van apparaten beter te beveiligen of maken we ook gebruik van actief beheer van de apparaten, een goede firewall? Hier is belangrijker hoeveel geld het bedrijf eraan wil besteden. Er zijn verschillende vormen van datastorage en verwerking, waarbij de ene manier voor een bedrijf beter werkt dan de andere - en zo kunnen beide varianten goedkoper zijn.”

Drie varianten van in de cloud gaan:

- Alles uitbesteden, een publieke SaaS-dienst met standaard security.
- Zelf elementen op security-gebied toevoegen aan een cloud-dienst om tot een acceptabele beveiliging te komen, of dit door een derde partij laten doen.
- Bij een aanbieder van housing capaciteit inhuren en verder alles zelf regelen: eigendom, onderhoud, security. Ook dan kun je alles uitbesteden aan gespecialiseerde hosting en IT security partijen, maar zelf hou je meer de regierol.

Bedrijfskritisch of niet?
Wanneer is iets bedrijfskritisch? Wat mag niet, nooit in verkeerde handen vallen? Zelfs dan bestaat 100 procent zekerheid niet, maar je kunt dan wel beter bepalen in welke mate en wat voor soort cloud-security je toepast, of je iets in een cloud zet of niet. Ga je voor bescherming of ga je voor monitoring? Een goede monitoring kan ervoor zorgen dat je direct afwijkingen opmerkt in gebruik van data en daar op kan reageren. Dan hoef je niet alles te beschermen. Een perimeterdefensie-mentaliteit werkt namelijk niet meer in een cloud-omgeving met overal toegang.

Businessbelang
Hoe groot is het belang van de business bij een open organisatie? Over het algemeen geldt dat hoe opener je business is, hoe groter de innovatiefactor en hoe meer kans op succes en groei. Dan hebben we het even niet over defensienetwerken of de belastingdienst, daar heb je ook andere prioriteiten. Maar hoe opener je organisatie – en daarmee ook je netwerk – is naar partners, toeleveranciers, klanten, hoe groter de kans op zakelijk succes. Het is wel een extra uitdaging om dat in een zo flexibele omgeving als 'de cloud' toe te passen.

Niet alles hoeft in de cloud
Verder hoeft niet alles in de cloud. Steeds meer grotere organisaties gaan er toe over om hun kernprocessen – CRM- of ERP-systemen bijvoorbeeld, op locatie of in een private cloud te laten draaien. Wat meer aan de randen draait, zoals een werkomgeving of communicatie – unified communications, collaboration – wordt wel steeds meer op cloudbasis afgenomen. Ook hier geldt de afweging kosten versus de mate van veiligheid. Hybride cloud-oplossingen maken momenteel de grootste groei door. Deels publieke cloud, soms deels private cloud en oplossingen of data op een eigen locatie. Die mix kan veranderen al naar gelang het belang van data of oplossingen verandert.

Uitbesteden, zelf doen?
Uitbesteden of zelf doen ligt volgens Gemma Kerkhof mede aan de kwaliteiten die een bedrijf in huis heeft en aan de IT-afdelingen. Soms is het beter om afhankelijk advies in te winnen en dan de implementatie zelf te doen, of alleen de software (en evt. hardware) uit te besteden. In andere gevallen kun je beter het hele traject uitbesteden.

Peter Vermeulen: "Voor security geldt dit net zozeer als voor elke IT-oplossing: moet je of wil je alles uitbesteden, en doe je dat bij één aanbieder (de school van de 'totaaloplossing'), of kies je mede op basis van eigen kennis en eventueel extern advies voor een best of breed oplossing van meerdere leveranciers? Volledig uitbesteden van security is wellicht het meest handig voor SOHO-bedrijven en de onderkant van het mkb, aangezien zij de capaciteit er niet voor hebben. Gaat het om oplossingen van in verticals gespecialiseerde cloud-aanbieders, dan zit security ook steeds vaker al in de oplossing ingebakken."

In veel gevallen is 'zelf alles doen' een vorm van schijnzekerheid, meent Gerard Klop. "Je hebt niet de controle als je niet de expertise hebt. Zeker bij veel kleinere organisaties ontbreekt de expertise op security-gebied. IT-mensen werken liever voor een grotere organisatie. In dat opzicht is het beter om ook security voor je cloud diensten uit te besteden."

True: 'Cloudbeleid begint en eindigt met bewustwording'
Algemeen security-beleid, specifiek cloudbeleid, alles valt of staat met bewustwording van de mensen in de organisatie. Zonder bewustwording, zonder kennis van de risico's van het gebruik van cloud-diensten, heeft technologie weinig toegevoegde waarde.

Dat heeft Jan-Paul van Burgsteden, CTO van True, aanbieder van cloud-oplossingen, managed en hosted diensten voor de zakelijke markt, zowel in de eigen onderneming als bij klanten ervaren."Onze interne ervaringen zijn weinig anders dan bij klanten. Maar aangezien wij ook verantwoordelijk zijn voor klantdata, is het voor ons wel noodzaak om in ons beleid voor de muziek uit te lopen."

Inzicht in risico's
Zonder inzicht in de mogelijke risico's van cloudgebruik in een organisatie, heeft bewustzijn kweken weinig zin. "Zonder kennis van risico's kun je geen enkele maatregel nemen, of het nou gaat om policies, om wat wel of niet mag of om duidelijkheid over gevaren van het gebruik van cloud-diensten."

Als bijvoorbeeld zwakke wachtwoorden een groot risico blijken te zijn, kun je bepalen wat de beste aanpak is. Van Burgsteden: "Je kunt wel het gebruik van moeilijke wachtwoorden afdwingen, of wachtwoorden vaak laten wijzigen. Maar dan is het menseigen om wachtwoorden ergens te noteren en zo het beleid te ondergraven. Dergelijk beleid heeft ook niets te maken met bewustwording. In zo'n geval kan uit een risico-inventarisatie blijken dat technologie meer resultaat oplevert. Bijvoorbeeld het opzetten van een veilige VPN-verbinding om toegang tot data of diensten in de cloud te ontsluiten. Of het vereenvoudigen van het gebruik van wachtwoorden, via meerdere authenticatieniveaus, of een single sign on."

Geen one-size-fits-all
Zelf werkt True veel met versleutelde verbindingen. Soms wordt de data zelf versleuteld. Van Burgsteden : "Je moet nooit op één niveau van beveiliging vertrouwen. Er is geen one-size-fits-all. De bestellijst voor de lunch heeft een andere waarde dan financiële data." Aan de andere kant: wie doorschiet in differentiatie van security-niveaus, maakt het weer erg complex voor een gebruiker. "Je hebt data die publiek mag zijn, informatie en toepassingen die voor iedereen intern toegankelijk zijn en je hebt gegevens die ook intern slechts beperkt toegankelijk zijn. Dat is een prima, werkbare verdeling."

De juiste instrumenten
Faciliteren is ook een belangrijk onderdeel van cloudbeleid. Zonder de juiste instrumenten om een functie goed uit te voeren, zoeken werknemers alternatieven. Met de opkomst van mobiele devices is dat nog veel eenvoudiger voor gebruikers en lastiger te beheersen voor de IT-afdeling. Dropbox is een berucht voorbeeld van een publieke clouddienst die gebruikt wordt om (ook privacygevoelige) bestanden uit te wisselen. "Mensen moeten snappen wat gevoelige informatie is en hoe ze daarmee om dienen te gaan. De organisatie moet dan wel de juiste instrumenten bieden: een goede balans tussen gemak en veiligheid."

Waar ligt verantwoordelijkheid?
Wat vindt True als cloudaanbieder over waar verantwoordelijkheid ligt voor de beveiliging van clouddiensten? Van Burgsteden: "Dat ligt er aan. De organisatie bepaalt welke werknemer bij welke toepassing of informatie mag. De verantwoordelijkheid daarvoor ligt in eerste instantie bij die organisatie. Wil je zeker weten voor welke security-issues een app-ontwikkelaar of cloudprovider verantwoordelijk is, maak dan duidelijke afspraken. Zoek desnoods uit welke providers een eigen security-afdeling hebben en de lat al hoog leggen. Weet wat je kunt verwachten en weet wat je zelf moet doen. Vaak heeft een cloudprovider al meer geregeld dan je denkt. Zo hebben wij, met onze netwerkpartner Infradata, ons cloudplatform op meerdere lagen beveiligd."