Interview | Foto Marco Mekenkamp

‘Bij ons staat alles in cloud

Jeff Scipio

Maar al te vaak gaan IT-dienstverleners ervan uit dat wanneer zij data en zakelijke toepassingen van eindklanten in ‘de cloud’ hebben staan, het automatisch veilig is. Het staat immers in datacenters van deze cloud-aanbieders en je mag ervan uitgaan dat deze voldoende beveiligd zijn. Maar is dat wel zo? “Hoe kan het dan dat gerenommeerde bedrijven die hun data en bedrijfskritische applicaties in de cloud hebben toch het nieuws halen met datalekken, doordat ze gehackt zijn of dat ze gegijzeld zijn door ransomware?” Aan het woord is Jeff Scipio, Partner Director bij de Nederlandse security vendor Guardian360 met kantoren in Utrecht en Rotterdam.

Eigenlijk leven we in een vreemde tijd, vindt Jeff Scipio. “We praten allemaal over de cloud en security, maar vraag aan een groep willekeurige ondernemers wat zij onder cloud en security verstaan en je zal versteld staan van de verschillende betekenissen die zij hieraan geven. Cloud? Dan staat onze data toch ergens bij een andere partij die verantwoordelijk is voor die data? Security? Dat heeft toch te maken met zaken zoals firewalls en antivirussoftware? En zo kan ik nog veel meer voorbeelden van antwoorden geven waaruit blijkt dat veel klanten hun eigen betekenis geven aan cloud en security.”

Maar is dat dan erg? “Op zich niet, maar het is voor de eindklant wel erg onhandig als je als leverancier niet goed kunt uitleggen waar het echt om gaat bij de cloud en bij security. Helemaal als je dat gesprek pas voert op het moment dat het mis is gegaan. Eigenlijk is de cloud heel simpel: de cloud is een verzameling

en daarom zijn we veilig. Of toch niet?'

van servers, vaak verdeeld over meerdere datacenters, waar data opgeslagen wordt en applicaties aangeboden kunnen worden. Informatiebeveiliging vertegenwoordigt het geheel van preventieve, mitigerende en curatieve maatregelen aangevuld met procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van data en systemen garanderen."

Security binnen de cloud

Scipio vervolgt: "Het in de cloud plaatsen van je data en applicaties betekent eigenlijk alleen maar dat je de investering in servers hebt omgezet naar een abonnement en dat je in veel gevallen hogere beschikbaarheid ervaart. Die business case is voor veel eindklanten wel duidelijk, de beveiliging echter niet. Een IT-dienstverlener zou de volgende vragen moeten stellen: Heb je voor jezelf goed in beeld welke diensten online toegankelijk mogen zijn en welke je strikt voor jezelf houdt? Heb je gecontroleerd of het land waarin de servers staan voldoen aan Europese wetgeving, bijvoorbeeld als het gaat om de verwerking van persoonsgegevens? Heb je de beveiliging van je data in de cloud gecontroleerd? Hoe toon ik aan dat ik mij maximaal heb ingespannen om data veilig te houden?"

De feiten

In 2018 zijn 16.000 zogenaamde vulnerabilities geconstateerd, bijna 50 per dag, zo weet Scipio te vertellen. "Deze kwetsbaarheden in IT-omgevingen waren tot dan toe nog niet bekend en zorgden ervoor dat hard- en software 'opeens' kwetsbaar werd voor kwaadwillenden. Het gaat om systemen bij eindklanten op kantoor, bij IT-dienstverleners in het datacenter en, je raadt het al, bij cloud-aanbieders. Cloudbeveiliging kan sterk zijn, maar is niet kogelvrij. Hoewel veel cloud-aanbieders een hoger beveiligingsniveau kunnen bieden dan een IT-dienstverlener of een eindklant zelf, blijven hacks plaatsvinden."

Preventie

Hoe dienen we om te gaan met al deze digitale gevaren en bedreigingen? "Preventie is hier het sleutelwoord", zegt Scipio. "Als we uit gaan van 16.000 IT-kwetsbaarheden in 2018, dan is het niet reëel om te verwachten dat je deze allemaal kunt kennen, laat staan handmatig kunt opsporen. Hier heb je eenvoudigweg een geautomatiseerde oplossing voor nodig: vulnerabilty scanning en managementsystemen. Gelukkig zien we dat de bewustwording van het belang van informatiebeveiliging toeneemt, mede door AVG, GDPR en alle bekendgemaakte cyberaanvallen en datalekken. Opvallend is dan dat het in gebruik nemen van vulnerabilty scanning en managementsystemen minder significant toeneemt."

'Het zakendoen met een Nederlandse securityvendor is steeds vaker een vereiste van de klant'

Zes punten

Als we Scipio vragen waar volgens hem de partner zijn klanten op zou moeten wijzen, benoemt hij een zestal punten. "Ten eerste zal de IT-partner richting zijn klanten zelf ook moeten kunnen aantonen dat hij met betrekking tot de informatiebeveiliging van zijn eigen diensten, data en applicaties 'in control' is.

Ook zal de IT-partner zich moeten realiseren dat het zakendoen met een Nederlandse securityvendor steeds vaker een vereiste is van de klant. Als derde zal de klant erop gewezen moeten worden dat het belangrijk is dat er niet met één maar met meerdere scanners gescand moet worden. Daarnaast zal er op gewezen moeten worden dat het van belang is dat gevonden IT-kwetsbaarheden afgezet kunnen worden tegen normeringen, zodat klanten compliant kunnen zijn met normen. Ten vijfde: de meeste scanners kijken alleen naar preventie (netwerkscanning), dus zorg ervoor dat je scanners kiest die ook aan detectie doen. Tot slot de zesde: zorg dat het scanplatform AVG-aanbevelingen levert om beter te kunnen voldoen aan deze regelgeving."

Scipio besluit het gesprek met de woorden: "Binnen Guardian360 kijken net even wat anders naar informatiebeveiliging dan andere fabrikanten. Die andere kijk op informatiebeveiliging heeft ervoor gezorgd dat het platform van Guardian360 volledig voldoet aan de punten die ik zojuist noemde."

www.guardian360.nl @ j.scipio@guardian360.nl ☎ 088 225 1500