Open Brief

Overstappen naar de Cloud, bezint eer ge begint

De afgelopen tijd hebben de media uitvoerig geschreven over de ransomware aanvallen op gemeenten, universiteiten, hogescholen en het NWO. Naast deze bekende ransomware aanvallen zien we echter ook veel aanvallen op Microsoft Exchange mailservers, waarin steeds nieuwe fouten worden gevonden. Het blijkt dat hierdoor veel e-mail systemen gehackt kunnen worden, en systeembeheerders hebben dan ook hun handen vol met het verhelpen van fouten in de Microsoft software. Gelukkig lijken de Cloud-gebaseerde e-mail systemen van Microsoft (Office 365), en die van de andere big-techbedrijven relatief veilig. Het lijkt dan ook niet meer dan begrijpelijk dat er stemmen opgaan om e-mail en andere diensten uit te besteden aan de ogenschijnlijk veilige Cloud oplossingen van de Amerikaanse Big Tech industrie.

Ook universiteitsbesturen besluiten steeds vaker om het onderhoud van ICT-diensten uit te besteden aan Amerikaanse Cloud-giganten. Dat is bijzonder, want in de Volkskrant van december 2019 roepen de rectoren van de Nederlandse universiteiten juist op “om een grens te trekken” teneinde de afhankelijkheid van Amerikaanse techbedrijven te verminderen. Blijkbaar verliest het lange termijn strategisch denken het van de korte termijn operationele problemen. Maar is dat wel verstandig, en zal de rekening van een falend strategisch handelen ons op termijn niet opbreken? Voordat er onomkeerbare besluiten worden genomen is er een aantal aandachtspunten waar bestuurders en universiteitsraden zich eerst over zouden moeten buigen.

Privacy en veiligheid
Voor studenten is het van belang dat zij een veilige leeromgeving vinden, waar ruimte is om fouten te maken en hiervan te leren. Het moet onmogelijk zijn dat privacygevoelige data van studenten voor andere doeleinden misbruikt wordt. Commerciële bedrijven die een Cloud oplossing bieden kunnen data echter voor meerdere doeleinden gebruiken. Met bijvoorbeeld het Cambridge Analytica schandaal in het achterhoofd, moeten we constateren dat de veiligheid en privacybescherming van onze studenten bij commerciële Cloud providers niet altijd gegarandeerd is.

Politiek
Door de data van medewerkers en studenten van Nederlandse universiteiten onder te brengen bij Amerikaanse Cloud providers plaatsen we die data niet alleen buiten het Europese grondgebied, maar ook binnen de ‘ommuurde tuinen’ van deze Cloud providers, die vallen onder Amerikaanse wet- en regelgeving. Maar niet alleen de data, maar zelfs de autorisatie tot diensten besteden we uit. We verheffen daarmee de Facebooks, Googles, Amazons en Microsofts van deze wereld niet alleen tot beheerder van onze data, maar ook tot grenspolitie van die data. Wanneer de NSA een juridische grondslag formuleert, dan kan het zo maar zijn dat de Amerikaanse overheid daarmee toegang krijgt tot het e-mail verkeer en de data van studenten en medewerkers aan Nederlandse universiteiten. Neem als analogie de fysieke toegang tot ons land: zouden we de grenscontrole op Schiphol en de uitgifte van paspoorten aan een buitenlandse natie uitbesteden?

Buitenlandse studenten
De laatste jaren hebben we moeten constateren dat de Amerikaanse regering bedrijven en organisaties kan dwingen om mee te werken aan Amerikaanse politieke wensen. Dit roept vragen op ten aanzien van de data van buitenlandse studenten en medewerkers uit landen waarmee geopolitieke spanningen bestaan, bijvoorbeeld uit China of Iran. Is het voorstelbaar dat een Amerikaanse regering ons dwingt studenten uit bepaalde landen te weren? Hebben Iraanse studenten die in deze tijd van Corona thuiswerken vanuit hun moederland nog wel toegang tot Office 365? Vinden we dat acceptabel?

Juridisch
In 2016 hebben de EU en de VS het “Privacy Shield” verdrag gesloten, waardoor de privacy van Europese burgers gewaarborgd zou moeten zijn. Maar afgelopen zomer hebben rechters van het Europese Hof besloten dat ook dit verdrag niet aan de Europese privacywetgeving voldoet. Er is dus een reële kans dat binnenkort ook Nederlandse rechters de universiteiten verbieden om nog langer gegevens in de Amerikaanse Cloud op te slaan. Met het oog op deze juridische onzekerheid lijkt het dus onverstandig om nu te migreren naar een Amerikaanse cloud.

Financieel
Op korte termijn kan het inderdaad voordelig zijn ICT-diensten uit te besteden aan de Cloud. Maar heeft men ook berekend wat de migratiekosten zijn als we er ooit weer vanaf willen, bijvoorbeeld omdat de rechter ons daartoe dwingt? Wat zijn de lange termijn kosten en hebben we dan nog wel de experts met verstand van de materie? Hebben we hiervan een helder beeld?

Ethiek
Is het te verdedigen als een bedrijf er niet in slaagt om veilige e-mail software te leveren, het dan te belonen door je compleet van dat bedrijf afhankelijk te maken en al je e-mail en ICT-diensten aan dat bedrijf uit te besteden?

Het is begrijpelijk dat de recente ransomware en de Exchange mail aanvallen voor sommige universiteiten (extra) argumenten zijn om het beheer van cruciale ICT-diensten uit te besteden. Cybersecurity is een steeds groter probleem, en het continue veilig houden van de eigen infrastructuur wordt steeds lastiger. Maar waarom wordt de e-mail infrastructuur en andere diensten (waaronder autorisatie) niet vaker samen met hogescholen, UMCs, MBOs en andere instellingen opgedragen aan SURF, de organisatie van en voor ons? Alhoewel het uitbesteden aan SURF op korte termijn moeilijker kan zijn dan uitbesteden aan de (Amerikaanse) Big Tech bedrijven, kunnen op de wat langere termijn veel problemen worden voorkomen.

Wij, de Nederlandse cybersecurity wetenschappers die zich hebben verenigd binnen de Academic Cyber Security Society (ACCSS)[1], roepen universiteitsbesturen en universiteitsraden op om een strategische visie te ontwikkelen, voordat voldongen feiten worden gecreëerd. Vergeet niet dat voor de Big Tech bedrijven geldt: “you can check-in anytime you like, but you can never leave”.

Prof. dr. ir. Aiko Pras - hoogleraar internet security (UT)
Prof. dr. Andreas Peter - adjunct hoogleraar data security (UT)
Prof. mr. Arno Lodder - hoogleraar Internetrecht (VU)
Prof. dr. Bart Jacobs - hoogleraar Security, Privacy and Identity (RUN)
Prof. dr. Bert-Jaap Koops - hoogleraar regulering van technologie (Tilburg University)
Prof. dr. Bibi van den Berg - hoogleraar Cybersecurity Governance (Univ. Leiden)
Prof. dr. ir. Cees de Laat - hoogleraar System and Network Engineering (UvA)
Prof. dr. Frederik Zuiderveen Borgesius - hoogleraar ICT en recht (RUN)
Prof. dr. ir. Herbert Bos - hoogleraar Systems and Network Security (VU)
Prof. dr. Joris van Hoboken - UHD informatierecht (UvA) en hoogleraar (VUB)
Prof. dr. Jeanne Mifsud Bonnici - hoogleraar European Technology and Human Rights (RUG)
Prof. mr. Lokke Moerel - hoogleraar Global ICT Law (Tilburg University)
Dr. Marleen Weulen Kranenbarg - Universitair Docent criminologie (VU)
Prof. dr. Marten van Dijk - groepsleider Computer Security (CWI)
Prof. dr. Michel van Eeten - hoogleraar governance of cybersecurity (TUD)
Prof. dr. ir. Roland M. van Rijswijk-Deij - adjunct hoogleraar network security (UT)
Prof. dr. Ronald Leenes - hoogleraar Regulating Socio-Technical Change (TILT)
Prof. dr. Stijn Ruiter - hoogleraar social & behavioural sciences (UU), senior onderzoeker (NSCR)
Prof. dr. Tanja Lange - hoogleraar Coding Theory and Cryptology (TU/e)

Vragen, opmerkingen bij deze open brief kunnen gestuurd worden naar: info@accss.nl

[1] www.accss.nl