Cloud-security kun je nooit volledig uitbesteden

5 februari 2016 10:00 | Jeroen Renard | 1

Als je de recente security-onderzoeken leest, dan wordt het internet of things (IoT) vrijwel overal aangemerkt als een groot risico voor de toekomst. Met name de 'headless devices' spelen een steeds grotere rol in ons leven en zijn daarom ook een interessant doelwit voor hackers. In de meeste gevallen zijn echter de bedrijfsrisico's die ze introduceren nog beperkt. Cloud introduceert wat dat betreft veel grotere risico's. Wordt dit wel voldoende erkend?

Nederland is een uiterst progressief land als het gaat om technologie-adoptie. Daar komt bij dat wij een zeer groot mkb hebben en steeds minder van deze bedrijven er nog voor kiezen om hun it zelf te beheren. Er wordt daardoor steeds meer gebruik gemaakt van cloud-diensten, van kant-en-klare SaaS-diensten tot virtuele infrastructuur. In dit model is traditionele security helaas niet toereikend, wat zowel voor de gebruiker als de aanbieder geldt.

Eindgebruikers zouden veel bewuster moeten zijn van het feit dat hun bedrijfsapplicaties en data in principe overal ter wereld toegankelijk zijn voor mensen met de juiste login-credentials. Die gegevens zijn vaak maar al te gemakkelijk te stelen van een nietsvermoedende gebruiker via bijvoorbeeld een phishing e-mail. Maar ook de cloud-aanbieders hebben te maken met continue aanvallen op hun infrastructuur. Er is immers enorm veel waardevolle bedrijfsdata in hun publieke clouds opgeslagen. Hackers zullen daarom zeer ver gaan om hier op in te breken. Dit is de huidige stand van zaken in ons cloud-landschap, maar dat is pas het begin.

Hoe veilig is de publieke cloud?

Vanzelfsprekend kan geen enkele cloud-dienstverlener zich de reputatieschade van een grootschalig beveiligingslek permitteren. Toch vind ik dat zij lang niet allemaal even open zijn over de beveiligingsmaatregelen die zij hebben getroffen om de bedrijfsdata van hun klanten te beschermen. Je kunt wel beweren dat bedrijfsdata 'optimaal is beveiligd' en dat er wordt gewerkt op basis van de ISO 27001-certificering, maar wat zegt dat?

Ook al zal niet elke klant er behoefte aan hebben, mijn ervaring is dat het veel vertrouwen schept wanneer een bedrijf inzichtelijk maakt hoe er precies met security wordt omgegaan, zowel technisch als procesmatig. Bovendien zorgt het ervoor dat de klant zich ook bewuster wordt van zijn rol bij de beveiliging van zijn data. Dit is volgens mij het belangrijkste aspect bij het veilig omgaan met bedrijfsdata in de cloud.

Organisaties moeten hier ook hun eigen verantwoordelijkheid bij nemen. Security kun je niet volledig uitbesteden, maar dit moet in overleg en samenwerking met de dienstverlener geregeld worden. De cloud-dienstverleners hebben zelf vaak al een doorlopend programma van *vulnerability scans* en *penetration tests* om hun eigen security te testen, maar ook hun klanten hebben in veel gevallen een *right to audit*. Organisaties die daar gebruik van maken, hebben het goed begrepen, ook al moet het wel binnen bepaalde grenzen gebeuren. Het heeft immers geen zin om dubbel werk te doen. Daarom is het ook zo belangrijk dat cloud-dienstverleners open communiceren over de getroffen security-maatregelen.

Doorlopende wapenwedloop

Zijn bedrijven nog wel veilig in ons groeiende cloud-landschap? Ik denk dat daar geen eenzijdig antwoord op mogelijk is. Het palet aan leveranciers en dienstverlening is daar te divers voor. Wel zie ik dat er in Nederlandse datacenters steeds zwaardere maatregelen worden overwogen om de security van it-infrastructuren te borgen. Geavanceerde oplossingen voor *vulnerability scanning, firewalling*, reguliere pentests en zelfs het inrichten van volwaardige Security Operation Centers (SOC). Dit zijn veel kostbaardere diensten dan voorheen noodzakelijk werden geacht.

Men hoopt natuurlijk dat deze intelligentere vormen van security je als organisatie beter beschermen tegen aanvallen. Dit geldt volgens mij alleen voor scriptkiddies, de echte goede hacker hou je er niet mee tegen. Om die reden is iets als *responsible disclosure* ook van groot belang. Ofwel: het goed omgaan met white hat hackers die security-lekken in je omgeving melden. Zij helpen je immers om potentiële gaten in je beveiliging te dichten. Toch komt het nog steeds voor dat dit soort meldingen worden beantwoord met een aangifte bij de politie.

We moeten accepteren dat security in de cloud een wapenwedloop is en dat dit waarschijnlijk altijd zo zal blijven. Bedrijven moeten daar steeds in mee gaan om risico's beheersbaar te maken. Dit betekent dat zij continue aandacht moeten hebben voor hun it-security en de ontwikkelingen op het gebied van beveiligingslekken.

Daarnaast moet er kritisch gekeken worden naar de risico's van populaire trends als IoT, byod, maar bijvoorbeeld ook naar het gebruik van persoonlijke e-mail of andere online diensten voor werkdoeleinden. Het is onmogelijk om goede security te garanderen als je tegelijk allerlei onbeheerde devices en diensten toelaat te verbinden met je bedrijfsnetwerk.

Security draait uiteindelijk om de vertrouwelijkheid van data en de 24/7 beschikbaarheid van je bedrijfsinfrastructuur. Je kunt veel van deze verantwoordelijkheden uitbesteden naar een cloud-dienstverlener, maar uiteindelijk ben je zelf eindverantwoordelijk. Ga daarom in gesprek met je dienstverlener over security en vraag om meer dan het standaard riedeltje. Alleen dan kun je een acceptabel niveau van veiligheid garanderen.

Bron: Computable
URL: https://www.computable.nl/artikel/opinie/cloud-computing/5695152/1509029/cloud-security-kun-je-nooit-volledig-uitbesteden.html