## Reactie op IT-deltaplan voor de overheid

Als je naar de kwaliteit van de strategische inzet van IT kijkt, zijn jaarplannen en jaarverslagen een prachtige bron voor informatie. Ik heb vanuit mijn ervaring een representatieve steekproef genomen onder ZBO's en gemeenten. Dan zie ik dat de overheidsorganen nauwelijks IT-doelen hebben. In hun plannen noemen ze wel vele wensen voor IT, maar zonder de stappen die het meetbaar doel maken. Is dit OK? In de overheid is IT het universele middel, en niet een doel. We moeten hier dus anders naar kijken.

Het bedrijfsleven gebruikt IT ook als het universele middel. Daar beseffen bestuurders dat de IT-kwaliteit op orde moet zijn in deze wereld met cyberdreigingen. Security is daarin een belangrijk kwaliteitsaspect. De bestuurders geven daarvoor in hun enterprise-architectuur parallel aan de bedrijfsvoering aparte ruimte aan IT in een overkoepelende IT-architectuur, die IT een logische plaats in de enterprise geeft, met lagen en compartimenten om verantwoordelijkheden duidelijk te beleggen en te scheiden. Een lichte architectuur die duidelijk is, flexibel en een weerbaar IT-landschap oplevert. Deze architectuur is ingericht volgens principes en patronen. Deze IT-architectuur bevat een palet aan bruikbare centrale diensten voor alle bedrijfsonderdelen die deze willen gebruiken.

Binnen de overheid kennen we ook een paar van deze centrale diensten, zoals DigiD en eHerkenning. Er kunnen veel meer diensten geleverd worden, en ook deze zie je mondjesmaat opkomen. Ik noem monitoring (SIEM/SOC) en incident response (CSIRT). Wordt er echter vanuit de overheid gekeken naar kansen vanuit een overkoepelende IT-architectuur met de overheidsorganen? Welke diensten kunnen effectief gecentraliseerd worden?

Hier komt de politieke realiteit om de hoek kijken: anders dan bedrijven moeten de overheidsorganen rekening houden met het invullen van veranderlijke politieke doelen, die niet altijd soepel in IT te regelen zijn. Dit maakt de inzet van IT (te) complex. Jaarplannen en jaarverslagen van overheidsorganen stellen dit duidelijk, ik noem een voorbeeld:

> *"Er is ook wetgeving die een dusdanig grote impact op onze organisatie heeft dat we ervoor kiezen deze gefaseerd in te voeren om te voorkomen dat onze primaire taken en onze bedrijfsvoering in de knel komen"*

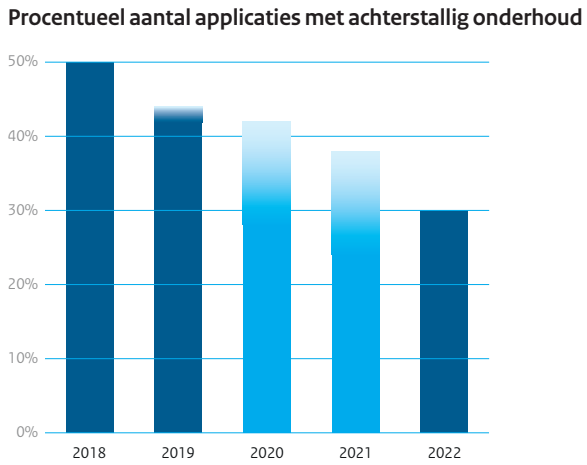
We focussen veel op gefaalde IT-projecten. Maar wat weten we van de kwaliteit van de IT-operatie en het IT-beheer binnen de overheid? Hierover staat weinig in de plannen van de afgelopen jaren en wat er staat is een vage wens:

> *"We hebben de afgelopen jaren een belangrijke stap gezet in het stabiel maken van ons ICT-landschap en willen nu meer energie steken in de volgende stap"*
>
> *"... hebben we in 2018 vooral gewerkt aan de verbetering van de kwaliteit en het functioneren van de ICT-prestaties"*

*"Door ICT is in samenwerking met strategische partners het eerste plateau van een Security Operations Center ingericht dat op stedelijk niveau de informatiebeveiliging monitort en actie onderneemt bij incidenten, zoals DDOS aanvallen"*

*"Informatiebeveiliging vraagt continue aandacht van de gemeentelijke organisatie. Daarom houden we risicoanalyses, voeren we beheersmaatregelen door, toetsen we de werking van die maatregelen en voeren we verbeteringen door"*

Ik maak een kleine uitzondering voor de Belastingdienst: Zij geven bijvoorbeeld een specifiek overzicht van het procentueel aantal applicaties met achterstallig onderhoud, met ambities tot verbetering:




In mijn steekproef van jaarplannen hebben genoemde IT- en IT-securitydoelen geen specifieke plannen waartegen verantwoording afgelegd kan worden. In de jaarverslagen wordt ook achteraf geen specifieke verantwoording afgelegd. Volwassen plannen horen specifiek te zijn, stappen te definiëren en verantwoordelijkheid mogelijk te maken.

Het is niet allemaal sturing van bovenaf wat nodig is. Besef dat de overheids-IT niet als eenheid georganiseerd kan worden, daarvoor varieert context van inzet te veel. Daarom moet de overkoepelende IT-architectuur licht zijn en slechts compartimenten, principes en patronen duiden. Enterprises die dit doen hebben hierdoor een wendbare en weerbare IT-inzet. Besef ook dat de overheids-IT niet bij wet gedicteerd kan worden. Om de passing van politieke doelen op IT te richten binnen de overkoepelende IT-architectuur kunnen stuurgroepen of klankbordgroepen ingericht worden. Waarbij de politiek bereidheid hoort te tonen politieke doelen eventueel bij te stellen.

De kwaliteit van de inzet van IT als middel moet duidelijk genoeg zijn om achteraf te kunnen controleren op navolging van de overkoepelende IT-architectuur. Een aantal zaken zijn 'no-brainers' om informatiebeveiliging in te vullen in deze wereld met cyberdreigingen:

- Operatie en beheer op orde: incidentmanagement, software-updates, medewerker-awareness;

- Toegangsbeveiliging op orde, hierbij zijn er veel centralisatie- en kansen om IT te herbruiken;
- (Cyber)risico's moeten goed in beeld zijn;
- Aan de AVG moet voldaan worden.
- Preventie op orde, met o.a. vulnerability-scanning en malware-detectie;
- Detectie en respons op orde, met o.a. SIEM/SOC en CSIRT-diensten;
- Bijblijven met nieuwe dreigingen, penetratietesten (laten) uitvoeren;

Wat moet het bestuur van overheidsorganen hiervoor doen?

- Een strategie hebben voor de kwaliteit van IT-inzet, met operationele doelen en beheersdoelen, met verantwoording achteraf, ook als ZBO of ander overheidsorgaan;
- De strategie moet in lijn zijn met de overheidsarchitectuur, wees hierbij bereid om experts in te zetten. Neem deze aan en huur ze in, wees bereid hiervoor de marktwaarde te betalen;
- Zorg voor flexibiliteit en weerbaarheid van de IT. Hier zit de grote uitdaging! De overheid neigt naar statisch vastslaan bij twijfel en moeilijkheden;
- Wees in-control op een risico gebaseerde wijze, neem dus risico's geïnformeerd en bewust;
- Dit betekent voldoende budget hebben voor kwaliteit (operationeel, beheersmatig en voor veranderingen).

Vormt dit een groot deltaplan? Het is meer een bewuste keuze maken vanuit de overheid als geheel om IT-inzet realistisch, duidelijk als apart en universeel bedrijfsmiddel te positioneren, hier in gezamenlijkheid afspraken over te maken en per overheidsorgaan concrete plannen voor maken met afleggen van verantwoording tegenover die plannen achteraf.

Lex Borger
Specialist informatiebeveiliging