Defensie & Veiligheid
Oude Waalsdorperweg 63
2597 AK Den Haag
Postbus 96864
2509 JG Den Haag

www.tno.nl

T +31 88 866 10 00
F +31 70 328 09 61

TNO-rapport

TNO 2020 R12232

Verdieping Valorisatieketens: Basis voor de routekaart "Veilig werken in een onveilige cloud"

Datum	januari 2021
Auteur(s)	Dr. D. Tiggelman Drs. Ing. D.H. Hut T.H. Bontekoe MSc
Aantal pagina's	34 (incl. bijlagen)
Aantal bijlagen	-
Opdrachtgever	Ministerie van Economische Zaken en Klimaat
Projectnaam	EZK: Verdieping valorisatieketens
Projectnummer	060.45190

Samenvatting

Bij de Rijksoverheid is een trend waarneembaar dat steeds meer wordt gewerkt in de ‘cloud’ [1, 2]. Omdat hierdoor beveiligingsrisico’s kunnen ontstaan, vraagt dit in de toekomst mogelijk om nieuwe sterkere beveiligingsmaatregelen voor veilige opslag van deze informatie. Op dit moment spelen de (internationale) multinationals die deze clouds aanbieden een belangrijke rol wat betreft de beveiliging van de opgeslagen informatie. Maar daar is vaak niet exact duidelijk of, en zo ja hoe, de data van klanten wordt beveiligd. Naast de mogelijke beveiligingsrisico’s die ontstaan door deze trend, komt ook de Nederlandse datasoevereiniteit steeds meer in het geding. Deze multinationals vallen vaak niet onder de Nederlandse wet- en regelgeving. Hierdoor kan een situatie ontstaan waarbij de dataeigenaar in land X de verzamelde data opslaat bij een cloud-provider in land Y. Vervolgens blijkt dan dat in land Y andere wet- en regelgeving geldt voor toegang tot de daar opgeslagen klantdata.

In de Nationale Crypto Strategie zijn acht thema’s geïdentificeerd. Eén van deze thema’s is “Crypto en Cloudbeveiliging”. In dit rapport wordt verslag gedaan van onze analyse over mogelijke oplossingsrichtingen voor de Rijksoverheid om vertrouwelijke informatie veilig op te kunnen slaan in de cloud. De volgende stap is om richting te geven aan het ontwikkelen van een beveiligingsproduct om vertrouwelijke informatie veilig op te slaan samen in de cloud met de Nederlandse industrie en kennispartijen voor de Nederlandse markt. De richting kan worden beschreven in een routekaart. In dit rapport wordt een plan van aanpak geschetst hoe te komen tot een routekaart voor het beveiligen van vertrouwelijke informatie in de cloud. Hierbij komt een aantal aspecten naar voren die verdere uitwerken behoeven:

a) De stip op de horizon is het vergezicht waar in een gezet aantal jaar naar toe wordt gewerkt. Een mogelijke stip voor dit onderwerp is dat over 1 á 2 jaar de medewerkers van de Rijksoverheid op een veilige manier vertrouwelijke informatie kunnen opslaan in de cloud. Na de fase waarin de gewenste functionaliteit is geïmplementeerd in een applicatie, volgt mogelijk een accreditatie-fase waarin de software geaccrediteerd moet worden.
b) In de valorisatieketen zitten de partijen die betrokken zijn bij productontwikkeling van fundamenteel onderzoek tot het daadwerkelijke gebruik van een product. Deze keten kan door middel van literatuur onderzoek en interviews in kaart worden gebracht. De partijen binnen de valorisatieketen kunnen grofweg ingedeeld worden in 1) kennisinstellingen, 2) ontwikkelpartijen, 3) eindgebruikers. Door de partijen te plotten op de vijf ontwikkelfases (*Discovery/basic research, Technology development, Validation and demonstration, Integration and operationalization, Deployment*) wordt duidelijk welke partij zich in welk stuk van het ontwikkeltraject bevindt.
c) Het is van belang de barrières binnen de valorisatieketen inzichtelijk te maken om hier in de ontwikkeling van de routekaart rekening mee te kunnen houden. Dit kunnen barrières zijn tussen de ontwikkelfases (‘valleys of death’) of meer fase overstijgend. Bij de ontwikkeling van cloud beveiligingsproducten is bijvoorbeeld de afzetmarkt klein en is samenwerking tussen de ontwikkelpartijen van groot belang voor de modulariteit van oplossingen. Dit zijn twee voorbeelden waar bij de ontwikkeling van producten rekening mee moet

worden gehouden en die kunnen worden meegenomen in de stappen binnen de routekaart.

d) Om te komen tot de stip op de horizon wordt gewerkt aan bepaalde sporen binnen de routekaart. De vier mogelijke sporen waar langs gewerkt kan worden voor dit traject zijn a) de beveiliging van opslag in de cloud, b) veilig gegevens verwerken in de cloud, c) samenwerkingsverbanden tussen de stakeholders binnen de valorisatieketen en d) het instrumentarium wat hiervoor nodig is.

Voor het eerste spoor, beveiliging van de opslag in de cloud, geeft dit rapport drie mogelijke oplossingsrichtingen: 1) GAIA-X, 2) Dutch Secure Autonomous Cloud (DUSAC), 3) Client-side encryptie. In dit onderzoek is gekozen om oplossingsrichting nr. 3 gedetailleerder te onderzoeken aan de hand van drie cloud-providers (Amazon, Google en Microsoft) en enkele beveiligingsproducten uit de markt. Om te komen tot een eindoplossing wordt gekeken naar de functionaliteiten van bestaande producten en in hoeverre de Nederlandse markt kan zorgen voor een alternatief dat werkt voor de Rijksoverheid, en die aan alle beveiligingsaspecten voldoet en zorg draagt voor datasoevereiniteit.

Een uitstap naar het tweede spoor, veilig verwerken van gegevens in de cloud, wordt in dit rapport ook gemaakt. Echter wordt hier vooral een mogelijke uitdaging geschetst die de oplossingen voor een veilige opslag met zich mee kunnen brengen. Wanneer de data veilig wordt opgeslagen kan bijvoorbeeld als consequentie hebben dat bepaalde functionaliteit die de cloud aanbieder levert niet meer werkt (bijvoorbeeld het indexeren van documenten of datasets of het maken van back-ups). Dit is een nieuwe uitdaging waar in de routekaart rekening mee kan worden gehouden, bijvoorbeeld door dergelijke functionaliteit op een andere manier te implementeren.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

De ‘cloud’ is niet meer weg te denken uit onze moderne samenleving en is tegenwoordig onmisbaar voor veel mensen en bedrijven. Volgens Gartner is het zelfs de nieuwe norm geworden[1]. Met ‘cloud’ wordt bedoeld dat bedrijven of consumenten (een netwerk van) externe computers gebruiken op internet om gegevens op te slaan, te beheren en te verwerken, in plaats van eigen computers en servers te gebruiken. Typische voorbeelden zijn Amazon Web Services, Google Cloud Platform en Microsoft Azure. Maar er zijn ook diensten zoals Dropbox, Office365 en SharePoint die wat herkenbaarder zijn voor eindgebruikers als producten maar eigenlijk zijn dit ook gewoon clouddiensten.

Naast de vele voordelen van de cloud kunnen er ook nadelen zitten aan deze manier van werken. De cloud-trend zorgt ervoor dat we het zicht op en de controle over onze informatie beetje bij beetje verliezen. Er kunnen tegenwoordig weliswaar ook ‘eigen’ clouds gemaakt worden waarbij computers en servers gebruikt worden die bij bedrijven zelf staan of in een datacenter ergens in Nederland. Maar de trend is duidelijk: langzaam maar zeker vloeit onze data, en daarmee ook de controle over en het zicht op de data, weg naar grote multinationals[2]. En dit betreft vaak grote buitenlandse bedrijven die juridisch niet onder de Nederlandse of EU wet- en regelgeving vallen[3].

In de Nationale Crypto Strategie zijn acht thema’s geïdentificeerd. Eén van deze thema’s is “Crypto en Cloudbeveiliging”. In dit onderzoek wordt de problematiek van dit thema geanalyseerd en worden enkele beveiligingsvraagstukken uitgewerkt. Hiermee proberen we dit thema concreet in te vullen en nieuwe mogelijkheden te realiseren voor de markt, voor de industrie en voor gebruikers. Zodat ook in de toekomst cryptografische beveiligingsmaatregelen om gevoelige informatie te beschermen beschikbaar komen en blijven.

1.2 Doelstelling

Binnen de Rijksoverheid wordt niet alleen gewerkt met ‘gewone’ data, maar ook met vertrouwelijke of geclassificeerde informatie[4] [3]. Geclassificeerde informatie is informatie die omwille van de inhoud beperkt gedeeld mag worden met alleen daarvoor geautoriseerde personen. Geclassificeerde informatie wordt vaak ingedeeld in verschillende categorieën, waarbij elke categorie aangeeft hoe gevoelig de informatie is. In Nederland spreekt men van "gerubriceerde informatie" en de behandeling daarvan wordt geregeld in het “Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie” (VIRBI)[5].

---

1 https://www.gartner.com/en/information-technology/insights/cloud-strategy
2 https://www.cnbc.com/2019/03/11/tim-berners-lee-the-web-is-dysfunctional-with-perverse-incentives.html
3 https://tweakers.net/nieuws/169812/eu-hof-haalt-streep-door-privacy-shield-en-blokkeert-datatransfers-naar-vs.html
4 https://nl.wikipedia.org/wiki/Geclassificeerde_informatie
5 https://wetten.overheid.nl/BWBR0033507/2013-06-01

Bij het opslaan van informatie in de cloud door de Rijksoverheid in combinatie met het vertrouwelijkheidsaspect van informatie, kunnen nieuwe beveiligingsuitdagingen ontstaan met bijbehorende onderzoeksvragen:

1 Is het mogelijk om gewone, vertrouwelijke of zelfs gerubriceerde informatie veilig op te slaan in een onveilige cloud?
2 Wat maakt een cloud veilig of onveilig?
3 Moet de cloud-aanbieder zelf beveiligingsmaatregelen nemen of kan de Nederlandse industrie daar een rol spelen?
4 Zijn er producten denkbaar die dermate goed zijn dat ze Common Criteria gecertificeerd kunnen worden?[6]

Deze vragen schetsen de problematiek waar men in de zoektocht naar betere informatiebeveiliging in de cloud [4] mee geconfronteerd kan worden en deze vragen komen in dit onderzoek aan bod. De doelstelling van dit onderzoek is:

1 Inzicht krijgen in de beveiligingsrisico's van het opslaan van, al dan niet vertrouwelijke of gerubriceerde, informatie in de cloud en mogelijke oplossingen voor dit probleem.
2 Een eerste aanzet geven tot de ontwikkelen van een routekaart met de volgende aspecten:
   a. Economisch: De Nederlandse markt voor beveiligingsproducten laten groeien.
   b. Informatiebeveiliging: Het gebruik van beveiligingsproducten voor clouddiensten stimuleren zodat Nederland veiliger wordt.
   c. Soevereiniteit: Meer autonomie over de eigen data c.q. digitale soevereiniteit voor Nederland.

Kort samengevat is dit een vooronderzoek voor een roadmap die als doel heeft om de beperkingen die er nu zijn voor het gebruiken van vertrouwelijke informatie in de cloud aan te pakken.

1.3 Aanpak

De beschreven doelstellingen van de roadmap zijn ambitieus en vragen om een meerjarige aanpak. Aan deze aanpak kan richting worden gegeven door het opzetten van een routekaart met een duidelijke stip op de horizon. Met dit project vormen we de basis voor de ontwikkeling van die routekaart, aan de hand van onderstaande activiteiten (zie Tabel 1).

[6] https://en.wikipedia.org/wiki/Common_Criteria

Tabel 1 Gevolgde aanpak.

Activiteit	Beschrijving
1	Kort marktonderzoek naar type clouds en cloud-aanbieders.
2	Onderzoeken welke beveiligingsvraagstukken een rol kunnen spelen in de context van werken in de cloud.
3	Uitwerken van één van deze beveiligingsvraagstukken en analyseren of hier oplossingen voor bestaan, zoals aangeboden door de cloud-aanbieders.
4	Analyseren of er door andere partijen in de markt, dus buiten de cloud-aanbieders om, oplossingen voor het beschreven probleem worden aangeboden door derde partijen.
5	Verwerken van de gevonden informatie naar de vormgeving van een routekaart voor Nederland.

In vervolgonderzoek kan het concrete meerjarenplan, de routekaart, worden ontwikkeld om de Nederlands industrie te betrekken om nieuwe beveiligingsproducten daadwerkelijk te gaan ontwikkelen. Vervolgens kunnen de nieuwe beveiligingsproducten worden getest en bij de Rijksoverheid worden geïntroduceerd.

1.4 Scope

Om binnen de doorlooptijd van dit onderzoek een zo goed mogelijk beeld te geven van de problemen en de mogelijke oplossingen, zijn de volgende keuzes gemaakt:

- Omdat de cloud een bijzonder breed en complex fenomeen is, leggen we de focus op ‘cloud storage’. Dat wil zeggen opslag van informatie in de cloud (‘data-at-rest’).
- Omdat gerubriceerde informatie onder speciale wet- en regelgeving valt en de beveiligingsuitdaging hier het grootst is, richten we ons op een toekomst-pad om gerubriceerde informatie veilig op te kunnen slaan in de cloud.
- We bekijken de beveiliging van informatie die in de cloud wordt opgeslagen vanuit het perspectief van de klant van de cloud-provider: de Rijksoverheid. De klant wil de toegang tot haar vertrouwelijke informatie zoveel als mogelijk afschermen van de buitenwereld, hieronder valt ook de desbetreffende cloud-provider of eventuele andere betrokken serviceproviders.

2 Context cloudopslag

In dit hoofdstuk schetsen we een gedetailleerder beeld van de context van het probleem en het probleem zelf. We geven eerst een overzicht van de relevantie begrippen op het gebied van cloudopslag om zo een beeld te krijgen van het landschap.

Hierdoor wordt het ook duidelijk waar in het landschap onze scope (Cloud Storage) valt en welke onderwerpen nog verder onderzocht kunnen worden. Vervolgens leggen we uit hoe we dit beveiligingsvraagstuk kunnen classificeren aan de hand van het BIV-model en het begrip datasoevereiniteit. In de tweede helft van dit hoofdstuk volgt een probleembeschrijving en schetsen we de gradaties van het probleem aan de hand van drie categorieën van cloudopslag.

2.1 Begrippen

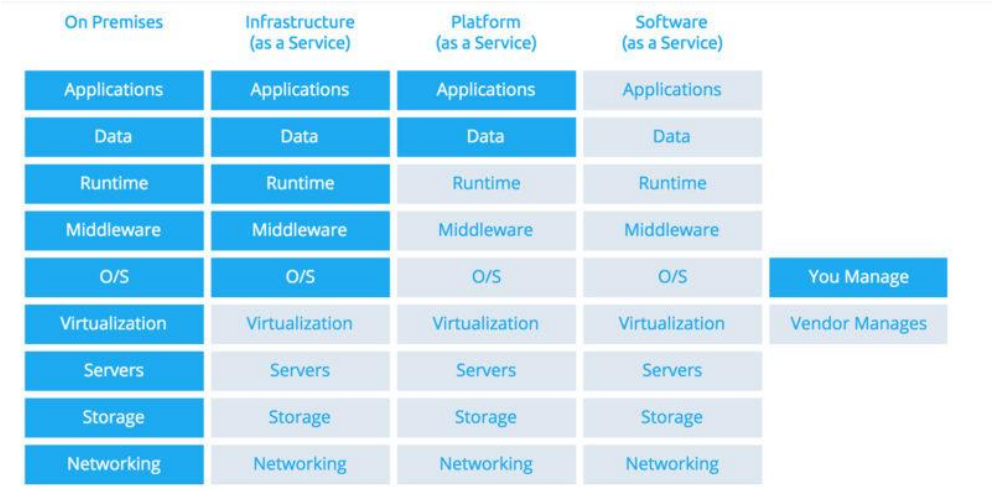
Cloud Storage is een cloud-computing model dat gegevens opslaat bij een cloud-provider die deze gegevensopslag beheert en exploiteert als een service. Het wordt op aanvraag geleverd met ‘just-in-time’ capaciteit en kosten, en er hoeft geen eigen infrastructuur voor gegevensopslag te worden aangekocht of te worden beheerd.[7]

Cloud Computing is de ‘on-demand’ levering van IT-middelen via internet tegen betaling per gebruik. In plaats van fysieke servers te kopen, te bezitten en te onderhouden, kan naar behoefte toegang worden gekregen tot technologische services, zoals rekenkracht, opslag en databases van een cloud-provider.[8]

Cloud Computing Services is een dienstenmodel dat wordt aangeboden door cloud-computing bedrijven en kan worden onderverdeeld in drie basistypen[9,10] (zie Figuur 1):

a) “Infrastructure as a Service” (IaaS). Bij IaaS wordt de infrastructuur samen met alle daarvoor benodigde netwerkelementen naar de cloud gebracht. De eindgebruiker behoudt echter het beheer op het operating systeem, de database, applicaties en data.
b) “Platform as a Service” (PaaS). PaaS oplossingen nemen nog iets meer werk uit handen van de organisatie vergeleken met IaaS. Naast de hardware, worden ook het operating systeem en de database in de cloud geplaatst.
c) “Software as a Service” (SaaS). SaaS applicaties worden als webapplicatie via het internet afgenomen. Dit betekent dat de gehele applicatie gemanaged en beheerd wordt door de cloud-provider. SaaS oplossingen nemen nog iets meer werk uit handen van de organisatie vergeleken met PaaS.

[7] https://aws.amazon.com/what-is-cloud-storage/
[8] https://aws.amazon.com/what-is-cloud-computing/
[9] https://www.akamai.com/us/en/resources/cloud-computing-services.jsp
[10] https://www.valueblue.nl/cloud-services-iaas-paas-saas-hoe-zit-ook-alweer/



Figuur 1 Iaas, PaaS, Saas. (Bron[11])

Eindgebruikers zullen bij de term ‘cloud computing services’ waarschijnlijk niet direct aan bovenstaand dienstenmodel denken, maar meer aan handige extra functionaliteiten die ze kunnen gebruiken zoals bijvoorbeeld het samenwerken aan documenten of presentaties en het kunnen doorzoeken en indexeren van documenten of grote datasets.

2.2 Het BIV-beveiligingsmodel

Er zijn verschillende type beveiligingsproblemen denkbaar die zich kunnen voordoen bij het opslaan van vertrouwelijke data in een ‘public’ cloud. Het BIV-model[12] is een veelgebruikte methode voor het opstellen van beleid op het gebied van informatiebeveiliging[13]. Bij de BIV-classificatie wordt er naar drie aspecten van beveiliging gekeken: Beschikbaarheid, Integriteit en Vertrouwelijkheid.

2.2.1 Beschikbaarheid

Informatie moet toegankelijk zijn op elk gewenst moment. De classificatie van hoe erg beschikbaarheid is aangetast, hangt af van de hoeveelheid informatie die niet beschikbaar is en hoe lang deze niet beschikbaar is.

Beschikbaarheid is van toepassing op het gebied van cloud in de zin dat informatie die ergens anders opgeslagen wordt (in de cloud) ook altijd beschikbaar moet zijn. Cryptografie is hier niet direct op van toepassing, maar het inrichten van enige redundantie in de opslag van data in de cloud, een snelle hersteltijd bij een storing, en het verdelen van data over verschillende plekken kunnen een positieve bijdrage hebben op de beschikbaarheid van data opgeslagen in de cloud.

2.2.2 Integriteit

Aan informatie mag niet zomaar iets worden toegevoegd, aangepast, of verwijderd door een niet-geautoriseerde partij. Als dit wel gebeurt, moet dit direct merkbaar en eventueel omkeerbaar zijn. De classificatie van hoe erg integriteit is aangetast hangt af van de soort informatie en in welke mate deze informatie aangepast is.

[11] https://valueblue.nl
[12] https://nl.wikipedia.org/wiki/BIV-classificatie
[13] https://en.wikipedia.org/wiki/Information_security#Key_concepts

Data die niet in eigen beheer is opgeslagen, kan onder andere door de eigenaar van de opslaglocatie worden aangepast, zelfs zonder dat de dataeigenaar dit door heeft. Een veelgebruikte manier om hier mee om te gaan is door te vertrouwen op certificeringen van de cloud-provider door bevoegde instanties (bv. ISO audits). Cryptografie kan echter ook uitkomst bieden om de integriteit van data te waarborgen. Traditioneel gezien wordt cryptografie hier al veel voor ingezet, met name voor het waarborgen van de integriteit bij het versturen van berichten. Voor de cloud zou dit op een vergelijkbare manier kunnen worden toegepast, waarbij elke ongeautoriseerde aanpassing van de data gedetecteerd kan worden door de eigenaar van de data.

2.2.3 Vertrouwelijkheid

Vertrouwelijke informatie mag niet door een niet-geautoriseerde persoon worden ingezien. De classificatie van hoe erg vertrouwelijkheid is aangetast, hangt af van de soort informatie en in hoeverre deze informatie inzichtelijk is door andere actoren.

Data onbeveiligd in een cloud opslaan, betekent dat de eigenaar of de beheerder van de cloud infrastructuur toegang heeft tot de data. Vaak is dit geen probleem en wordt dit risico geaccepteerd door de gebruikers van de cloud. Cryptografie, het versleutelen van data, is een manier om controle te krijgen over wie de data kan inzien. Versleutelde data kan alleen ingezien worden door partijen die beschikken over de encryptie / decryptie sleutel.

2.2.4 Datasoevereiniteit

Naast de hierboven beschreven BIV-classificatie wordt er in de context van dataopslag in de cloud ook gesproken over datasoevereiniteit [5]. *Datasoevereiniteit* is het concept dat data valt onder bepaalde wet- en regelgeving van een land dat niet compatibel (genoeg) is met de eisen en wensen die gelden in Nederland. In de context van cloudopslag komt deze situatie vaak voor, waarbij de dataeigenaar in land X de verzamelde data opslaat bij een cloud-provider in land Y. Vervolgens blijkt dan dat in land Y andere wet- en regelgeving geldt voor toegang tot de daar opgeslagen klantdata.

2.3 Probleemstelling

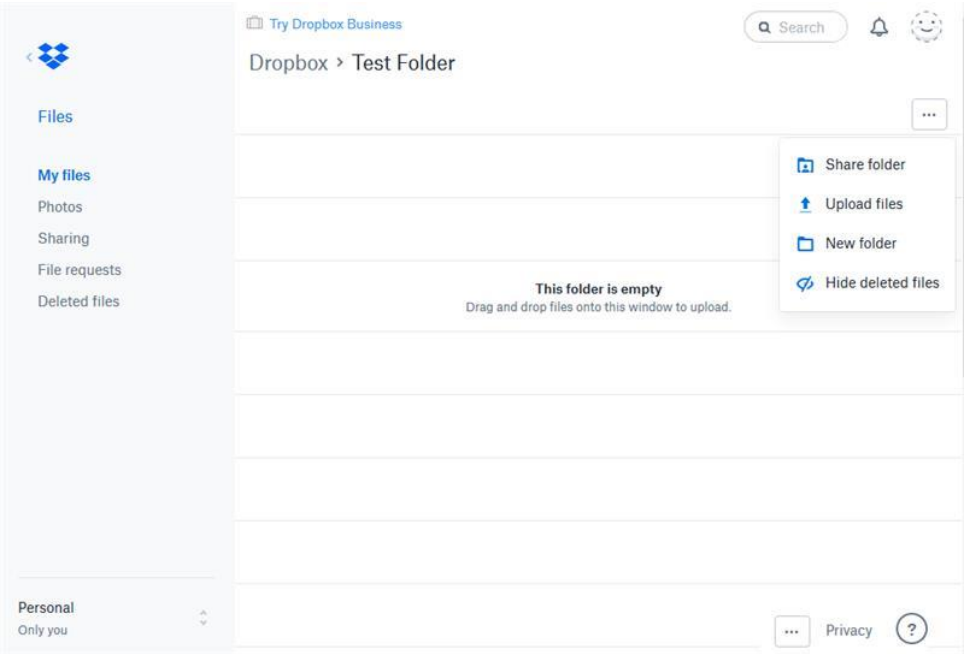
2.3.1 Bekeken vanuit het perspectief van informatiebeveiliging

De scope van dit onderzoek ligt bij het opslaan van data in de cloud, de zogenoemde ‘data-at-rest’ in de context van Cloud Storage. Maar wat betekent dit nu precies? En wat is eigenlijk het beveiligingsprobleem? In deze sectie schetsen we dit probleem aan de hand van het voorbeeld van Dropbox[14], een veelgebruikte Cloud Storage oplossing die velen bekend zal voorkomen.

Dropbox biedt haar gebruikers de mogelijkheid om bestanden en mappen met bestanden op haar servers op te slaan. Dit betekent dat de klantdata niet meer lokaal, op de eigen computer, staat opgeslagen, maar in een datacentrum ergens in de wereld. In eerste instantie heeft alleen de gebruiker die het bestand heeft geüpload naar Dropbox toegang tot het bestand. Het is namelijk alleen toegankelijk

[14] https://www.dropbox.com

vanaf het account van de eigenaar. De interface waarmee een gebruiker dit kan regelen, is te zien in Figuur 2.

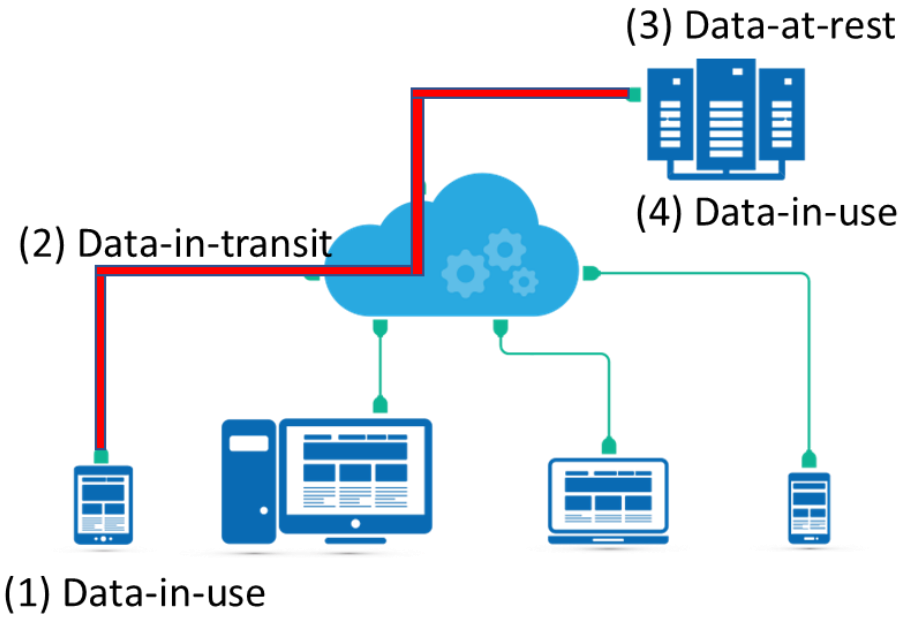


Figuur 2 Dropbox Cloud Storage applicatie.

Tot zover lijkt Cloud Storage nog heel erg op het lokaal opslaan van data, behalve dat de fysieke locatie is veranderd. Echter, heeft Cloud Storage nog meer functionaliteiten die het interessant maken voor gebruik in bijvoorbeeld organisaties. Zoals het geven van toegang tot klantdata aan andere gebruikers. Zonder dat je eigen computer aan hoeft te staan, en ook zonder dat anderen toegang tot jouw computer krijgen.

Dit biedt veel mogelijkheden om samen aan dezelfde data te werken. De ene gebruiker schrijft bijvoorbeeld iets in een document en tegelijkertijd kan een andere gebruiker de wijzigingen zien. Dit wordt mogelijk gemaakt doordat Dropbox continu data synchroniseert met de data in de cloudopslag zodat iedereen altijd de meest recente versie heeft. Er ontstaat een soort virtueel ‘overlay network[15], zoals afgebeeld in Figuur 3, waarbij meerdere gebruikers op meerdere apparaten tegelijkertijd kunnen samenwerken aan bestanden met documenten of andere informatie over het internet. Hierbij is de cloud de centrale opslaglocatie, en kunnen verschillende gebruikers vanaf hun verschillende locaties, op hun eigen apparaten allemaal bij dezelfde gedeelde data.

[15] https://en.wikipedia.org/wiki/Overlay_network



Figuur 3 Referentiemodel van een clouddienst over internet.

Voor wat betreft de beveiligingsproblematiek (zie Figuur 3) zijn er meerdere plaatsen in de keten tussen gebruiker en Dropbox waar aanvallers de beschikbaarheid, integriteit en vertrouwelijkheid kunnen aantasten. Men spreekt in deze beveiligingscontext vaak over de verschillende fases waarin data zich kan bevinden:

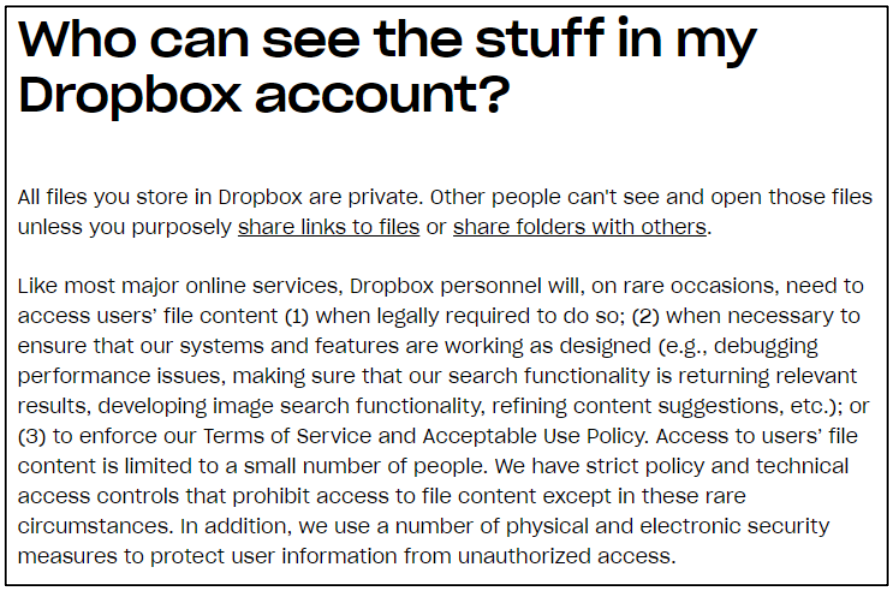
1 “Data-in-use” (bij de klant)
2 “Data-in-transit” (tussen klant en cloud)
3 “Data-at-rest” (bij de cloud-provider)
4 “Data-in-use” (bij de cloud-provider)

In het geval van Dropbox is de beveiliging van klantdata in al deze fases een belangrijk onderwerp, zo is te lezen op hun website. Maar is dit genoeg? Dropbox zegt hier zelf op haar website het volgende over: “*Dropbox files at rest are encrypted using 256-bit Advanced Encryption Standard (AES)*”[16]. Dus Dropbox versleutelt de klantdata en daarmee is het beveiligingsrisico verdwenen? Nou, nee. Want Dropbox doet weliswaar encryptie voor klanten, maar heeft zelf de sleutels en doet zelf de encryptie. En is daardoor ook in een positie om decryptie van klantdata te kunnen doen met deze sleutels.

De consequentie van deze redenering is dat Dropbox daardoor altijd toegang tot de ‘plaintext’ klantdata heeft, of tenminste kan krijgen. Op dezelfde webpagina onder kopje “Encryption and private keys with Dropbox” is te lezen: “*Dropbox doesn't provide for client-side encryption. Dropbox also doesn't support the creation of your own private keys. However, Dropbox users are free to add their own encryption*.”

Dropbox zegt verder nog onder kopje “*Who can see the stuff in my Dropbox account?” het volgende: “Like most major online services, Dropbox personnel will, on rare occasions, need to access users’ file content*…”[17] (zie Figuur 4).

[16] https://help.dropbox.com/accounts-billing/security/how-security-works
[17] https://help.dropbox.com/accounts-billing/security/file-access



Who can see the stuff in my Dropbox account?

All files you store in Dropbox are private. Other people can't see and open those files unless you purposely share links to files or share folders with others.

Like most major online services, Dropbox personnel will, on rare occasions, need to access users' file content (1) when legally required to do so; (2) when necessary to ensure that our systems and features are working as designed (e.g., debugging performance issues, making sure that our search functionality is returning relevant results, developing image search functionality, refining content suggestions, etc.); or (3) to enforce our Terms of Service and Acceptable Use Policy. Access to users' file content is limited to a small number of people. We have strict policy and technical access controls that prohibit access to file content except in these rare circumstances. In addition, we use a number of physical and electronic security measures to protect user information from unauthorized access.

Figuur 4 Dropbox Access Policy[17].

Probleemstelling (informatiebeveiliging)
De centrale hypothese die wordt gehanteerd in dit onderzoek, is dat de cloud-provider zelf, als service provider, toegang heeft tot de klantdata. En daarom gezien kan worden als een beveiligingsrisico voor de opslag van vertrouwelijke informatie. Daarnaast gaan we er van uit dat ook andere service-providers die betrokken zijn bij de opslag van de informatie (denk bijvoorbeeld aan datacenters waar de cloud-providers hun servers hebben staan) ook toegang hebben tot de klantdata.

Merk op dat we voor dit onderzoek niet uit zijn op het bewijzen van deze hypothese (het is een aanname) maar op het vinden van mogelijke oplossingsrichtingen.

2.3.2 *Bekeken vanuit het perspectief van datasoevereiniteit*

In het online artikel “Baas over eigen gegevens: pleidooi voor meer datasoevereiniteit”[18] wordt niet zozeer naar wet- en regelgeving gekeken maar naar controle: het controle-aspect van een dataeigenaar over haar data. Op de vraag “wat is datasoevereiniteit?” antwoordt Mariane ter Veen (INNOPAY): “Het betekent dat je baas bent over je eigen data. Je weet wie je data heeft. Je hebt de controle om die onder bepaalde voorwaarden te delen met anderen. En je hebt de vrijheid om je data over te zetten naar andere platformen.”

Mark Esseboom (IBM): “Voor mij gaat datasoevereiniteit niet over Europa versus andere blokken in de wereld. Elk bedrijf dat diensten aanbiedt in de Europese Unie moet zich houden aan de regels rond data. En die Europese regels vertrekken vanuit het juiste perspectief: het perspectief van de gebruiker. Hoe geven we hem of haar de controle over de gegevens terug? Datasoevereiniteit gebaseerd op deze waarden, en niet op protectionisme, zijn dan ook een meerwaarde voor de gebruiker.”

[17] https://help.dropbox.com/accounts-billing/security/file-access

[18] https://www.ibm.com/blogs/think/nl-en/2020/12/16/baas-over-eigen-gegevens-pleidooi-voor-meer-datasoevereiniteit/

Henk-Jan Vink (TNO): “Wat regulering rond data betreft, is de Europese Unie een absolute trendsetter in de wereld. Denk aan de GDPR en de wetgeving rond IT-veiligheid. Toch staan we rond datadeling nog maar aan het begin. De GDPR gaat over: je gegevens beschermen. De volgende stap is dat je zelf op een veilige manier je gegevens kunt delen en er voordeel uit haalt.”

Dat brengt ons op het tweede deel van de probleemstelling in de context van dit onderzoek: de mogelijke relatie tussen informatiebeveiliging en datasoevereiniteit.

Probleemstelling (datasoevereiniteit)
In het geval van opslag in de cloud, is de klantdata per definitie overgedragen aan een andere partij. Doordat de cloud-provider toegang heeft tot de klantdata, is de klant niet meer *volledig* baas over eigen data. Je weet niet meer precies wie je data heeft en waar deze bewaard wordt en je hebt ook geen *volledige* controle om die onder bepaalde voorwaarden te delen met anderen. Je hebt wel *gedeeltelijk* controle want de klantdata kan nog steeds door de klant worden gedeeld met anderen. Maar de klantdata kan ook door de cloud-provider worden gedeeld met anderen[19].

Voor dit onderzoek wordt de nadruk vooral gelegd op het beveiligingsaspect. Indien we klantdata beter kunnen beveiligen, krijgen we daarmee mogelijk (een deel van) onze datasoevereiniteit terug.

2.4 Gradaties van het probleem

De opslag van informatie in de cloud kan op allerlei verschillende manieren, afhankelijk van het type cloud. Om hier in de context van informatiebeveiliging enige structuur in te scheppen, hanteren we voor dit onderzoek onderstaande opdeling[20]. De mate van controle over beschikbaarheid, integriteit en vertrouwelijkheid hangen af van de categorie waarin een cloudoplossing valt. Deze categorieën zijn voor dit onderzoek uitgesplitst in drieën: (a) on-premise private cloud, (b) off-premise private cloud en (c) off-premise public cloud. Let wel, dat het hebben van controle niet betekent dat de beveiligingsmaatregelen niet meer goed geregeld moeten worden. Het hebben van controle zorgt er alleen voor dat je als dataeigenaar ook daadwerkelijk in staat bent om je er van te verzekeren dat je data veilig (genoeg) is opgeslagen, zonder dat je daarbij (teveel) afhankelijk bent van anderen[21].

2.4.1 On-premise, private cloud

Bij deze vorm van opslag wordt data bewaard op eigen hardware op eigen terrein. Deze cloud is vanuit het perspectief van informatiebeveiliging gezien een verlengstuk van het interne netwerk. Zodoende is de cloud digitaal en fysiek alleen toegankelijk voor eigen mensen.

In deze situatie heeft de eigenaar van de data volledige controle over de data. De beschikbaarheid, integriteit en vertrouwelijkheid is goed te regelen. Alleen eigen

[19] https://www.wsj.com/articles/microsoft-sues-justice-department-over-secret-customer-data-searches-1460649720
[20] https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/
[21] https://www.isms.online/iso-27001/information-security-risk-management-explained/

personeel heeft toegang tot de data en met technische, procedurele en organisatorische beveiligingsmaatregelen kan deze toegang ingeregeld worden. Deze vorm van cloudopslag hoeft dan ook niet wezenlijk anders beveiligd te worden dan andere vormen van interne dataopslag.

2.4.2 Off-premise, private cloud

Deze vorm van opslag bewaart data op eigen hardware, maar niet op eigen terrein. De data staat opgeslagen in een datacenter in Nederland en de toegang tot de data kan grotendeels worden beperkt door technische, procedurele en organisatorische beveiligingsmaatregelen die worden geïmplementeerd door de eigenaar van de data en/of de beheerder van het datacenter.

Er is in dit geval geen sprake van *volledige* controle over de eigen data, immers een deel van de controle ligt bij een andere partij. Maar aangezien de data nog steeds in Nederland staat opgeslagen en de medewerkers van een datacenter geacht worden zich te houden aan bepaalde afspraken en procedures, is er meestal sprake van *voldoende* controle.

2.4.3 Off-premise, public cloud

Deze vorm van opslag wordt onder andere aangeboden door grote cloud-providers als Amazon, Google, Microsoft, Dropbox enzovoort. De data wordt opgeslagen op hardware van de cloud-provider en staat vaak in het buitenland bij grote datacenters.

Deze vorm van cloud is digitaal en fysiek toegankelijk voor een relatief grote groep mensen waar weinig tot geen zichtbaarheid op is en waar vrijwel geen controle op kan worden uitgevoerd. In het geval van een public cloud heeft de eigenaar van de data niet *volledig* zicht op of controle over de (beveiliging van de) data. Ook hier geldt dat de medewerkers van een datacenter en/of een cloud-provider geacht worden zich te houden aan bepaalde afspraken en procedures in de contractuele sfeer. Vaak zijn er wel afspraken mogelijk voor het garanderen van de beschikbaarheid in de vorm van “Service-Level Agreements” (SLA) met betrekking tot bepaalde ‘uptime’[22] garanties.

[22] https://en.wikipedia.org/wiki/High_availability

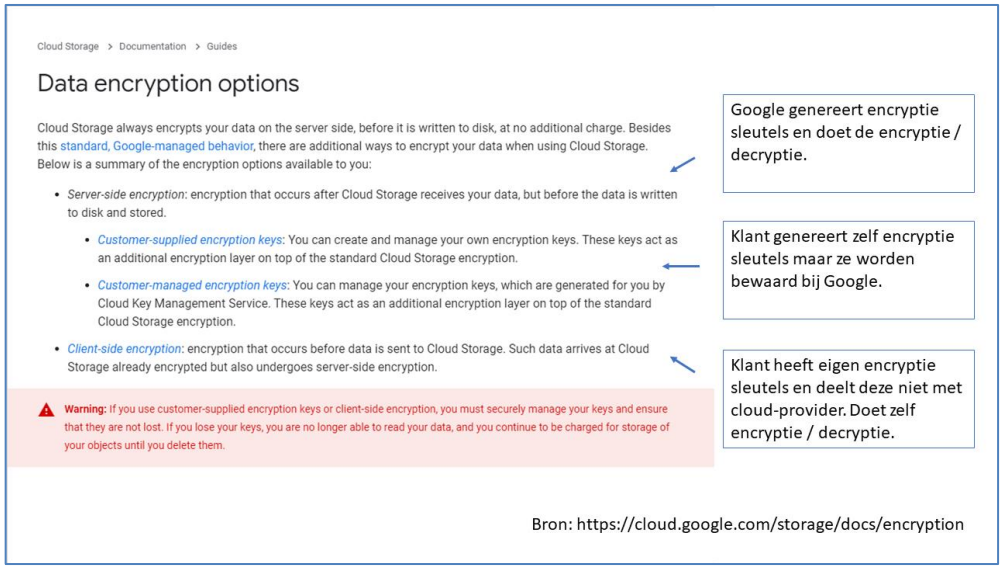
3 Aangeboden cryptografie door cloud-providers

Om een duidelijker beeld te krijgen van de aanwezigheid, vorm en omvang van het informatiebeveiligingsprobleem in de cloud werpen we in dit hoofdstuk een blik op de mogelijkheden die de grote cloud-providers hun gebruikers als oplossing aanbieden.

Aangezien de scope van dit rapport op de beveiliging van ‘data-at-rest’ ligt, kijken we met dit perspectief naar data versleutelingsmogelijkheden. Zoals aangegeven in het vorige hoofdstuk biedt versleuteling van data mogelijkheden tot meer controle over zowel vertrouwelijkheid als integriteit. Deze twee factoren verhogen ook de mate van soevereiniteit wat betreft de eigen data. Controle over de beschikbaarheid in de context van cloud storage komt minder prominent aan de orde, aangezien dit met andere maatregelen zoals *replicatie* kan worden verhoogd.

3.1 Google

Google biedt verschillende mogelijkheden met betrekking tot ‘Data encryption options’ (zie Figuur 5).



Figuur 5 Google data encryption options.

Google meldt dat er verschillende opties mogelijk zijn voor klanten: server-side encryptie en client-side encryptie[23].

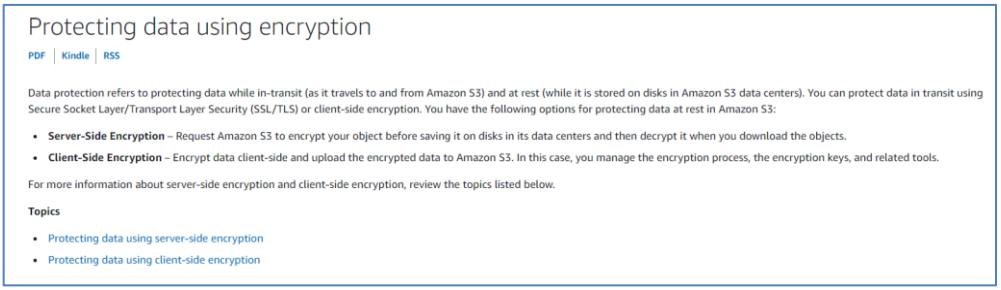
‘Server-side encryptie’ is gegevensversleuteling die wordt uitgevoerd nádat Google de (plaintext) data van de klant heeft ontvangen. Soms gebeurt dit met een sleutel van Google en soms met een sleutel van de klant. Maar in al deze gevallen beschikt Google over de encryptie sleutel en heeft daarmee de mogelijkheid om de klantdata te ontcijferen en in te zien.

[23] https://cloud.google.com/storage/docs/encryption

‘Client-side encryptie’ is gegevensversleuteling die wordt uitgevoerd vóórdat gegevens naar de Cloud Storage aanbieder worden verstuurd. Implementaties van cryptografische algoritmen en het beheer van sleutels worden bij deze variant client-side gedaan. Informatie die op deze manier aan de klant-kant wordt vercijferd, komt beveiligd aan bij Google Cloud Storage in de vorm van ciphertext. Google beschikt op deze manier niet over de sleutels en heeft geen mogelijkheid om de plaintext klantdata in te zien.

3.2 Amazon

Amazon biedt AWS S3 (Simple Storage Service) aan voor het opslaan van data in hun cloud. Ook Amazon geeft aan dat de eindgebruiker kan kiezen tussen server-side encryptie en client-side encryptie (zie Figuur 6).



Figuur 6 AWS S3 data encryptie opties[24].

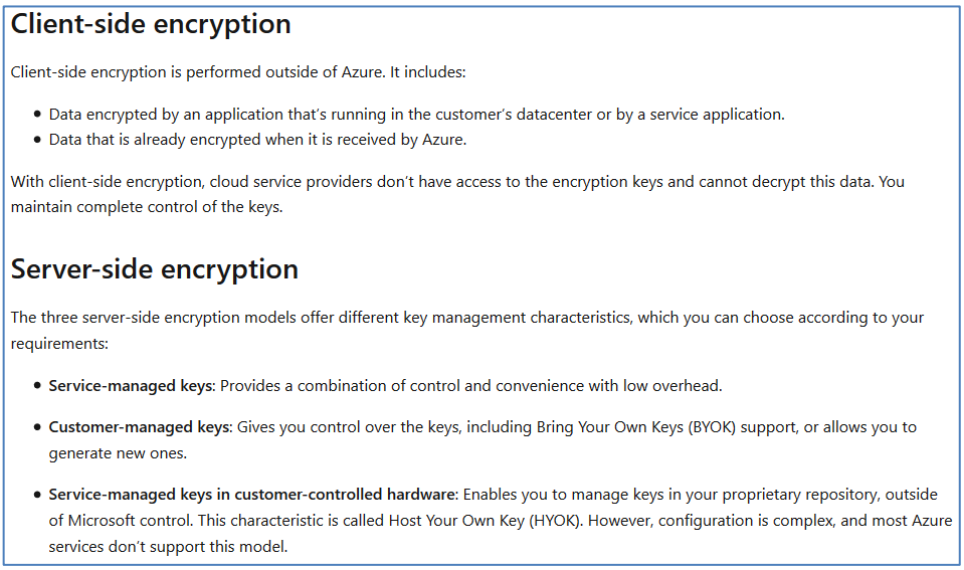
Server-side encryptie kan met behulp van sleutels die gegenereerd en beheerd worden door Amazon. Als alternatief kan de klant ook zelf een sleutel bij Amazon aanleveren voor gebruik bij de versleuteling. Ook Amazon heeft bij deze optie toegang tot de sleutels[25].

Bij c*lient-side encryptie* worden de sleutels aan de zijde van de klant van Amazon opgeslagen. Daarbij kunnen de sleutels worden opgeslagen in een applicatie van Amazon die de encryptie en decryptie bij de klant regelt. Als alternatief kan de klant ook de sleutels compleet in eigen beheer houden en in deze situatie worden de sleutels nooit naar Amazon toegestuurd[26]. Dit alternatief geeft de klant meer controle over en inzicht in de beveiliging van de klantdata.

3.3 Microsoft

Als laatste grote cloud-provider in ons onderzoek noemt ook Microsoft zowel client-side als server-side encryptie voor Microsoft Azure (zie Figuur 7).

[24] https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html
[25] https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html
[26] https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingClientSideEncryption.html



Client-side encryption

Client-side encryption is performed outside of Azure. It includes:

- Data encrypted by an application that's running in the customer's datacenter or by a service application.
- Data that is already encrypted when it is received by Azure.

With client-side encryption, cloud service providers don't have access to the encryption keys and cannot decrypt this data. You maintain complete control of the keys.

Server-side encryption

The three server-side encryption models offer different key management characteristics, which you can choose according to your requirements:

- **Service-managed keys**: Provides a combination of control and convenience with low overhead.
- **Customer-managed keys**: Gives you control over the keys, including Bring Your Own Keys (BYOK) support, or allows you to generate new ones.
- **Service-managed keys in customer-controlled hardware**: Enables you to manage keys in your proprietary repository, outside of Microsoft control. This characteristic is called Host Your Own Key (HYOK). However, configuration is complex, and most Azure services don't support this model.

Figuur 7 Microsoft Azure data encryptie opties.

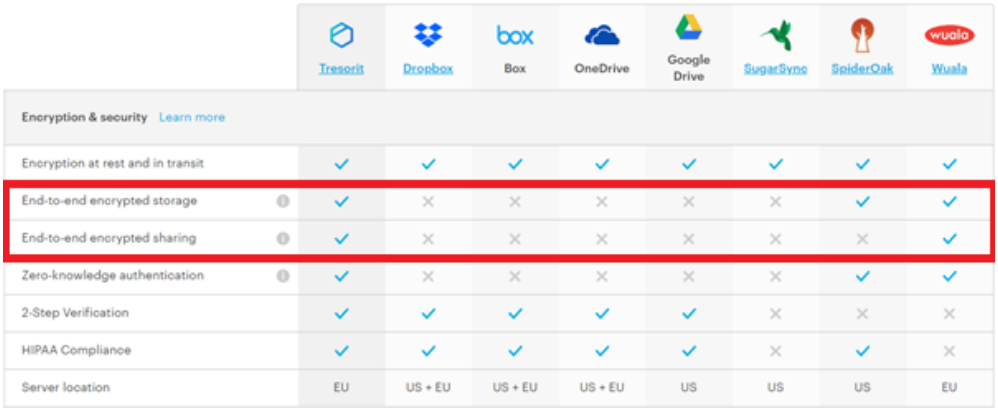
In het geval van *server-side encryptie* biedt Microsoft drie opties voor sleutelbeheer[27]. Bij *Service-managed keys* liggen zowel het creëren als het beheren van de sleutels in handen van Microsoft. *Customer-managed keys* worden gegenereerd door de klant, maar nog wel beheerd en opgeslagen door Microsoft. De laatste optie, *Service-managed keys in customer-controlled hardware*, biedt de mogelijkheid om zowel zelf sleutels te genereren als op te slaan. Deze laatste optie zorgt ervoor dat de sleutels alleen beschikbaar zijn voor de klant.

Daarnaast biedt Microsoft nog een mogelijkheid genaamd 'Double Key Encryption'[28]. Met Double Key Encryption kunnen klanten hun gevoelige gegevens beschermen om te voldoen aan speciale vereisten. Het helpt klanten om de controle over hun encryptie sleutels te behouden. Het gebruikt twee sleutels om gegevens te beschermen: één sleutel onder de controle van de klant en een tweede sleutel die is opgeslagen in Microsoft Azure. Voor het bekijken van gegevens die zijn beveiligd met Double Key Encryption is toegang tot beide sleutels vereist.

3.4 Vergelijking van aanbieders

De meeste providers van cloudopslag bieden een bepaald niveau van encrypted storage waarbij ze de inhoud van bestanden die een gebruiker heeft opgeslagen versleutelen. In de documentatie van Tresorit (zie Figuur 8) wordt een handige vergelijking gemaakt van enkele cloud-storage providers[29] .

[27] https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview
[28] https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption-overview?view=o365-worldwide
[29] https://tresorit.com/cloud-storage-comparison-business



	Tresorit	Dropbox	Box	OneDrive	Google Drive	SugarSync	SpiderOak	Wuala
Encryption & security Learn more								
Encryption at rest and in transit	✓	✓	✓	✓	✓	✓	✓	✓
End-to-end encrypted storage	✓	×	×	×	×	×	✓	✓
End-to-end encrypted sharing	✓	×	×	×	×	×	×	✓
Zero-knowledge authentication	✓	×	×	×	×	×	✓	✓
2-Step Verification	✓	✓	✓	✓	✓	×	×	×
HIPAA Compliance	✓	✓	✓	✓	✓	×	✓	×
Server location	EU	US + EU	US + EU	US + EU	US	US	US	EU

Figuur 8 Cloud storage security vergelijking.

Voor de context van ons onderzoek zijn twee ‘features’ vooral interessant: “end-to-end encrypted storage” en “end-to-end encrypted sharing”.

Beide zijn de zogenaamde ‘end-to-end encryption’[29] (E2EE) features van encryptie waarbij alleen de gebruiker de beschikking heeft over de encryptie sleutels. Dit betekent dat service providers (telecom provider, internet provider, cloud-provider, datacenter enzovoort) geen toegang hebben tot de (plaintext) klantdata. Om de klantdata te kunnen ontcijferen, is de sleutel nodig. De meeste providers van cloudopslag houden de sleutel namens de gebruiker in beheer en bieden dus geen E2EE aan, zoals te zien is in Figuur 8 door het ontbreken van vinkjes bij de E2EE features. In deze gevallen moet de gebruiker wederom vertrouwen op gedragsregels en wet- en regelgeving dat het bedrijf de toegang tot bestanden niet zal misbruiken of de sleutel niet zal verliezen of aan derden geeft.

[29] https://en.wikipedia.org/wiki/End-to-end_encryption

4 Oplossingsrichtingen

Globaal zien we op dit moment (medio december 2020) verschillende type initiatieven opkomen in de markt voor het beter beveiligen van informatie in de cloud. Sommige van deze initiatieven zijn ook bruikbaar voor het terughalen van datasoevereiniteit. Hieronder staan de initiatieven waar wij op dit moment zicht op hebben:

1 **GAIA-X**. Men kan proberen data terug te halen naar de EU waar het kan worden opgeslagen bij partijen die voldoen aan EU wet- en regelgeving.
2 **Dutch Secure Autonomous Cloud (DUSAC).** Men kan proberen data terug te halen naar een Nederlandse cloud die voldoet aan beveiligingseisen voor het mogen opslaan en verwerken van vertrouwelijke informatie zodat recht wordt gedaan aan veiligheidsstandaarden, privacywetgeving en digitale autonomie[30]
3 **Client-side encryptie**. Men kan proberen de data zo te beveiligen dat anderen er niks mee kunnen met betrekking tot I en V. Voor de I van Integriteit en de V van Vertrouwelijkheid bestaan mogelijkheden om dit te realiseren. Voor de B van Beschikbaarheid geldt dat deze niet verbeterd kan worden met cryptografie maar wel met andere methodieken zoals bijvoorbeeld *replicatie*.

Deze nieuwe cloud initiatieven kunnen ook gecombineerd worden met *client-side encryptie*. Want zelfs als het lukt om alle data weer op eigen bodem te krijgen en zelfs als het lukt om een speciaal gecertificeerde cloud te realiseren, dan nog is er vaak sprake van een groep van niet-geautoriseerde mensen die bij de informatie kunnen komen: namelijk de medewerkers van de cloud-provider en de datacenters.

4.1 GAIA-X

In 2019 is in Europa door de verschillende Europese overheden waaronder Duitsland en Frankrijk een nieuw initiatief gelanceerd met de naam GAIA-X[31]. GAIA-X is bedoeld om cloud en edge diensten van Europese aanbieders te verenigen in een data-infrastructuur met gemeenschappelijke regels, normen en technologieën. Organisaties die deelnemen aan GAIA-X moeten deze regels en normen naleven en leveren diensten op basis van technologieën die door alle deelnemers van GAIA-X worden onderschreven.

Het is nog niet duidelijk welke normen, regels en afspraken ten grondslag zullen liggen aan GAIA-X. Zeker is wel dat het doel van GAIA-X, namelijk het herpakken en behoud van soevereiniteit over data voor de EU, de lidstaten, overheden, bedrijven en burgers, leidend zal zijn bij de verdere uitbouw van het initiatief.

4.2 Dutch Secure Autonomous Cloud (DUSAC)

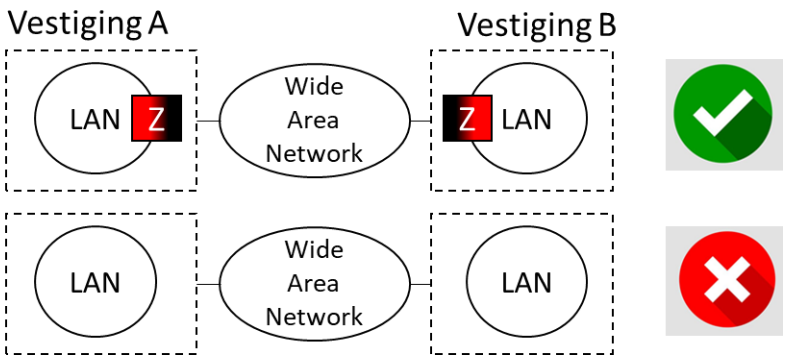
Nederlandse overheden en bedrijven zijn voor opslag, beheer en verwerking van groeiende hoeveelheden data afhankelijk van buitenlandse hardware- en softwareleveranciers. Hierdoor verliezen zij zichtbaarheid, controle en zeggenschap over hun data. Op dit moment zijn er vrijwel geen harde garanties en moet vertrouwd worden op een complexe hardware- en softwarestack van Amerikaanse

[30] https://ivi.uva.nl/content/events/events/2020/12/workshop-dutch-secure-autonomous-cloud.html
[31] https://en.wikipedia.org/wiki/GAIA-X

en Chinese makelij in combinatie met grote buitenlandse multinationals: “Big Tech”. De ontwikkeling van een transparante, nationale cloud met veiligheidsgaranties voor de verwerking en opslag van vertrouwelijke informatie kan het tij keren zodat recht wordt gedaan aan veiligheidsstandaarden, privacywetgeving en digitale autonomie.[32]

4.3 Client-side encryptie voor de cloud

Het veilig opslaan van data in een onveilige cloud lijkt voor wat betreft de beveiligingsrisico’s op het versturen van gerubriceerde informatie over een publiek telecommunicatienetwerk ("ongecontroleerd gebied"). Stel dat medewerkers van één bedrijf moeten samenwerken aan gerubriceerde projecten over meerdere fysiek-gescheiden vestigingen heen. En stel dat het bedrijf daarvoor gebruik maakt van de netwerkdiensten van een externe netwerkleverancier. Dan dicteren de beveiligingseisen dat de medewerkers van de netwerkleverancier niet mogen kunnen meekijken met de klantdata. Een manier om dat technisch vorm te geven is door gebruik te maken van goedgekeurde[33] “Virtual Private Network” (VPN) producten, zgn. lijn-vercijferaars (zie Figuur 9).



Figuur 9 VPN-technologie.

Op deze manier ontstaat één groot beveiligingsdomein waarin het bedrijf volledig verantwoordelijk is voor - en in controle is over - de beveiliging van de binnen het bedrijf opgeslagen en over het netwerk gecommuniceerde vertrouwelijke informatie. De mensen, de gebouwen, de techniek, de procedures enzovoort vallen allemaal onder verantwoordelijkheid en controle van het bedrijf. Omdat er (naast organisatorische en procedurele maatregelen) technologie voorhanden is die in voldoende mate de risico’s verlagen tot een acceptabel niveau.

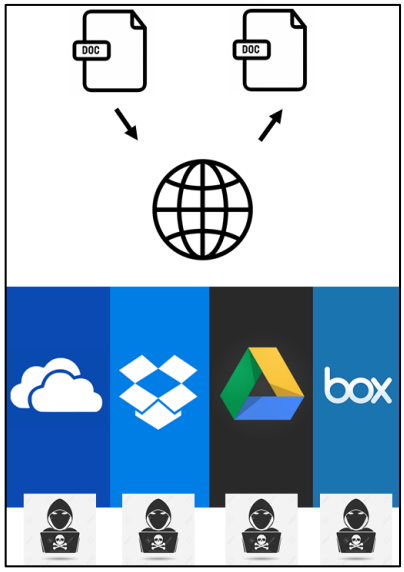
Dus encryptie kan het verschil maken tussen het wel of niet mogen verwerken van gerubriceerde informatie van een bepaald niveau in een bepaalde context. Zijn er voor veilig werken in de cloud technologieën denkbaar die lijken op de hierboven genoemde VPN-technologie? Immers in deze producten zitten algoritmen en sleutels die goedgekeurd zijn om op een bepaalde manier bepaalde informatie te mogen opslaan, versturen en verwerken [6].

[32] https://portals.project.cwi.nl/dutch-secure-autonomous-cloud/
[33] https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten

Om dit uit te zoeken, schetsen we hieronder een drietal incrementele scenario's die weergeven hoe een dergelijk product zou kunnen werken. Het eerste scenario omschrijft de huidige, niet beveiligde, uitgangspositie. In het tweede scenario schetsen we een eerste product dat, vergelijkbaar met de genoemde VPN-technologie, data voor cloudopslag kan vercijferen vóórdat het naar de cloud wordt gestuurd. Het derde en laatste scenario beschrijft een mogelijke toekomstige verbetering van het tweede scenario die samenwerking tussen eindgebruikers van de cloud toepassing makkelijker maakt en extra beveiligingsmaatregelen voorstelt.

4.3.1 *Scenario A - Geen encryptie (uitgangspositie)*

Als startscenario (uitgangspositie) hanteren we een denkbeeldig referentiemodel waarbij gebruikers een bestand opslaan in een public cloud zonder extra beveiligingsmaatregelen te treffen (zie Figuur 10).



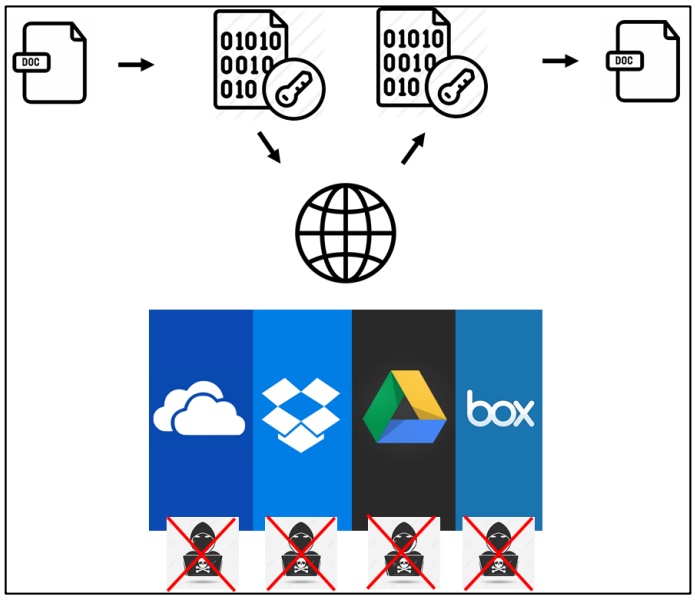
Figuur 10 Cloud opslag zonder encryptie.

In dit simpele scenario zouden medewerkers van een serviceprovider kunnen optreden als aanvaller (een 'insider attack'[34]) en kunnen meekijken met de bestanden die staan opgeslagen in de cloud.

4.3.2 *Scenario B - GnuPG of Virtual Encrypted Disk*

Als tweede scenario hanteren we een denkbeeldig referentiemodel waarbij gebruikers eerst een bestand vercijferen met een sleutel die alleen zij hebben en pas daarna de data opslaan in de public cloud (zie Figuur 11).

[34] https://en.wikipedia.org/wiki/Cyberattack#Types_of_attack



Figuur 11 Cloud opslag met encryptie.

In dit scenario kunnen medewerkers van een serviceprovider niet meer meekijken met de bestanden die staan opgeslagen in de cloud. Vanuit het perspectief van een cloud-provider is de opgeslagen klantdata dan een niet te interpreteren reeks van 0'en en 1'en geworden ('ciphertext'). Dit is vergelijkbaar met een netwerkprovider die kijkt naar netwerk 'packets' die in vercijferde vorm over het netwerk heen en weer gestuurd worden.

Alleen het werken met bijvoorbeeld GnuPG[35] in combinatie met Google Drive of een Virtual Encrypted Disk product zoals VeraCrypt[36] in combinatie met een Dropbox Sync Folder is complex. En bovendien zijn dit geen 'enterprise' type producten waarbij een makkelijke User Interface wordt gecombineerd met typische enterprise 'features'. Zoals bijvoorbeeld een centrale vorm van sleutel-beheer gecombineerd met Microsoft Active Directory om voor alle eindgebruikers de sleutels op te kunnen slaan.

4.3.3 *Scenario C - Toekomstige oplossing*

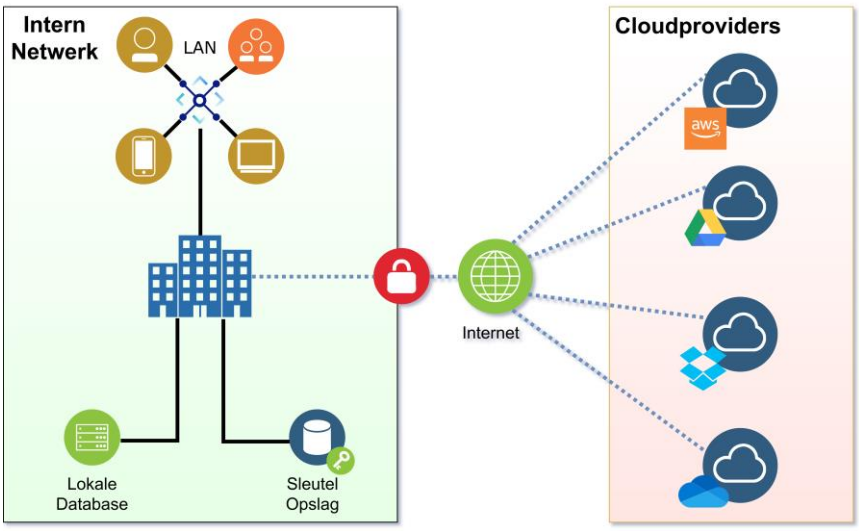
Als derde scenario hanteren we een denkbeeldig referentiemodel voor een toekomstige oplossing. We zijn op zoek naar een flexibele en schaalbare client-side encryptieoplossing voor de zakelijke cloud. Eindgebruikers moeten eenvoudig en veilig samen aan projecten kunnen werken in wisselende samenstellingen. Dit betekent dat een oplossing niet alleen:

a. de *veiligheid* moet adresseren, maar ook
b. het *samenwerken* van mensen in een organisatie.

De klantdata moet veilig in de cloud kunnen worden opgeslagen maar de sleutels mogen daar niet staan; deze moeten aan de klant-zijde kunnen worden opgeslagen en beheerd. De oplossing moet bij voorkeur ondersteuning hebben voor het kunnen werken met meerdere cloud-providers om 'vendor lock-in' te voorkomen (zie Figuur 12). Ook moet het idealiter mogelijk zijn om zelf een "on-premise private-

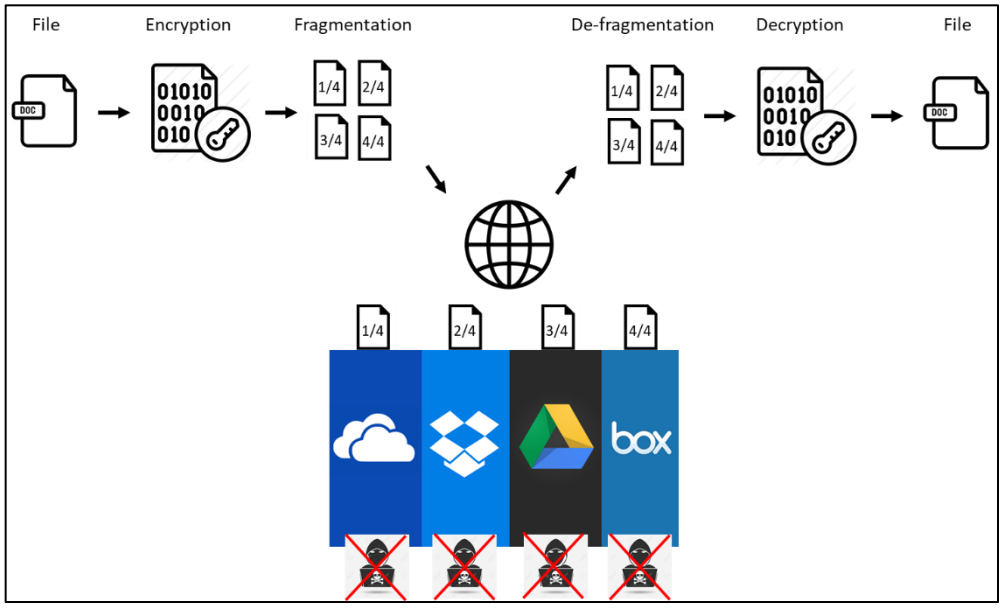
[35] https://gnupg.org/
[36] https://en.wikipedia.org/wiki/VeraCrypt

cloud” oplossing te gebruiken en bij te schakelen naast de commerciële publieke aanbieders zodat een zgn. “Hybrid Cloud” ontstaat.



Figuur 12 Enterprise oplossing.

Als extra beveiligingsmaatregel zou het mogelijk moeten zijn om de data eerst te fragmenteren in stukken en dan de stukken op te slaan bij verschillende cloud-providers (zie Figuur 13).



Figuur 13 Cloud opslag met encryptie en data-fragmentatie.

Als de klantdata wordt opgesplitst in brokjes, dan weet de cloud-provider niet welk brokje bij welke klantdata hoort. En als verschillende brokjes data bij verschillende cloud-providers worden opgeslagen zodanig dat niet één cloud-provider alle brokjes in handen heeft, dan wordt het bovenop de encryptie-maatregel nog moeilijker om de klantdata te achterhalen.

Voor de veiligheid moet de software-architectuur bij voorkeur modulair zijn, dat wil zeggen dat het mogelijk moet zijn om verschillende encryptie-algoritmen te kunnen kiezen. Als blijkt dat een algoritme zwakheden bevat, moet voor nieuwe projecten gewisseld kunnen worden naar nieuwe algoritmen waarbij de oude algoritmen langzaam worden uitgefaseerd.

4.4 Voorbeelden van producten in de markt

Nu we een beeld hebben van hoe toekomstige oplossingen in de markt er uit kunnen zien, is het tijd om een aantal producten van de huidige markt uit te lichten. De producten die we hieronder bespreken voldoen niet altijd volledig aan het door ons geschetste beeld, maar geven wel een goede weergave van de te realiseren functionaliteit voor eindgebruikers en de manieren waarop de informatiebeveiliging geregeld kan worden.

Merk op dat onderstaande producten binnen de context van dit onderzoek niet praktisch zijn uitgeprobeerd. Onderstaande beschrijvingen zijn slechts gemaakt op basis van productbeschrijvingen en/of productdocumentatie.

4.4.1 UtahFS

UtahFS[37] is een cryptografie oplossing voor veilige cloud opslag. Het presenteert zichzelf als een opslagschijf op de computer van de gebruiker waar bestanden op gezet kunnen worden. Onder de motorkap worden deze bestanden opgeknipt in kleine blokken en vercijferd en daarna verdeeld over meerdere cloud-providers. Vanuit het perspectief van de cloud-provider worden er blokken data opgeslagen waarbij niet meegelezen kan worden. De encryptie zorgt er ook voor dat ongeautoriseerde aanpassingen kunnen worden gedetecteerd. De beschikbaarheid wordt verhoogd door elk blok redundant bij meerdere providers neer te zetten.

4.4.2 Boxcryptor

Boxcryptor[38] is een applicatie die gebruikt kan worden om cryptografie aan bestaande cloudopslag toe te voegen. Het is een oplossing die data versleutelt voordat het in de cloud wordt opgeslagen. De lokale Boxcryptor applicatie biedt ook ondersteuning voor sleutelbeheer kan alle gebruikte sleutels beveiligd opslaan op basis van het wachtwoord van de gebruiker. Hierdoor zou Boxcryptor zelf geen toegang tot de bestanden in de cloud moeten kunnen krijgen. Ondersteuning voor access control en user management is ook aanwezig voor zowel kleine als grote groepen gebruikers.

4.4.3 Cryptomator

Cryptomator[39] is een andere third-party oplossing om de informatie in bestaande cloudopslag te versleutelen voordat deze de lokale omgeving verlaat. Cryptomator stelt de gebruiker in staat om verscheidene kluizen aan te maken waarin data versleuteld wordt opgeslagen. De gebruiker kan een dergelijke *vault* uploaden naar een bestaande cloudopslag en zo overal toegang krijgen tot dezelfde data. Na het binnenhalen van een kluis, kan alleen de eigenaar met het ingestelde wachtwoord de kluis openen en de data inzien en bewerken. Hierna wordt de kluis weer gesloten en wordt de data versleuteld met de cloud gesynchroniseerd.

---

[37] https://github.com/cloudflare/utahfs
[38] https://www.boxcryptor.com/en/
[39] https://cryptomator.org/

4.4.4 ODrive

Odrive[40] is een applicatie die bedoeld is om cloudopslag bij verschillende providers in één applicatie te kunnen beheren. Echter biedt Odrive ook ondersteuning voor encryptie van alle data voordat deze naar de cloud wordt gestuurd. Odrive versleutelt elk bestand met een unieke sleutel die onder andere is afgeleid van het wachtwoord van de gebruiker. Deze sleutels en het wachtwoord worden nooit gedeeld met Odrive of een andere derde partij. Dit zorgt ervoor de data alleen voor de eigenaar toegankelijk is. Data kan ook gedeeld worden met andere gebruikers door deze in een gedeelde map te plaatsen met een speciaal gedeeld wachtwoord.

4.4.5 Tresorit

Tresorit[41] is een cloud-provider met een sterke focus op privacy en informatiebeveiliging. Er wordt client-side encryptie geboden, waarbij het gebruikte wachtwoord nooit het lokale apparaat verlaat. Daarnaast kunnen bestanden ook gemakkelijk gedeeld worden met andere gebruikers en biedt Tresorit mogelijkheden om security policies in te stellen. Een laatste interessante mogelijkheid is de keuze om data in een datacentrum in een land naar keuze op te slaan, waarbij dit kan verschillen per bestand. Dit biedt de klant ook mogelijkheden om meer zekerheid te krijgen over onder welke wet- en regelgeving de locatie valt.

4.4.6 SureDrop

SureDrop[42] is een versleutelde cloud oplossing ontwikkeld door Senetas en Senetas Corporation is onderdeel van de Thales Group[43]. De servers waar de data worden opgeslagen kunnen zowel off- als on-premise aangeboden worden en compatibiliteit met andere cloud solutions als AWS en Office365 wordt geboden. SureDrop biedt client-side encryptie aan, waarbij het sleutelbeheer volledig in handen van de dataeigenaar blijft. Data die op de cloud opgeslagen dient te worden, wordt lokaal versleuteld en vervolgens verdeeld over meerdere fysieke servers opgeslagen, door SureDrop ook wel ‘fragmented storage’ genoemd.

4.4.7 Storro

Storro[44] is een applicatie om bestanden veilig op te slaan en te delen. Ongeacht het bestandsformaat, type inhoud of grootte. Storro maakt een virtuele harde schijf aan op een computersysteem waarmee bestanden kunnen worden geopend, bewerkt en worden bewaard in de Windows File Explorer (Windows Verkenner). Alle bestanden die hier worden opgeslagen, worden automatisch versleuteld en vervolgens gesynchroniseerd met de cloud. Wijzigingen in gedeelde mappen worden automatisch gedeeld met de collega’s, klanten of partners die hiertoe zijn geautoriseerd.

4.5 Handelingsperspectief

Mogelijk gaan de initiatieven zoals GAIA-X en DUSAC leiden tot veilige(re) oplossingen die in de toekomst mogen worden gebruikt voor deze vorm van dataopslag in de cloud gecombineerd met deze vorm van klantdata.

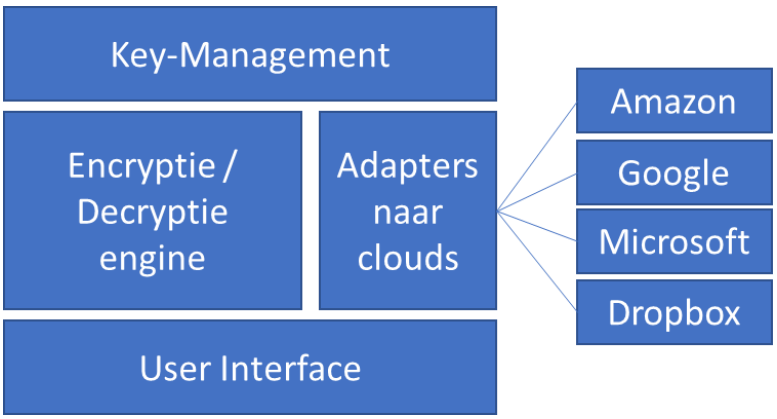
---

[40] https://www.odrive.com/features/encryption
[41] https://tresorit.com/
[42] https://www.sure-drop.com/
[43] https://cpl.thalesgroup.com/partners/senetas-corporation
[44] https://storro.com/applicatie/#product

Maar zelfs als deze initiatieven voldoende veilig zullen blijken te zijn om te mogen worden gebruikt, dan nog is een ‘defense-in-depth’ strategie[45,46,47] aan te bevelen waarbij overlappende beveiligingsmaatregelen een sterkere oplossing kunnen bieden.

Client-side encryptie is een sterke beveiligingstechnologie waarbij een klant of eindgebruiker van een cloud-provider meer ‘in control’ is voor wat betreft integriteit en vertrouwelijkheid van klantdata [7, 8]. Met deze technologie wordt een gebruiker van een cloud-provider minder afhankelijk van de organisatorische, procedurele en technische maatregelen van service providers. De gevonden aanbieders in de markt beloven een vorm van client-side encryptie in combinatie met lokale sleutels volledig in eigen beheer. Maar het zijn bijna allemaal oplossingen van buitenlandse leveranciers waarbij inzage in de broncode van hun producten niet altijd mogelijk is.

We willen een vergelijkbaar type product ontwikkeld in Nederland door een Nederlandse softwareleverancier waarbij het product gecertificeerd kan worden door de bevoegde instanties. Zo’n product vergroot de kansen om in de toekomst te kunnen voldoen aan de beveiligingseisen die gesteld gaan worden aan het werken met vertrouwelijke of gerubriceerde informatie van een bepaald niveau in de context van een public cloud.



Figuur 14 Modulaire opzet van een applicatie.

Daarvoor zou een innovatieproject gestart kunnen worden met industriële partners in combinatie met kennispartijen, zoals universiteiten, om zo samen in een co-creatie traject een Nederlands beveiligingsproduct te ontwikkelen die een modulaire architectuur heeft (zie Figuur 14).

4.6 Aandachtspunten

De fundamentele spanning tussen end-to-end encryptie enerzijds en behoud van bepaalde cloud functionaliteit anderzijds, kan wel zorgen voor onverwachte consequenties. Bijvoorbeeld, het end-to-end vercijferd opslaan van klantdata kan als gevolg hebben dat bepaalde cloud diensten niet meer mogelijk zijn. Denk aan het in de cloud laten indexeren en doorzoekbaar maken van documenten of grote

[45] https://en.wikipedia.org/wiki/Defense_in_depth_(computing)
[46] https://www.schneier.com/blog/archives/2006/02/security_in_the.html
[47] https://www.security.nl/posting/675017

datasets. Of het maken van automatische back-ups in de cloud in het kader van ‘Data Loss Prevention’[48] (DLP).

Het gebruik van end-to-end encryptie zou ook kunnen betekenen dat dergelijke functionaliteit wel mogelijk is, maar opnieuw geïmplementeerd moet worden aan de klant-zijde, omdat daar wel volledig inzicht is in de (plaintext) klantdata.

Tegelijkertijd ontstaan er ook nieuwe technieken zoals “homomorphic encryption”[49] met bijbehorende producten[50] waarbij het mogelijk is om toch bewerkingen te kunnen uitvoeren in en op encrypted datasets[51] [52].

[48] https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies
[49] https://en.wikipedia.org/wiki/Homomorphic_encryption
[50] https://shieldio.com/
[51] https://www.microsoft.com/en-us/research/project/homomorphic-encryption/
[52] https://www.microsoft.com/en-us/research/project/microsoft-seal/

5 Plan van aanpak om te komen tot de routekaart ‘veilig gebruik van een onveilige cloud’

5.1 Doel van de routekaart

Het doel van de routekaart ‘veilig gebruik van een onveilige cloud’ is om de Nederlandse markt voor beveiligingsproducten te laten groeien en om het gebruik van beveiligingsproducten voor clouddiensten te stimuleren zodat Nederland veiliger wordt. Meer specifiek gaat het over het beveiligen van vertrouwelijke gegevens die de Rijksoverheid wil opslaan in de cloud. Dit vraagt om een meerjarige investering in kennis en technologieontwikkeling, die beschreven kan worden in een routekaart. De stip op de horizon is dat de Rijksoverheid over 1 á 2 jaar door innovatieve producten op een veilige manier vertrouwelijke informatie van een bepaald vertrouwelijkheidsniveau kan opslaan in de cloud. In de daarop volgende jaren zou gewerkt kunnen worden aan extra functionaliteit zoals het client-side indexeren en doorzoekbaar maken van klantdata en aan de accreditatie van het product.

De start om te komen tot een routekaart voor productontwikkeling begint bij het in kaart brengen van de valorisatieketen, door middel van literatuuronderzoek en interviews, welke daarna geplot worden op de vijf ontwikkelfases: *Discovery/basic research, Technology development, Validation and demonstration, Integration and operationalization, Deployment*. De valorisatieketen is de keten die zich bezig houdt met productontwikkeling van wetenschappelijk onderzoek, tot technologieontwikkeling en de implementatie en ingebruikname daarvan. Binnen de valorisatieketen zijn drie hoofdgroepen te onderscheiden, a) de kennisinstellingen (universiteiten, hoge scholen, toegepaste onderzoeksinstellingen); b) de ontwikkelpartijen; en c) de eindgebruiker (in dit geval de Rijskoverheid). Daarnaast kunnen per onderwerp nog andere partijen een rol spelen. In dit geval bijvoorbeeld de ‘open source community’, die zelf producten ontwikkeld, of de toezichthouders en beleidsmakers. De partijen hebben allemaal hun eigen expertises en vaardigheden en zullen daardoor niet in elke fase van het ontwikkeltraject een rol spelen. Door de partijen te plotten op de ontwikkelfases wordt een beeld geschetst van welke partij zich waar in de ontwikkelfases bevindt.

Binnen de valorisatieketen zijn drie hoofdgroepen te onderscheiden, a) de kennisinstellingen (universiteiten, hoge scholen, toegepaste onderzoeksinstellingen); b) de ontwikkelpartijen; en c) de eindgebruiker (in dit geval de Rijksoverheid). Daarnaast kunnen per onderwerp nog andere partijen een rol spelen. In dit geval bijvoorbeeld de ‘open source community’, die zelf producten ontwikkelt, of de toezichthouders en beleidsmakers. De partijen hebben allemaal hun eigen expertises en vaardigheden en zullen daardoor niet in elke fase van het ontwikkeltraject een rol spelen. Door de partijen te plotten op de ontwikkelfases wordt een beeld geschetst van welke partij zich waar in de ontwikkelfases bevindt.

Barrières om te komen tot productontwikkeling kunnen aan het licht komen tijdens het in kaart brengen van de valorisatieketen [9]. Dit kunnen barrières zijn tussen de ontwikkelfases (de zogeheten ‘valleys of death’), maar ook meer fase overstijgende barrières. Hieronder staan een tweetal barrières die het ontwikkelen van cloudbeveiligingsproducten kunnen bemoeilijken:

- **De kleine afzetmarkt**: Wanneer een ontwikkelpartij wordt gevraagd een product te ontwikkelen zitten hier hoge kosten aan vast. De afzetmarkt voor beveiligingsproducten voor de cloud is klein en daarmee wordt het risico voor de ontwikkelpartij groot. As er geen klanten komen, kan de investering niet terugverdiend worden.
- **Noodzaak voor afstemming tussen leveranciers**: Voor de veiligheid van een systeem is modulariteit, de mogelijkheid om losse elementen te vervangen, van groot belang. Dit betekent namelijk dat bij een veiligheidsprobleem in één onderdeel, niet meteen de hele applicatie vervangen hoeft te worden, maar simpelweg alleen het onveilige onderdeel door een alternatief. Een oplossing voor het veilig kunnen opslaan van gegevens in de cloud zal bestaan uit verschillende onderdelen, die dus vervangen moeten kunnen worden. Dit vereist dat bij de ontwikkeling van een eindproduct zorg moet worden gedragen dat onderdelen van verschillende leveranciers goed met elkaar kunnen samenwerken, en ook vervangen kunnen worden door een alternatief van een nieuwe leverancier. Hierbij komt de vraag of de ontwikkelpartijen informatie met elkaar willen delen die dit mogelijk maakt.

5.2 Aanzet voor de routekaart

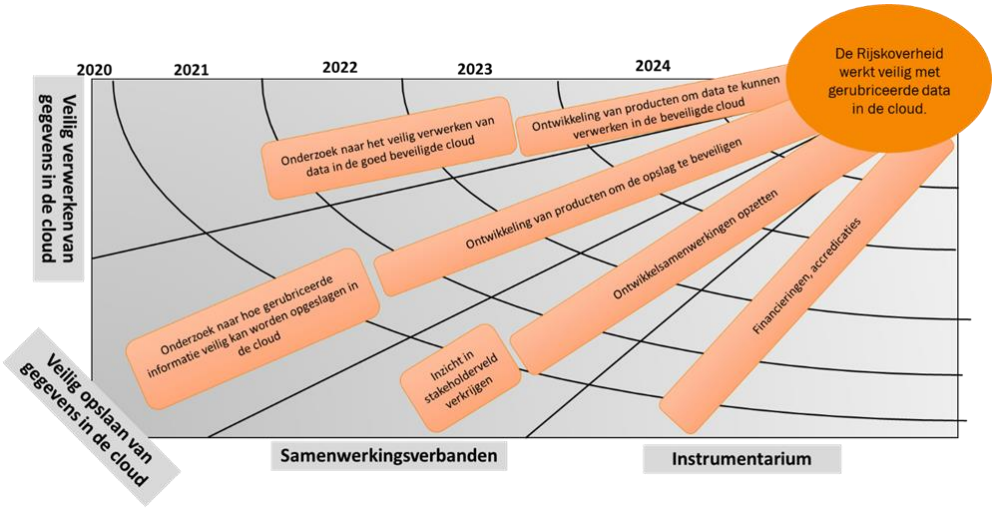
De daadwerkelijke routekaart ‘veilig werken in een onveilige cloud’ kan worden ingevuld aan de hand van een aantal sporen. De focus van dit rapport ligt op het veilig op kunnen slaan van vertrouwelijke informatie in de cloud (spoor 1). Kijkend naar de mogelijke oplossingsrichtingen zit hier een sterke link met het veilig kunnen verwerken van informatie in de cloud (spoor 2). Om te komen tot een goed functionerende valorisatieketen is samenwerking van groot belang. In de beschreven barrières kwam dit al naar voren in het kader van modulariteit. Daarom is een derde spoor meegenomen waarin richting gegeven moet worden aan de samenwerking tussen de partijen binnen de valorisatieketen. Om uiteindelijk producten te ontwikkelen is enerzijds een kader nodig op basis waarvan de prioriteit voor innovatie wordt aangegeven en anderzijds een financiële ondersteuning. De richting om te komen tot een kader en de uitwerking van financiële mogelijkheden kan worden gegeven in het vierde spoor.

Hieronder staan de vier mogelijke sporen in meer detail beschreven:

1 **Veilig opslaan in de cloud**: Allereerst moet onderzoek worden gedaan hoe gerubriceerde data veilig opgeslagen kan worden in de cloud. Bij dit onderzoek komen mogelijke oplossingsrichtingen naar voren. Voor deze oplossingsrichtingen zijn nieuwe producten nodig die tezamen aan de beveiligingseisen voldoen en zorgdragen aan de datasoevereiniteit. In dit spoor kunnen het onderzoek en de nieuw te ontwikkelen producten worden uitgezet in de tijd.
2 **Veilig verwerken van data in de cloud**: Niet alleen veilig opslaan, maar ook het veilig verwerken van gegevens in de cloud is van belang voor de Rijksoverheid. Bij het onderzoek naar mogelijke oplossingsrichtingen voor het veilig opslaan van gegevens in de cloud kwam naar voren dat het mogelijk is dat bij deze oplossingen de gegevensverwerkings functionaliteiten van de cloudleveranciers niet meer werken (bijvoorbeeld het kunnen indexeren). Verder onderzoek naar oplossingsrichtingen voor deze uitdaging is nodig en kan worden beschreven in de routekaart. Hierbij kan de ontwikkeling van benodigde innovaties ook worden weggezet in de tijd.

3 **Samenwerkingsverbanden**: Om tot onderzoeksrichtingen en productontwikkeling te komen zijn samenwerkingsverbanden nodig tussen de partijen in de valorisatieketen.
4 **Instrumentarium**: Partijen moeten een kader hebben waar onderzoeks- en ontwikkelbehoefte ligt. Daarnaast zit er een financiële noodzaak om het doen van onderzoek en productontwikkeling te bekostigen.

De beschreven mogelijke sporen zien er op een abstract niveau uit zoals weergegeven in Figuur 15.



Figuur 15 Abstracte invulling van de routekaart.

6 Conclusies

Bij de Rijksoverheid is een trend waarneembaar dat steeds meer wordt gewerkt in de cloud. Omdat hierdoor beveiligingsrisico's kunnen ontstaan, vraagt dit in de toekomst mogelijk om nieuwe sterkere beveiligingsmaatregelen voor veilige(re) opslag van deze informatie. Tegelijkertijd is het misschien mogelijk om met sterkere beveiligingsmaatregelen (een deel van) de datasoevereiniteit terug te halen en weer bij de klant te leggen, zelfs in het geval van een public cloud.

Een eindgebruiker of klant van een (public) cloud kan voor de opslag van niet-vertrouwelijke informatie in veel gevallen prima vertrouwen op de organisatorische, procedurele en technische maatregelen die een cloud-aanbieder heeft genomen. Maar voor sommige speciale gevallen, zoals bijvoorbeeld bij de opslag en verwerking van vertrouwelijke of zelfs gerubriceerde informatie, is een klant van een (public) cloud niet voldoende 'in control' over de eigen beveiligingsrisico's en de eigen beveiligingsmaatregelen ("ongecontroleerd gebied").

In dit onderzoeksrapport schetsen we de fundering (probleemstelling, analyse en mogelijke oplossingsrichtingen) voor een routekaart die als leidraad kan worden gebruikt voor de ontwikkeling en het gebruik van nieuwe producten voor het veilig kunnen opslaan van vertrouwelijke informatie in de (public) cloud. Voor deze oplossingsrichtingen is de ontwikkeling van nieuwe Nederlandse producten (waarschijnlijk) noodzakelijk, zowel voor de beveiliging van de opslag als het borgen van de datasoevereiniteit. Er zijn wel producten in de markt gevonden maar deze komen vrijwel allemaal uit het buitenland. Daarnaast lijkt bij deze oplossingsrichtingen een nieuw spanningsveld te ontstaan tussen enerzijds een betere beveiliging en anderzijds de door een cloud-provider geboden functionaliteit: bijvoorbeeld het indexeren en doorzoekbaar maken van documenten of datasets. Dit vormt een nieuwe uitdaging, waar eveneens onderzoek naar gedaan moet worden.

Met het opzetten van een routekaart kan richting worden gegeven aan het onderzoek en de ontwikkeling van nieuwe producten door de Nederlandse industrie. Daarbij is het doel om de Nederlandse markt voor beveiligingsproducten te laten groeien, om het gebruik van beveiligingsproducten voor clouddiensten te stimuleren zodat Nederland veiliger wordt en om meer autonomie over de eigen data c.q. digitale soevereiniteit voor Nederland te krijgen.

7 Referenties

1. Baseline Informatiebeveiliging Overheid (BIO) Thema Clouddiensten, Versie 1.0, 26-2-2020, https://www.cip-overheid.nl/media/1422/26022020-themadocument-clouddiensten-10.pdf
2. “Notitie Verkenning Cloudbeleid voor de Nederlandse Rijksdienst”, 29 november 2019, A.W. van der Togt, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
3. “Handreiking Quickscan Information Security”, Versie 1.0, 20 februari 2018
4. “Standpunt op Publieke clouddiensten en gerubriceerde gegevens”, 9 september 2019, J.L.M. Kuijpers
5. Whitepaper Strategische Autonomie op Cybersecurity. M.A. Veenendaal, T.C.C van Schie, M. Rademaker, et. al. TNO-rapport 11599, 2019.
6. “Host Your Own Key (HYOK) with Azure”, Utimaco, https://support.hsm.utimaco.com/documents/20182/336250/IG_HYOK_Azure.pdf
7. “Informatieveiligheid en Privacy in de zorg”, B.J. Bruins, minister voor Medische Zorg, Tweede Kamer, vergaderjaar 2019–2020, 27 529, nr. 193, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z19060&did=2019D39705
8. “Advies opslag medische data in de cloud”, 27 september 2019, Adviesbureau ICTRecht, https://www.tweedekamer.nl/downloads/document?id=8109413d-a291-468e-aba6-ea08e2ec989f&title=Advies%20opslag%20medische%20data%20in%20de%20cloud.pdf
9. Onderzoek naar het versterken van de innovatieketen op het terrein van cybersecurity. G. Bodea, H. Boonman, P. van den Brink, et al. TNO-rapport 10769, 2020.

8 Ondertekening

Den Haag, januari 2021

TNO
Networked Organisations

Drs. K.Y. de Jong
Research manager

Dr. D. Tiggelman
Auteur