Implementatierichtlijn voor een veilige gemeentelijke cloudinrichting

De transitie van ICT-infrastructuur naar “cloud” is volop gaande. Ook bij gemeenten is dit een steeds belangrijker wordend thema. Soms vanuit een eigen visie maar vaker door de marktontwikkelingen gedreven. Daarmee is het gebruik van cloud onmisbaar en onontkoombaar.
Er zijn diverse redenen om gebruik te maken van een clouddienst, zoals: snelheid, schaalbaarheid, beveiliging, kosten en flexibiliteit. Het uitgangspunt is daarbij dat je de leverancier zoveel mogelijk het werk laat doen en bijvoorbeeld eist dat de leverancier bewijst dat hij aan de gestelde eisen en voorwaarden voldoet, bij zowel de inrichting als in de operationele fase. Daarbij dienen de continuïteit van dienstverlening, privacybescherming en informatiebeveiliging te zijn geborgd, conform wet- en regelgeving; ‘public’ waar kan, ‘private’ waar moet. Gemeenten hebben en houden verantwoordelijkheid, beschikking en eigenaarschap over de eigen data.
Uit onderzoek blijkt echter dat minder dan de helft van gemeenten zich voldoende in control vindt ten aanzien van regelgeving zoals BIO en AVG.

GGI-Cloud Expertisecentrum
Het GGI-Cloud Expertisecentrum van VNG ondersteunt gemeenten bij hun transitie naar de cloud. Met de collectieve ondersteuning van het expertisecentrum zijn gemeenten beter in staat om regie te voeren over hun clouddiensten. Gemeenten verbeteren daarmee hun leveranciersmanagement en versterken de digitale veiligheid van hun SaaS- en PaaS/IaaS-diensten. Het GGI-Cloud Expertisecentrum werkt onder andere aan de Gemeentelijke Implementatierichtlijn voor het gebruik van public cloud.

Public cloud
Public cloud is een type computing-model waarbij cloud resources, zoals servers en applicaties, volledig als managed service worden aangeboden. Een public cloud wordt beheerd door cloud service providers zoals Microsoft , AWS, Google of Oracle en heeft voordelen zoals flexibiliteit, schaalbaarheid en lagere kosten. Gebruik van public clouddiensten biedt potentiële voordelen, er zijn echter ook risico’s die beheerst moeten worden. Onder voorwaarden mogen overheidsorganisaties public clouddiensten gebruiken.
In de eerste plaats gelden voorwaarden voor de verwerking van persoonsgegevens in public clouddiensten. Dit vergt een goedgekeurde pre-scan gegevens-beschermingseffectbeoordeling (ook wel pre-scan DPIA genoemd). Bij een hoge BBN-klasse dient een volledige data protection impact assessment (of formele DPIA) uitgevoerd te worden, waarin zowel de verwerking zelf als de geldende grondslagen, de aard van de verwerking en de bijbehorende risico’s en maatregelen zijn beschreven. Dit geldt ook bij verwerking van gegevens in een public cloud. Elke gemeente is zelf verantwoordelijk om de relevante risico’s van het gebruik maken van een public cloud toepassing in beeld te hebben en tijdens het gebruik in beeld te houden. Op basis van deze risicoafweging kan de betreffende gemeente voor tot en met departementaal vertrouwelijk gerubriceerde informatie besluiten tot gebruik van de public cloud.
Kortom: Je kan prima naar public cloud maar zorg wel dat je je goed verantwoordt. Dat betekent risicogebaseerd beveiligen. Risico gaat over kwetsbaarheidseisen maar ook beschikbaarheid. Data van burgers moeten goed beveiligd zijn maar je wilt ook slim met kosten omgaan.

Uitgangspunten

Gehanteerde uitgangspunten bij onze invulling van een veilige gemeentelijk cloudomgeving:

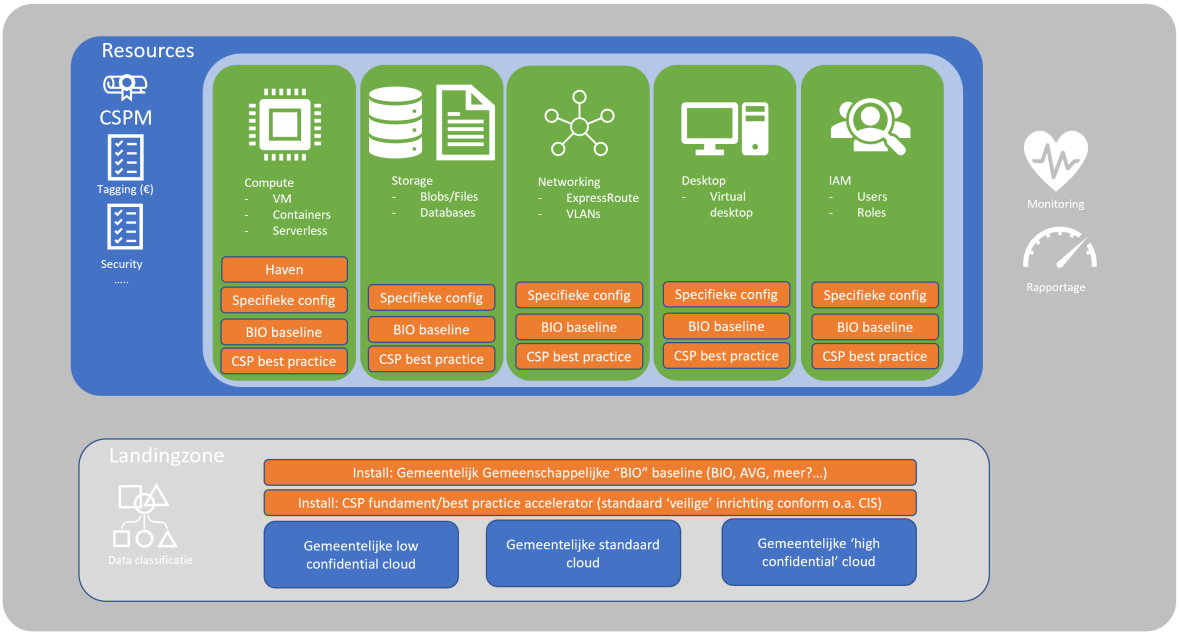
- Met de juiste inrichtingskeuzes is het public cloud aanbod beter in staat om een veilige omgeving te creëren dan dat men dat lokaal kan realiseren. Daarmee kan public cloud toegepast worden voor dataclassificaties t/m BBN3.
- Het is noodzakelijk om een risicoanalyse uit te voeren. Bijvoorbeeld op basis van het "implementatiekader-risicoafweging-cloudgebruik-v11".
- Controleer continu of de omgeving voldoet aan de Gemeentelijke Implementatierichtlijn m.b.v. de beschikbare controlemiddelen. Deze zijn actueel en onafhankelijk gevalideerd.

Onafhankelijk gevalideerd

Het GGI-Cloud Expertisecentrum werkt samen met het Rijk en met leveranciers om één onafhankelijk getoetste, generieke set best practices te definiëren voor een veilige public cloudomgeving (landingzone, resources en DPIA's). Dit samen heet de implementatierichtlijn voor een veilige gemeentelijke cloudomgeving, waarmee kan worden voldaan aan de eisen van BIO en AVG en die óók voldoet aan de eisen van bijvoorbeeld de Autoriteit Persoonsgegevens en het Rijksbrede cloudbeleid.

Minimaal beveiligingsniveau

Deze richtlijn kan gebruikt worden door (implementatiepartners van) alle gemeenten. Het grote voordeel van deze richtlijn is dat de cloudomgevingen van alle gemeenten op een onafhankelijk vastgesteld minimaal beveiligingsniveau kunnen komen. Door de best practices in de richtlijn te volgen, kunnen gemeenten bovendien tijd en kosten besparen zonder in te boeten op de veiligheid van hun omgeving.



Daarnaast werkt het GGI-Cloud Expertisecentrum in samenwerking met marktpartijen aan controlemiddelen waarmee gemeenten continu kunnen bewaken in hoeverre hun omgeving nog steeds compliant is aan de Gemeentelijke Implementatierichtlijn. Deze compliance

checkers zijn onafhankelijk gevalideerd en kunnen in de gangbare securitydashboards worden bewaakt. De compliance checkers worden ontwikkeld voor:

- Microsoft 365
- Microsoft Azure
- Amazon Web Services (AWS)
- Google Workspace
- Google Cloud

Kennismaken met het GGI-Cloud Expertisecentrum

- Het GGI-Cloud Expertisecentrum zal op zowel het Overheid 360 Congres als het VNG Jaarcongres aanwezig zijn in de stand van het Servicecentrum Gemeenten van VNG Realisatie. Belangstellenden kunnen zich nog voor beide congressen opgeven (Overheid 360 / VNG Jaarcongres).
- Meer informatie over het GGI-Cloud Expertisecentrum vindt u op de website van de VNG: https://vng.nl/projecten/ggi-cloud. Het onderzoek naar cloudondersteuning is terug te lezen op het (besloten) GGI-Cloud forum .
- U kunt ook een e-mail sturen aan info@scgemeenten.nl.