



In de Cloud of wel?

In de logistieke wereld kun je er bijna niet om heen om met clouddiensten te werken. Maar vanwege geopolitieke spanningen is het allerm minst zeker, dat het altijd, onbeperkt en veilig bruikbaar is. Daarnaast kunnen we ook te maken hebben met een tekort aan stroom, bijvoorbeeld door een hack op energiecentrales.

Omdat logistiek een internationaal karakter heeft moet je met diensten werken die internationaal toegankelijk zijn en vaak uit Amerika komen. Onderstaand een aantal voorbeelden:

- Video- conferencing: Hiervoor heb je Zoom (Google) Teams (Microsoft) of Webex (Cisco) nodig.
- Bankieren: Hiervoor heb je SWIFT nodig, dat staat in Amerika.
- Betalen: Dat gebeurt vaak met VISA of MasterCard, beiden Amerikaans
- Satellieten voor het bepalen van Geo posities, zijn nagenoeg allemaal Amerikaans, zoals Trimble, Qualcomm en Starlink.
- Office applicaties zoals Google of Microsoft zijn Amerikaans.
- Communicatie en socials, zijn nagenoeg allemaal Amerikaans. Denk aan Meta of
- Daarnaast is het om een andere reden niet mogelijk om te stoppen met de Cloud:
- Het gebruik van (mobiele) applicaties, zoals navigatie, trailer-tracking, geofencing, etc. is niet mogelijk zonder internet. Ook in een TMS wordt vaak gebruik gemaakt van internet diensten, bijvoorbeeld kaartmateriaal en of email functies.

De gevaren:

1. Als Internet er uit ligt kun je niets meer. Bijvoorbeeld bij een breuk in kabelverbindingen
2. Als er geen stroom meer is, ligt internet er uit en kun je niets meer.
3. Als de Amerikanen besluiten om geen Cloud diensten meer te leveren aan Europa vallen we stil
4. De data staat vaak opgeslagen op servers die onder de patriot wetgeving van de NSA vallen. Ook de servers die in Nederland staan. Amerika kan besluiten om de data niet meer toegankelijk te maken of de data te gebruiken om analyses te doen of de markt te manipuleren.
5. Applicaties zijn ontwikkeld met of werken samen met Amerikaanse software zoals C#, .net, IBM, etc. Dat geldt ook voor applicaties die in Nederland ontwikkeld zijn.
6. Het intellectueel eigendom van de ontwikkelsoftware is alleen beschermd voor bedrijven in Amerika. Je kunt dus niet de sources opvragen als Microsoft besluit om jou niets meer te leveren. Dat geldt zelfs ook deels voor open source software.
7. Er wordt veel apparatuur gebruikt uit Amerika of China, denk maar aan camera's, scanners, etc. In deze apparaten zit zogenaamde firmware, software die de leverancier van de hardware is ingebouwd en niet door de gebruiker aangepast kan worden. Anderen kunnen deze apparaten gebruiken om data te verkrijgen en het zelfs niet ondenkbaar dat er een kill switch inzit.
8. Voor bepaalde documenten/ gegevens is er een wettelijke bewaarplicht. Voorbeelden zijn CMR's, gegevens voor de fiscus zoals facturen, salarisgegevens, etc.
9. Hackers kunnen je software en data gijzelen en deze pas na het betalen van een afkoopsom vrijgeven.
10. Vendor lockin is een vaak onderschat probleem. Als je eenmaal gebruik maakt van de diensten van een partij dan kan die doen en laten wat hij wil. Bijvoorbeeld exorbitante prijsverhogingen doorvoeren of de data niet vrijgeven als je naar een ander leverancier wilt overstappen.

Tips:

1. Maak een noodplan (op papier) waarin staat wie wat moet doen, bij welk soort calamiteit.
2. Breng in kaart welke partijen aan jou cloud diensten leveren.
3. Vraag hoe en waar de gegevens worden opgeslagen.
4. Vraag of de leverancier een mogelijkheid tot Escrow heeft.
5. Zorg ervoor dat alle belangrijke documenten, zoals overeenkomsten, SLA's, statuten e.d. lokaal worden opgeslagen. Bijvoorbeeld op een versleutelde USB stick.
6. Als jouw applicatie met een database werkt, vraag dan periodiek een kopie, maar ook de inlogprocedure en inlog gegevens.
7. Zorg ervoor dat de wachtwoorden veilig zijn en goed worden bewaard (op papier in een kluis)
8. Installeer office applicaties ook lokaal op de PC of laptop, zodat je altijd kunt doorwerken.
9. Zorg ervoor dat de bestanden tussen je lokale opslag ook gesynchroniseerd worden met bijvoorbeeld One drive of Google drive.
10. Zorg voor een back-up procedure voor je laptop of PC.
11. Zorg voor een noodstroomvoorziening zoals een UPS
12. Zorg ervoor dat de besturingssoftware up-to-date is.
13. Zorg ervoor dat je je op tijd je abonnement betaald.
14. Bewaar de belangrijkste contactgegevens van leveranciers, grootste klanten en medewerkers op papier.
15. Maak goede afspraken met je leverancier over prijsverhogingen en het vrijgeven van data als je vertrekt.
16. Probeer zoveel mogelijk gebruik te maken van Europese leveranciers. En beter nog Zwitserse.
17. Kijk ook eens je verzekeringspolissen na om te zien wat er wel en niet gedekt is.
18. Voor bedrijven die cloud- of IT diensten aan opdrachtgevers leveren is het probleem zo mogelijk nog groter als het fout gaat. Stel voor dat je als logistiek dienstverlener de facturatie aan afnemers voor jouw klant regelt en je kunt dat om welke reden dan ook niet meer, dan kun je een aanzienlijke claim verwachten.
19. Bepaal een exit strategie voor als je wilt overstappen.
20. Omdat bepaalde verladers/opdrachtgevers bepaalde voorwaarden stellen aan de IT-omgeving van hun leveranciers is het handig om ook hen te betrekken in je eigen strategie en uitvoering. Soms wordt er geëist dat je aan de ISO27001 of NIS2 norm voldoet en dat tijdens audits ook controleert.

Uiteraard kosten deze zaken allemaal geld en verdienen ze aandacht. Het gesprek daarover moet in de directiekamer plaats vinden en niet op een kantoortje van een applicatie-beheerder, met alle respect. Het is aan de directie om vast te stellen hoe groot het risico is en hoe groot de schade is als er zich een calamiteit voordoet. Alle afdelingen van het bedrijf moeten hierin betrokken worden en het moet een regelmatig terugkerend agendapunt zijn.

Meer weten, kijk ook eens op:

<https://www.redbus.nl/europese-alternatieven/>

Stichting Digitale Infrastructuur Nederland www.dinl.nl

Bert Hubert: www.berthub.eu

Nederland digitaal: www.nederlanddigitaal.nl

www.Escrow4all.com