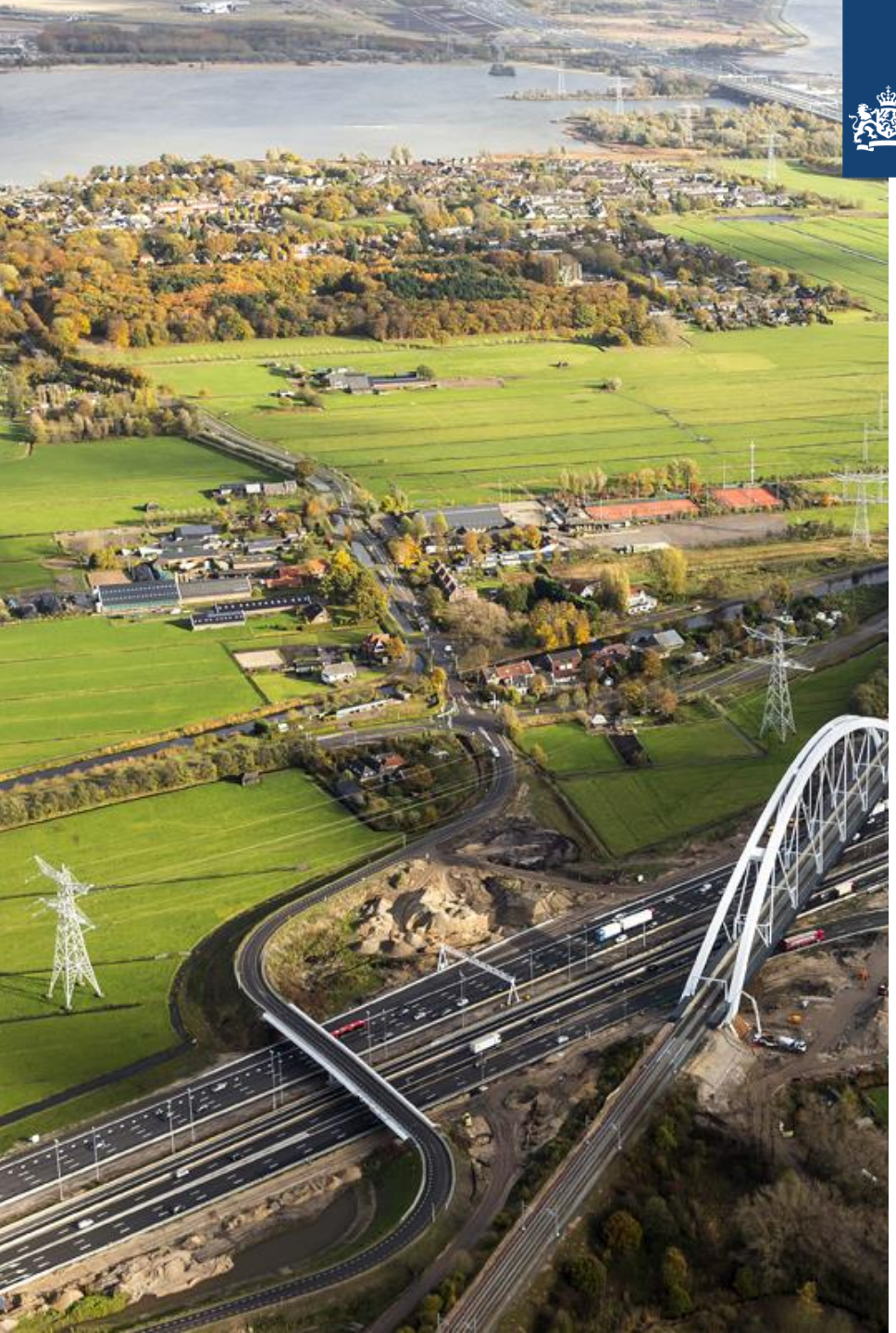
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

(Publieke) clouddienstverlening

Enkele ervaringen uit onze cloud journey

NCSC



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Doel en aanleiding

Het NCSC ondersteunt en adviseert organisaties in Nederland bij het vergroten van hun digitale weerbaarheid. Eén van de technische uitdagingen waar organisaties op dit moment mee te maken hebben vormt de adoptie van (publieke) clouddiensten. De inzet daarvan heeft namelijk aanzienlijk gevolgen voor hun security- en procesarchitectuur, het benodigde kennisniveau in de organisatie en het eigen technisch landschap.

Net als de meeste andere Rijksorganisaties staan we als NCSC nu nog aan het begin van onze *cloud journey*. De afgelopen twee jaar hebben we wel al ervaring op gedaan met de inzet van enkele private en public clouddiensten. Inzet van clouddiensten helpt ons beter (want, sneller) in te spelen op de veranderingen die zich in het dynamische cyberlandschap afspelen. Daarbij geldt dat de belangrijke technische innovaties van de komende jaren, zoals AI, *advanced analytics* en IoT alleen goed werken vanuit de publieke cloud. Een beheerste adoptie van cloud is daarom onontbeerlijk.

In dit document beschrijven we een aantal van onze ervaringen en de aanpassingen die we hebben gedaan of (gaan) doen aan ons technisch landschap, processen en vooral ook aan onze security architectuur. Onze belangrijkste leerervaring is namelijk dat cloud adoptie majeure gevolgen heeft voor de wijze waarop we onze informatievoorziening organiseren.

Het delen van ervaringen, zoals met deze publicatie, kan daarbij hopelijk voor andere organisaties van nut zijn. Daarin volgen we het voorbeeld van NCSC-UK en de Europese Commissie. Beide organisaties zijn al aanzienlijk verder in hun cloud adoptie en hanteren daarbij een '*cloud-first*'-benadering. Hun ervaringen daarmee zijn respectievelijk hier en hier te vinden.

Arnoud van Petersen
CIO NCSC

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Inhoud

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Wij zijn het Nationaal Cyber Security Centrum

Het NCSC bestaat sinds 2012 en vormt sinds januari 2019 een zelfstandige taakorganisatie binnen het ministerie van Justitie en Veiligheid. Wij zetten ons in voor de nationale veiligheid. Dit doen we door het beschermen van de Nederlandse digitale infrastructuur om maatschappelijke ontwrichting te voorkomen. Hiervoor leveren we inzichten, advies en ondersteuning op het gebied digitale kwetsbaarheden, -dreigingen en -weerbaarheid. Ook ondersteunen we vitale organisaties en rijksoverheidsorganisaties bij het oplossen van cyberincidenten.

Als verbindend expert werken we zo aan een digitaal veilig, open en weerbaar Nederland. Onze Nederlandse digitale infrastructuur is van levensbelang: voor het betalingsverkeer, voor schoon water uit de kraan en om de voeten droog te houden. We onderzoeken en analyseren kwetsbaarheden en dreigingen en identificeren en duiden risico's en trends. Als overheidsorganisatie zijn we de verbindende schakel in een netwerk van nationale en internationale partners op het gebied van cyber security.

Het NCSC is een relatief kleine en jonge organisatie. In tegenstelling tot veel andere kleine Rijksorganisaties hebben we een groot deel van onze IT voorzieningen in eigen beheer. Dit komt omdat de aard van het werk hele specifieke eisen stelt aan de beschikbaarheid, beveiliging, innovatief vermogen en wendbaarheid van onze informatievoorziening. Deze eisen en kenmerken werken door in onze adoptie van (public) clouddiensten.

NCSC in cijfers

budget

24 mln *Het totaal budget (materieel en personeel) voor 2020 bedraagt 24 mln.*

medewerkers

140 *De formatie van het NCSC bedraagt voor 2020 in totaal 140 FTE.*

hard- en software

6 mln *Voor 2020 is 7 mln. begroot voor de bekostiging van hardware, software en managed services.*

Samen maken we Nederland digitaal veilig

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

(public) cloud gebruik in een overheidscontext

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

de Rijksoverheid en de cloud

Als Rijksoverheidsorganisatie heeft het NCSC te maken met de Rijksbrede kaders en afspraken die gelden rondom de inzet van clouddienstverlening. Het gebruik van cloudvoorzieningen binnen de Rijksoverheid wordt in belangrijke mate bepaald door keuzes die gemaakt zijn rond 2011. Op dat moment was 'de cloud' een hot topic en waren de verwachtingen hoog gespannen ten aanzien van wat het zou betekenen voor de wendbaarheid en efficiency van IT. Het was ook de tijd dat cloudvoorzieningen als Azure (2010) en Office 365 (2011) voor het eerst op de markt kwamen.

In mei 2010 vraagt de Tweede Kamer het Kabinet in Motie Van der Burg om een 'cloud computing strategie' en 'cloud-first strategie' uit te werken. Een jaar later geeft de minister van BZK in een reactie aan dat public cloud voorzieningen feitelijk nog te onvolwassen en onveilig zijn om binnen het Rijk adequaat te kunnen gebruiken. Het Rijk zal deze daarom niet gaan gebruiken en in plaats daarvan inzetten op de ontwikkeling van private cloudvoorzieningen die (zullen) worden ontwikkeld binnen de vier dan net aangewezen OverheidsDataCenters (ODC's). Deze keuze drukt in de jaren daarna een belangrijke stempel op de ontwikkeling en adoptie van cloudvoorzieningen binnen het Rijk. Door het *de facto* verbod op het gebuik van public cloudvoorzieningen blijft dit achter bij de private sector en bij mede overheden zoals gemeenten en provincies. In de periode 2014-2017 wordt wel gewerkt aan de ontwikkeling van private cloudvoorzieningen. Het aanbod hiervan blijft relatief beperkt. Op dit moment biedt feitelijk alleen ODC Noord rijksbreed (private) clouddiensten aan.

Het gevolg is dat de Rijksoverheid op dit moment nog maar in beperkte mate gebruik maakt van public clouddiensten. Dit vormt in zekere zin een risico omdat veel nieuwe technologische ontwikkelingen de inzet van public cloud vereisen. Het gebruik van public cloudvoorzieningen vraagt tegelijkertijd ook een meerjarig ontwikkeltraject, omdat dit aanpassingen verlangt in zaken als techniek, processen, kennis, architectuur en beveiliging. Het inlopen van de ontstane achterstand vraagt de komende tijd om aandacht. Op dit moment vindt rijksbreed een verkenning plaats naar de vorming van nieuw cloudbeleid. Als NCSC dragen we bij aan dit traject.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

European Commission Cloud Strategy 2019

' Cloud-first with a secure hybrid multi-cloud service offering'

'Cloud computing (...) unlocks access to future and emerging technologies, such as artificial intelligence, high performance computing, the Internet of Things and blockchain.'

Ook op Europees niveau vormt de inzet van (public) clouddiensten een strategisch vraagstuk dat de lidstaten en de organisaties die daar deel vanuit maken, zoals wij als NCSC, raakt. De Europese Commissie (EC) beziet de inzet van cloud voorzieningen en de waarde die dit kan genereren vanuit een financieel-economisch, (geo)politiek en maatschappelijk perspectief. Zo is volgens de Commissie de inzet van cloud bijvoorbeeld randvoorwaardelijk om de Europese AI aspiraties en maatschappelijke opgaven zoals die ten aanzien van de Green Deal, te kunnen realiseren. Deze kijk op cloud wordt weerspiegeld in het feit dat de EC de afgelopen tien jaar de adoptie van cloudvoorzieningen actief heeft willen bevorderen via onder meer de European Cloud Strategy (2012) en het 'Cloud for Europe' programma.

Ook voor de eigen informatievoorziening heeft de EC de afgelopen jaren (public) clouddiensten ingezet. Op basis van de ervaringen daarmee heeft het in 2019 ook een nieuwe cloudstrategie geformuleerd met als adagium ' *Cloud-first with a secure hybrid multi-cloud service offering*' . *Cloud-first* betekent hier dat er bij de ontwikkeling van nieuwe (informatie)voorzieningen van wordt uitgegaan dat deze zo effectief mogelijk binnen cloud omgevingen moeten kunnen draaien en daarom *cloud native* worden ontwikkeld. De strategie stelt ook dat er sprake zal zijn van een gecombineerde inzet van on-prem en (public) cloudvoorzieningen die door verschillende partijen zullen worden geleverd.

Als onderdeel van de eerste Europese Cloud Strategie heeft de EC vanaf 2012 ingezet op de ontwikkeling van standaarden en certificeringsschema's voor public clouddiensten. Doel hiervan was om daarmee de adoptie van clouddiensten Europa breed, te vergemakkelijken. Met de introductie van de Cybersecurity Act (CSA) medio 2019 heeft die certificering van cloud diensten een hernieuwde impuls gekregen.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cloudgebruik bij het NCSC

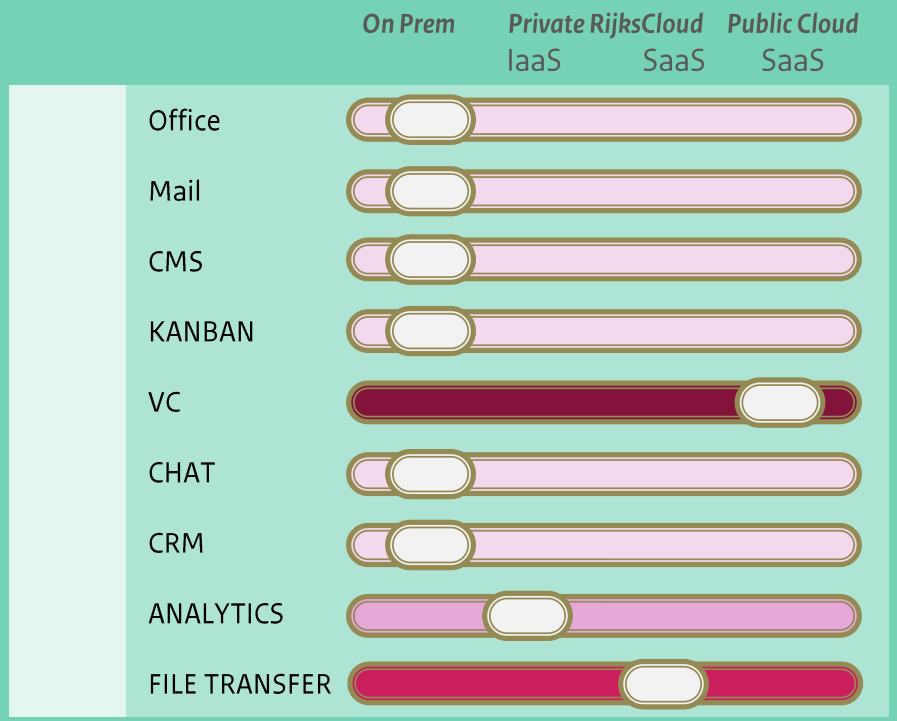
Het gebruik van cloudvoorzieningen bij het NCSC

Het Rijksbeleid ten aanzien van (public) cloudvoorzieningen is terug te zien in het gebruik van clouddienstverlening bij het NCSC. Het overgrote deel van onze IV voorzieningen beheren we zelf op een eigen on-prem infrastructuur. Redenen hiervoor liggen behalve op het vlak van restrictief cloudbeleid op Rijksniveau ook op terreinen als beveiliging, BCM en een relatief beperkte organisatorische *cloud readiness*.

De afgelopen twee jaar zijn we stapsgewijs enkele, voor ons nieuwe, IaaS en SaaS voorzieningen gaan gebruiken. Zo maken we buiten de cloud diensten die zijn opgenomen in de figuur hiernaast, op dit moment gebruik van private cloud IaaS-diensten in ODC Noord. Daarnaast zijn we gestart met enkele experimenten met public clouddiensten. Hierbij gaat het voornamelijk om intelligence en analytics voorzieningen die uitsluitend geleverd worden als SaaS dienst. Ook zijn we gestart met een PaaS experiment bij AWS. Daarmee willen we verkennen of de inzet van een dergelijke voorziening ons kan helpen bij het vergroten van de (door-) ontwikkelsnelheid van onze bedrijfsapplicaties.

Deze situatie weerspiegelt onze cloud-adoptieaanpak, waar we later in dit document dieper op ingaan. Ons gebruik van cloud is, zeker voor wat betreft public clouddiensten, nog beperkt, maar groeiende. We kiezen voor een stapsgewijze introductie en doen dit lerenderwijs aan de hand van experimenten en PoC's. Hierbij volgen we de departementale lijn rondom cloud gebruik zoals vastgelegd in het 'Cloud Afwegingskader JenV'. Met name bij de introductie van public clouddiensten kiezen we ervoor om te beginnen met niet-bedrijfskritische systemen die geen (diepe) integratie met de eigen on-prem voorzieningen vereisen. De keuze voor een cloudvoorziening is daarmee ook altijd gebaseerd op een uitgebreide risicoafweging. In dit kader is het ook relevant dat de *cloud readiness* van de organisatie nu nog beperkt is. Het introduceren van een nieuwe technologie waar de organisatie geen ervaring mee heeft en die, zoals bij clouddiensten het geval is, een majeure impact heeft, brengt risico's met zich mee. Door de inzet van experimenten en relatief eenvoudig in te zetten voorzieningen, bouwen we aan onze ervaring en onze *cloud readiness*.

In onderstaande figuur staan enkele van onze IV voorzieningen weergegeven en de wijze waarop die binnen het NCSC op dit moment worden geleverd; on prem of vanuit een cloud situatie. We hebben hierbij de voorzieningen opgenomen waarvoor in de markt zowel on-prem als cloudoplossingen voorhanden zijn. Ons uitgangspunt op dit moment is dat voorzieningen waarin gevoelige gegevens verwerkt worden in beginsel on-prem draaien. Dit is bijvoorbeeld de reden waarom wij onze Confluence omgeving on-prem hebben staan in plaats van deze af te nemen als SaaS voorziening vanuit ODC Noord.



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Waarom zetten we in op (public) cloud dienstverlening ?

Er is een drietal hoofdredenen waarom we de afgelopen twee jaar (public) cloud-diensten zijn gaan gebruiken. Eén daarvan is een veelgehoorde reden, namelijk het vergroten van de wendbaarheid van onze eigen informatievoorziening. De veranderlijke omgeving waarin we als organisatie opereren vraagt dat van ons. Daarnaast zien we dat bepaalde technische voorzieningen en diensten vooral beschikbaar komen in de publieke cloud. Daarom willen we er ervaring mee op doen om technisch niet achterop te raken. De organisaties die wij tot onze doelgroep rekenen zullen naar wij verwachten om diezelfde redenen ook clouddiensten gaan gebruiken. Onze eigen ervaringen met clouddienstverlening kan onze advisering daarover ondersteunen.

Verschillende kenmerken van clouddienstverlening zoals on-demand beschikbaarheid, schaalbaarheid en standaardisatie helpen de IV dienstverlening van het NCSC sneller en daarmee wendbaarder te maken. Het managed service karakter van de dienstverlening zorgt dat schaarse IT-capaciteit op andere zaken ingezet kan worden, bijvoorbeeld op de doorontwikkeling van eigen specifieke IV-voorzieningen. Door daarbij gebruik te maken van een PaaS-platform kan dit bovendien sneller en toekomstbestendiger gebeuren.

We willen de snelheid en wendbaarheid van onze IV vergroten.

We willen 4th industrial revolution technologies adequaat kunnen (helpen) benutten

We stimuleren *public cloud readiness* en de adoptie van *public clouddiensten* vanuit de wetenschap dat alle belangrijke technische innovatie de komende jaren alleen geleverd kunnen worden met inzet van de public cloud. Dit geldt bijvoorbeeld voor IoT, AI en geavanceerde *data analytics*. Dit zijn tevens technologische voorzieningen die van groot belang zijn voor onze economische slagkracht en toekomstig verdienvermogen. Op het moment dat we als Nederland of Nederlandse (Rijks)overheid niet in staat zijn om deze public cloud gebaseerde technische innovaties adequaat te omarmen, schaadt dit onze positie op economisch en geopolitiek vlak. Wij zien het daarmee als een opgave om te helpen bij het veilig gebruik van public clouddiensten en de adoptie daarvan te bespoedigen. Daar komt bij dat deze public cloud based '*4th industrial revolution technologies*' behalve economisch en geopolitiek ook in brede zin belangrijke maatschappelijke waarde hebben doordat ze een voorname bijdrage kunnen leveren aan het realiseren van de *Sustainable Development Goals*.

We willen cloud ready zijn als (IV) organisatie en als cybersecurity adviseur.

We willen in de toekomst op een goede manier public clouddienstverlening kunnen toevoegen en integreren met ons zelf beheerde IV portfolio. We zullen dit ook wel moeten, omdat in toenemende mate IT-diensten alleen nog maar vanuit de public cloud geleverd (gaan) worden. Door nu beheerst stappen te zetten vergroten we onze *cloud readiness*. Dit is nodig want public cloud gebruik vereist aanzienlijke aanpassingen in techniek, proces, kennis, architectuur, security en (*continuous change*) mindset. Doordat we dit traject zelf doormaken kunnen we hier ook gerichter en beter extern over adviseren.

In dat kader verwachten we dat het NCSC de komende jaren zelf ook *public cloud based AI* en *analytics* voorzieningen zal gaan gebruiken om de eigen taak adequaat te kunnen blijven uitvoeren.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Risico's en risico management bij cloud gebruik

Iedere introductie van nieuwe technieken en -diensten brengt risico's met zich mee. Dat geldt ook voor (public) clouddienstverlening. Vaak wordt er in dit kader gesproken over risico's op het vlak van beveiliging, privacy en compliance. Dit zijn echter zeker niet de enige. Er zijn ook financiële, juridische, technische en sourcingsgerelateerde risico's. Het risico van clouddienstverlening wordt daarnaast in belangrijke mate bepaald door de wijze waarop deze wordt ingezet. Is dat alleen voor een experimentele omgeving en de verwerking van (semi-) open data of moet de clouddienst een centrale rol vervullen in een kritiek bedrijfsproces (bijv. ERP) ? Bij de keuze om een (cloud) dienst in te zetten wegen we de daarom de verschillende risico's, voor- en nadelen af. Hierbij is het van belang om ook mee te wegen dat het *niet* overstappen op een cloudvoorziening eveneens risico's met zich mee kan brengen. Zo leveren de grote cloud aanbieders een beveiligings- en beschikbaarheidsniveau dat maar weinig organisaties in staat zijn om te evenaren met eigen on-prem voorzieningen. En op het moment dat een organisatie ervoor kiest om geen clouddiensten in te zetten zorgt dit er ook voor dat er (nog) geen kennis en ervaring wordt opgedaan die nodig is om de organisatie toekomstbestendig te maken. Onze ervaring is dat het daarom van belang is om een integrale, holistische risicoafweging uit te voeren waarin de voor- en nadelen van alle relevante opties worden meegewogen. In de praktijk blijkt dan dat er sprake is van een rijkgeschakeerd pakket aan public en private cloudvoorzieningen, die ieder, afhankelijk van de leveringsvorm en beoogde inzet, een eigen risico afweging kennen.

Meer weten over risico management bij de inzet van cloud diensten ?

- NCSC Whitepaper Cloudcomputing
- NIST Cloud Risk Management Framework
- Enisa Cloud Computing Risk Assessment

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cloud gebruik bij het NCSC - onze cloud journey

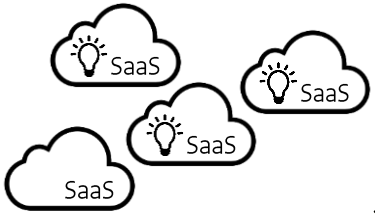
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cloud adoptie is vooral ook een integratievraagstuk

Het NCSC heeft sinds eind 2018 stapsgewijs clouddiensten toegevoegd aan het eigen technisch landschap, dat tot dan toe uitsluitend een on-prem voorziening was. Het toevoegen van de clouddiensten is ingegeven vanuit de hiervoor genoemde overwegingen. In eerste instantie waren dit private cloud IaaS voorzieningen, geleverd vanuit een ODC. Hiermee konden we sneller, vrijwel on-demand, infradiensten beschikbaar krijgen, waar dit intern binnen de eigen on-prem infraomgeving vaak (te) lang duurde. We zijn vervolgens ook SaaS voorzieningen van dezelfde Rijksleverancier gaan gebruiken en gestart met verschillende *public cloud* SaaS diensten. Deze *public cloud* SaaS diensten zijn vrijwel allemaal data analyse voorzieningen die nu als PoC worden uitgeprobeerd. Dat geldt ook voor de recent opgestarte PoC met een *public cloud* PaaS voorziening. Alle *public cloud* voorzieningen die we nu als PoC uitproberen worden niet geleverd vanuit een ODC of zijn sowieso niet beschikbaar in on-prem vorm. Het gebruik van deze clouddiensten maakte al snel zichtbaar dat een structurele inzet van clouddiensten ook structurele en soms fundamentele aanpassingen in techniek, proces, kennisniveau en architectuur met zich meebrengt en dat cloudintegratie en –adoptie aanzienlijke implicaties voor de organisatie heeft. De vraag die hierbij steeds aan de orde komt is: 'wat kan of mag wel en niet' en wat betekent de inzet van deze clouddienst voor de integratie met de rest van ons landschap, bijvoorbeeld in termen van *identity & access management* (IAM), *single sign-on* en de integratie van datastromen tussen on-prem en cloud omgeving? Ten aanzien van IAM geldt bijvoorbeeld dat ons bestaande IAM systeem alleen toegang verschaft tot onze on-prem voorzieningen. Het gevolg is dat voor alle clouddiensten steeds apart moet worden ingelogd. Dit belemmert gebruikersgemak, maar werkt ook negatief uit op beveiliging. Verderop gaan we erop in wat het integratievraagstuk in brede zin voor ons, en onze security architectuur, betekent.

Public SaaS diensten

De afgelopen periode zijn we gestart met een aantal public cloud SaaS diensten. Vrijwel allemaal in PoC vorm:

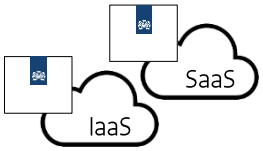


Public PaaS diensten

Recent zijn we gestart met een PaaS PoC waarmee we willen proeven wat de voordelen en gevolgen zijn als we onze ontwikkel- en test omgevingen in de public cloud onderbrengen.

Private IaaS en Saas diensten

We maken gebruik van enkele private cloud IaaS en SaaS diensten van ODC Noord.



Als basis infrastructuur gebruiken we onze on-prem netwerk omgeving. Deze bouwen we nu om tot een software defined netwerk (SDN) wat enerzijds de snelheid geeft van een IaaS en anderzijds de integratie met cloud omgevingen helpt te vergemakkelijken.

Traditional Infra on-prem

Software defined – hyper converged Infra on-prem

In onze *cloud journey* kregen we al snel te maken met integratie uitdagingen; van het realiseren van een gezamenlijke IAM tot het integreren van data stromen. Centrale vraag hierbij is steeds: Hoe blijven we onze data adequaat beveiligen, ook on-prem, en kunnen we tegelijk naadloos voorzieningen, ook die in de cloud, met elkaar integreren?

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

De eerste stappen in onze *cloud journey*: leren en verkennen, op weg naar *cloud readiness*

In onze *cloud journey* hanteren we een aantal uitgangspunten:

- De eerste stappen die we nu zetten, hebben primair tot doel om te verkennen en te leren. Zodat we op basis van die leerervaringen kunnen komen tot enerzijds een *cloud ready* organisatie en anderzijds een integratiesystematiek die veilig en schaalbaar is en waarmee we eenvoudig cloudvoorzieningen kunnen op- en afschalen. Op basis van de ervaringen die we nu opdoen kunnen we ook beter en gerichter bepalen wat voor ons wel en niet werkt of nuttig is. Zo kunnen we beter gefundeerd komen tot een cloud visie, -strategie en intern beleidskader.
- Van een significante verplaatsing van werklasten richting de cloud is de komende tijd nog geen sprake. We hebben op dit moment ook niet de intentie of ambitie om ons volledige technische landschap naar de (public) cloud te bewegen. Cloudmigratie is niet ons doel. We voegen clouddiensten toe aan ons landschap waar dit functioneel en nuttig is, veelal vanwege de hogere snelheid die we daar kunnen bereiken of omdat de functionaliteiten alleen in de public cloud beschikbaar zijn.
- Op dit moment verwerken we nog geen eigen bedrijfsgegevens in *public cloud* omgevingen. Pas wanneer we dit op een veilige en compliante wijze kunnen organiseren, gaan we dit doen.
- Het belangrijkste motief om IaaS diensten te gebruiken is dat onze bestaande on-prem-infraomgeving niet (tijdig dwz) on-demand kon leveren. Met de vernieuwing van onze on-prem-omgeving verwachten we na oplevering dezelfde leversnelheid te kunnen behalen als we nu krijgen bij de IaaS-dienst. We verwachten daarmee dat er minder reden zal zijn om dan nog IaaS-diensten extern af te nemen. Enkele voorzieningen die nu extern op een IaaS omgeving draaien halen we dan ook weer terug on-prem omdat we dan ook gevoeligere gegevens in die voorziening kunnen gaan verwerken. Het is daarmee ook niet dat we verwachten dat voorzieningen die, wanneer zij éénmaal in de cloud zijn, niet meer on-prem terug komen.
- In diezelfde lijn koersen we er vooralsnog evenmin op om bestaande on-prem-voorzieningen te gaan vervangen door cloud varianten. Zo blijven we de komende jaren de on-prem-variant van Office gebruiken en stappen we niet over op O365 in de *public cloud*.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Onze cloud journey

Het adopteren en kunnen inzetten van public clouddiensten vormt voor ons, net als voor veel andere organisaties, een meerjarig ontwikkeltraject. We zien dit als een reis, onze '*cloud journey*', waarbij we de richting, ambitie en een aanzienlijk deel van de uitdagingen en oplossingen al wel voor ogen hebben maar waarvan we ook weten dat er zich gaandeweg nieuwe uitdagingen en vraagstukken zullen voordoen. Het is een reis die een aanzienlijk deel van de organisatie raakt, omdat cloudadoptie veel meer is dan alleen een technisch vraagstuk. Het adopteren en kunnen gebruiken van cloud diensten is tegelijkertijd geen doel op zich. Het maakt onderdeel uit van, en is ondersteunend aan, een bredere veranderopgave waarbij we ons als organisatie doorontwikkelen op vlakken als datagedreven werken, digitalisering van werkprocessen en de digitale, informatiegestuurde interactie met doelgroeprganisaties en ketenpartners. Een ontwikkeling die tot doel heeft actueler, completer en sneller ontwikkelingen in het cyberlandschap inzichtelijk te hebben en op basis daarvan gerichter en sneller partijen tot handelen aan te kunnen zetten en zo Nederland Digitaal Veilig te maken. Hieronder zijn op drie assen enkele belangrijke mijlpalen weergegeven die een rol spelen in onze *cloud journey*. In veel gevallen gaat het zoals gezegd om stappen die we zetten als onderdeel van onze brede veranderopgave en niet slechts alleen in het kader van de cloud adoptie. De mijlpalen hieronder bevinden zich op de assen 'organisatie', 'proces' en 'kennis'. Op de volgende pagina staan de mijlpalen weergegeven op technisch gebied. Een deel van de genoemde mijlpalen is reeds gerealiseerd, aan een ander deel, die in de toekomst liggen, werken we nog.

Onze cloud journey – technische mijlpalen

Ook op het gebied van techniek zijn er verschillende mijlpalen te onderscheiden in onze cloud journey. In eerste instantie hebben we ons daarbij gericht op het introduceren van nieuwe cloud diensten om daar eerste ervaringen mee op te doen. Zoals aangegeven werd duidelijk dat met name op twee vlakken aanvullende aanpassingen nodig zijn, buiten het traject dat we al waren gestart met het ombouwen van onze on-prem infraomgeving naar een modern software defined network (SDN). Die twee aspecten betreffen enerzijds de technische opgave rondom de integratie van de verschillende cloud omgevingen en daaraan gekoppeld de (technische) veranderingen die we doorvoeren in onze security architectuur. We merken ondertussen dat de stappen die we hebben gezet naar een *software defined networking* omgeving van groot belang zijn voor het kunnen realiseren van alle benodigde technische aanpassingen.

Techniek ontwikkeling

- bouw/ontwikkeling on-prem SDN/HCI
- eerste private cloud SaaS-voorziening
- eerste private cloud IaaS-voorziening
- eerste public cloud SaaS-voorziening
- inzet PaaS experimenteer-omgeving
- introductie IAM-voorziening tbv cloud integratie
- zonering en koppeling zones via koppelnetwerk
- maximale automation van on-prem infra werkzaamheden en -processen
- micro-segmentering
- introductie CASB

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cloud adoptie en de gevolgen voor onze security-architectuur

kaders voor cloudsecurity

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Voor de beveiliging van cloud omgevingen en het mitigeren van beveiligingsrisico's zijn diverse *best practices* en sets met control richtlijnen beschikbaar. Bekende voorbeelden hiervan zijn:

- ISO 27017 ; een onderdeel van de ISO 27000 familie en specifiek bedoeld voor het informatiebeveiliging (27017) en privacy (27018) in cloud omgevingen. Specifiek voor de Nederlandse overheid heeft het Centrum voor Informatiebeveiliging en Privacy (CIP) het ISO 27017 kader vertaald naar het inzetgebied van de BIO 2019.
- Cloud Controls Matrix van de Cloud Security Alliance (CSA);
- Cloud Computing Compliance Criteria Catalogue (C5) van de Duitse BSI. Dit normenkader is mede gebaseerd op de ISO en CSA control sets;

Inhoudelijk liggen deze kaders vrij dicht bij elkaar.

De kenmerken van clouddienstverlening maken het toepassen en borgen van beveiligingsmaatregelen niet altijd eenvoudig. Dit heeft onder andere te maken met het feit dat het gaat om *managed services* waarbij een ander (de Cloud Service Provider - CSP) grotendeels verantwoordelijk is voor de inzet van benodigde maatregelen maar de gebruiker verantwoordelijk blijft voor de juiste beveiliging van zijn data en voorzieningen. Niet zelden blijkt het vervolgens lastig om het bestaan en de werking ervan te (laten) controleren (*right to audit*). Verder speelt dat clouddiensten sterk gestandaardiseerd zijn, wat voordelen biedt, maar ook niet toestaat dat de leverancier op verzoek van individuele klanten additionele beveiligingsmaatregelen implementeert.

Bij de levering van clouddiensten is vaak een complex systeem van toeleveranciers en onderaannemers betrokken, in het bijzonder wanneer cloud diensten hoger in de stack worden afgenomen. Dit maakt het lastig om inzicht te krijgen in de juiste implementatie van maatregelen. Het ecosysteem en de daarbinnen geleverde dienstverlening is bovendien continu in beweging. *Continuous change* is immers één van de kenmerken van cloud dienstverlening en de bouwstenen waaruit het is opgebouwd. Dit maakt de gehele *supply chain* van clouddienstverlening diffuus, complex en sterk veranderlijk.

Vertrouwen (trust) en cloud beveiliging

Op beveiligingsvlak is de overstap naar cloudvoorzieningen belangrijk omdat daarmee de traditionele begrenzing van het netwerk verder vervaagt. Voorheen konden organisaties in beginsel alles vertrouwen wat zich binnen de zelf beheerde netwerkomgeving bevond. Die eigen, zelf beheerde netwerkomgeving, is steeds meer aan het verdwijnen en dat vraagt om een fundamenteel andere kijk op informatiebeveiliging. Het netwerk waar systemen draaien en waar data wordt verwerkt is een lappendeken geworden. De onderdelen worden steeds vaker beheerd door serviceproviders en hun toeleveranciers en door ketenpartners en hun leveranciers. Een totaaloverzicht is er niet, wat onder andere ook komt door de continue technische doorontwikkeling *binnen* het netwerk en continue verandering *ván* het netwerk. Dit betekent ook dat een organisatie die binnen dat netwerk gegevens verwerkt geen zekerheid of vertrouwen meer kan hebben dat alles op het juiste niveau beveiligd is. We zien dat er zich op dit moment twee ontwikkelingen voordoen die hier een oplossing voor proberen te vinden. Beiden kijken op een heel verschillende manier kijken naar vertrouwen (*trust*) en de wijze waarop dat al dan niet in een cloud context kan worden zeker gesteld.

Cloud Certificering

'Building trust through certification & assurance'

De beveiligingscertificering van clouddiensten helpt inzichtelijk te maken aan gebruikers en afnemers aan welk niveau van beveiliging deze dienstverlening voldoet door middel van een onafhankelijke toetsing. Het doel hiervan is om vertrouwen te creëren in de adequate beveiliging van cloud dienstverlening. Internationaal zijn er verschillende cloud certificeringsschema's. Eén van de meest bekende is de CSA-STAR. Binnen Nederland kennen we daarnaast bijvoorbeeld de Zeker-Online cloud certificering.

De inzet van cloud certificering wordt met name vanuit de EU gestimuleerd, onder ander via de nieuwe Europese CyberSecurity Act. De komende jaren word gewerkt aan een Europa breed stelsel van cloud certificeringen met drie niveaus (licht, midden en zwaar). De uitdaging hierbij is om met name voor het zware niveau een certificeringsmechaniek te ontwikkelen dat rekening houdt met de dreigingen en risico's waar gebruikersorganisaties mee te maken hebben en tegelijk kan omgaan met het uiterst dynamische en diffuse karakter van het cloud ecosysteem.

Terwijl Zero Trust vooral een veranderopgave betekent voor cloud gebruiker zoals wij als NCSC, is het realiseren van cloud certificering vooral een opgave voor Cloud Service Providers (CSP's).

Zero Trust

' Trust Nothing, Verify Everything'

Zero Trust is een beveiligingsprincipe dat ervan uit gaat dat het digitale ecosystem, waar organisatie IT-diensten uit afnemen en waar clouddienstverlening deel vanuit maakt, dusdanig complex, diffuus en veranderlijk is dat het onmogelijk is om nog zekerheid te krijgen over het beveiligingsniveau van de gehele dienstverleningsketen. In de wetenschap dat je niet kunt vertrouwen op de wijze waarop alle individuele partijen, die een rol hebben in de uiteindelijke beveiliging van je IT omgeving, omgaan met hun beveiliging, moet je je daar als organisatie jezelf op aanpassen. Zero Trust gaat er vanuit dat je als organisatie het vertrouwen in de beveiliging van een ander ook niet meer zou moeten willen hebben of krijgen en dat je er naar zou moeten streven om zo min mogelijk afhankelijk te zijn van vertrouwensrelaties : '*minimize the need for trust*'. ZT is daarmee vooral een opgave of richtsnoer voor de organisaties die cloud diensten afnemen.

Zero Trust stelt je eigen data centraal. Om die data heen wordt, liefst zo fijnmazig mogelijk, beveiliging georganiseerd. Gebruikers of applicaties kunnen alleen toegang krijgen tot die data als zij daar expliciet toe gerechtigd zijn. Belangrijke elementen in een Zero Trust beveiligingsaanpak zijn IAM, RBAC, encryptie, zonering en microsegmentatie.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cloud-certificering & -assurance

De verschillende certificering en assurance schema's voor cloud diensten helpen meer grip op en inzicht te krijgen in de beveiliging van die diensten. Bekende schema's zijn die van CSA, C5, SecNum, ENS en FedRamp.

Met de introductie van de Europese Cyber Security Act (CSA) in juni 2019 heeft cloud certificering een aanzienlijke impuls gekregen. In de CSA is opgenomen dat er een Europees cloud certificeringsschema komt en zijn kaders afgesproken waaraan deze dient te voldoen. Zo krijgt het schema drie assurance niveau's; 'laag', 'midden' en 'hoog'. Gebruikers zullen op basis van een risicoafweging moeten bepalen welk niveau voor hen passend is. De verwachting is dat voor overheidsorganisaties en organisaties in het vitale domein met name 'hoog' en 'midden'-diensten relevant zijn.

Op dit moment vindt een nadere uitwerking plaats van het certificeringsschema. Eén van de uitdagingen daarbij vormt de inzet van *continuous auditing*. Waarschijnlijk zal beveiligingsniveau 'hoog' dit gaan vereisen. *Continuous auditing* is echter relatief nieuw en vereist het continu monitoren van de clouddienst en de veranderingen die daarin plaats vinden.

Onduidelijk is op dit moment nog hoe dwingend of vrijblijvend het EU certificeringsschema in de praktijk zal zijn. Behalve dat het klanten meer zekerheid verschaft over de beveiliging van cloud dienstverlening kunnen ook andere partijen zoals de wetgever, toezichthouders of verzekeraars, cloud certificering als vereiste of richtlijn hanteren, bijvoorbeeld wanneer die wordt ingezet door overheden of in vitale processen. Dit is vergelijkbaar met de situatie in de VS waar public clouddiensten die ingezet worden door de federale overheid een FedRAMP autorisatie vereisen.

Certificeringen of andere vormen van assurance helpen bij het inzetten van veilige clouddiensten. De verantwoordelijkheid hiervoor ligt primair bij de CSP. Het op een veilige manier inzetten van clouddiensten is echter een gezamenlijke opgave van CSP en eindgebruiker, waarbij deze laatste veelal aanpassingen zal moeten doen aan processen, werkwijzen, techniek en zijn security architectuur. Ten aanzien van dit laatste punt introduceren verschillende organisaties, en wij als NCSC ook, principes uit de Zero Trust Architecture (ZTA) in hun security-architectuur.

*"**Zero trust** (ZT) provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. **Zero trust architecture** (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies."* NIST Special Publication 800-207 (februari 2020)

ZTA zorgt voor een paradigma wijziging in de security architectuur van een organisatie. De nadruk ligt niet meer op de (perimeter) beveiliging van de eigen netwerkomgeving maar op de beveiliging van data en voorzieningen (assets), waarbij het niet meer van belang is waar die data en voorzieningen staan (binnen of buiten het eigen netwerk). Het uitgangspunt daarbij is dat alleen die gebruikers toegang krijgen tot data en voorzieningen die daartoe expliciet geautoriseerd zijn. Deze paradigma wijziging van een netwerk gestuurde security architectuur naar een data (assets) gestuurde security architectuur zorgt voor verschillende veranderingen in proces, organisatie, werkwijze en techniek, zo merken we ook zelf.

ZTA kent een aantal belangrijke bouwstenen, drie daarvan zijn:
- Identity & Access management (IAM)
- Micro segmentering
- Access control

Verderop beschrijven we hoe we in de transitie naar ZTA deze drie bouwstenen binnen het NCSC vormgeven.

ZTA uitgangspunten en de NCSC security architectuur

Als NCSC hebben we verschillende redenen waarom we ZTA principes inzetten:

- We willen ons op de juiste manier beschermen tegen geavanceerde cyberdreigingen. Hiervoor willen we onder andere de mogelijkheden voor *lateral movement* minimaliseren. ZTA helpt daarbij. We zetten ZTA bouwstenen zo dus ook in om BIO-BBN3 compliant te kunnen zijn.
- Onze bestaande beveiligingsarchitectuur gaat (ging) uit van perimeter beveiliging. Dit heeft geleid tot een sterke en uiterst robuuste netwerk infrastructuur. Deze werkwijze is echter niet toekomstbestendig, zoals ook uit dit document blijkt. Met name de introductie van cloud diensten maakt dat we onze security architectuur anders moeten organiseren. ZTA biedt hier een oplossing voor. De inzet van ZTA zien we als randvoorwaardelijk voor veilige cloud adoptie.
- Het NCSC heeft om verschillenden redenen meerdere apart van elkaar staande netwerkinfrastructuren, die onderling bijvoorbeeld verschillen in beveiligingsniveau. Dit naast elkaar bestaan heeft geleid tot silovorming. Om dit op te lossen worden de separate netwerken samen gebracht als zones van één nieuw netwerk, waartussen onderling eenvoudiger informatieuitwisseling mogelijk is. Ook hier helpt ZTA bij.

Er wordt op dit moment veel geschreven over de inzet van ZTA. In de kern is het echter geen nieuw concept. ZTA gaat over een aantal architectuur principes en technische bouwstenen. De exacte inzet daarvan hangt in belangrijke mate af van de technische omgeving, business uitdagingen en feitelijk dus van de organisatiespecifieke omstandigheden. Voor ZTA bestaat geen standaard blauwdruk. Dit maakt dat organisaties vooral zelf moeten onderzoeken hoe ZTA binnen de eigen omgeving kan worden toegepast. De implementatie van ZTA is veelal echter niet eenvoudig omdat het vraagt om een kanteling in werken en denken. Het vereist aanpassingen in processen, werkwijzen, kennisniveaus en technische voorzieningen. Die zijn niet in één keer te realiseren. ZTA implementatie is daarom vaak, net als cloud adoptie, een traject van meerdere jaren. Bij de implementatie van ZTA kiezen we eenzelfde pad als bij cloud in brede zin: begin klein, experimenteer, leer en schaal beheerst.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

ZTA: IAM & device management

Robuust *Identity & Access Management* (IAM) is een belangrijke bouwsteen van een ZTA. Bij het NCSC combineren we dit met stringent *device management*. Daarmee kunnen we zeker stellen dat we precies weten wie, wanneer en waartoe toegang wil krijgen en borgen we dat data en voorzieningen alleen toegankelijk zijn voor de gebruikers die dit mogen.

Het NCSC heeft al jaren een sterke manier van IAM, gebaseerd op *multi factor authentication* (MFA). Medewerkers krijgen alleen toegang tot hun NCSC-omgeving via hun door het NCSC zelf beheerde device. Hierop loggen ze in met meerdere wachtwoorden en token, waarbij er een cryptotunnel opgezet wordt naar het NCSC netwerk.

Deze vorm van IAM in combinatie met device management, is ontworpen en bedoeld voor een *perimeter-based* beveiligingsarchitectuur. We blijven deze manier in eerste instantie ook binnen onze ZTA implementatie gebruiken omdat we 1) hiermee zicht kunnen blijven houden op alle datastromen van en naar de device en gebruiker, 2) de producten technisch en economisch nog niet end-of-life zijn en 3) de organisatie gewend is aan het werken op deze manier en de daarbij gehanteerde vorm van MFA.

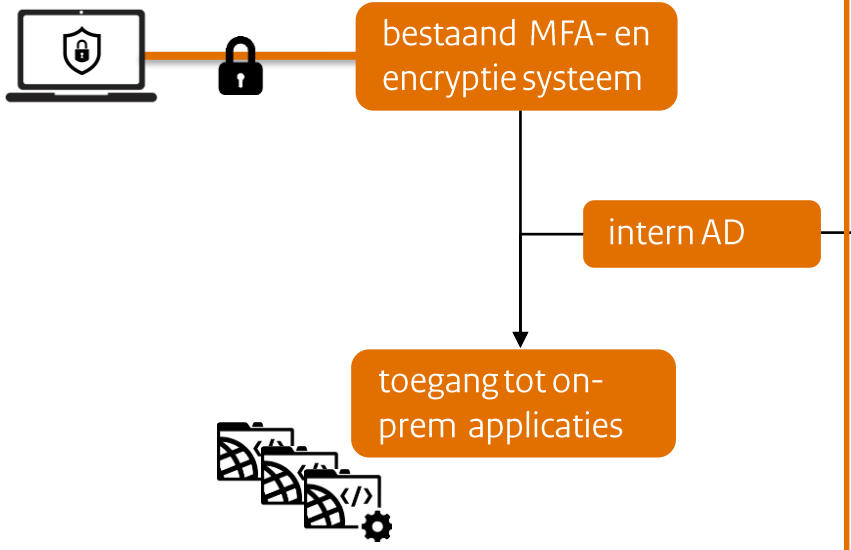
De uitdaging is nu om deze traditionele IAM manier zodanig bij te stellen dat deze ook ingezet kan worden voor cloud diensten. Zonder die koppeling moeten gebruikers voor iedere ‘externe’ (cloud) dienst apart inloggen, wat leidt tot een slechte gebruikerservaring en beveiligingsrisico’s. Een oplossing is om een aparte vorm van IAM met *single sign on* in te te zetten voor externe diensten. Dit is een suboptimale oplossing, zowel vanuit het perspectief van de gebruiker als vanuit het perspectief van ZTA. Een andere meer toekomstbestendige oplossing is de huidige IAM oplossing te combineren met bijvoorbeeld een *cloud access security broker* (CASB) waarmee eindgebruikers eenvoudig toegang kunnen krijgen tot on-prem en cloud voorzieningen via de bestaande IAM. We verkennen op dit moment welke risico’s en uitdagingen een dergelijke koppeling met zich mee brengt.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

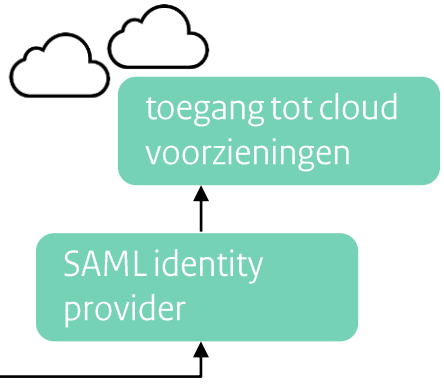
Transitie naar IAM in een hybride cloudsituatie

De structurele inzet van clouddiensten vereist dat deze gekoppeld worden aan het identity- & access management mechaniek dat ook gebruikt wordt om toegang te krijgen tot on-prem voorzieningen. Gebruikers merken dan geen verschil tussen voorzieningen die on-prem draaien of in een cloud omgeving. Dit is ook veiliger omdat gebruikers nu niet voor iedere cloud dienst een apart wachtwoord en gebruikersnaam hoeven te onthouden. Voor de integratie van ons IAM systeem verkennen we een getrapte aanpak waarbij we ons huidige bestaande on-prem systeem als uitgangspunt nemen. Een eerste stap in dit integratie proces draait om het realiseren van een '*single identity*'; een inlog identiteit voor iedere gebruiker die voor alle on-prem en cloud voorzieningen gelijk is. Een vervolgstap vormt de introductie van een cloud access security broker. Dit wordt in ons geval met name relevant wanneer we bedrijfsgegevens in *public cloud* SaaS-omgevingen (zouden) gaan verwerken. Een tweede traject (hieronder niet uitgewerkt) vormt de introductie van onze API Gateway waarmee on-prem en cloud voorzieningen ook worden geïntegreerd en waarmee ook *policy/rule based access*, monitoring en logging kan worden ingeregeld.

huidige IAM systeem als startpunt

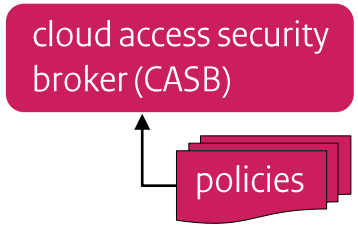


introductie 'single identity'



Een eerste integratie stap draait om identity federatie. Dit maakt het mogelijk voor gebruikers om voor de gehele gedistribueerde IT omgeving te werken met één identiteit waar-mee zowel ingelogd kan worden op on-prem voorzieningen als cloud diensten.

introductie *rule based access*



Een vervolgstap vormt de introductie van een CASB. Deze maakt het mogelijk om *rule/policy based access* richting cloud voorzieningen in te zetten. Ook kunnen we hiermee logging en monitoring vergemakkelijken.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Zonering als eerste stap naar microsegmentering

Zonering van de netwerkinfrastructuur vormt voor ons een belangrijke eerste stap op weg naar een veilige cloud adoptie. In de verschillende zones, zoals die hieronder staan weergegeven, worden processen en dataverwerkingen gegroepeerd op basis van het voor hen benodigde beveiligingsniveaus. Dit zorgt ervoor dat de beveiliging van verwerkingen en voorzieningen niet over- of onder gedimensioneerd is en vergemakkelijkt ook cloud adoptie voor die verwerkingen of (deel)processen waar dit mogelijk is. De verschillende zones worden via een koppelnetwerk aan elkaar verbonden die werkt op basis van een aantal uitwissel-regels. Hiermee worden de eerste infrastructurele basis stappen gezet naar segmentering. Door zonering krijgen we ook beter inzicht in data flows, wat helpt bij de verdere (micro)segmentering.

Witte zone

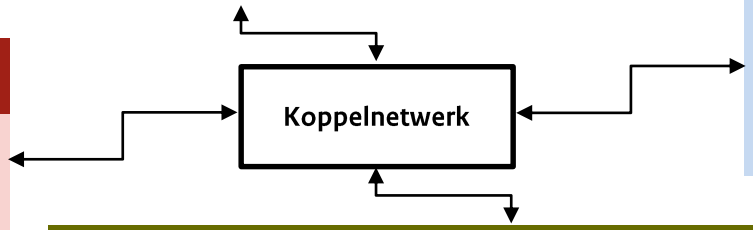
Bedoeld voor o.a.:
- Uitvoeren van PoC's, innovatietrajecten en experimenten met testgegevens of (semi-)open data;
- OT(A) ontwikkelstraten voor applicaties/voorzieningen die ingezet worden in andere zones en die specifiek baat hebben bij de CI/CD ontwikkelvoorzieningen in PaaS omgevingen;
- Overige verwerkingen van (semi-)open data, of informatie van derden/commerciele partijen;

Deze processen/voorzieningen kunnen worden ondergebracht binnen een public cloud omgeving.

Blauwe zone

Bedoeld voor de verwerking en opslag van:
- niet bedrijfskritische processen en informatie op BBN2 niveau,

Deze informatie/processen kunnen worden ondergebracht binnen een (private) cloud omgeving mits deze voldoet aan BIO BBN2.



Rode zone

Bedoeld voor de verwerking en opslag van:
- gegevens/processen die risico's met zich mee brengen voor andere verwerkingen (bijv malware analyse) en die daarmee dus gescheiden moeten zijn van andere processen/verwerkingen ('toxicity')
- gegevensverwerking/processen die vanwege hun aard of randvoorwaarden niet in de overige zones kunnen plaats vinden

Verwerking in cloud omgevingen kan, mits de rubricering/classificering dit toelaat.

Groene zone

Bedoeld voor de verwerking en opslag van:
- Bedrijfskritische gegevens/processen;
- Informatie die beveiligd moet worden tegen statelijke actoren en/of georganiseerde hackersverbanden, en daarmee bedoeld voor BIO-BBN3 informatie;
- Informatie in deze zone kan op dit moment niet op een beheerste manier verwerkt worden in een private- of public cloud omgeving. Deze informatie wordt on-prem verwerkt en opgeslagen.

Van zonering naar microsegmentering

Een security-architectuur gebaseerd op Zero Trust principes steunt onder andere op microsegmentatie van de netwerkomgeving. In de transitie naar een netwerkomgeving met microsegmentatie onderscheiden we voor onszelf een aantal veranderopgaven, deels technisch, deels organisatorisch.

Zonering

We komen uit een situatie waarin de organisatie gebruik maakt van verschillende separate infrastructuur omgevingen. Daar waar dat kan vormen we deze aparte netwerken om tot segmenten binnen één en dezelfde netwerkstructuur (zie vorige pagina). De segmenten verschillen onderling onder andere in termen van beveiligingsniveau en het niveau van invloed en zekerheid die we als organisatie daarover kunnen uitoefenen. Ons hoofdsegment is het hoogst beveiligde zone (BBN3) en houden we on-prem. Cloudvoorzieningen zijn onder gebracht in één of meer van de ander segmenten. Netwerkzonering maakt het mogelijk om dataverzamelingen en verwerkingen die een bepaald niveau van beveiliging of controle vereisen te isoleren en maakt het mogelijk om veilig cloud voorzieningen in te zetten voor die verwerkingen en processen waar dat kan.

Techniek

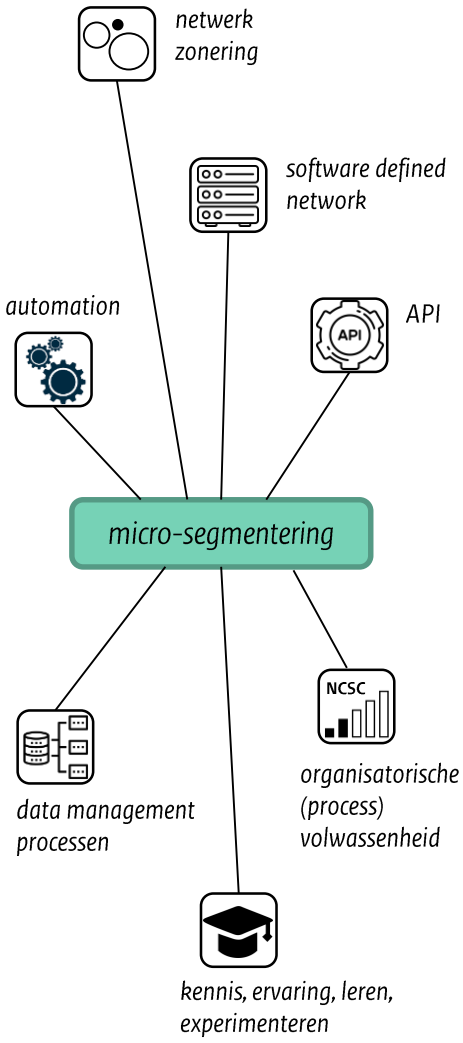
Om microsegmentatie in technische zin mogelijk te maken is software defined networking (SDN) en automation randvoorwaardelijk. Op dit moment vernieuwen we ons primaire (on prem) netwerk onderdeel (de groene zone) en bouwen dit om naar een SDN omgeving. Daarmee verwachten we binnen deze netwerkzone microsegmentatie te kunnen toepassen en tevens de veilige integratie met andere netwerkzones te kunnen organiseren. Een andere technische voorziening die we mede hiervoor hebben geïntroduceerd is de API Gateway. Die maakt het mogelijk om geautomatiseerde informatiestromen (via API's) tussen segmenten, zones en met externe partijen gedetailleerd en veilig te kunnen regelen en monitoren.

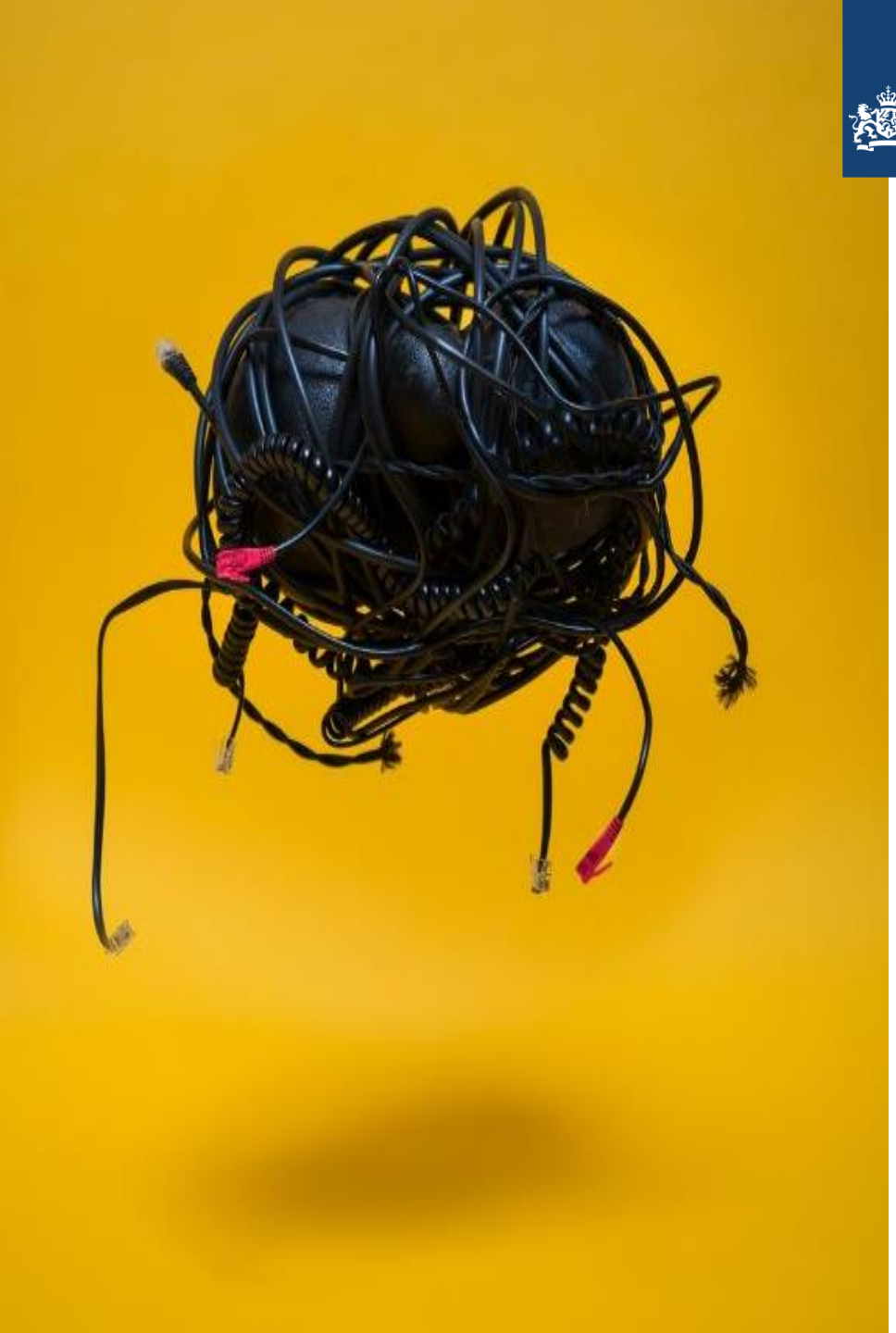
Organisatorische volwassenheid

Microsegmentatie stelt aanzienlijke eisen aan de (proces)volwassenheid van een organisatie, bijvoorbeeld op het vlak van dataclassificatie, gegevens- en informatiearchitectuur en andere datamanagement processen. Om te kunnen bepalen wie (of welk systeem), wanneer, welke gegevens wel en niet mag verwerken of raadplegen dient er bijvoorbeeld een fijnmazig *access control* model beschikbaar te zijn. Deels is die gebaseerd op de rollen (*role based*) van medewerkers en dat vereist heldere taken en bevoegdheden, procesbeschrijvingen en een adequate proces discipline. Al deze zaken vereisen een relatief hoge organisatorische volwassenheid.

Kennis en ervaring

Het introduceren van nieuwe technische voorzieningen en mogelijkheden op het gebied van SDN, API gedreven informatie uitwisseling, microsegmentatie en *automation* vereist dat collega's hier op een adequate manier mee overweg kunnen. Dit vereist een aanzienlijke investering in trainingen en het opbouwen van kennis en ervaring. Het betekent ook dat de transitie naar SDN en microsegmentatie een meerjarig traject is met diverse afhankelijkheden op technisch, organisatorisch, personeel en financieel vlak.





ZTA: Access Control

ZTA gaat er vanuit dat geen gebruiker of systeem toegang heeft tot informatie of voorzieningen tenzij hij daar expliciet voor geautoriseerd is en dat deze toegang op het moment van benaderen wordt gevalideerd. Die autorisatie kan afhangen van de rol die die gebruiker binnen een organisatie heeft, of bepaald worden aan de hand van specifieke *rules* of *attributes*. Zo zou een gebruiker alleen toegang kunnen krijgen tot bepaalde informatie als hij gebruik maakt van het bedrijfsnetwerk of inlogt met een *managed device* tijdens kantoortijd. Is dat niet het geval dan krijgt hij geen toegang, of bijvoorbeeld alleen tot algemene, niet gevoelige, informatie.

Het NCSC hanteert voor verschillende systemen *role based access*. Voor andere systemen willen we *role/attribute based access* verder doorontwikkelen en fijnmaziger neerzetten. In de situatie waar we vandaan komen - een kleine organisatie met een overzichtelijk IT landschap en een sterke *perimeter based* beveiliging - was dat minder nodig. Met de introductie van zonering, segmentering, cloud voorzieningen en groeiende complexiteit van het landschap, wordt dit relevanter.

Deze doorontwikkeling betekent waarschijnlijk dat we bepaalde nieuwe voorzieningen moeten gaan introduceren, zoals de eerder beschreven cloud access security broker die in een hybride cloud situatie, op basis van vooraf gedefinieerde *policies* bepaalt, wie of wat, waartoe toegang mag krijgen. Om micro-segmentering goed te kunnen laten werken hebben we ook stappen te zetten op het scherp definiëren van rollen (in processen), de daarvoor benodigde informatie, bijbehorende informatiestromen en toegangsrechten.

Voor de uitwisseling van informatie uitwisseling tussen systemen (machine to machine; M2M) geldt dat de API Gateway hier een belangrijk rol in in neemt. Via de API Gateway kunnen we toegangsregels instellen, afdwingen en monitoren.

Conclusie

Cloud adoptie is geen kwestie van *of*, maar een kwestie van *wanneer*. Dit geldt in het bijzonder ook voor public cloud gebruik. Zoals iedere verandering of nieuwe technologie brengt ook de inzet van cloud risico's met zich mee. Deze dienen adequaat gemanaged te worden. In dat kader geldt dat het uitstellen van cloud adoptie eveneens risico's met zich meebrengt voor de continuïteit en functioneren van organisaties. De inzet van publieke clouddiensten is noodzakelijk voor een adequate inzet van AI, IoT, analyticts, bioengineering, en ander technologische innovaties.

Het adequaat kunnen inzetten van (*public*) clouddiensten vereist aanpassingen aan processen, werkwijzen, kennisniveaus en techniek. Deze veranderingen kunnen aanzienlijke gevolgen hebben voor een organisatie wat maakt dat de adoptie van (public) clouddiensten vaak een periode van meerdere jaren omvat. Dat geldt ook voor onze *cloud journey*. Een belangrijke uitdaging ligt hierbij op vlak van cloud integratie; het verbinden en integreren van IAM en datastromen tussen on-prem en cloud omgevingen. Cloud adoptie stelt tevens hogere eisen aan procesvolwassenheid op domeinen als sourcing, datamanagement, gegevensarchitectuur en leveranciersmanagement.

Beveiliging vormt één van de centrale opgaven bij de introductie en integratie van cloudvoorzieningen. Certificering van clouddiensten en andere vormen van *assurance* kunnen helpen beter zicht en grip te krijgen op de beveiliging van individuele clouddiensten. Daarvoor ligt een belangrijke opgave en verantwoordelijkheid bij de Cloud Service Provider (CSP). Het vervolgens op een veilige manier inpassen en integreren van die diensten in het eigen landschap is en blijft echter primair een verantwoordelijkheid van de klantorganisatie.

De inzet van Zero Trust Architecture principes kan organisaties helpen om cloudvoorzieningen op een veilige manier te integreren, zowel onderling als met een (bestaande) on-prem voorziening. ZTA zorgt voor een verschuiving van een op netwerk (perimeter) gerichte security architectuur naar een data & asset gerichte security architectuur. Die paradigmawisseling heeft, zo leren we, aanzienlijke gevolgen voor de organisatie en vereist vanwege het centraal stellen van data en assets bijvoorbeeld een volwassen inzicht in en beheersing van die assets, datastromen, gegevensarchitectuur en datamanagement.

De introductie van ZTA om op een veilige manier cloud voorzieningen mogelijk te maken kan stapsgewijs plaats vinden waarbij bestaande pre-cloud voorzieningen, bijvoorbeeld die ten aanzien van IAM, worden gecombineerd met nieuwe voorzieningen voor cloud integratie. Onze ervaring tot nu toe is dat *rip & replace* niet nodig is. Wel vormt het omvormen van onze on-prem infravoorziening naar een software defined network (SDN) oplossing een belangrijke pijler in onze cloud journey. Deze is namelijk randvoorwaardelijk voor de automation van processen die nodig is voor microsegmentatie. En daarbij zorgt het on-prem SDN voor een eenvoudigere (softwarematige) integratie met off-site cloudvoorzieningen, zoals met de public PaaS voorziening waar we sinds kort mee werken. Inzet van ZTA is daarmee voor ons ook een meerjarig traject, wat leidt tot een soort hybride overgangsperiode. ZTA is een principe; een strategie en geen one-size-fits all oplossing en geen blauwdruk. Keuzes en implementaties hangen af van bestaande IT-infrastructuur, gebruikers en processen. Zoals we laten zien is het ook niet alleen een technische opgave, of alleen een opgave voor de IT-afdeling.

Voor zowel cloud adoptie als ZTA geldt; begin klein en experimenteer veel, waar mogelijk parallel. Kies zeker in eerste instantie voor eenvoudig te beheersen oplossingen met weinig risico's en zonder gevoelige gegevens. Bepaal op basis van die ervaringen wat werkt voor je eigen organisatie en definieer langs die lijn een eigen cloud visie, strategie en vervolgens beleids- en gebruikskaders.