

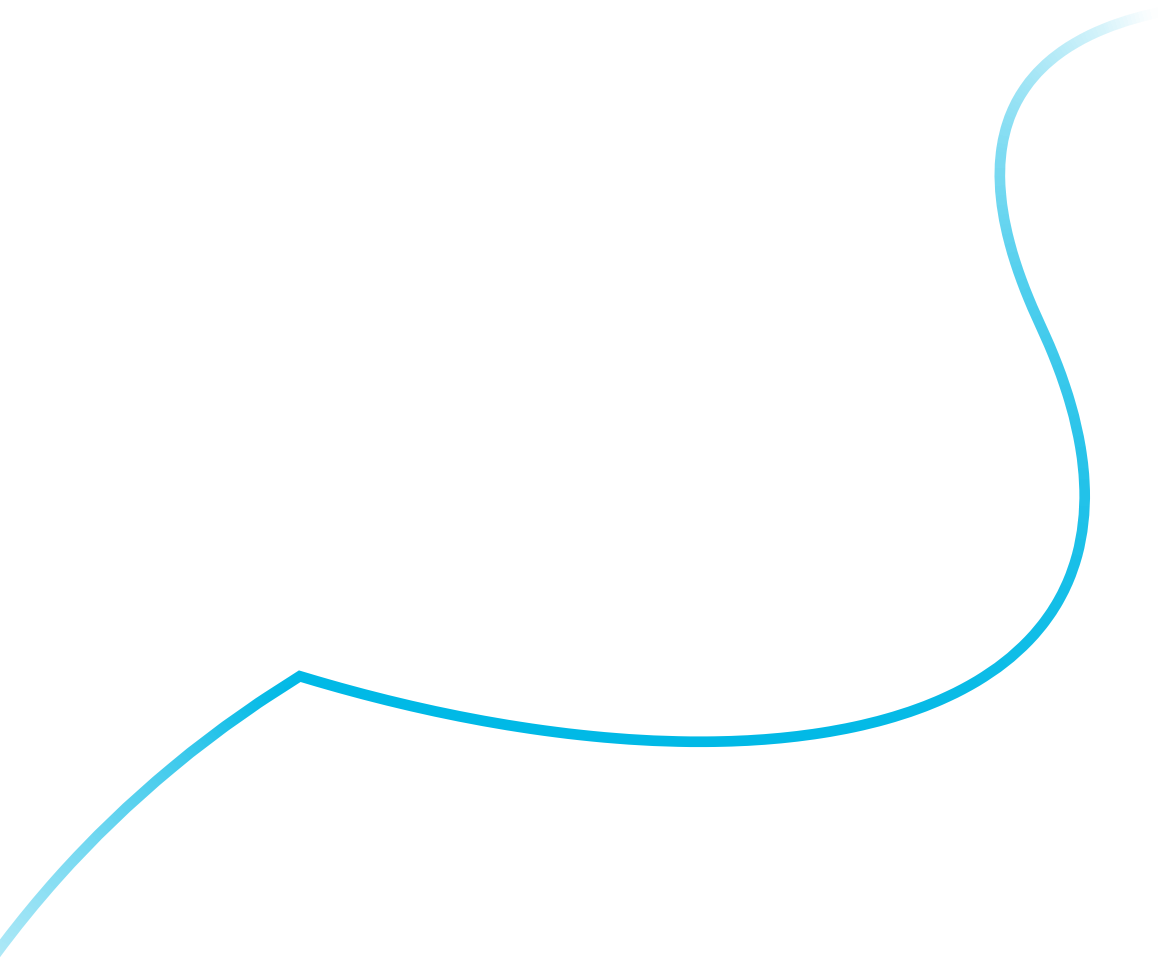


Society 5.0

Wendbare overheid in tijden
van disruptie

2025

Capgemini 



Inhoudsopgave

	Voorwoord	02
1.	Organisatorische wendbaarheid	05
	<i>Interview: Het digitale hart van de Nederlandse infrastructuur</i>	06
	Wendbare publieke organisaties: sterker door verandering met Agile-werkwijzen	08
	Visie op de Shared Service organisatie van de toekomst	13
	Samenwerken in ecosystemen: een sleutel tot wendbaarheid	18
	Hoe ontsnap je aan de wurggreep van legacy-systemen?	22
	
2.	Personele wendbaarheid	27
	<i>Interview: De 5.0-wal keert het schip</i>	28
	Het belang van wendbare en weerbare medewerkers in sterk veranderende tijden	30
	Doorbraak in duurzame inzetbaarheid door Design Thinking	35
	
3.	Technologische wendbaarheid	41
	<i>Interview: 'Wat kan er nog wel?'</i>	42
	Nederland bepaalt zelf hoe de super slimme samenleving eruit ziet	44
	De AI-verordening: tijd voor actie voor een weerbare publieke sector	49
	Cbw: wetgeving maakt weerbaar, strategie houdt wendbaar	55
	Data Trust by Design: de sleutel tot vertrouwen, wendbaarheid en weerbaarheid	61
	Autonomie uitbesteden? De rol van soevereine cloud	67

Voorwoord

Het zijn turbulente tijden. De afgelopen jaren zijn Nederland en Europa in een fase van disruptie en transitie beland. In de private sector wordt deze transitie (vanuit bedrijfseconomisch perspectief) aangeduid als Industry 4.0. Voor de publieke sector hanteren wij het narratief van Society 51: de Super Slimme Samenleving. In voorgaande publicaties is ingegaan op de pijlers Duurzaamheid, Dienstverlening met de menselijke maat en de Toekomst van werk. Deze publicatie richt zich op de laatste pijler van Society 5.0: Wendbaarheid.

In 2023 schreef professor Jan Rotmans al dat we ons in een 'perfecte storm' bevinden, waarbij verschillende transitie elkaar onderling versterken². Denk aan de energie-, ruimtelijke-, uitvoerings- en grondstoffentransitie. Daarnaast verschuiven de panelen op het geopolitieke toneel razendsnel sinds het aantreden van president Trump. Door zijn transactionele machtspolitiek wordt Europa gedwongen veel zelfbewuster om te gaan met genoemde transitie. Als we onze Europese waarden willen beschermen, moet de Europese strategische autonomie worden versterkt.

Dit komt ook tot uiting in het rapport van Mario Draghi 'The Future of European Competitiveness' van september 2024³. Het dichten van de innovatiekloof met China en de Verenigde Staten, het versterken van het concurrentievermogen in balans met decarbonisatie, en het verminderen van strategische afhankelijkheden vormen de hoofdgebieden voor Europese actie. Nu de trans-Atlantische alliantie in onzeker vaarwater is beland, is snelheid geboden. Het versterken van de (digitale) autonomie is tevens een belangrijk onderwerp in de Nationale Digitaliseringsstrategie. Deze is nog in ontwikkeling, maar duidelijk is dat de positie van cloud, het datastelsel, de verantwoorde benutting van AI, autonomie en digitaal vakmanschap daarin een prominente rol spelen. Met de burger en ondernemer als uitgangspunt voor de te maken ontwerpkeuzes.

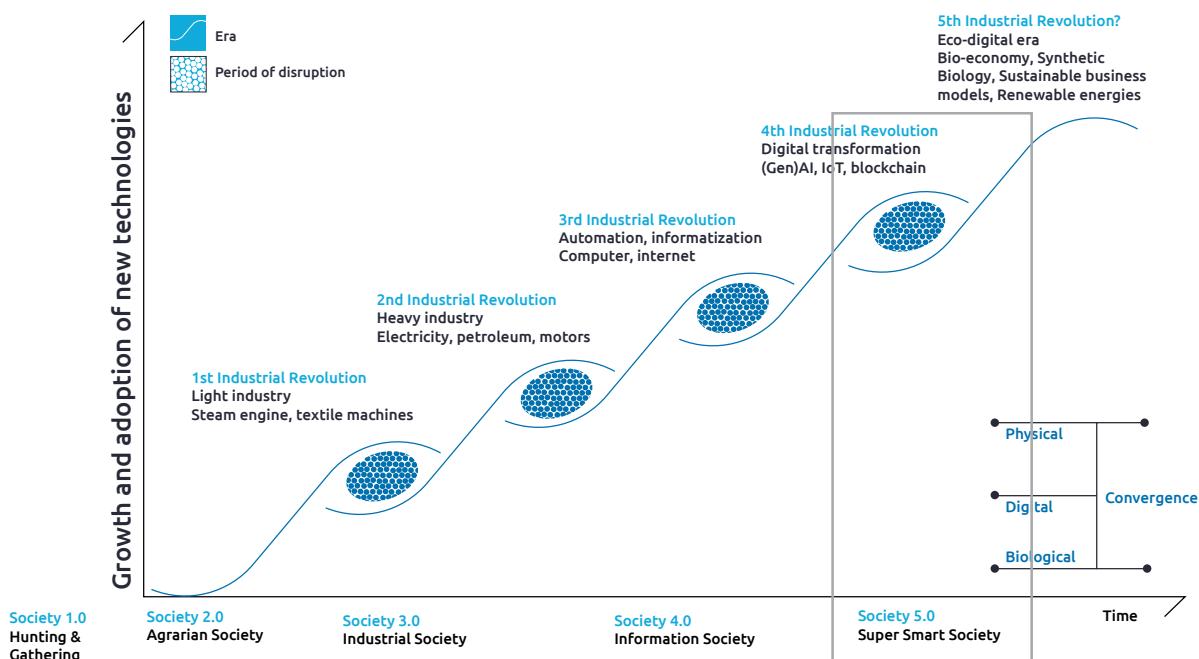
Voor de publieke sector in Nederland (en vele andere organisaties) vereist deze combinatie van ontwikkelingen en de daarmee gepaard gaande onzekerheid, een hogere mate van wendbaarheid. Wij onderscheiden (niet uitputtend) drie perspectieven die bijdragen aan

het verhogen van de wendbaarheid: Organisatorische, Personele en Technologische wendbaarheid. Elk perspectief wordt ingeleid door een praktijkinterview met Logius, de Koninklijke Marine en Schiphol. Hieronder zijn de 11 artikelen per perspectief kort samengevat:

Organisatorische wendbaarheid

1. Wendbare overheidsorganisaties proberen niet de toekomst te voorspellen, ze zijn toekomstbestendig georganiseerd. Wendbaarheid vertaalt zich in het Engels als 'agility'. Agile methoden helpen om in te spelen op veranderingen. Om effectief en transparant te opereren, dienen overheidsorganisaties voldoen aan strikte wet- en regelgeving en tegelijkertijd flexibel blijven in de uitvoering. Agile werken doorbreekt traditionele silo's en stimuleert samenwerking in multidisciplinaire teams. Klein beginnen en continu leren is daarbij het devies.

The waves of growth are driven by new technologies, and phases of disruption in between with great effect on society



2. Een belangrijke schakel binnen de organisatie van de (rijks)overheid wordt gevormd door Shared Service Organisaties (SSO's). Deze zijn in het leven geroepen om verschillende organisatiefuncties te integreren. Door het centraliseren van functies in SSO's worden taken verminderd, dataduplicatie vermeden en efficiëntie verhoogd. De steeds sneller opvolgende veranderingen en technologische ontwikkelingen vragen echter wel om aanpassingen in de besturing, de inzet van technologie en de cultuur. In essentie vraagt dit om een hybride benadering met balans tussen operational excellence en customer intimacy.
3. De transities en maatschappelijke opgaven zoals benoemd in de inleiding zijn te veelomvattend om door één enkele partij op te lossen. Samenwerking in ecosystemen biedt uitkomst door de unieke sterke punten van verschillende partners te combineren. Publieke organisaties hebben een cruciale rol als katalysator in deze ecosystemen. Ze kunnen randvoorwaarden scheppen door beleid, financiering en infrastructuur te bieden. Tegelijkertijd moeten ze zichzelf openstellen voor meer netwerkgerichte werkwijzen. Goede voorbeelden hiervan zijn de wijkgerichte aanpak van verduurzaming en de lokale samenwerking op het gebied van energie in de zogenaamde energiehubs.
4. Wendbaarheid van publieke organisaties wordt in de praktijk echter vaak belemmerd door verouderde IT-systemen. Denk aan oplopende kosten, beveiligingsproblemen en gebrek aan innovatie. Een voorbeeld is het doorvoeren van nieuwe fiscale regelgeving bij de Belastingdienst die wordt uitgesteld omdat 'de systemen' het niet aankunnen. Organisaties lijken in een 'wurggreep' van legacy-systemen te zitten. Ontsnappen is gelukkig mogelijk. Niet door risicovolle grootschalige vervangingen, maar door een gefaseerde aanpak. Het 'Strangler Pattern', GenAI en Robotic Process Automation (RPA) bieden praktische oplossingen om geleidelijk te komen tot modernisering en wendbaarheid.

Personele wendbaarheid

5. Met een historische arbeidskrachte, toenemende flexibilisering en deeltijdwerk en grotere verandering van taken en vaardigheden binnen bestaande banen, staan organisaties voor de uitdaging om werknemers en het personeelsbestand toekomstbestendig te maken. Technologie speelt hierbij een belangrijke rol. Zowel als aanjager van deze veranderingen, en als oplossing. Strategische personeelsplanning, kennismanagement, skills based werken en talentmanagement zijn effectieve personeelsstrategieën die aan kracht winnen wanneer technologie hierbij wordt ingezet. Door deze noodzakelijke (digitale) personeelsstrategieën in te voeren, kunnen publieke organisaties hun personeelsbestand ('human capital') optimaliseren en tegelijkertijd een waardevolle bijdrage blijven leveren aan de taak waar zij voor aan de lat staan. Door een sterke focus te leggen op continue ontwikkeling van medewerkers met de inzet van digitale tools en platforms wordt de wendbaarheid vergroot.
6. Cijfers laten echter zien dat er nog veel te winnen is. Uit trendonderzoek blijkt dat een leven lang ontwikkelen stagneert⁴. Ten aanzien van gezond en veilig werken geldt dat 36% van de bedrijven niet beschikt over een preventief arbobeleid met een inventarisatie van de arbeidsrisico's en maatregelen om werknemers hiertegen te beschermen⁵. Dit terwijl het werk gerelateerd ziekverzuim en aantal arbeidsongevallen nog steeds te groot is. De veelheid aan kennis en instrumenten die beschikbaar zijn voor duurzame inzetbaarheid, worden in de praktijk nog beperkt toegepast⁶. Door het toepassen van Design Thinking en het differentiëren van werkgevers kan dit worden verbeterd.

Technologische wendbaarheid

7. Technologie speelt een onmisbare rol in de Society 5.0; de superslimme samenleving. Technologische innovatie is cruciaal om Nederland wendbaar te houden. Innovatie lijkt

- ook een sleutel tot het oplossen van maatschappelijke opgaven. In het Regeerprogramma van Kabinet Schoof is het woord ‘innovatie’ 85 keer genoemd als mogelijke oplossing voor maatschappelijke problemen. Echter, met het stopzetten van het Nationaal Groeifonds zijn 60 innovatieprojecten gestopt. Zonder technologische innovatie en opschaling blijven we afhankelijk van de grote tech-bedrijven. De Nationale Technologie Strategie (NTS) biedt echter hoop. Dit raamwerk voor strategisch technologiebeleid onderscheidt tien sleuteltechnologieën voor economische groei, het aanpakken van maatschappelijke uitdagingen en het waarborgen van wendbaarheid en weerbaarheid.
8. Bij de toepassingen van nieuwe technologieën dienen onze Europese publieke waarden centraal te staan. De AI-verordening stelt geharmoniseerde regels vast voor de ontwikkeling, het in de handel brengen, en het gebruik van AI-systemen binnen de EU. Kunstmatige intelligentie vormt één van de belangrijkste aanjagers van Society 5.0. Door duidelijke eisen en verplichtingen te stellen aan AI-toepassingen, helpt de verordening om potentiële risico's te beheersen en de maatschappelijke weerbaarheid te vergroten.
 9. Ook de Nederlandse implementatie van de Network and Information Security Directive 2 (NIS2) – de Cyberbeveiligingswet (Cbw) zal dit jaar zijn intrede maken. Hierdoor wordt de weerbaarheid bevorderd via onder andere risicobeheer en het creëren van bewustwording. Een cybersecuritystrategie, gekoppeld aan de organisatiedoelen, versterkt de wendbaarheid. In combinatie zorgen ze dat de burger kan vertrouwen op de continuïteit van onmisbare digitale diensten.

10. Vertrouwen gaat echter verder dan de naleving wet- en regelgeving door publieke organisaties. Vertrouwen van burgers en bedrijven in de overheid wordt gevoed door security, privacy, data-ethiek en datakwaliteit. En dit zijn bij uitstek de pijlers onder Data Trust by Design. Dit is een toekomstgerichte benadering die organisaties in staat stelt om zowel digitaal vertrouwen op te bouwen als om de uitdagingen van wendbaarheid en weerbaarheid effectief aan te pakken.
11. Hoog op de agenda in het kader van technologische wendbaarheid staat de rol van soevereine cloud. De geopolitieke onrust benadrukt de noodzaak van digitale autonomie en Europese zelfredzaamheid op dit gebied. Het gaat daarbij om veel meer dan de ICT-infrastructuur, hardware en netwerkkabels. Het gaat ook om innovaties, flexibiliteit en veiligheid. Daarin lopen de hyperscalers ver voor. Als we autonomie invullen met ‘zorgen dat we alternatieven hebben’ en ‘snel genoeg kunnen switchen’ en ‘een fall back scenario’, dan kunnen we aangesloten blijven bij de wereldwijde schaalbare innovaties en tegelijkertijd sturen op onze eigen belangen. Europese samenwerking en consolidatie is daarbij nodig om voldoende schaalbaarheid te creëren.

Bovenstaande samenvatting geeft een beeld van de aspecten die aangepakt dienen te worden om de wendbaarheid en weerbaarheid van de publieke sector te vergroten. De afzonderlijke artikelen bieden meer inzicht en handvatten om concrete stappen te zetten. De maatschappelijke opgaven zijn groot. Het internationale krachtenveld is dynamisch. Ik wens u veel wendbaarheid.

Over de auteurs



Erik Hoorweg

Vice President Publieke Sector bij Capgemini Invent

Erik Hoorweg is Vice President bij Capgemini Invent en verantwoordelijk voor de dienstverlening aan de publieke sector. Erik en zijn team combineren strategie, technologie, data science en creative design om duurzame innovatie en transformatie mogelijk te maken.

 erik.hoorweg@capgemini.com

 <https://www.linkedin.com/in/erik-hoorweg-296b593/>

Bronnen

1. Zie voor meer duiding van Society 5.0 de eerdere publicaties van Capgemini: Brochure Potrait.
2. Jan Rotmans, De perfecte storm. Op zoek naar een nieuwe balans. Uitgeverij De Geus. September 2023.
3. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.
4. Leren en ontwikkelen in Nederland, Researchcentrum voor Onderwijs en Arbeidsmarkt (ROA), mei 2024.
5. Arbo in bedrijf 2022-2023, Monitoronderzoek naar de naleving van Arboverplichtingen, blootstelling aan arbeidsrisico's, maatregelen en gezond en veilig werken in de praktijk, Arbeidsinspectie, september 2024.
6. Quicksan Duurzame inzetbaarheid en leven lang ontwikkelen, Capgemini Invent, februari 2021.

1. Organisatorische wendbaarheid



Interview



Het digitale hart van de Nederlandse infrastructuur

Hoe Logius de Nederlandse samenleving weerbaar houdt – Bert Voorbraak en Guido Gihaux

De vraag naar digitale overheidsdiensten blijft groeien. Vorig jaar kende Logius 550 miljoen authenticaties, een stijging van 15%. Dat komt mede doordat nieuwe sectoren, zoals de zorg, DigiD ontdekken als betrouwbaar authenticatiemiddel. Logius vormt daarmee het digitale hart van de Nederlandse infrastructuur.

“Logius is een IT-leverancier met een overheidslicentie. We maken grootschalige, betrouwbare producten die bijdragen aan de digitale infrastructuur van Nederland,” zegt Bert Voorbraak, algemeen directeur Logius. “Wanneer een platform zoals DigiD uitvalt, zijn de gevolgen onmiddellijk merkbaar. Dan krijgen we direct berichten uit de zorgsector dat bijvoorbeeld patiënten niet meer in hun dossiers kunnen omdat DigiD het authenticatiemiddel is. Niet beschikbaar zijn, is uitgesloten. Daarom staat weerbaarheid bovenaan onze prioriteitenlijst.”

De dagelijkse strijd tegen cyberdreigingen

Logius wordt continu geconfronteerd met cyberaanvallen. “Ook nu, *as we speak*, liggen we onder vuur,” vertelt Guido Gihaux, waarnemend directeur Strategie & Regie Logius. “Gemiddeld zijn er wel 200 aanvallen per maand. Van de meeste aanvallen merken gebruikers vrijwel niets. Soms is er een nieuwe aanvalstechniek die we nog niet eerder zijn tegengekomen. Dat kan ervoor zorgen dat systemen even onbereikbaar zijn. De dreigingen zijn overigens niet alleen technisch van aard, maar worden ook gevoed door huidige geopolitieke ontwikkelingen. We reageren altijd pijlsnel: de volgende dag hebben we onze filters al aangepast, waardoor het probleem niet opnieuw optreedt. Dat is de kracht van onze organisatie; we moeten zowel extreem weerbaar als wendbaar zijn.”

Toekomstige uitdagingen: strategische keuzes

Hoe geavanceerd de huidige aanvallen ook zijn, ze vallen waarschijnlijk in het niet bij een van de grootste technologische uitdagingen voor de komende jaren: kwantum computing. Voorbraak: “Over een paar jaar kan kwantum computing wachtwoorden en encryptiesystemen kraken. Wij bereiden ons daar nu al op voor. Dat vraagt om een bredere aanpak, waarbij Nederland als geheel een kenniscentrum moet opbouwen.

Logius heeft al een sterke basis op het gebied van encryptie. Onze PKI (Public Key Infrastructure) is goed, en we hebben een solide beleid om encryptie veilig te houden. Maar het moet telkens vernieuwd worden. Ons BSNK en koppelregister zijn state-of-the-art, maar ook die moeten we doorontwikkelen.”

Digitale weerbaarheid betekent niet alleen bescherming tegen cyberaanvallen, maar ook het maken van strategische keuzes. “Met welke partijen wil je zaken doen?” zegt Gihaux. “Want wat als een Amerikaanse cloudleverancier in de problemen komt? Wat betekent dat voor de overheid en samenleving? Dit soort risico’s spelen een belangrijke rol in het strategisch leveranciersmanagement binnen Logius. Moeten we nog wel op *single points of failure* vertrouwen? Of moeten we kritieke diensten verdelen over meerdere leveranciers? Zulke vragen worden steeds urgenter.”

Open source softwareontwikkeling, zonder AI

Weerbaarheid kan op gespannen voet staan met transparantie: de overheid vereist open source voor het ontwikkelen van software. “Deze transparantie geldt ook voor DigiD,” zegt Voorbraak. “We hebben de back-end van DigiD openbaar gemaakt. Iedereen kan nu zien hoe het werkt. Daardoor kunnen anderen helpen met verbeteringen. Uiteraard houden we bepaalde delen afgeschermd, maar we geloven sterk in de *wisdom of the crowd*.”

Hoewel het voor de hand ligt om software te ontwikkelen met AI, is Logius daarmee terughoudend. “We werken alleen met bewezen technologie. AI wordt gebruikt om wet- en regelgeving doorzoekbaar te maken, maar altijd met menselijke controle. Experimenten lopen bijvoorbeeld bij onze helpdesks: kunnen we met AI onze gebruikersvragen beter structureren? Maar we laten AI geen software schrijven. De overheid stelt strikte eisen aan AI-gebruik, zoals het algoritmeregister en de vierogencontrole. AI moet altijd transparant en herleidbaar zijn. Kortom, we experimenteren, maar betrouwbaarheid en veiligheid moeten gegarandeerd zijn.”

De Nationale Digitaliseringsstrategie

De Nationale Digitaliseringsstrategie (NDS) is nog niet volledig vastgesteld, maar Logius bereidt zich alvast voor. Voorbraak: "We passen onze organisatie nu al aan: we ronden migraties af en voeren verbeteringen door naar aanleiding van eerdere rapporten. We willen zoveel mogelijk opruimen en afronden voordat de NDS beschikbaar komt, zodat we ons daar volledig op kunnen richten."

Een belangrijk uitgangspunt van de NDS is eenheid binnen de overheid. "We moeten meer denken vanuit één overheid en de grenzen tussen Rijksoverheid, gemeentes, provincies en waterschappen loslaten. Veel diensten van Logius passen al binnen deze gedachte, zoals MijnOverheid en DigiD. We zijn dan ook goed voorgesorteerd op deze ontwikkelingen," zegt Gihaux. "Veel van onze diensten werken al over departementsgrenzen heen. Toch zien we ook overlap tussen de diensten die wij leveren aan overheden en wat coöperaties zoals SURF bijvoorbeeld aanbieden. Waarom zouden we niet nauwer samenwerken? Daar kan de NDS bij gaan helpen."

Digitale weerbaarheid voor iedereen

Hoewel Society 5.0 uitgaat van een steeds slimmere samenleving, is de digitale weerbaarheid van burgers geen gegeven. Voorbraak: "We moeten als Logius zorgen dat mensen veilig en zelfstandig gebruik kunnen maken van digitale diensten. De complexiteit van digitalisering neemt toe, en daarmee ook de groep die moeite heeft met online diensten. Belastingaangifte doen, een rijbewijs verlengen, of een ziekenhuisafspraak regelen kan voor veel mensen enorm ingewikkeld zijn. Dat geldt niet alleen voor ouderen, maar ook voor mensen die (tijdelijk) minder digitaal vaardig zijn, bijvoorbeeld door stressvolle situaties of een fysieke beperking."

Gebruikersgerichte overheid

Logius werkt daarom volgens de 'help de helper'-strategie, zegt Gihaux. "In plaats van zelf mensen met lage digitale vaardigheden te ondersteunen, richten we ons op lokale steunpunten. Er zijn nu veel offline hulppunten, zoals de Informatiepunten Digitale Overheid (IDO) in bibliotheken, waar mensen uitleg krijgen over digitale diensten. Ook ondersteunen we de helpdesks van grote uitvoerders zoals UWV, SVB en gemeenten."

Het is overigens een misvatting dat alleen ouderen moeite hebben met het tempo van een digitaliserende samenleving, meent Voorbraak. "Ik dacht altijd, 'dit probleem lost zichzelf op: de nieuwe generatie groeit op in een digitale wereld'. Maar recente rapporten laten zien dat dat naïef is. Jongeren kunnen misschien TikTocken, maar digitale vaardigheden en met digitale overheidsdiensten omgaan; dat is echt iets anders."

Gihaux vult aan: "We ontwikkelen onze diensten daarom steeds meer vanuit UX-design en gebruikersonderzoek. Samen met burgers kijken we hoe voorzieningen intuïtiever kunnen worden ontworpen. Niemand heeft een steunpunt nodig om Instagram te gebruiken. Dat moet ook ons uitgangspunt zijn. Zo werken we nu aan een nieuw machtigingssysteem en kijken kritisch naar MijnOverheid. We werken bijvoorbeeld samen met een koepelorganisatie voor mensen met autisme. Hoe ervaren zij onze diensten en waar lopen ze tegenaan? Deze doelgroep was nog relatief onbekend voor ons. Door ze actief te betrekken, kunnen we onze dienstverlening sterk verbeteren."

De noodzaak van een één-loketfunctie

Ook de versnippering van overheidsdiensten vormt een uitdaging voor de weerbare burger die zijn weg moet vinden binnen de digitale overheid. Zo moeten 18-jarigen zelf hun zorgverzekering, toeslagen en DUO-aanmeldingen regelen, maar er is geen centrale plaats waar alles samenkomt. Hoewel er plannen waren voor een 'één loket'-functie, blijkt de uitvoering complex.

Toch blijft de gedachte van één overheid relevant, meent Voorbraak. "Onze berichtenbox fungeert al enigszins als een centraal loket, maar er moeten meer diensten aan gekoppeld worden om het gebruik te stimuleren. Dat geldt niet alleen tussen departementen maar ook over sectoren heen. Ook gemeenten die willen aansluiten bij cloudinitiatieven, lopen nu nog tegen beperkende wetgeving aan. Dit soort barrières moeten we doorbreken om een écht geïntegreerde overheid te realiseren."

De toekomst: overheidscloud en digitale autonomie

Logius denkt nu na over de overstap naar één overheidscloud. Voorbraak: "We maken nog veel gebruik van commerciële partijen, maar we willen meer grip op onze digitale autonomie. Als je alles in de Big Tech-centers onderbrengt, wordt

je weerbaarheid bepaald door anderen. Er zijn onderdelen van clouddiensten die we als overheid uitstekend zelf kunnen beheren om onafhankelijker te worden. Denk aan basisadministraties zoals de BRP of magistrale gegevens. Hier hangen rechten van burgers aan. Wil je die wel in een publieke cloud zetten, waar je minder grip op hebt?"

Een overheidscloud zou ook een ander issue oplossen, meent hij. "Door de verplichte aanbestedingstrajecten lijken we soms wel een verhuisbedrijf: elke acht jaar pakken we alles in, brengen de data ergens heen en pakken alles weer uit. Een overheidscloud biedt dus niet alleen weerbaarheid maar ook efficiëntie. Als we niet telkens opnieuw aanbestedingen uitzetten, dan besteden we onze tijd en geld slimmer en kunnen we onze toegevoegde waarde voor de maatschappij vergroten. Tegelijkertijd werken we in een soevereine omgeving aan verbetering van onze digitale diensten: een win-win-win situatie kortom."

Wendbare publieke organisaties: sterker door verandering met Agile-werkwijzen

Hoe kunnen overheidsorganisaties wendbaar worden en waarom is dit in de huidige tijd essentieel?



Highlights

- Wendbare overheidsorganisaties proberen niet langer om de toekomst te voorspellen, ze zijn toekomstbestendig georganiseerd.
- Agile werken en 'Agile zijn' zijn nooit een doel op zich. Agile is een middel en het is essentieel dat de overheid dit middel inzet om maatschappelijke waarde te leveren aan inwoners, bedrijven en het maatschappelijk middenveld.
- Agile kan op verschillende niveaus worden toegepast binnen publieke organisaties.
- Agile werken doorbreekt traditionele silo's en stimuleert samenwerking in multidisciplinaire teams.
- Wendbaarheid is de sleutel naar een overheid die sneller, efficiënter en effectiever inspelt op veranderende behoeften.

In een wereld die voortdurend verandert, is het vermogen om je als organisatie snel aan te passen en te reageren op nieuwe uitdagingen cruciaal. Agile methoden bieden een krachtige manier om deze wendbaarheid te bereiken. Maar wat betekent wendbaarheid voor overheidsorganisaties en waarom is het voor overheidsorganisaties in de huidige tijd essentieel om wendbaar te zijn?

Wat betekent 'wendbaar zijn' eigenlijk?

Wanneer druk wordt uitgeoefend op iets kwetsbaars, wordt het zwakker of breekt het zelfs. Vaak worden termen als veerkrachtig, sterk, robuust of flexibel gebruikt om het tegenovergestelde van kwetsbaar te beschrijven, waarbij iets buigt en weer terugkeert naar de oorspronkelijke staat. Echter, terugkeren naar de oorspronkelijke staat is niet het tegenovergestelde van kwetsbaar. Het tegenovergestelde van kwetsbaar is iets dat juist sterker wordt wanneer er kracht of druk op wordt uitgeoefend. Dit noemen we wendbaarheid: wanneer je door verandering floreert, sterker wordt en dit een bron van maatschappelijke waarde wordt.

Wendbare overheidsorganisaties proberen niet langer om de toekomst te voorspellen, ze zijn toekomstbestendig georganiseerd. Hoewel sommige trends bekend zijn, bestaan ook trends die vooralsnog onzichtbaar zijn, deze 'unknown unknowns' zullen ongetwijfeld de toekomst van organisaties vormgeven. Een 'unknown unknowns' verwijst naar risico's of situaties die zo onverwacht zijn dat ze niet in overweging worden genomen omdat we ons er niet van bewust zijn dat ze bestaan. Niemand weet wat de volgende COVID-19 zal zijn, hoe AI onze levens gaat beïnvloeden of wat de impact zal zijn van de oorlog in Oekraïne, maar zekerder dan ooit is dat de maatschappij zich moet voorbereiden op de onvermijdelijke disruptie. Zelfs voor publieke organisaties die denken zich in een stabiele omgeving te bevinden, is het van belang klaar te staan om met deze verstoringen om te gaan.

De vraag die steeds meer overheidsorganisaties zichzelf stellen is: "Hoe kun je deze wendbaarheid

als overheidsorganisatie bereiken?" Agile methoden spelen hierin een essentiële rol. In dit artikel lichten we toe wat Agile inhoudt en hoe het bijdraagt aan wendbaarheid om beleidsmakers en bestuurders de benodigde ondersteuning te bieden.

Hoe een Agile werkwijze publieke organisaties wendbaar maakt

Wendbaarheid vertaalt zich in het Engels als 'agility'. Als reactie op de beperkingen van traditionele projectmanagementmethoden en om in te kunnen spelen op veranderingen in het ICT-landschap, is de Agile-filosofie ontstaan. Het Agile Manifesto, opgesteld in 2001, benoemt vier kernwaarden:

1. Individuen en interacties boven processen en tools;
2. Werkende software boven uitgebreide documentatie;
3. Samenwerking met de klant boven contractonderhandelingen;
4. Reageren op verandering boven het volgen van een plan.

Agile is niet alleen een werkwijze, maar ook een mindset. Inmiddels wordt Agile breder toegepast, zoals in marketing, HR en productontwikkeling.

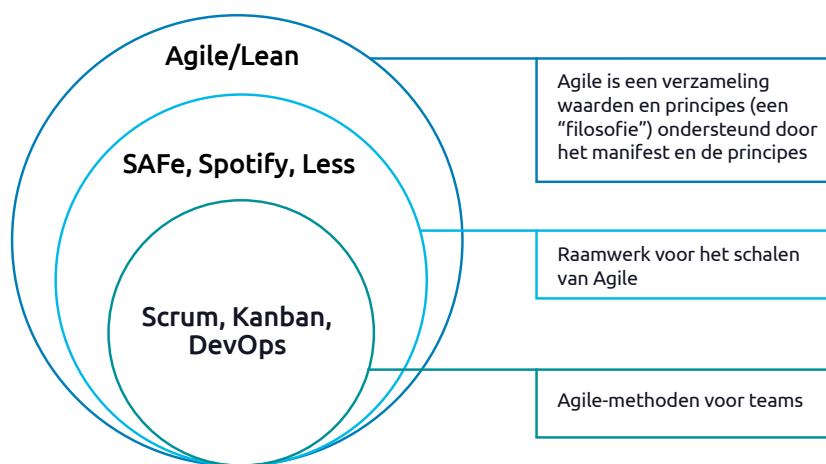
Om effectief en transparant te opereren, moet een overheidsorganisatie voldoen aan strikte wet- en regelgeving en tegelijkertijd flexibel blijven in uitvoering. Door Agile werkwijzen te hanteren, wordt compliance niet langer gezien als een belemmering, maar als een integraal onderdeel van het werkproces. Auditbaarheid, traceerbaarheid en transparantie worden vanaf het begin ingebouwd, waardoor verantwoordingsprocessen efficiënter en minder bureaucratisch verlopen.

Een Agile overheid is waardegedreven, transparant, toegankelijk en wendbaar. Ze behandelt haar inwoners klantvriendelijk en zet deze centraal zonder de waarden van de democratische rechtstaat, zoals rechtvaardigheid, gelijkheid, representatie en participatie, uit het oog te verliezen. Een agile organisatie stelt een helder doel, maar de koers kan onderweg veranderen. De nadruk ligt op flexibiliteit, samenwerking en het leveren van maatschappelijke waarde door werk in iteraties op te delen. Zo werk je met de verwachting dat plannen zullen wijzigen, je omarmt de verandering en richt het proces daarop in. Agile methoden stimuleren teams om in korte cycli te werken, zogenaamde 'sprints', waarbij ze regelmatig feedbackmomenten inbouwen en een continu verbeterproces doorlopen. Dit stelt de teams én hun leidinggevenden in staat snel te reageren op nieuwe inzichten en zich voortdurend te verbeteren. Agile werken en 'Agile zijn' zijn nooit een doel op zich. Agile is een middel en het is essentieel dat de overheid dit middel inzet om maatschappelijke waarde te leveren aan inwoners, bedrijven en het maatschappelijk middenveld.

Agile in de praktijk

Agile kan op verschillende niveaus worden toegepast binnen publieke organisaties. Teams kunnen gebruikmaken van Scrum, Kanban of DevOps voor het dagelijkse werk. Grotere organisaties of programma's met meerdere teams kunnen gebruik maken van Agile frameworks zoals Scaled Agile Framework (SAFe), Spotify-model of LeSS. SAFe is een van de meest gebruikte Agile frameworks in de publieke sector. Aangezien elke organisatie en diens strategische doelen verschillen, wordt het SAFe-framework (of een van de andere frameworks) vaak gebruikt als inspiratie en startpunt en vervolgens aangepast naar eigen context om het tot een succesvolle Agile schaalmethode

te brengen. Binnen de SAFe-omgeving kan Scrum als methode worden toegepast voor onderlinge samenwerking binnen de teams. Kanban is een tool die binnen SAFe- of Scrum-raamwerken kan worden gebruikt, maar ook onafhankelijk buiten deze raamwerken kan functioneren. Kanban is een visueel managementsysteem dat helpt bij het optimaliseren van de workflow door taken te visualiseren.



Hoe zijn de verschillende Agile-methodes en het Agile gedachtegoed met elkaar verbonden?

Afhankelijk van de specifieke behoeften en doelen van elk organisatieniveau kan Agile worden toegepast. Het uitgangspunt blijft altijd het leveren van maatschappelijke waarde, in nauwe samenwerking met inwoners, bedrijven en het maatschappelijke middenveld.

- Op **teamniveau** werken kleine, zelfsturende teams die verantwoordelijk zijn voor het plannen, uitvoeren en leveren van werkende oplossingen in korte iteraties. Door regelmatig feedback te verzamelen en aanpassingen te maken, kunnen teams snel inspelen op veranderingen en continu verbeteren.

- Op **programmaniveau** wordt de samenwerking tussen meerdere teams gecoördineerd om gezamenlijke doelstellingen te bereiken. Dit vereist coördinatie en samenwerking tussen teams om afhankelijkheden te beheren. SAFe biedt een gestructureerde aanpak voor het implementeren van Agile op grote schaal binnen overheidsorganisaties.
- **Agile portfolio management** beheert grote programma's en helpt organisaties flexibel en doelgericht te werken door werk efficiënt te identificeren, prioriteren en beheren voor duurzame waardecreatie. Teams werken zelfstandig binnen deze kaders en kiezen initiatieven met de grootste impact.

Wat levert een wendbare overheid en waardegedreven werken op?

Agile werken doorbreekt traditionele silo's en stimuleert samenwerking in multidisciplinaire teams. Door grote, complexe vraagstukken op te delen in kleinere werkpakketten en regelmatig voortgang te evalueren, kunnen overheidsorganisaties sneller inspelen op maatschappelijke behoeften en efficiënter beslissingen nemen. Dit leidt tot betere afstemming tussen beleidsmakers, uitvoerders en belanghebbenden.

Bij grote en complexe overheidsprogramma's is het essentieel om structuur en coördinatie te behouden zonder aan wendbaarheid in te boeten. Agile biedt hiervoor kaders waarmee teams op verschillende niveaus efficiënt samenwerken. Door middel van flow-gebaseerde werkmodellen, zoals Kanban, wordt werk zichtbaar en beheersbaar, terwijl iteratieve werkwijzen zorgen voor continue voortgang en bijsturing. Dit stelt overheidsorganisaties in staat om omvangrijke systemen en beleidsprogramma's effectiever te managen en sneller tastbare resultaten te leveren.

Tot slot stimuleert Agile een cultuur van continu leren en verbeteren. Besluitvorming wordt steeds vaker gebaseerd op data en meetbare resultaten, waardoor beleid en dienstverlening beter aansluiten op de praktijk. Door regelmatig feedback te verzamelen en te verwerken, wordt niet alleen sneller waarde geleverd, maar blijft de overheid ook adaptief in een steeds veranderende wereld. Het uitgangspunt blijft altijd het leveren van maatschappelijke waarde, in nauwe samenwerking met inwoners, bedrijven en het maatschappelijke middenveld.

Hoe kunnen overheidsorganisaties succesvol transformeren naar wendbaarheid?

Bij Agile transformaties is een flexibele en iteratieve aanpak essentieel, omdat er geen 'one size fits all' oplossing bestaat. Daarnaast helpen iteraties om de Agile mindset goed te embedden binnen organisaties, Agile wordt namelijk geïntroduceerd op een iteratieve (Agile) werkwijze. In plaats van direct een definitieve organisatiestructuur vast te leggen, werk je iteratief toe naar een werkbaar prototype van het toekomstige operationele en organisatie-model. Begin bijvoorbeeld met één afdeling of beleidsdomein en test nieuwe werkwijzen in korte periodes van twee maanden. Elke iteratie levert waarde op voor burgers en biedt ruimte voor verbetering.

Elke iteratie omvat elementen zoals Agile visie, organisatieontwerp, leiderschap, werkwijze, technologie, metrics en cultuur. Organisaties kunnen binnen bepaalde kaders zelf bepalen hoe ze Agile het beste kunnen toepassen op basis van hun dagelijkse werk, waardoor ze leren door te doen en de verstoring van de operatie minimaliseren. Door het prototype stapsgewijs te testen en verfijnen, ontstaat een structuur die beter aansluit bij de behoeften van de organisatie en de maatschappij.

Conclusie

Het geheim van een succesvolle Agile transformatie ligt in klein beginnen en continu leren. Wendbaarheid is de sleutel naar een overheid die sneller, efficiënter en effectiever inspeelt op veranderende behoeften. Elke stap vooruit is winst. Start klein, leer snel en bouw samen aan een toekomstbestendige publieke organisatie.



Over de auteurs



Tom van den Eijnden

Specialist in Agile transformaties en organisatie-inrichting bij Capgemini

Tom heeft een sterke focus op strategische vraagstukken en het creëren van wendbare, toekomstbestendige organisaties.

✉ tom.vanden.eijnden@capgemini.com

in <https://www.linkedin.com/in/tom-vanden-eijnden/>



Linde de Groot

Consultant Organization Purpose & Strategy bij Capgemini Invent

Linde is gespecialiseerd in organisatie inrichting in het publieke domein en richt zich op vraagstukken met betrekking tot nieuwe manieren van werken.

✉ linde.de.groot@capgemini.com

in <https://www.linkedin.com/in/linde-de-groot-09946117b/>



Sophie Hendriks

Consultant Organization Purpose & Strategy bij Capgemini Invent

Sophie is gespecialiseerd in organisatieveranderingen binnen de publieke sector en helpt organisaties met Agile Transformaties.

✉ sophie.hendriks@capgemini.com

in <https://www.linkedin.com/in/sophie-hendriks-3a596619a/>

Bronnen

1. Brochure Potrait
2. © Scaled Agile, Inc Government - Scaled Agile Framework © Scaled Agile, Inc.
3. © Scaled Agile, Inc <https://www.scaledagile.com/enterprise-solutions/enterprise-challenges/>
4. Agile Portfolio Management_Politie.pptx
5. Handreiking Wie A(gile) zegt moet ook B zeggen

Visie op de Shared Service Organisatie van de toekomst

Redt 'Muskiandity' onze Shared Service Organisaties of is er een alternatief?



Highlights

- Het bestaansrecht van de publieke SSO lijkt een vanzelfsprekendheid, maar de doelstellingen worden dikwijls niet bereikt.
- De afgelopen decennia is de digitalisering in de primaire processen sterk toegenomen en ging deze gepaard met een grotere verandersnelheid.
- Aanbeveling 1: aanpassen van het demand-supplymodel om de wendbaarheid en kwaliteit van SSO's te verhogen.
- Aanbeveling 2: omarming van technologie en innovatie voor optimalisatie en schaalvergroting van huidige producten en diensten.
- Aanbeveling 3: een cultuuromslag zowel intern als richting de afnemers voor proactieve en klantcentrale dienstverlening.

In dit artikel zetten we onze visie uiteen voor de SSO van de Toekomst omdat deze de bodem legt voor een efficiënte én wendbare, maar bovenal een betrouwbare, mensgerichte overheid.

“Let that sink in.” Het is 6 november 2024: een X-bericht met een lachende Elon Musk in het Witte Huis, inclusief wasbak, maakt expliciet hoe nauw kopstukken in de techwereld vervlochten zijn met de Amerikaanse politiek. Hoewel het verleidelijk is vooral gefascineerd te raken door het extreme gedrag van Musk, wijzen ook verkiezingen in Nederland (en Europa) op de behoefte aan een hernieuwde overheid.

Ondertussen is Musk op zoek naar ‘super high-IQ small-government revolutionaries willing to work 80+ hours per week on unglamorous cost-cutting’ voor zijn DOGE, The Department of Government Efficiency. Dit Muskiaanse initiatief beoogt president Trump in staat te stellen de overheid te ontdoen van excessieve regulering en organisatieonderdelen te herstructureren. De rode draad binnen de door Musk geleide organisaties is de unificatietheorie. Deze theorie probeert alle fundamentele krachten en componenten te bundelen binnen één samenhangend veld op een zo efficiënt mogelijke manier. In de praktijk betekent dit dat zijn tech-imperium een keten aan organisaties is die functioneel verbonden zijn met gedeelde doelen en operationele afhankelijkheden. Ook publieke Shared Service Organisaties (SSO’s) zijn door de Rijksoverheid in het leven geroepen om verschillende organisatiefuncties te integreren en vormen met hun afnemers en eindgebruikers een samenhangend geheel met als missie: werken aan

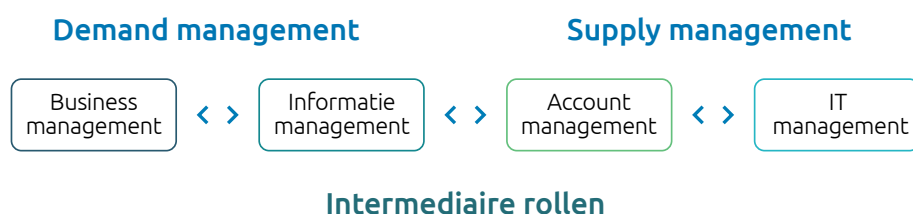
een rechtvaardige, ondernemende en duurzame samenleving.

Door het centraliseren van functies in SSO’s worden taken verminderd, dataduplicatie vermeden en efficiëntie verhoogd. Het bestaansrecht van de publieke SSO lijkt hiermee een vanzelfsprekendheid, maar de doelstellingen worden dikwijls niet bereikt, omdat er onvoldoende aandacht is voor de inrichting en besturing die aan heel specifieke eisen moeten voldoen¹. Dat dit probleem nog steeds actueel is, werd met de Toeslagenaffaire en de Gaswinningsproblematiek weer eens pijnlijk duidelijk.

De oorsprong van de SSO’s

SSO’s zijn oorspronkelijk opgericht om generieke en/of gemeenschappelijke (ICT-) dienstverlening gestandaardiseerd, efficiënt en betrouwbaar te leveren aan meerdere afnemers. In het model van Treacy & Wiersema² lag de nadruk op ‘operational excellence’. Periodiek werd de product-/dienstencatalogus aangevuld of aangepast en werd de verwachte jaarlijkse afname door de verschillende afnemers geprognosticeerd en gebudgetteerd. Het zogenaamde demand-supplymodel vormde hiervoor de basis. De nadruk lag hierbij op het bieden van infrastructurale voorzieningen en dienstverlening gericht op de ondersteunende processen: de bedrijfsvoeringssystemen.

Figuur 1: het traditionele demand-supply model



De impact van digitalisering in de primaire processen

De afgelopen decennia is de digitalisering in de primaire processen sterk toegenomen en ging deze gepaard met een grotere verandernelheid. Veranderingen in de ondersteunende en primaire processen volgen elkaar sneller op en vragen om kortcyclische aanpassingen in de dienstverlening.

Dit heeft impact op de roep naar productlifecyclemanagement³ en innovatie. Bovendien worden tegenwoordig hogere eisen gesteld aan zowel de weerbaarheid (bijvoorbeeld cybersecurity en privacy) als de wendbaarheid.

Het traditionele demand-supplymodel en de inrichting van SSO's met een focus op 'operational excellence' staan hierdoor sterk onder druk. Ze worden beoordeeld als te duur, onvoldoende innovatief en onvoldoende wendbaar. Het volledig verleggen van de focus naar 'customer intimacy' lijkt dan voor de hand te liggen, maar staat op gespannen voet met de beoogde en gewenste efficiëntie van operational excellence. Zie daar de spagaat, onder hoge druk, binnen een web van strikte regelgeving.

Ondanks dat ondergetekenden geen voorstanders zijn van DOGE-methodiek, zijn er wel stappen te zetten om niet ten onder te gaan aan de alternatieven. Commerciële aanbieders zijn immers minder gebonden aan regels, legacy systemen, in de basis competitief en daarmee aantrekkelijk (denk aan het succes van Starlink en SpaceX). Teruggaan in de tijd kan ook: Afnemers nemen de diensten weer in eigen beheer.

Liever kijken we vooruit naar de stappen die gezet kunnen worden richting wendbare en weerbare SSO's in de toekomst:

1. Aanpassen van het demand-supplymodel om de wendbaarheid en kwaliteit van SSO's te verhogen;
2. Omarming van technologie en innovatie voor optimalisatie en schaalvergroting van huidige producten en diensten;
3. Een cultuuromslag zowel intern als richting de afnemers voor proactieve en klantcentrale dienstverlening.

Wat betekent dit in de praktijk?

1. Aanpassen van het demand-supplymodel om de waarde van SSO's te verhogen

Belangrijke opgaven voor SSO's zijn om maatwerk te verminderen, processen en producten te standaardiseren en tegelijkertijd wendbaar te blijven of te worden. In de organisatie en governance zal daarbij duidelijk onderscheid moeten worden gemaakt tussen generieke/gemeenschappelijke en specifieke dienstverlening.

a. Generieke dienstverlening:

Hierbij ligt de nadruk op operational excellence, efficiëntie, betrouwbaarheid en veiligheid. Standaardisatie is van groot belang. In de behoeften van afnemers wordt voorzien met standaard bouwblokken die per afnemer worden gecombineerd in optimale pakketten van dienstverlening (mass customization). Door gedegen productlifecyclemanagement en innovatie wordt deze dienstverlening steeds doorontwikkeld en up-to-date gehouden.

b. Specifieke dienstverlening:

Hierbij ligt de nadruk op customer intimacy, waarbij kennis van de (primaire) processen van de afnemers en wendbaarheid in de dienstverlening centraal staan. Nauwe samenwerking in agile teams is hierbij het meest voor de hand liggend.

In beide gevallen is het traditionele demand-supplymodel niet meer toereikend. Bij generieke en gemeenschappelijke diensten is een hogere mate van wendbaarheid en samenwerking wenselijk, anders dan de jaarlijkse afstemming over aantallen en serviceniveaus.

Specifieke dienstverlening vergt een samenwerkingsmodel zonder de 'intermediaire rollen' van demand(informatie)management en supply(account)management en niet het vooral op eenvoudige, voorspelbare transacties gebaseerde demand-supplymodel.

2. Omarming van Technologie en Innovatie

Technologie en innovatie dienen als integraal onderdeel van de (product) kosten van de dienstverlening te worden gezien in plaats van als apart budget. Dit vraagt om het bespreekbaar maken van de financiële uitdagingen en budgettaire beperkingen, waarmee organisaties in de publieke sector worden geconfronteerd bij het implementeren van nieuwe SSO-technologieën en het up-to-date houden van lifecycle management. Relevante onderwerpen zijn:

- Product life cycle management als integraal onderdeel van de SSO-diensten;
- Technologische vooruitgang: ontdek de nieuwste technologische ontwikkelingen, zoals multi-factor authenticatie (MFA), biometrische verificatie, low/no-code, Gen AI, soevereine cloud en blockchain;
- Bespreek hoe AI SSO's kan verbeteren door de beveiliging te optimaliseren, gebruikerservaringen te personaliseren en identiteitsbeheertaken te automatiseren; toekomstige innovaties: verken toekomstige innovaties en hun mogelijke impact op SSO's in de publieke sector.



3. Cultuuromslag naar Samenwerking en Verantwoordelijkheid

Musk's droom van de mens als 'multiplanetaire' soort is vanzelfsprekend van een andere orde dan sociaal-maatschappelijke vraagstukken in het publieke domein. Al zou het mogelijk zijn om op termijn naar Mars te migreren, er blijven nog voldoende uitdagingen op aarde (bijvoorbeeld eenzaamheid, verslavingsproblematiek) die om meer vragen dan een monomane efficiëntiebenadering. Echter, het komt de wendbaarheid van SSO's ten goede om, in navolging van Musk's gedachtegoed, medewerkers te betrekken bij het stellen van doelen en hen verantwoordelijk te houden voor hun prestaties.

In een recent verbetertraject bij een publieke SSO, met als vertrekpunt het verbeteren van processen, kregen wij door kwalitatieve interviews met medewerkers en leidinggevendenden inzicht in de onderliggende redenen van suboptimaliteit van processen. Dit had te maken met de 'eilandsjescultuur': een gebrek aan gezamenlijke doelstellingen, of lokaal afwijkende prioriteiten, waardoor eigenaarschap en samenwerking op brede schaal ontbraken. Om de transformatie strategie te ondersteunen, werden vijf cultuurwaarden gedefinieerd: continu leren, verantwoordelijkheid nemen, samenwerken, klantgericht en innovatief. De meerwaarde van dit cultuurtraject zat in het samen verkennen en vaststellen van deze waarden en gedragingen met directie, teamleiders en hun teams. Door in co-creatie op organisatie-, leiderschaps- en teamniveau gedrag te definiëren, ontstond draagvlak voor de verandering en werd het concreet hoe dit tot leven komt op de werkvloer. Ook aan de behoefte van medewerkers om zich meer verbonden te voelen met de directie kon door dialoogsessies over 'wie we zijn' en 'wat de transformatie voor ons betekent' worden voldaan. Een ander belangrijk onderdeel is

het normaliseren van feedback op gedrag en resultaat. Niet alleen formeel met KPI's die tweejaarlijks in een 1-op-1 met de teamleider besproken worden, maar als nieuw normaal waarbij het uiteindelijke doel is dat een werknemer zelf in staat is het eigen werk en dat van het team op kwaliteit en prioriteit te beoordelen. Tenslotte is het interessant om te benoemen dat het idee dat efficiëntie en samenwerken op gespannen voet staan in dit project werd ontkracht. Sterker nog, door inzicht in capaciteit en manieren van werken wordt het potentieel van mens en middelen beter benut en kan verbetering plaatsvinden. Bovenstaande benadering zorgt ervoor dat er, met enige verandermanagementondersteuning, op organische wijze feedbackloops ontstaan tussen organisatieonderdelen. Door het doorbreken van de 'eilandsjescultuur' kunnen aanbevelingen voor standaardisatie en capaciteitsplanning bottom-up worden aangedragen en geïmplementeerd waarbij het onderling vertrouwen en lerend vermogen van medewerkers wordt gestimuleerd. Deze cultuuromslag werkt van binnen naar buiten en is de basis die nodig is voor schaalvergroting en klantgerichte innovatie dienstverlening.

Conclusie

SSO's kunnen nog steeds van grote waarde zijn voor de publieke dienstverlening in de publieke sector. De steeds sneller opvolgende veranderingen en technologische ontwikkelingen vragen echter wel om aanpassingen in de besturing (het demand-supplymodel is achterhaald), de inzet van technologie en de cultuur. In essentie vraagt dit om een hybride benadering met een goede balans tussen operational excellence en customer intimacy. Een dergelijk hybride model vraagt iets van SSO's in de toekomst en ze hebben zich dan ook hierop aan te passen/in te richten, niet alleen op de harde kant (technologie processen/organisatie), maar juist ook in hun cultuur en manier van werken. Door dit te doen blijven SSO relevant en in staat om toegevoegde waarde leveren aan hun klanten tegen een concurrerende prijs en worden ook de beloftes van het huidige kabinet: 'Hoop, Lef en Trots', waargemaakt.

Over de auteurs



Ernest-Jan Mutsaers

Vice President Public Sector bij Capgemini Invent

Ernest-Jan is een ervaren professional op het gebied van digitale transformatie. Ernest-Jan heeft meer dan 35 jaar ervaring in het leiden van grote (digitale) transformatieprojecten. Hij heeft ervaring opgedaan in verschillende sectoren (telecom, transport & logistiek, financiële dienstverlening), maar de laatste 12 jaar volledige focus op de Publieke Sector.

✉ ernest-jan.mutsaers@capgemini.com

in <https://www.linkedin.com/in/ejmutsaers/>



Eline Tan

Senior Manager Program and Change Acceleration bij Capgemini Invent

Eline is een consultant met meer dan 8 jaar ervaring op het gebied van People Analytics, Digital & Culture Transformation en DEI. Eline is gespecialiseerd in het ontwerpen van veranderprogramma's en het begeleiden van leidinggevenden en veranderinitiatieven gedurende impactvolle verandertrajecten bij SSO's en IT-onderdelen in het Publieke Domein.

✉ eline.a.tan@capgemini.com

in <https://www.linkedin.com/in/eline-van-der-mech%C3%A9-tan-b453367b/>



Sjoerd Ruitenbeek

Senior Director | Hoofd van Organization bij Capgemini Invent

Sjoerd heeft 18 jaar ervaring in het leiden van (digitale) organisatie transformaties in de publieke sector. In de afgelopen jaren begeleidde hij meerdere publieke SSO's in hun transformatie. Bij Capgemini is Sjoerd verantwoordelijk voor een team van professionals die zich bezig houden met organisatie strategie, inrichting en verandering.

✉ sjoerd.ruitenbeek@capgemini.com

in <https://www.linkedin.com/in/sjoerd-ruitenbeek-5573434/>

Bronnen

1. Willems F., Opheij W. Shared Service Centers: balanceren tussen pracht en praal, Holland Management Rev. 2004.
2. Treacy M, Wiersema F. Customer intimacy and other value disciplines. Harv Bus Rev. 1993.
3. Betreft een optimale inrichting van het proces van het verkrijgen, implementeren, beheren, onderhouden en uitfaseren/vervangen van (digitale) IT middelen. Het gaat om de gehele levenscyclus van de IT middelen, om ervoor te zorgen dat deze up-to-date blijven en niet tot legacy verworden.

Samenwerken in ecosystemen: een sleutel tot wendbaarheid

Waarom is samenwerking in ecosystemen essentieel voor het aanpakken van complexe maatschappelijke uitdagingen?

Highlights

- Specialisatie vereist samenwerking: De toenemende specialisatie binnen disciplines maakt samenwerking essentieel om silo's te doorbreken en complexe maatschappelijke uitdagingen aan te pakken.¹
- Ecosystemen versterken wendbaarheid: Samenwerking in ecosystemen biedt flexibiliteit en innovatiekracht, waardoor we beter kunnen inspelen op veranderende omstandigheden en nieuwe kansen.²
- Publieke instellingen als katalysator: Door beleid en infrastructuur te faciliteren, kunnen publieke instellingen samenwerking stimuleren en bijdragen aan een wendbare en duurzame samenleving.³



Vandaag de dag staan we voor immense uitdagingen – van klimaatverandering tot digitalisering – die geen enkele partij alleen kan oplossen. Toch werken we vaak in hokjes en missen we de kracht van samenwerking. Hoe kunnen we, net als Leonardo, silo's doorbreken en innovatie stimuleren?

Homo universalis

Leonardo da Vinci, de ultieme homo universalis, is een van de meest iconische voorbeelden van veelzijdigheid en verbinding. Hij combineerde wetenschap, kunst, technologie en natuur in zijn werk, waardoor hij grenzen tussen disciplines overbrugde en innovatieve oplossingen kon creëren. Zijn benadering laat zien hoe waardevol het is om vanuit een breed perspectief te denken en te handelen. Deze gedachtegang staat in schril contrast met de steeds verder gaande specialisatie van mensen en instituties in onze huidige tijd.

De uitdaging van specialisatie

Waar Leonardo da Vinci excelleerde in het verbinden van verschillende disciplines, zien we tegenwoordig een versnippering van kennis en vaardigheden. Specialisatie heeft ontegenzeggelijk voordelen – het leidt tot diepere expertise en innovatieve oplossingen binnen specifieke domeinen – maar kan ook silo's creëren die samenwerking bemoeilijken.

Deze specialisatie vraagt om samenwerking, zeker in het licht van de grote uitdagingen van vandaag. De grote maatschappelijke vraagstukken – zoals klimaatverandering, ongelijkheid en digitalisering – vereisen een integrale aanpak waarin de krachten van verschillende disciplines en actoren worden gebundeld. Dit kan door het stimuleren van multidisciplinaire teams, het integreren van verschillende perspectieven in beleidsvorming, en het creëren van platforms waar diverse partijen elkaar kunnen ontmoeten en van elkaar kunnen leren. Publieke instellingen spelen hierbij een sleutelrol door deze verbindingen actief te faciliteren.¹

Ecosystemen als model voor samenwerking

Een ecosysteem is meer dan de som der delen. Het bestaat uit een diversiteit aan actoren – bedrijven, overheden, maatschappelijke organisaties, kennisinstellingen en burgers – die elkaar wederzijds versterken. Door samenwerking in ecosystemen kunnen we complexe vraagstukken zoals klimaatverandering, sociale ongelijkheid en digitalisering beter aanpakken.

Net zoals in de natuur speelt elk organisme een unieke rol binnen een ecosysteem, dragen organisaties en individuen bij aan de wendbaarheid en innovatiekracht van het geheel. Maar dat vraagt wel om een gedeeld doel, duidelijke spelregels en een cultuur van vertrouwen.²

Waarom samenwerken in ecosystemen cruciaal is

De wereld wordt steeds complexer en meer verweven. Publieke instellingen en maatschappelijke organisaties staan voor uitdagingen die geen enkele partij alleen kan oplossen. Denk bijvoorbeeld aan de energietransitie, die vraagt om technologische innovatie, gedragsverandering en beleidsvorming op lokaal, nationaal en internationaal niveau. Samenwerking in ecosystemen biedt hier oplossingen door de unieke sterke punten van verschillende partners te combineren.

Een concreet voorbeeld is de Nederlandse aanpak van de energietransitie, waarbij diverse actoren – van overheid en bedrijven tot kennisinstellingen en burgers – samenwerken in regionale energieagenda's. In deze ecosystemen worden oplossingen zoals het ontwikkelen van waterstofinfrastructuur, wind- en zonneparken en energiebesparende

maatregelen gezamenlijk opgepakt. Zo werken gemeenten samen met bedrijven aan innovaties zoals slimme netwerken om energie efficiënter te verdelen, terwijl burgerinitiatieven helpen om bewustwording en draagvlak te vergroten. Deze gezamenlijke aanpak zorgt niet alleen voor technologische vooruitgang, maar maakt het proces ook flexibel genoeg om in te spelen op nieuwe wet- en regelgeving of maatschappelijke behoeften.³ Cruciaal hierbij is een consistent overheidsbeleid. Samenwerking in ecosystemen heeft baat bij lange termijn zekerheid en duidelijke kaders. Beleidswijzigingen die ingrijpende veranderingen teweegbrengen, zoals het schrappen van de Regionale Energiestrategieën (RES) na 2030, kunnen juist averechts werken. Ze creëren onzekerheid, ondermijnen investeringsbeslissingen en belemmeren voortgang in samenwerkingsverbanden. Een stabiele koers is essentieel om partijen te motiveren en te zorgen voor een duurzame en effectieve energietransitie.

Een belangrijk voordeel van ecosystemen is hun wendbaarheid. Net zoals natuurlijke ecosystemen zich aanpassen aan veranderingen, kunnen samenwerkingsverbanden flexibel inspelen op nieuwe omstandigheden. Dit maakt ze beter in staat om te innoveren en proactief te reageren op nieuwe kansen en uitdagingen.⁴ Voor individuele organisaties en bedrijven is deelname aan een ecosysteem eveneens van strategisch belang. Door actief samen te werken binnen een netwerk van diverse partners, krijgen zij sneller toegang tot nieuwe kennis, technologieën en marktkansen. Bovendien maakt

het hen veerkrachtiger in een veranderende wereld, doordat ze sneller kunnen schakelen en inspelen op ontwikkelingen in beleid, markttrends en maatschappelijke behoeften. Wendbaarheid is niet alleen een eigenschap van het geheel, maar ook een concurrentievoordeel voor de deelnemende partijen zelf.

Publieke instellingen in het ecosysteem

Publieke instellingen hebben een cruciale rol als katalysator in ecosystemen. Ze kunnen randvoorwaarden scheppen door beleid, financiering en infrastructuur te bieden die samenwerking bevorderen. Tegelijkertijd moeten ze zichzelf openstellen voor input van buitenaf en hun traditionele hiërarchische structuren transformeren naar meer netwerkgerichte werkwijzen.

Een mooi voorbeeld hiervan is de samenwerking tussen gemeenten, bedrijven en bewoners in de wijkgerichte aanpak van verduurzaming. Hierin wordt niet alleen gekeken naar technische oplossingen zoals isolatie en zonnepanelen, maar ook naar sociale cohesie en eigenaarschap van bewoners. Dit soort integrale benaderingen versterkt de wendbaarheid van samenwerkingen.⁵

Daarnaast tonen sectorale netwerken binnen woon-, wijk-, zorg- en energiecoöperaties aan hoe publieke instellingen burgerinitiatieven kunnen versterken. In Rotterdam zijn bijvoorbeeld in de wijken Vreewijk en Afrikaanderwijk coöperaties van wijkbewoners ontstaan die diensten in groenbeheer, schoonmaak en andere gebieden leveren. Door

opdrachten niet langer uit te besteden maar zelf uit te voeren, worden werk en middelen in de wijk gehouden. Deze initiatieven benaderen de gemeente als samenwerkingspartner, wat leidt tot betere oplossingen en versterkte sociale cohesie.

Een ander voorbeeld is het mogelijk maken van energiehubbs. Een energiehub (e-hub) is een lokale samenwerking tussen meerdere partijen op het gebied van energie. Opwekkers én verbruikers werken samen bij het opwekken, verhandelen, consumeren en/of opslaan van energie en zorgen hiermee dat het lokale energienet efficiënter wordt benut. Zij halen hiermee een economisch of sociaal rendement. Door de vraag naar en het aanbod van energie lokaal af te stemmen, is er minder transportcapaciteit van het elektriciteitsnet nodig. Dit zorgt voor minder belasting van het net en kan ruimte vrijmaken voor groei of verduurzaming.⁶

Deze voorbeelden illustreren hoe publieke instellingen, door actief deel te nemen en samen te werken binnen netwerken, de effectiviteit en wendbaarheid van ecosystemen kunnen vergroten.



Conclusie

Leonardo da Vinci inspireert ons om verder te kijken dan onze eigen grenzen en de kracht van verbinding te omarmen. Samenwerking in ecosystemen biedt een model voor de wendbare en innovatieve samenleving van de toekomst. Door diversiteit en samenwerking centraal te stellen, kunnen publieke instellingen en maatschappelijke organisaties niet alleen effectiever inspelen op complexe uitdagingen, maar ook bijdragen aan een duurzamere en rechtvaardigere wereld.

Net zoals Leonardo een pionier was in het verbinden van werelden, kunnen wij vandaag de dag pionieren in het bouwen van ecosystemen die ons helpen om gezamenlijk vooruitgang te boeken en oplossingen te formuleren voor complexe maatschappelijke vraagstukken. Laten we die uitdaging samen aangaan.

Over de auteurs



Tom van den Nieuwenhuijzen

Director Sustainability, Strategy and Innovation Public Sector bij Capgemini Invent

Tom is werkzaam als Director Sustainability, Strategy en Innovation en werkt als Global Lead Sustainability Public Sector voor de Capgemini Group. Tom adviseert en ondersteunt publieke organisaties op het gebied van duurzaamheid, (bestuurlijke-, proces- en democratische-) innovatievraagstukken en complexe politiek-maatschappelijke opgaven.

 tom.vanden.nieuwenhuijzen@capgemini.com

 <https://www.linkedin.com/in/tomvandennieuwenhuijzen/>



Dennis Kersten

Director Energy Transition & Utilities bij Capgemini Invent

Dennis is werkzaam als director binnen de marketunit Energy Transition & Utilities. Dennis adviseert, ondersteunt en verbindt private en publieke organisaties op het gebied van de energietransitie, de (organisatorische, compliance en technische) uitdagingen en de nieuwe commerciële kansen en businessmodellen die daarmee samenhangen.

 dennis.kersten@capgemini.com

 <https://www.linkedin.com/in/denniskersten77/>

Bronnen

1. Gibbons, M., Limoges, C., Nowotny, H., et al. (1994). *The New Production of Knowledge: The Dynamics of Science and Research in Contemporary Societies*. Sage Publications.
2. Folke, C., Carpenter, S. R., Walker, B., et al. (2010). "Resilience Thinking: Integrating Resilience, Adaptability and Transformability." *Ecology and Society*, 15(4).
3. Energie Nederland. (2021). "Samen werken aan een duurzame toekomst: Regionale Energie Strategieën in de praktijk."
4. Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press.
5. Moore, M.-L., & Westley, F. R. (2011). "Surmountable Chasms: Networks and Social Innovation for Resilient Systems." *Ecology and Society*, 16(1).
6. TenneT (2025). <https://www.tennet.eu/nl/energiehubs>

Hoe ontsnap je aan de wurggreep van legacy-systemen?

Hoe ga je als overheidsorganisatie om met de structurele worsteling omtrent legacy-systemen?



Highlights

- Wat legacy is, is relatief: Een mainframe met Cobol-software uit de jaren '70 of '80 laat zich terecht omschrijven als 'legacy', maar veel .net of Java-applicaties van 10 of 15 jaar oud zijn dat in feite ook.¹
- De dilemma's omtrent legacy spelen bij nagenoeg alle overheidsorganisaties: Toren hoge beheerkosten (de zogenaamde 'technische schuld'), beveiligingsproblemen en ontevredenheid onder gebruikers zijn bekende thema's.²
- Er is licht aan het einde van de tunnel: GenAI, Robotic Process Automation, maar vooral ook het toepassen van het 'Strangler Pattern' en levenscyclusedenken zijn zaken die helpen bij het stapsgewijs oplossen van de wurggreep.³

Vaak wordt vastgehouden aan legacy-systemen onder het motto 'als het niet kapot is, repareer het dan niet'. In dit artikel geven we duiding aan dit voor veel overheidsorganisaties herkenbare fenomeen.

Wat verstaan we onder legacy-systemen?

Wat legacy is, is relatief. ICT ontwikkelt zich in 'generaties'. Een mainframe met Cobol-software uit de jaren '70 of '80 laat zich terecht omschrijven als 'legacy'.

Maar veel .net of Java-applicaties van 10 of 15 jaar oud zijn dat in feite ook. Wordt het vinden van de juiste mensen om iets te onderhouden moeilijker? Of bevatten systemen niet vervangbare componenten waar geen upgrades meer voor komen, geen support meer op is en dus ook geen security garanties voor zijn? Dan is er in onze ogen ook sprake van legacy.

Legacy ontstaat door ouderdom van systemen, plus onvoldoende aandacht voor onderhoud. Het is gemakkelijk om te beknibbelen op onderhoud, maar op den duur leidt dat tot onvoorziene en grote niet zo zichtbare kosten.¹

Wetenswaardigheden en uitdagingen legacy-systemen

Wij herkennen een aantal wetenswaardigheden en uitdagingen die gelden voor legacy-systemen (los van de ouderdom ervan). Deze geven we hieronder weer.

Operationele inefficiëntie: tijd en middelen verspillen aan verouderde technologie

Een van de belangrijkste nadelen van legacy-systemen is dat ze traag zijn voor gebruikers. Vooral in vergelijking met AI-gestuurde oplossingen. Legacy-applicaties gaan vaak samen met tijdrovende procedures en vereisen handmatige gegevensinvoer. Bovendien is hun automatiseringspotentieel enigszins beperkt, dus je hebt geen andere keuze dan tijd en energie te verspillen aan zelfs de meest eenvoudige taken.

Volgens onderzoek van Harvard Business Review¹ blijkt dat een enkele werknemer dagelijks ongeveer 350 keer tussen 22 verschillende applicaties schakelt als gevolg van de inefficiëntie van verouderde systemen. Dit resulteert in een verminderde productiviteit en een stijging van de productiekosten.

Met Robotic Proces Automation (RPA) is daar veel aan te doen. Dit zijn bots die het handmatige invoerwerk nadoen en stappen in dat proces met elkaar verbinden. Deze bots werken 24x7 en maken nooit fouten. De AI-revolutie maakt dat de mogelijkheden op dit gebied snel groeien. Het haalt efficiëntieproblemen weg, maar verandert weinig aan de structurele situatie of de security daarvan.

Onderhouds- en ondersteuningskosten

Volgens een onderzoek van Atera² besteden IT-afdelingen tot 80% van hun budget aan doorlopend onderhoud van legacy-systemen (en dit aantal groeit jaarlijks). Deze kosten variëren qua tijd en het geld dat nodig is voor onderhoud en upgradevereisten tot de financiële risico's die worden veroorzaakt door verouderde beveiligingsprotocollen en onjuiste managementrapportage. CTO's noemen als een van de belangrijkste problemen de 'technische schuld' - bijna 60% van de door Forrester ondervraagde CTO's in de financiële dienstverlening³ zegt dat hun legacy tech-stack te duur en ontoereikend is voor moderne applicaties.

Bovendien vereist het onderhoud van legacy-applicaties experts met unieke vaardigheden, maar naarmate het gebruik van technologie afneemt en deze vaardigheden verouderd raken, wordt de pool van beschikbaar talent elk jaar kleiner. Bedrijven moeten

mensen met deze vaardigheden in dienst blijven nemen of zowel nieuwe als huidige werknemers bijscholen om deze competenties te behouden. Juist omdat de specialisten die er nog wel zijn er belang bij hebben tot hun pensioen dat werk te blijven doen, zijn er op dit gebied vaak veel grotere verborgen kosten en risico's dan inzichtelijk.

Beveiligingsrisico's: verborgen kwetsbaarheden in legacy-systemen

Legacy-systemen brengen veelal ernstige beveiligingsproblemen met zich mee, zeker voor wat betreft datalekken. Uit een IBM-onderzoek⁴ blijkt dat de gemiddelde kosten van een datalek 4,88 miljoen dollar bedragen en naar verwachting zullen blijven groeien. Ook leidt dit tot aanzienlijke reputatieschade en een daling van het klantvertrouwen.

Bovendien zijn verouderde systemen vaak vatbaarder voor beveiligingsrisico's zoals malware

en datalekken. Het is namelijk goed mogelijk dat ze niet zijn gebouwd met hedendaagse beveiligingsmaatregelen in gedachten, waardoor ze kwetsbaar zijn voor aanvallen of niet in staat zijn om ze te herkennen.⁵ Legacy-systemen kunnen bijvoorbeeld on gepaste authenticatieprocedures hebben omdat wachtwoordbeveiliging en coderingstechnieken in de loop van de tijd zijn geëvolueerd.

Impact op innovatie en groei: legacy-systemen als barrières voor vooruitgang

Een organisatie kan eronder lijden als haar technologie de huidige snelheid van digitalisering niet kan bijhouden. Kansen voor hogere productiviteit, betere klantervaringen en nieuwe inkomstenstromen worden misgelopen wanneer verouderde technologie gebruikt blijft worden. Deze hobbel om te moderniseren leidt tot een verlies aan concurrentievoordeel, waardoor innovatie wordt bemoeilijkt en de algehele marktrelevantie afneemt.

Bovendien kunnen legacy-systemen alle innovaties nauwelijks aan. Hierdoor kunnen er geen nieuwe functies en functionaliteiten voor producten of interne workflow worden geïmplementeerd, wat een aanzienlijk obstakel voor wendbaarheid wordt. Deze starheid kan creativiteit verstikken en het een uitdaging maken om nieuwe goederen en diensten te creëren of reeds bestaande goederen en diensten te verbeteren.

Klant- en medewerkerservaring: concurrentievoordeel verliezen

Het hebben van toegankelijke en functionele systemen is cruciaal waar het gaat om het bieden van een positieve gebruikerservaring.

De klant- en medewerkerservaring kan nadelig worden beïnvloed door legacy-systemen.



Frustratie en ontevredenheid kunnen het kunnen het gevolg zijn van trage en verouderde gebruikersinterfaces, beperkte online functionaliteit en uitdagingen bij de integratie met hedendaagse technologieën.⁶

Hoe te ontsnappen aan de wurggreep?

Het lijkt verleidelijk om met een groot plan in één keer een legacy-systeem te vervangen. Bij vrijwel ieder legacy-systeem is dat minstens al één en vaak wel twee of drie keer geprobeerd. Hoe vaker zo'n groot project misgaat, hoe moeilijker het wordt de organisatie te bewegen om het nog een keer te proberen. Het zijn vaak kostbare mislukkingen. Het is ook waar dat we alles wat goed gaat, te vaak als gewoon beschouwen en ons erg druk maken over mislukkingen. Dit neemt niet weg dat het Rijks ICT Dashboard⁶ meestal niet zo'n vrolijkstemmend beeld oplevert. Een van de redenen is dat zo'n grootschalige legacy-vervanging onherroepelijk lang duurt. Ten tweede leidt het vaak tot een 'big bang' van oud naar nieuw, of een langere periode van parallel draaien van oud en nieuw. Beide zijn moeilijk. Niet alleen technisch, maar vooral ook om gebruikers mee te krijgen. Klassiek is de vraag of je een legacy systeem 'as is' moet vervangen, of dat je intussen ook functionele verbeteringen, dingen die de business en de gebruikers graag willen, moet doorvoeren. Als je dat niet doet, gaat het sneller en is het makkelijker om te checken of het nieuwe systeem hetzelfde doet als het oude. Minder risicovol in de overgang. Maar omdat het lang duurt is er altijd toenemende druk om toch tegelijk wijzigingen door te voeren.

Is een alternatief in kleine stappen mogelijk? Technisch kan er altijd erg veel, er zijn altijd wel technische scenario's om het in stapjes te doen. Je kunt beginnen met RPA. Je kunt het zogeheten 'strangler pattern'

toepassen⁷. Het legacy systeem wordt uitgebreid met moderne stukjes code en voorzieningen er omheen totdat het geheel 'ingepakt' is en steeds meer van de input en de output via deze schil gaat. Dit ontkoppelt de gebruikers van de legacy. Daarna kun je de legacy zelf gaan vervangen, zo mogelijk in delen. Het voorkomt dat de organisatorische kant de technische kant gevangen houdt, en omgekeerd.

Maar, organisatorisch en qua veranderproces is de aanpak in kleine stappen moeilijker dan je zou denken. Als er grote afstand is tussen de ICT-afdeling die de legacy beheert en de business die nodig is om de stappen goed te bepalen en te implementeren is het geen haalbare weg. De reden dat er vaak voor grote veranderprogramma's wordt gekozen, is dat er vaak ook organisatorische problemen moeten worden opgelost rondom de legacy transformatie. Ook al is ieder stapje kleiner, het gehele veranderproces blijft lang en kan zelfs langer zijn dan de duur die aan de start van een grootscheepse aanpak wordt verwacht. Een grootscheepse aanpak brengt ook de voordelen – en schijnbare voordelen – van een veranderproces met zich mee.

Ook in financieel opzicht is een groot veranderprogramma met eigen budget naast de bestaande 'legacy' budgetten vaak in eerste instantie aantrekkelijker. Maar al te vaak creëert het echter perverse prikkels. De legacy-organisatie heeft er belang bij zo lang mogelijk het bestaande legacy budget op te maken, de programma organisatie zal hoe dan ook het programma-budget opmaken. Vertragingen worden meteen duur, want leiden tot langer dan geplande dubbele kosten.

Zoals bij veel dingen is de vraag of de AI-ontwikkelingen dit veranderen relevant maakt. De huidige generatie AI is goed in taal en bijzonder goed in programmeertaal. Zowel de



'taal' van oude legacysystemen als het omzetten naar en testen van een vervangend modern systeem kan sterk worden versneld met AI-hulpmiddelen. Cultureel en organisatorisch staan sommige legacy organisatieonderdelen niet het meest open voor deze aanpak. Maar als de laatste het licht heeft uitgedaan, is het zeker een relevante optie!

Organisaties die levenscyclusdenken dieper in het DNA hebben, zijn veel beter in staat de stapsgewijze aanpak te volgen en daarmee het uit de hand lopen van legacy issues voor te blijven. De DevOps-beweging is een aspect daarvan, maar op organisatorisch gebied wordt er veel meer gevraagd.

Conclusie

Het dilemma rondom legacy-systemen is een herkenbaar probleem voor overheidsorganisaties, met gevolgen voor kosten, beveiliging en innovatie. In plaats van te vertrouwen op risicovolle grootschalige vervangingen, kunnen organisaties profiteren van een gefaseerde aanpak. Het 'Strangler Pattern', GenAI en Robotic Process Automation (RPA) bieden praktische oplossingen om legacy-systemen geleidelijk te moderniseren. Door deze strategieën te omarmen en een cultuur van levenscyclusdenken te bevorderen, kunnen organisaties niet alleen hun huidige uitdagingen overwinnen, maar zijn ze ook voorbereid op de toekomst. De tijd om te handelen is nu.

Over de auteurs



Michael Stoelinga

Chief Architect Public Sector bij Capgemini

Michael geeft binnen Capgemini als Chief Architect Public Sector vorm aan het toepassen van de technologie van vandaag voor betere publieke diensten onder het motto 'beleid is technologie, technologie is beleid!'. Michael verdiept zich daarbij in relevante vraagstukken in de publieke sector en neemt actief deel aan een breed netwerk van in- en externe collega's.

 michael.stoelinga@capgemini.com

 <https://www.linkedin.com/in/mstoelinga/>



Diederik Journée

Senior Manager Program and Change Acceleration bij Capgemini Invent

Diederik is werkzaam als Senior Manager binnen de competence group 'Program & Change Acceleration'. Diederik leidt omvangrijke strategische programma's en projecten op het raakvlak tussen ICT, processen en verandering, zowel in de publieke als private sector en heeft daarnaast ervaring als lijndirecteur en ondernemer.

 diederik.journee@capgemini.com

 <https://www.linkedin.com/in/diederikjournee/>

Bronnen

1. Harvard Business Review 'How Much Time and Energy Do We Waste Toggling Between Applications?' (Augustus 2022)
2. Atera Research: 'Unveiling the hidden costs of legacy IT' (Juli 2024)
3. Forrester's Modern Technology Operations Survey, 2024
4. IBM 'Cost of Data Breach' report, 2024
5. Nationaal Coördinator Terrorismebestrijding en Veiligheid: 'Cybersecuritybeeld Nederland 2024'
6. <https://www.rijksictdashboard.nl/>
7. <https://martinfowler.com/bliki/StranglerFigApplication.html>



2. Personele wendbaarheid

Bekleedt er al 33 jaar diverse functies. "Ons werk vereist vaak een langdurige inzet. Dat is nu een uitdaging: mensen willen graag varen, maar niet meer langere tijd van huis zijn."

Interview



De 5.0-wal keert het schip

Hoe de Marine (sinds 1488) zich aanpast aan Society 5.0 - Commandeur Carolien Verberne, directeur Personeel en Organisatie

Werkgevers moeten zich aanpassen aan een nieuwe generatie medewerkers met veranderende verwachtingen. Dat geldt ook voor het oudste onderdeel van de Nederlandse defensie: de Koninklijke Marine. Commandeur Carolien Verberne is directeur Personeel en Organisatie en

Verberne ziet hoe de Marine zich aanpast aan een nieuwe generatie: "Waar vroeger financiële compensatie voldoende was om personeel te binden, draait het nu meer om werk-privébalans, welzijn en vrijheid. Toen ik in dienst trad gingen mensen rustig een half jaar achter elkaar weg. In de naoorlogse tijd was dat zelfs nog langer. Dat wordt niet meer geaccepteerd, en dat kun je ook met geld niet compenseren. Ook technologie van de laatste decennia, zoals internet en WIFI, verandert de dynamiek aan boord: privékwasties blijven niet langer thuis, maar reizen mee met ons werk. Dat is zeker niet slecht, maar anders."

De Marine is bij uitstek een technische organisatie, verduidelijkt Verberne. "Een schip is een bemenst wapen; technologie is onze basis. De vraag naar technisch opgeleid personeel wordt steeds groter, terwijl de vijver om in te vissen steeds kleiner wordt. De concurrentie is fors. Om aantrekkelijk te blijven voor jong talent, moeten we inspelen op hun waarden en ambities. Want werken bij de Marine is niet meer een 'way of life' zoals vroeger."

Binden van jonge professionals

De Marine heeft haar hoofdbasis in Den Helder. "Niet iedereen wil daar wonen en werken. Ook dat maakt het werven van personeel extra uitdagend. Vooral hoog- en middelbare opgeleiden in schaarse vakgebieden zijn lastig te vinden. Tegelijkertijd is de jonge generatie steeds bewuster bezig met zingeving en de wens om iets goeds te doen voor de wereld. Dat is een mooie ontwikkeling, maar het is onduidelijk in hoeverre de huidige spanningen hen aantrekken of juist afstoten."

Verberne vat de uitdagingen samen: "Hoe boeien en binden we als Marine jonge professionals? Hoe blijven we relevant in een arbeidsmarkt waar flexibiliteit steeds belangrijker worden? De sleutel ligt in ons aanpassingsvermogen. We investeren daarom structureel in een moderne, mensgerichte organisatiecultuur. Dat helpt ons om wendbaar te blijven."

Diversiteit als sleutel

De Marine zet actief in op diversiteit en flexibiliteit. "Wij zijn van oudsher een organisatie van witte mannen," vertelt Verberne, "maar dat verandert. Sinds januari 2017 zijn vrouwen welkom bij de mariniers en sinds januari 2020 bij de onderzeedienst, waar zij voorheen wettelijk waren uitgesloten. Dit is een belangrijke stap, maar er is meer nodig."

Diversiteit gaat niet alleen over man-vrouwverhoudingen of etnische achtergronden, maar ook over instroomleeftijd en afwijkende loopbaantrajecten. "Wij zijn oorspronkelijk een instroomorganisatie waar je jong begint en uitstroomt bij het bereiken van de pensioenleeftijd. Dat is niet langer houdbaar; we moeten veel meer zijinstroom faciliteren. Daarom biedt de Marine steeds meer mogelijkheden voor latere instroom. Daarbij zijn er veel functies voor burgers met relevante expertise."

De focus op diversiteit is belangrijk om een breder publiek aan te spreken, licht ze toe. "We laten in onze werving zien dat de Marine niet per se een masculiene cultuur is. Waar programma's als Special Forces Vips vroeger als wervend werden gezien, blijkt dat sommige kandidaten af te schrikken, waaronder vrouwen. Daarom richten we ons in onze communicatie op een breder beeld. Het gaat niet om fysieke kracht alleen, ook andere vaardigheden en kwaliteiten zijn voor ons essentieel."

Flexibel inzetbaar

Daarnaast is flexibiliteit steeds belangrijker. "Dat geldt vooral voor medewerkers met een gezin", zegt Verberne. "Werk en zorg worden steeds vaker door partners gedeeld. We hebben hier stellen werken die bijvoorbeeld allebei varen als commandant, en dat afwisselen. We proberen daarin maatwerk te leveren en deze drukke fase in ieders carrière te faciliteren. Dit is niet altijd gemakkelijk, zeker bij schaarse functies waar mensen hard nodig zijn. We kijken dan naar oplossingen als walplaatsingen of buitenlandplaatsingen waarbij gezinnen samen kunnen zijn. En we hebben de 180-dagen-van-huis-richtlijn. Als iemand die grens bereikt, gaan we in gesprek. Niet omdat het per se moet, maar om te kijken wat de persoon zelf wil."

Wendbaar werven

Werven en selecteren: ook dat verandert, vertelt Verberne. “Voorheen keken we vanuit de functie: welke mensen zijn daar geschikt voor? Nu denken we ook omgekeerd: iemand toont belangstelling, waar kunnen we die kwijt? We kijken dus naast vaste instroomkanalen en verticale loopbaantrajecten, ook naar zijinstroom en maatwerkopleidingen.”

Tegenwoordig worden ook eerder verworven competenties (EVC) erkend. “Daardoor kunnen we iemand op latere leeftijd binnenhalen. Wat neemt diegene aan ervaring mee en hoe kunnen we dat vertalen naar opleidings- en functie-eisen? Zo kunnen we ervaren talent efficiënter inzetten en opleidingstrajecten verkorten.” Daarnaast is de aanpak bij opleidingsuitval aangepast. “Vroeger vielen mensen af als ze bijvoorbeeld een blessure opliepen of het even moeilijk hadden. Nu krijg je hersteltijd, ga je trainen en mag je opnieuw de opleiding in. We geven mensen een tweede kans, omdat we ze graag behouden.”

Baan wordt maatwerk

Toekomstig maatwerk gaat volgens Verberne nog een stap verder: “We willen mensen eerst een initiële opleiding geven en ze daarna pas laten kiezen voor een vervolgopleiding. Nu maken veel jongeren meteen bij aanvang een keuze voor een dienstvak, maar dat leidt ook tot uitval. Als iemand mag wachten met die keuze, dan kun je op een beter moment de juiste optie aanbieden. Hiermee willen we niet alleen meer jongeren aantrekken, maar kunnen we ze ook beter begeleiden en langer vasthouden.”

Ook de technische werving wordt flexibeler. “We hebben nu een project, ‘TD-er onder één knop’. Als iemand een technische achtergrond heeft en graag bij de Marine wil werken, nemen we diegene alvast aan. Daarna volgt de keuring en bepalen we waar iemand het beste past. En als iemand niet geschikt is voor een militaire functie, dan kijken we of er een plek is in een burgerfunctie.”

Omgekeerde werving

Met een omgekeerde wervingsstrategie kunnen geïnteresseerden sneller instromen en pas later definitief gekeurd worden. Verberne. “Voorheen volgde iemand een lang traject: keuring, selectie,

veiligheidsverklaring – dat kon maanden duren. Tegen de tijd dat diegene klaar was, was de opleiding net begonnen en moest je weer wachten. Jongeren willen niet wachten. Die drukken op de knop en zeggen: ‘Volgende week wil ik in de les zitten.’”

Daarom werkt de Marine nu ook met burger instroompools. “Tegen burgers zeggen we: ‘Kom bij ons werken, we hebben misschien niet direct een vaste plek, maar we willen je graag houden.’ Daarmee verlagen we de drempel voor instroom en zorgen we dat talent niet verloren gaat door bureaucratische vertragingen. Bij burgerinstroompools zit wel een einddatum – drie jaar – en binnen die tijd hopen we iemand een definitieve plek te kunnen bieden.”

Geopolitieke dreigingen

De Marine focuste zich de laatste jaren vooral op Hoofdtak 2 en Hoofdtak 3: het bevorderen van de (internationale) rechtsorde en stabiliteit. Men biedt onder meer hulp bij crisisbeheersingsoperaties, humanitaire hulpoperaties en rampen. Met de huidige geopolitieke spanningen komt er meer aandacht voor Hoofdtak 1: bescherming en verdediging van het Nederlands grondgebied en dat van bondgenoten. Toch doen we dit al bij de marine, meent Verberne. “We werken voortdurend aan bescherming en verdediging. Denk aan onze taken in de Golfregio waar we zorgen voor een veilige doorvaart en het patrouilleren op de Noordzee in verband met onze onderzeese infrastructuur. Hiermee beschermen we direct de Nederlandse economische belangen. Onze status van paraatheid is permanent hoog.”

“Tegelijkertijd realiseren we ons beter dat we op zee ver van huis zijn. Ook Nederland moet weerbaarder worden; onze bewustwording dat het spannend is in de wereld moet omhoog. Dan heb ik het niet alleen om de voorbereiding op het ontberen van stroom, water en energie, maar ook over de beschikbaarheid van onze reservisten. Er is een opkomstplicht in specifieke noodsituaties.; kun je die verplichting wel waarmaken, als je nu bij de politie of brandweer of in een ziekenhuis werkt? Heb je een vitale functie, dan is het zaak om daarover nu over na te denken.”

Data science en AI in strategisch personeelsbeleid

Gaan nieuwe technologieën veel veranderen voor de Marine? Volgens Verberne zijn veel veranderingen al langere tijd aan de gang. “Vroeger werkten zo’n 900 mensen aan boord van een kruiser; tegenwoordig zijn dat er 140 op een gemiddeld fregat. Bij de komende nieuwe generatie schepen wordt dit nog verder gereduceerd tot 120 personen. Met dezelfde oorlogstaken hebben we dus een reductie van meer dan 80% gerealiseerd. Digitalisering zorgt dat een schip meer een ‘verlengde arm’ wordt in oorlogsvoering. Natuurlijk blijven er mensen aan boord nodig maar dat is een kleiner aantal. Veel ondersteunende taken worden inmiddels vanaf de wal uitgevoerd.”

“In mijn eigen vakgebied zie ik mogelijkheden voor meer ‘predictive analytics’. Hoeveel mensen hebben we op welke vakgebieden wanneer nodig? Waar ontstaan de grootste knelpunten? Wanneer zitten we op de top van onze vergrijzing? Binnen vijf tot tien jaar zal een aanzienlijk deel van ons technisch personeel met pensioen gaan. Daar moeten we nu al op anticiperen. Of we zien bijvoorbeeld dat bepaalde groepen sneller uitstromen. Door te analyseren waarom dat gebeurt, kunnen we gericht verbeteringen doorvoeren. Data science en AI worden dan ook steeds belangrijker om personeelsstromen te analyseren en toekomstbestendige beslissingen te nemen.”

Voor de toekomst

Verberne is pas tevreden als er een goedgevulde, parate organisatie staat met het juist opgeleide personeel. “Inclusief schaarste-categorieën. Ik wil dat we aan al onze taken kunnen voldoen, daar ligt mijn opdracht. Het is een prachtige organisatie, dus ik hoop zoveel mogelijk mensen de gelegenheid te geven om dat te kunnen ervaren.”

Het belang van wendbare en weerbare medewerkers in sterk veranderende tijden

Hoe creëer je een personeelsbestand dat klaar is voor de uitdagingen van Society 5.0?



Highlights

- De publieke sector kampt met vergrijzing en gevolgen van arbeidsmarktkrapte, waardoor er problemen ontstaan aan zowel de in- als uitstroomkant van personeel.
- Society 5.0 wacht niet tot personeel goed voorbereid is, maar vraagt nu om proactief handelen.
- Strategische personeelsplanning is een cruciaal middel voor grip op in- en uitstroom.
- Digitale platforms ondersteunen kennisbehoud en strategisch talent management.
- Technologie omarmen vraagt ook sociale innovatie, zoals het skills based benaderen van arbeidspotentieel en het creëren van een cultuur van levenslang leren.

Publieke organisaties moeten hun personeelsstrategie herzien in de snel veranderde wereld van Society 5.0, zodat ze weerbaar en wendbaar genoeg zijn om hun doelstellingen te realiseren.

In een wereld die steeds sneller verandert, staan publieke organisaties voor de opgave om anders om te gaan met hun personeelsstrategie. Onderwerpen als digitalisering en de noodzaak om de burger centraal te stellen hebben grote impact op publieke organisaties en hun medewerkers. Society 5.0, met zijn nadruk op slimme technologie, biedt zowel kansen als uitdagingen voor een doelmatig personeelsbestand. Hoe kunnen publieke organisaties hun aanpassingsvermogen vergroten om niet alleen te overleven, maar ook uit te blinken in deze nieuwe realiteit? We verkennen personeelsstrategieën die publieke organisaties kunnen implementeren om hun personeel effectief in te zetten en te ontwikkelen. Ontdek hoe het omarmen van digitale middelen en een andere (meer flexibele) benaderingswijze de sleutel zijn tot succes in de publieke sector van de toekomst.

Grip op in- en uitstroom met strategische personeelsplanning en kennismangement

De publieke sector kampt met een vergrijzende beroepsbevolking, wat resulteert in de uitstroom van ervaren medewerkers en het verlies van cruciale kennis. Dit verhoogt niet alleen de werkdruk voor de huidige medewerkers, maar beïnvloedt ook de continuïteit van de publieke dienstverlening. Naast de uitstroom wordt de instroom bemoeilijkt door de huidige arbeidsmarktkrapte. Uit cijfers van het Centraal Bureau voor de Statistiek (2024) blijkt dat er eind 2024, 106 vacatures per 100 werklozen openstonden, wat op een hoge arbeidsmarktspanning duidt.¹ De verwachting is dat deze krapte zich ook dit jaar zal voortzetten. De noodzaak wordt gevoeld door publieke organisaties om zich te onderscheiden van andere werkgevers en zo nieuwe medewerkers aan te trekken.

Om deze uitdagingen aan te gaan, is een strategische aanpak op zowel instroom als behoud van medewerkers cruciaal. Strategische personeelsplanning in combinatie met kennismangement zijn middelen die publieke organisaties in kunnen zetten om grip te krijgen op de effecten van de huidige situatie rondom in- en uitstroom. Strategische personeelsplanning is het proces waarbij organisaties hun toekomstige personeelsbehoeften in kaart brengen, zodat ze de juiste mensen met de juiste skills op het juiste moment kunnen inzetten. Dit proces stelt organisaties in staat om proactief in te spelen op verwachte in- en uitstroom door tijdig interventies op te zetten. Daarnaast zorgt gedegen kennismangement ervoor dat de waardevolle kennis van ervaren medewerkers vindbaar wordt vastgelegd en gedeeld, zodat deze behouden blijft voor de organisatie. Dit kan worden gerealiseerd door bijvoorbeeld het implementeren van digitale kennisdelingsplatforms en het creëren van online (AI gedreven) interne opleidingsprogramma's die gericht zijn op kennisoverdracht. Deze digitale leeromgevingen stellen medewerkers in staat om effectief kennis over te dragen en tegelijkertijd in hun eigen tempo nieuwe skills te verwerven.

De combinatie van strategische personeelsplanning en digitaal kennismangement biedt dan ook een dubbele oplossing: het biedt de mogelijkheid om strategisch in te kunnen spelen op de verwachte in- en uitstroom zodat wordt voorzien in de benodigde personeelsbehoefte én het beperkt tegelijkertijd het risico van kennisverlies door uitstroom. Het resultaat hiervan is een personeelsbestand dat wendbaar en weerbaar is voor Society 5.0.

Van traditionele functies naar skills based werken

Een belangrijke verschuiving die momenteel al plaatsvindt, is de overgang naar skills based werken. Hiervan is de verwachting dat dit nog meer onder de aandacht zal komen in de komende jaren. Deze benadering houdt in dat medewerkers worden ingezet op basis van hun capaciteiten, skills en ervaringen, in plaats van op basis van traditionele functies en diploma's. Deze verschuiving stelt publieke organisaties in staat om flexibeler en efficiënter te opereren, doordat medewerkers zich breder kunnen ontwikkelen en daarmee breder inzetbaar zijn en het beschikbare arbeidspotentieel beter wordt benut. Digitalisering speelt hierbij een cruciale rol, aangezien technologie de implementatie van skills based werken vergemakkelijkt en versterkt. Om (digitaal) skills based werken succesvol te implementeren, dienen organisaties een aantal stappen te doorlopen:

1. Functies opsplitsen:

Breek bestaande functies op in specifieke werkpakketten die moeten worden uitgevoerd. Analyseer elk werkpakket zorgvuldig en beschrijf deze in detail, zodat het duidelijk is wat het pakket exact inhoudt, wie verantwoordelijk is voor de uitvoering, en welke (hulp)middelen nodig zijn om het werkpakket effectief en efficiënt te voltooien. Digitale tools kunnen helpen bij het vastleggen en visualiseren van deze pakketten, wat efficiëntie en transparantie vergroot.

2. Skills in kaart brengen: Breng de huidige, maar ook toekomstige skills in kaart die nodig zijn om de werkpakketten, geïdentificeerd in stap 1, succesvol uit te voeren. Dit kan worden gedaan door middel van digitale skill assessments en analyses die rekening houden met de bredere organisatiestrategie.

3. Skillprofielen koppelen:

Op basis van stap 1 en 2 kan worden vastgesteld welke skills vereist zijn om de werkpakketten, voortkomend uit de oorspronkelijke functies, succesvol te vervullen. Koppel hiervoor skillprofielen aan medewerkers, zodat zij aan de juiste werkpakketten kunnen worden toegewezen. Om uniformiteit te waarborgen in de skillprofielen kan je hiervoor een skill framework inzetten, een voorbeeld hiervan is e-CF voor IT gerelateerde profielen. Tot slot kunnen online skillplatforms worden ingezet om inzicht te krijgen in deze skills van medewerkers, zowel voor leidinggevenden als voor de medewerkers zelf. Deze platforms bieden niet alleen een overzicht van de huidige skills, maar ook aanbevelingen voor verdere ontwikkeling. Een waardevol inzicht voor medewerkers, maar ook voor de organisatie als geheel.

4. Continue skill ontwikkeling:

Integreer deze skills based aanpak in een cultuur van levenslang leren. Dit is een omgeving waarin individuen voortdurend worden aangemoedigd en ondersteund om nieuwe skills en kennis te verwerven gedurende hun hele leven. Dit bevordert persoonlijke en professionele groei, innovatie en aanpassingsvermogen binnen organisaties en samenlevingen. Een cultuur van levenslang leren kan onder andere worden gefaciliteerd door flexibele opleidingsprogramma's en digitale tools die medewerkers ondersteunen in hun leertraject.

Leidinggevenden spelen een sleutelrol door leren actief aan te moedigen, ruimte te geven voor groei en het goede voorbeeld te geven. In een tijd waarin technologie en werkmethoden snel evolueren, is het cruciaal dat medewerkers de gelegenheid krijgen om hun skills zelfstandig en regelmatig bij te werken. Hiermee wordt gewaarborgd dat medewerkers voortdurend hun skills kunnen uitbreiden en dat er snel

ingespeeld kan worden op nieuwe ontwikkelingen en trends.

De overgang naar skills based werken draagt bij aan de bredere inzetbaarheid van medewerkers in publieke organisaties. Hierbij is het van belang een organisatiecultuur te creëren waarin medewerkers zich continu en zelfstandig kunnen ontwikkelen. Dit helpt met het kunnen aanpassen van hun skills aan de behoeften van de organisatie en de maatschappij. Het hanteren van een digitale benadering kan dit proces versnellen. Het creëert dan ook wendbare medewerkers die in staat zijn om zich aan te passen aan veranderende omstandigheden.

Technologische impact en de inzet van strategisch talentmanagement

Hoewel de snelheid van technologische ontwikkelingen niets nieuws is, blijft de impact ervan actueel en ingrijpend. De ontwikkelingen volgen elkaar razendsnel op waardoor publieke organisaties voortdurend worden geconfronteerd met de noodzaak om zich aan te passen. Innovaties zoals AI, automatisering en digitale platforms bieden de mogelijkheid om werkprocessen te optimaliseren, maar vereisen tegelijkertijd dat medewerkers zich proactief ontwikkelen en hun skills uitbreiden. Dit houdt in dat publieke organisaties niet alleen moeten investeren in training en ontwikkeling, maar ook in het aantrekken en behouden van talent met de juiste skills en een groei mindset om de omgang met technologie eigen te maken.

Een strategische aanpak op talentmanagement kan handvatten bieden om technologische innovaties optimaal te omarmen en te benutten. Dit proces richt zich op het aantrekken, ontwikkelen en behouden van medewerkers. Zo kan een organisatie bijvoorbeeld door middel van een strategisch leer- en ontwikkelprogramma medewerkers gericht voorbereiden

op de implementatie van nieuwe digitale tools (zoals AI), waardoor zij niet alleen efficiënter werken, maar ook nieuwe skills ontwikkelen die hun inzetbaarheid vergroten.

Tegelijkertijd kunnen technologische innovaties het talentmanagementproces zelf ook verbeteren:

1. Aantrekken van talent:

AI-gestuurde wervingsplatforms en geavanceerde data-analyses helpen om sneller de juiste kandidaten te identificeren en een objectiever en inclusiever selectieproces te faciliteren.

2. Ontwikkelen van medewerkers:

digitale leerplatforms, gepersonaliseerde e-learning en VR-simulaties maken het mogelijk om medewerkers sneller en continu bij te scholen en hun skills af te stemmen op de veranderende eisen van de maatschappij, waaronder dus ook de impact van digitalisering.

3. Behoud van medewerkers:

technologieën zoals HR-analytics, feedback tools en AI-ondersteunde loopbaanplanning kunnen worden ingezet om een gepersonaliseerde

en motiverende werkomgeving te creëren, waarin medewerkers zich gewaardeerd en ondersteund voelen in hun professionele groei.

Deze integratie van technologie in de talentmanagementcyclus is niet alleen een middel om de prestaties van medewerkers te verbeteren, maar ook een belangrijke factor in het aantrekken en behouden van talent. Steeds meer medewerkers zoeken naar organisaties die moderne technologieën en digitale tools aanbieden om hun skills te ontwikkelen en toekomstbestendig te blijven. Organisaties die deze ontwikkelingen negeren, lopen het risico minder aantrekkelijk te worden voor zowel nieuw talent als huidige medewerkers. Zij vrezen dat hun technologische ontwikkeling achterblijft als hun werkgever hen hierin niet ondersteunt. Door technologie strategisch toe te passen binnen alle onderdelen van de talentmanagementcyclus versterken publieke organisaties dan ook hun employer brand en creëren ze een werkomgeving waarin medewerkers zich voorbereid voelen op de toekomst.



Conclusie

Gezien de huidige uitdagingen rondom in- en uitstroom en de impact van technologie zijn de komende jaren cruciaal voor publieke organisaties om het personeelsbestand toekomstbestendig te maken. De tijd om te handelen is dan ook nu. Investeren in mensen, kennis en technologie is de sleutel om niet alleen de uitdagingen van vandaag het hoofd te bieden, maar ook de fundamenten te leggen voor een duurzame en veerkrachtige publieke sector. Strategische personeelsplanning, kennismanagement, skills based werken en talentmanagement zijn effectieve personeelsstrategieën die aan kracht winnen wanneer technologie hierbij wordt ingezet. Door deze noodzakelijke (digitale) personeelsstrategieën door te voeren, kunnen publieke organisaties hun personeelsbestand ('human capital') optimaliseren en tegelijkertijd een waardevolle bijdrage blijven leveren aan de taak waarvoor zij aan de lat staan.

De toekomst vraagt om een proactieve en technologisch gedreven aanpak. Het is nu aan ons allen om deze uitdaging aan te gaan. Door een sterke focus te leggen op continue ontwikkeling van medewerkers met de inzet van digitale tools en platforms kunnen publieke organisaties niet alleen hun personeel beter voorbereiden op de toekomst, maar ook de kwaliteit van de geleverde diensten verbeteren en de maatschappelijke impact op lange termijn vergroten.

Over de auteurs



Jolien Weeda

Head of Workforce Transformation bij Capgemini Invent

Jolien is een resultaat gedreven HR-projectmanager met uitgebreide ervaring in het ontwerpen en implementeren van HR-strategieën en veranderaanpakken in onder andere Nederland en de Verenigde Staten zowel in de publieke als private sector. Onderwerpen waar Jolien zich op richt zijn onder andere strategische personeelsplanning, HR transformaties, leiderschapontwikkeling en verandermanagement.

[✉ jolien.weeda@capgemini.com](mailto:jolien.weeda@capgemini.com)

[in http://www.linkedin.com/in/jolienweeda](http://www.linkedin.com/in/jolienweeda)



Emma Reinders

Consultant Workforce Transformation bij Capgemini Invent

Emma is gespecialiseerd in organisatie- en personeelsvraagstukken met betrekking tot workforce skilling en strategisch talent management.

[✉ emma.reinders@capgemini.com](mailto:emma.reinders@capgemini.com)

[in http://www.linkedin.com/in/emmareinders](http://www.linkedin.com/in/emmareinders)



Megan Tolner

Manager Workforce Transformation bij Capgemini Invent

Megan is gespecialiseerd in transformatie van het personeelsbestand binnen het publieke veiligheidsdomein en richt zich op strategische personeelsplanning, strategisch talent management, en organisatieinrichting.

[✉ megan.tolner@capgemini.com](mailto:megan.tolner@capgemini.com)

[in https://www.linkedin.com/in/megantolner/](https://www.linkedin.com/in/megantolner/)

Bron

1. Centraal Bureau voor de Statistiek. (2024). Spanning op de arbeidsmarkt. Geraadpleegd op 28 januari 2025. <https://www.cbs.nl/nl-nl/visualisaties/dashboard-arbeidsmarkt/spanning-op-de-arbeidsmarkt>

Doorbraak in duurzame inzetbaarheid door Design Thinking

Hoe kan Design Thinking helpen bij de maatschappelijke opgave om werkenden tot hun pensioen duurzaam inzetbaar te laten zijn?



Highlights

- Society 5.0 is nauw verbonden met duurzame inzetbaarheid; een wendbaar arbeidspotentieel is cruciaal om de kansen van de superslimme samenleving te benutten.
- In de praktijk blijft de implementatie van duurzame inzetbaarheid achter, terwijl er veel kennis en instrumenten beschikbaar zijn hiervoor.
- Design Thinking kan ingezet worden om een doorbraak te realiseren. Onderdeel van deze aanpak is het goed leren kennen van de verschillende doelgroepen en het opstellen van klantreizen.
- Deze aanpak helpt om de wereld van werkgevers en werknemers te begrijpen en in te spelen op wat zij nodig hebben om duurzame inzetbaarheid in praktijk te brengen.

De snel veranderende arbeidsmarkt en de toenemende personeelstekorten maken duurzame inzetbaarheid belangrijker dan ooit. Design Thinking kan helpen om te komen tot effectief beleid dat werkgevers en werknemers activeert om daar daadwerkelijk mee aan de slag te gaan.

Het belang van actie op duurzame inzetbaarheid

Het werk en de arbeidsmarkt veranderen. Technologische ontwikkelingen creëren vooruitgang, maar hebben ook grote impact op de toekomst van werk. Banen verdwijnen of veranderen, zo heeft een automonteur door de opkomst van elektrische auto's met een heel andere techniek en werkzaamheden te maken. Ook ontstaan nieuwe banen, zoals Blockchain-ontwikkelaar, Drone piloot, Prompt engineer en AI-ethiekexpert. De platformeconomie is een fenomeen geworden waarbij traditionele arbeidscontracten vaak worden vervangen door flex-contracten, wat zowel kansen (flexibiliteit) als uitdagingen (werkzekerheid) biedt. Het Klimaatakkoord, de energietransitie en het streven naar een circulaire economie vergen andere vormen van produceren en daarmee andere kennis en vaardigheden.

Willen we als samenleving om kunnen gaan met deze ontwikkelingen, dan is het van belang dat organisaties en hun werknemers wendbaar zijn. Dit vraagt om het verder investeren in duurzame inzetbaarheid. Daaronder verstaan we dat werknemers in staat zijn om gedurende hun hele loopbaan competent, productief en gemotiveerd te werken. Een onderdeel hiervan is dat werknemers zich een leven lang ontwikkelen, zodat ze continu nieuwe kennis en vaardigheden opdoen voor het (veranderende) werk. Een ander onderdeel is het creëren van gezonde en veilige arbeidsomstandigheden, zodat werknemers niet ziek worden of uitvallen door het werk.

Duurzame inzetbaarheid is een vraagstuk waar veel partijen bij betrokken zijn. Werknemers kunnen zelf actie nemen om te zorgen dat zij tot hun pensioen competent, gezond en gemotiveerd aan het werk

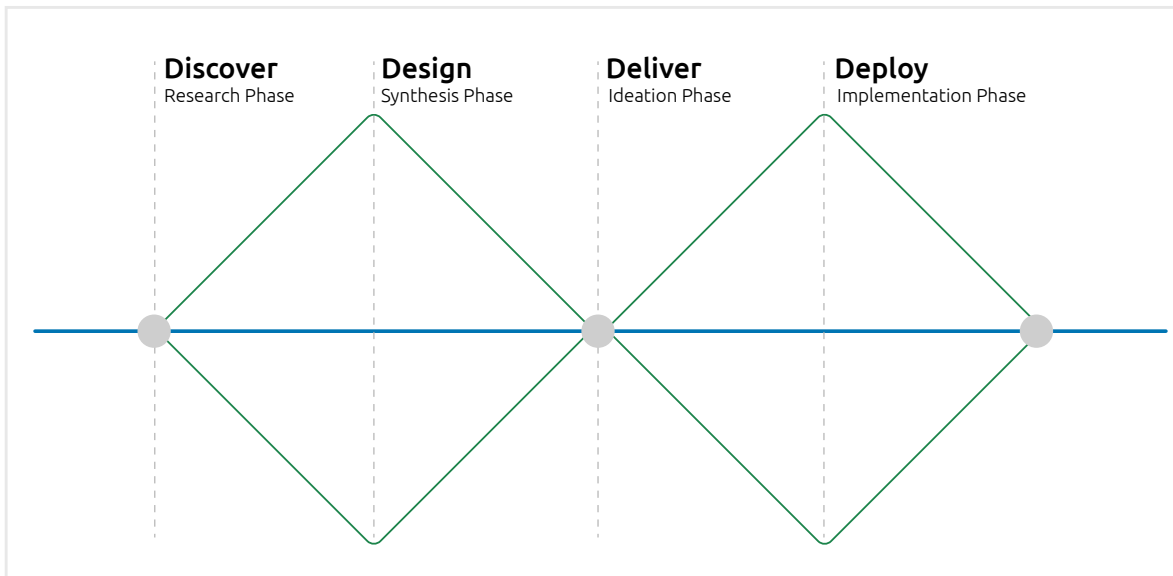
zijn. Wel hebben ze de werkgever hierbij nodig. De werkgever heeft vanuit de Arboregeling een zorgplicht voor gezonde en veilige arbeidsomstandigheden en heeft invloed op de competentieontwikkeling van werknemers. Intermediaire organisaties (zoals sectorale sociale partners) spelen een rol met bijvoorbeeld cao-afspraken, een arbocatalogus, scholingsfaciliteiten en advisering. Ook de overheid heeft een cruciale rol. De overheid stelt kaders (zoals met de Arboregeling), voert stimulerend beleid met publiekscampagnes, en stelt kennis, informatie en subsidies beschikbaar.

Niet alleen werknemers en organisaties hebben belang bij duurzame inzetbaarheid, het is ook maatschappelijk van belang. Duurzame inzetbaarheid draagt bij aan een sterke economie en innovatiekracht, minder arbeidstekorten en mismatch op de arbeidsmarkt, en zorgt voor lagere kosten in zorg en sociale zekerheid. Het is daarom niet voor niets dat de overheid haar rol hierin wil nemen.

De opgave waar we voor staan

Cijfers laten zien dat er nog veel te winnen is op het gebied van duurzame inzetbaarheid. Uit trendonderzoek blijkt dat een leven lang ontwikkelen stagneert, terwijl de huidige (technologische) ontwikkelingen juist extra inspanningen vragen. Scholingsdeelname blijft hangen rond 50% en informeel leren rond 23%, waarbij het percentage werkenden dat aangeeft de technologische ontwikkelingen bij te kunnen benen is gedaald van 70% in 2020 naar 66% in 2024¹. Ten aanzien van gezond en veilig werken geldt dat 36% van de bedrijven niet over preventief arbobeleid beschikt om arbeidsrisico's te voorkomen². Dit terwijl het werk gerelateerd ziekverzuim en aantal arbeidsongevallen nog

The double diamond framework



steeds te groot is. Schattingen gaan uit van 17 miljard euro aan loondoorbetaling over verzuimde uren, 100.000 arbeidsongevallen en 4.000 overlijdens door het werk op jaarbasis³.

Positief is dat er veel kennis en instrumenten beschikbaar zijn op het gebied van duurzame inzetbaarheid, zoals blijkt uit de quickscan die Capgemini heeft uitgevoerd⁴. In de praktijk worden deze kennis en instrumenten echter nog beperkt toegepast. Vaak blijft het beperkt tot pilots en kleinschalige initiatieven. De opgave is om een doorbraak te realiseren zodat werkgevers en werknemers wijdverbreid (verder) aan de slag gaan met duurzame inzetbaarheid.

De kracht van Design Thinking

Design thinking is een mensgerichte, iteratieve aanpak voor probleemoplossing die empathie, samenwerking en experimenteren bevordert. De aanpak is uitermate geschikt om tot opschaling en grotere inzet van beschikbare kennis en instrumenten op duurzame inzetbaarheid te komen. Design Thinking start met

een verkenningsfase en het goed begrijpen van de leefwereld en behoeften van de doelgroep, de eindgebruikers, waarmee het helpt om de menselijke maat terug te brengen in beleidsontwikkeling en publieke dienstverlening.

Bij toepassing van Design Thinking voor het vraagstuk van duurzame inzetbaarheid komt als belangrijk inzicht naar voren dat er grote verschillen bestaan tussen werkgevers in behoeften, context, kennis en uitvoeringskracht. Grote bedrijven hebben vaak specialistische kennis in huis, maar kunnen een uitdaging ervaren in de verbinding met de werkvloer en de werknemers. Kleine bedrijven hebben vaak een sterke verbinding met hun werknemers, maar missen vaak expertise en mankracht.

Is de doelgroep goed in beeld dan richt de verkenningsfase zich op het doel van de doelgroep en de reis daar naar toe. Daarbij wordt gekeken naar kansen en obstakels die weer helpen tot een duidelijke probleemstelling te komen in de vorm van 'Hoe helpen we de doelgroep te komen van waar ze nu staan naar de gewenste toekomst'.

Er zijn verschillende varianten van het Design Thinking proces. Het betreft echter altijd een iteratief proces waarbij verkenning in de praktijk – in het geval van duurzame inzetbaarheid ‘de werkvloer’ – en een duidelijke probleemstelling gevolgd wordt door een idee (ontwerp) fase, een realisatiefase en een uitrolfase. Toepassing in de praktijk kan weer de start van een nieuwe verkenningsfase inluiden. Met de opkomst van het Agile werken is er meer focus gekomen op het snel aan de slag gaan met oplossingen, prototypes bouwen, experimenteren en testen om vervolgens (eerder) te leren en verbeteren. De essentie blijft hetzelfde; vanuit de gebruiker – de verschillende soorten werkgevers – komen tot een duidelijke probleemstelling om vervolgens concrete oplossingen te bedenken, te bouwen en uit te proberen in de praktijk.

Inzichten uit klantreizen

De klantreis geeft belangrijke aangrijpingspunten voor oplossingen, waarbij de verschillen tussen wat werkgevers weten, wat ze kunnen en wat ze nodig hebben aan bod komen. De klantreis wordt opgesteld door met verschillende betrokkenen het gesprek aan te gaan, in de praktijk te gaan observeren en daarmee de wereld van de werkgevers en met name het mkb echt te begrijpen. Hoe ziet hun leefwereld eruit? Wat zijn hun belangrijkste doelen en activiteiten? Waar lopen zij in hun dagelijkse praktijk tegen aan? Hoe is hun beleving daarbij? Waar zitten de pijnpunten? En wat zijn de doorslaggevende momenten waarop het verschil kan worden gemaakt? Inzet van Design Thinking sluit daarbij goed aan op het *Kennis-Houding-Gedrag* model wat veel gebruikt wordt bij veranderingsopgaven in de publieke sector. Het gaat uit van



het belang dat achtereenvolgens de doelgroep kennis neemt van een te maken verandering, een positieve houding ontwikkelt ten aanzien van de verandering en vervolgens ook daadwerkelijk tot ander *gedrag* komt.

De klantreis van de werkgevers begint met een fase van bewustwording en het opdoen van kennis, waarbij ze bekend raken met duurzame inzetbaarheid en de verschillende facetten hiervan. Daarop volgt de fase waarin een houding wordt gevormd ten aanzien van duurzame Inzetbaarheid. Die kan variëren van 'interessant en belangrijk voor mijn bedrijf en medewerkers' tot 'belangrijk, maar niet voor mij', 'wat een onzin' of 'wat een gedoe'. Voor de werkgevers met een positieve houding volgt de beslissende fase; wordt de reis vervolgd en gaat men het daadwerkelijk anders doen... of

niet? Door opvolging zo makkelijk en aantrekkelijk mogelijk te maken neemt de kans op een positief antwoord aanzienlijk toe.

In het toepassen van Design Thinking in werkgeversdienstverlening rondom duurzame inzetbaarheid zijn verschillende praktijkinzichten aan het licht gekomen gekoppeld aan deze drie fasen van verandering:

1. Ten aanzien van *kennis* blijkt het vinden van informatie voor werkgevers een zoektocht door een versnipperde informatievoorziening. Ook sluit de vorm van de informatie vaak niet goed aan op de uitvoeringspraktijk. En waar een onderwerp niet direct de bedrijfscontinuïteit of de primaire bedrijfsprocessen raakt zijn er 'externe' triggers nodig om bekend te raken met het onderwerp.
2. Ten aanzien van *houding* blijkt duurzame inzetbaarheid één van de vele onderwerpen die aandacht vragen van werkgevers (naast cybersecurity, AVG, etc.), terwijl hun beschikbare tijd gering is. Daarnaast is voor werkgevers de toegevoegde waarde ('business case') van het investeren in duurzame inzetbaarheid niet altijd inzichtelijk.
3. Ten aanzien van *gedrag* blijkt dat het in praktijk brengen van duurzame inzetbaarheid als complex wordt ervaren. Informatie en middelen liggen verspreid over verschillende instanties en vergen vaak nog een vertaalslag naar de praktijk. Ook hebben kleine bedrijven beperkte uitvoeringskracht en specifieke praktische behoeften (zoals behoefte aan interactie buiten standaard kantooruren en -dagen) om rekening mee te houden.



Deze inzichten laten zien dat er meer nodig is dan het ontwikkelen van kennis en instrumenten om te komen tot navolging en wijdverbreid gebruik. Hierbij ligt een belangrijk deel van de oplossing niet ligt in de kwaliteit van de inhoud, maar in het aansluiten op de werkelijke wereld van de doelgroep.

Conclusie

Design Thinking is uitermate geschikt voor het adresseren van complexe maatschappelijke opgaven, waarvan het komen tot een doorbraak in duurzame Inzetbaarheid er één is. Er zijn goede kennis en instrumenten beschikbaar. De aansluiting op de uitvoeringspraktijk kan echter nog aanzienlijk worden verbeterd. Om tot creatieve oplossingen te komen die echt werken in de praktijk is het van belang de verschillen tussen werkgevers goed te begrijpen, evenals de te maken reis van waar ze nu staan naar een toekomst waarin duurzame Inzetbaarheid op het gewenste niveau is. Dit is iets wat in de essentie zit van Design Thinking.

Over de auteurs



Nanny Schoenmakers

Principal Consultant bij Capgemini Invent

Nanny heeft meer dan 25 jaar advieservaring in de publieke sector, in het bijzonder op het terrein van onderwijs, arbeidsmarkt en duurzame inzetbaarheid.

 nanny.schoenmakers@capgemini.com

 <https://www.linkedin.com/in/nanny-schoenmakers-a10a5010/>



Joost van der Made

Director Transport Services bij Capgemini Invent

Joost is opgeleid als industrieel ontwerper en heeft meer dan 25 jaar ervaring op gebied van innovatie voor een betere klantervaring en dienstverlening. Joost is in alle fasen van het Design Thinking proces actief geweest vanuit zijn verschillende rollen en adviesopdrachten.

 joost.vander.made@capgemini.com

 <https://www.linkedin.com/in/joostvdm/>

Bronnen

1. Leren en ontwikkelen in Nederland, Researchcentrum voor Onderwijs en Arbeidsmarkt (ROA), mei 2024.
2. Arbo in bedrijf 2022-2023, Monitoronderzoek naar de naleving van Arboverplichtingen, blootstelling aan arbeidsrisico's, maatregelen en gezond en veilig werken in de praktijk, Arbeidsinspectie, september 2024.
3. Arbovisie 2040: De trend gekeerd, samenwerken aan een gezond en veilig Nederland, Ministerie van Sociale Zaken, oktober 2023.
4. Quicksan Duurzame inzetbaarheid en leven lang ontwikkelen, Capgemini Invent, februari 2021.



3. Technologische wendbaarheid

Interview



“Wat kan er nog wel?”

Visie van Schiphol op weerbaarheid, Hedzer Komduur, Director Safety & Environment

Op Schiphol is de transitie naar een superslimme samenleving in volle gang. Fysieke en digitale werelden worden er steeds verder met elkaar verknoot. Technologische ontwikkelingen ondersteunen zowel ultiem reizigersgemak als optimale veiligheid. Dat lukt alleen als alle belangen op elkaar worden afgestemd.

Schiphol is op aarde om Nederland met de wereld te verbinden. Letterlijk, zegt Hedzer Komduur, Director Safety & Environment bij Schiphol. Met zijn team zorgt hij ervoor dat reizigers en medewerkers dagelijks veilig kunnen reizen en werken, op een manier

die zo min mogelijk overlast geeft voor de omgeving. Komduur: “De Schiphol-organisatie zelf is slechts een van de spelers hier: wij hebben gebouwen, parkeerplaatsen, start- en wandelingsbanen. Maar het grootste deel van het luchthavenproces, van paspoortcontrole, boarding, tanken tot de bagage-afhandeling: dat wordt allemaal door andere partijen geregeld.”

Schiphol kent zo’n 4.000 werknemers. Maar op de luchthaven werken dagelijks meer dan 70.000 mensen. Komduur: “Dat zijn mensen van zowel private partijen als de overheid. En al die werkprocessen moeten op elkaar afgestemd worden. Vroeger ging dat met papier en telefoon, nu uiteraard digitaal. Onze systemen praten continu met elkaar om de volledige operatie te laten draaien. Onze taak is dat zoveel mogelijk te optimaliseren.”

Werken aan complexe opgaven

“Weerbaarheid is in onze wereld dan ook een gezamenlijke opgave. Als Schiphol kennen we veel publiek-private samenwerkingen.” Komduur noemt het European Entry Exit Systeem als voorbeeld. Dat systeem vereist dat iedereen die van buiten de Europese Unie komt, bepaalde gegevens moet afgeven. “Denk aan vingerafdrukken, gezichtscans en andere biometrische gegevens. In de VS gebeurt dat al. We kennen die grote hallen met hokjes en controles. Niemand weet hoelang het duurt voordat je erdoorheen bent. Zulke hallen hebben we hier niet, maar we verkopen hier wel een bepaalde minimum connecting time. Je landt en kan binnen een bepaalde tijd weer doorvliegen. Wij moeten dus zorgen dat dit nieuwe screeningsproces, wat uiteindelijk een overheidstaak is, ingepast wordt in het grote Schiphol-ecosysteem. Dat vereist veel samenwerking. De overheid kan dat niet alleen vanwege de complexiteit en onderlinge verbondenheid van uiteenlopende operationele processen. Dan is een publiek-private samenwerking de meest succesvolle werkwijze.”

Bij zulke complexe trajecten schuiven allerlei partijen aan. Komduur: “Denk aan het ministerie van Defensie, als beheersorganisatie voor de Koninklijke Marechaussee. Maar ook het ministerie van Asiel en Migratie, dat gaat over de grens. Het ministerie van Infrastructuur

en Waterstaat gaat over hoe de mainport Schiphol functioneert. En verschillende private partijen en toeleveranciers praten ook mee over deze verandering. En dat is nog maar één voorbeeld. Want weerbaarheid wordt bijvoorbeeld ook in het platform Beveiliging en Publieke Veiligheid Schiphol (BPVS). Ook daar praten we met ministerie van Defensie, de NCTV, gemeente Haarlemmermeer, de Douane, en grote airlines. Je hebt elkaar echt nodig om complexe opgaven op te lossen.”

Wat kan er nog wel?

Komduur is naast directeur Safety & Environment ook CISO. Weerbaarheid gaat dan ook over risicomangement en het kunnen opvangen van onverwachte klappen. “Hoelang duurt het voordat we daar last van gaan ondervinden en hoe veerkrachtig zijn we als er iets gebeurt? Daarvoor houden we veel oefeningen en hebben we een crisisorganisatie met een commissie van overleg van operatie tot de burgemeester. De cruciale vraag is altijd: ‘Wat kan er nog wel’. Corona was zo’n situatie waarbij onze weerbaarheid is getest. Maar die ene vraag geldt eigenlijk voor alle fysieke of digitale incidenten die hier kunnen plaatsvinden.”

Vorig jaar werden verschillende airlines getroffen door het CrowdStrike-incident. Komduur lag op dat moment te slapen in New York en was vergeten zijn telefoon uit te zetten. “Ik werd gebeld door onze alarmcentrale: een defecte update van beveiligingssoftware leidde tot wereldwijde problemen in Microsoft Windows-systemen. Schiphol gebruikt CrowdStrike niet, maar Delta en KLM wel. Zo’n verstoring in een deel van onze operatie rolt meteen de hele luchthaven in. KLM was weer snel operationeel, dankzij die mindset ‘wat kunnen we nog wel?’. In Amerika zagen we op het journaal dat het airlines niet lukte snel weer operabel te zijn. Het benadrukte voor ons nogmaals hoe belangrijk ons ecosysteem is en hoe alles met elkaar samenhangt. Je moet elkaar blindelings weten te vinden. Uiteraard hebben we ook meteen gecheckt of we zelf alle update policies op orde hadden, en dat was zo. Toch zullen dit soort incidenten vaker gaan voorkomen omdat alles steeds meer geautomatiseerd is. Ook updates.”

Implicaties van NIS2

“Security is uiteraard topprioriteit hier. Cyberaanvallen vinden steeds frequenter plaats en dreigingen van buitenaf worden ook steeds groter. Een incident kan in potentie iedere partij op Schiphol raken. Zeker als het de operatie betreft, moet je elkaar razendsnel weten te vinden. Dat borgen we via kennisdeling. Het Cybersecurity Schiphol Ecosystem (CYSSEC) is daarin een belangrijke schakel; hier leren we elkaar kennen en kweken we bewustzijn, ook bij de kleinere spelers op Schiphol. Daarom vind ik NIS2 ook zo belangrijk: het helpt bij de bewustwording. Het is belangrijk te weten wat er speelt en over incidenten te vertellen. Want compliant zijn betekent niet dat je veilig bent. Ik merk met de komst van NIS2 dat onze raad van bestuur en onze raad van commissarissen meer vragen gaan stellen, en dat vind ik een goede ontwikkeling. Die bewustwording is allemaal winst.”

De combinatie van Safety Manager en de CISO-rol is een logische, vindt Komduur. “Bij enkele NIS2-vraagstukken heb ik letterlijk onze safety rapportages gegeven als voorbeeld hoe te rapporteren. Die vakgebieden kunnen enorm van elkaar leren. We proberen aan de voorkant bewustzijn te kweken, om kennis te delen en hulp te bieden waar nodig. Cybersecurity moet in de haarvaten van onze organisatie zitten.”

Vraagstukken rondom AI

Weerbaarheid betekent ook continu werken aan vernieuwing. Want natuurlijk, zegt Komduur, AI is onontkoombaar. “We kunnen en moeten bepaalde processen moderniseren. Denk aan robots in de bagagekelders of manieren om de KMar te helpen om passagiers hun gegevens op tijd te laten aanleveren zodat het screeningsproces makkelijker gaat. We krijgen weer nieuwe bagagescanners op onze security lanes. Dat soort zaken dient het reizigersgemak maar zorgt ook dat mensen hier veilig en gezond kunnen werken. Dat zijn ontwikkelingen waar ik dagelijks aan werk. AI wordt daarin steeds belangrijker.”

Een ander voorbeeld is van een AI-toepassing is ‘Deep Turnaround’. Komduur: “Camera’s zien welke voertuigen om een vliegtuig staan. Aan de hand daarvan kunnen we voorspellen hoelang het nog duurt voordat dat vliegtuig vertrekt. Wanneer komt een parkeerplaats vrij? Het algoritme detecteert vertragingen al 40 minuten vóór de beoogde ‘off-block-tijd’; het moment dat een vliegtuig beweegt om te gaan vertrekken. We kunnen hierdoor proactief ingrijpen. Digitaal en fysiek worden letterlijk met elkaar verknoot dankzij deze nieuwe technologie. Toch moeten we uiterst alert blijven hoe en waar AI wordt toegepast, en wat een algoritme doet. Als algoritmes zichzelf kunnen aanpassen, is het dan nog wel compliant? In een luchtvaartomgeving is dat van groot belang. We hebben extreem veel wetgeving op het gebied van veiligheid, zowel fysieke als digitale beveiliging. Je moet zelf aan het stuur blijven.”

Opgave voor de samenleving

Komduur komt terug op cyberveiligheid. “Wij kunnen dat hier intern goed regelen, maar dit is ook een belangrijke taak voor de overheid. Hoe communiceer je over het belang van veiligheid met de BV Nederland, op verschillende niveaus? Naar mijn idee moet iedereen in onze samenleving snappen waar cybersecurity over gaat; het hoort bij onze ‘burgerlijke basishygiëne’. Het zou in de haarvaten van onze samenleving moeten zitten. We zijn met elkaar té afhankelijk van alle infrastructuur die buiten ons wordt neergezet. Als samenleving 5.0 moeten we uiterst weerbaar worden. Daarin hebben we met elkaar een rol te vervullen.”

Gezamenlijke perspectieven voor de toekomst

Want wat betreft de implementatie van nieuwe technologieën loopt Nederland vaak voorop, zegt Komduur. “Schiphol kent bijvoorbeeld de meest geavanceerde screeningsapparatuur. Vooraf zei iedereen: ‘Dat gaat niet werken. Die

machines zijn te langzaam, te zwaar, te duur.’ Wij zagen de voordelen en zijn toch gaan investeren. Onze systemen zijn nu de hoogste standaard; reizigersgemak en veiligheid gaan hier echt hand in hand. Dat succes is te danken aan een PPS-constructie. We werken hiervoor samen met NCTV, de Koninklijke Marechaussee, de Europese Commissie kijkt mee, fabrikanten sluiten zich aan, en dan ontstaat er iets.”

“Er wordt vaak gezegd ‘In Nederland werken overheid en bedrijfsleven niet goed samen’, maar dat is onzin. Dat gaat in Nederland juist enorm goed. De kracht van Schiphol zit mede in de samenwerking met overheidspartijen, op uiteenlopende onderwerpen. Veel buitenlandse luchthavens kijken daar met jaloezie naar. En het geeft ons ook de kracht om snel op bepaalde dossiers te kunnen bewegen. Voor de toekomst willen we graag in Europa nog nauwere samenwerkingen op verschillende gebieden aangaan om elkaar, de Europese luchtvaart en de veiligheid, te versterken. Alleen gezamenlijk staan we sterk. We moeten voorbij durven gaan aan de nationale belangen en meer werken vanuit een gezamenlijk perspectief. Een meer eensgezind Europees beleid zou ons helpen om sneller weerbaar en wendbaarder te worden en onze toekomst te verstevigen.”

Nederland bepaalt zelf hoe de super slimme samenleving eruit ziet

Hoe geven we met een goed technologiebeleid zelf vorm aan onze Society 5.0 zonder inmenging van de grote tech-bedrijven?



Highlights

- Voor een wendbare en weerbare samenleving is technologie essentieel, maar dit vraagt wel een goed technologiebeleid.
- De Nationale Technologie Strategie biedt een goede basis, waarbij de grote uitdaging zit in de implementatie van nieuwe technologie in de samenleving wil beleid echt succesvol zijn.
- Grote publieke organisaties zoals defensie en de Nationale Politie spelen een cruciale rol in het ontwikkelen en implementeren van nieuwe technologieën.
- Er is meer durfkapitaal nodig om nieuwe technologieën naar implementatie te brengen.
- Nederland houdt de technologierace niet alleen bij en moet samenwerken in Europa om fragmentatie te voorkomen.

In dit artikel laten we zien hoe belangrijk technologie en technologiebeleid zijn in de super slimme samenleving. Hoe helpt innovatie de opkomst van nieuwe technologieën? En hoe stuurt de overheid en bereidt ze Nederland voor op nieuwe technologie voor een wendbare en weerbare samenleving?

Van de manier waarop we communiceren tot hoe we werken en leven, technologie is een integraal onderdeel van ons dagelijks leven (Society 5.0!). Maar bepalen de 'Magnificent 7'¹ van tech bedrijven hoe ons leven eruit gaat zien of bepalen we onze toekomst zelf?

Het regeerakkoord van 2024 benadrukt de cruciale rol van innovatie in het bevorderen van economische groei en maatschappelijke vooruitgang. Innovatie wordt gezien als een sleutel tot het oplossen van grote maatschappelijke uitdagingen zoals klimaatverandering, gezondheidszorg en veiligheid. Het kabinet-Schoof heeft in haar regeerprogramma 2024 het woord 'innovatie' 85 keer genoemd als mogelijke oplossing voor een probleem. Helaas komen deze woorden niet tot uitdrukking in de begroting en zijn fondsen voor innovatie steeds kleiner geworden. Met het Nationaal Groeifonds investeerde het vorige kabinet miljarden in projecten die bijdragen aan onder meer digitalisering en ontwikkeling van innovatieve technologie voor gezondheidszorg, onderwijs en energietransitie. Het nieuwe kabinet heeft het fonds en daarmee 60 projecten gestopt. Er wordt 6,8 miljard euro minder uitgegeven aan innovaties. Zonder duidelijke doelen en voldoende middelen om innovatie te stimuleren via investeringen in onderzoek en ontwikkeling, en zonder het creëren van een gunstig klimaat voor startups en technologiebedrijven, zijn we overgeleverd aan de wil van de grote tech-bedrijven.

Ontwikkeling van Nationale Technologie Strategie

Toch is er nog hoop. Afgelopen jaar is vanuit het ministerie van Economische Zaken de Nationale Technologie Strategie (NTS) ontwikkeld². Deze strategie biedt een raamwerk voor strategisch technologiebeleid. Hierin worden de 10 sleuteltechnologieën die essentieel zijn voor de toekomstige economische groei van Nederland beschreven. Deze variëren van optische systemen, geïntegreerde fotonica, kwantumtechnologieën, kunstmatige intelligentie, tot biotechnologie en cybersecurity. Deze

technologieën zijn niet alleen belangrijk voor economische groei, maar ook voor het aanpakken van maatschappelijke uitdagingen en het waarborgen van wendbaarheid en weerbaarheid in onze super slimme samenleving.

De strategie stelt lange termijn doelen voor 2035, zoals het aantrekken en behouden van talent, voldoende faciliteiten voor technologieontwikkeling en -toepassing, en voldoende financiering en markttoegang. De focus ligt op de ontwikkeling, toepassing en opschaling van technologieën door middel van innovatiebeleid, ondernemerschapbeleid en industriebeleid zodat Nederland gepositioneerd wordt als een technologisch leider en de concurrentiepositie op internationaal niveau wordt versterken.

Nederland heeft al een sterke positie dankzij hoogwaardig wetenschappelijk onderzoek, een goed opgeleide bevolking, sterke internationale relaties en veel publiek-private samenwerkingen. Toch is er extra aandacht nodig voor investeringen in R&D en het creëren van meer bekendheid voor de 10 sleuteltechnologieën. Samen met de 'topsectorenstructuur'³ en het bedrijfsleven streeft de overheid in een thematische opzet naar verschillende kennis- en innovatieagenda's (KIA's) om invulling te geven aan haar technologie strategie.

Digitalisering belangrijk thema in de Nationale Technologie Strategie

De Topsector ICT⁴ speelt een cruciale rol in de digitalisering van Nederland. Door samen te werken met overheden, bedrijven en kennisinstellingen, bevordert de Topsector ICT de ontwikkeling en toepassing van digitale technologieën. Dit draagt bij aan het oplossen van maatschappelijke vraagstukken en versterkt de positie van Nederland als voorloper op het gebied van digitalisering. Een voorbeeld van de implementatie van de NTS is de KIA Digitalisering 2024-2027⁵. In deze agenda staat de programmering van kennis en innovatie

op het gebied van digitalisering en digitale informatietechnologieën. Met een Kennis- en Innovatieconvenant tussen overheden, wetenschap, hogescholen, bedrijfsleven, innovatief mkb en maatschappelijke organisaties wordt gewerkt aan de implementatie van sleuteltechnologieën zoals kunstmatige intelligentie, cybersecurity, data science, softwaretechnologieën en digitale connectiviteit. Binnen de gezondheidszorg worden bijvoorbeeld innovaties getest met patiënten en zorgverleners in verschillende contexten, zoals bij de patiënt thuis, op het werk, op school en uiteraard in de zorgpraktijk.

Implementatie van technologie als katalysator voor economische groei

Nederland beschikt met haar technologiebeleid over een stevige basis, maar de uitdaging zit in de implementatie van de nieuwe technologieën in de samenleving. We zien te vaak dat interessante onderzoeken en pilots niet resulteren in toepassing van nieuwe technologie.

We weten dat nieuwe technologie een belangrijke bijdrage levert aan de economische groei van Nederland. Defensie is van oudsher een aanjager van technologisch onderzoek en een katalysator voor de ontwikkeling en toepassing van technologie. Vanuit Defensie-technologie zijn toepassingen voortgekomen zoals mobiele telefoons, internet, computerchips en drones. Onderzoek van de Rabobank toont aan dat elke euro die geïnvesteerd is in onderzoek voor defensie, 8 tot 9 euro aan welvaartswinst heeft opgeleverd. Daarmee doet Defensie het een stuk beter dan bedrijven en kennisinstellingen buiten de defensiesector. Daar leverde een geïnvesteerde euro maximaal 1,8 euro aan welvaartswinst op.⁶

Als voorbeeld voor toepassing van technologie en de vormgeving van onze weerbare en wendbare samenleving kunnen we dus naar het ministerie van

Defensie kijken. In de Defensie specifieke Strategische Kennis- en Innovatieagenda (SKIA)⁷ geeft zij richting. Deze agenda richt zich op het versterken van de technologische en industriële basis van Defensie en kanaliseert ook de aandacht, prioritering, fondsen en lange termijn aandacht die nodig is. Door nauw samen te werken met wetenschap, industrie en mkb-bedrijven worden maatschappelijke uitdagingen door de krijgsmacht vormgegeven. Naast Defensie speelt ook de Nationale Politie een actieve rol in het ontwikkelen en implementeren van nieuwe technologieën om de weerbaarheid en wendbaarheid van de samenleving te verbeteren. Door middel van programma's met onderzoekinstellingen voor het opbouwen van lange termijn kennis en het Q-Innovatorsprogramma⁸ voor het op korte termijn implementeren van technologie wordt innovatie binnen de politieorganisatie vormgegeven. Daarmee zorgt zij dat onze samenleving proactief nieuwe dreigingen en criminaliteit het hoofd kan bieden.

Society 5.0: implementatie van NTS-sleuteltechnologie

We staan op het punt om Society 5.0 vorm te geven door middel van de implementatie van de digitale sleuteltechnologie uit de NTS. Als eerste natuurlijk de transformerende technologieën **Kunstmatige intelligentie (AI) en generatieve AI (GenAI)** die al een enorme impact hebben. Van het automatiseren van routineprocessen tot het ondersteunen van creatieve taken, AI biedt veel nieuwe mogelijkheden voor innovatie en efficiëntie. Een samenleving die AI omarmt, kan haar productiviteit verhogen, nieuwe producten en diensten ontwikkelen en economisch groei realiseren. Een tweede technologie die bepalend gaat zijn, is **5G en de toekomstige ontwikkeling van 6G**⁹. Deze technologie biedt ongekende mogelijkheden voor connectiviteit en gegevensverwerking. 5G zorgt voor snellere en betrouwbaardere

verbindingen wat essentieel is voor toepassingen zoals het Internet of Things (IoT) en autonome voertuigen. 6G belooft nog hogere snelheden en een grotere capaciteit. Dat opent de deuren voor geavanceerde technologieën zoals augmented reality en slimme steden.

In de (nabije) toekomst zien we steeds meer ontwikkeling op het vlak van robotisering in de samenleving. Door de inzet van **'AI driven robots'** kunnen bedrijven efficiënter werken en de productiviteit verhogen, ondanks tekorten op de arbeidsmarkt. Samen met AI en 6G bieden multipurpose robots nieuwe kansen voor de industrie om te groeien en te concurreren¹⁰.

Voor Post Quantum Cryptografie (PQC) moeten nu belangrijke keuzes worden gemaakt. Hoewel **Quantum computing** er nog niet is, heeft de technologie het potentieel om een revolutie teweeg te brengen in onze 'connected society'. Daarom moeten we nu al nadenken over de versleuteling van onze huidige gevoelige data. Versleutelde datasets die nu 'verzameld' worden, zijn met komst van quantum computer eenvoudig toegankelijk te maken. Doordat complexe berekeningen heel snel kunnen worden uitgevoerd, kan met quantum computing het huidige algoritme veel sneller worden ontsleuteld dan de traditionele computers van nu dat kunnen.

Hoe Nederland weerbaar en wendbaar blijft door technologie en innovatie

De Nationale Technologie Strategie geeft richting en prioriteert. Nederland streeft ernaar een weerbare en wendbare samenleving te blijven door strategische investeringen in technologie en innovatie te stimuleren. Maar hier blijven Nederland en Europa achter bij de VS en China. In het rapport van Draghi over de 'competitiveness of Europe'¹¹ stelt hij dat er een toenemende innovatiekloof is tussen de EU en de VS, veroorzaakt door een relatief stagnerende investering in onderzoek en

innovatie. Europa geeft te weinig geld uit aan innovatieve technologieën en heeft te veel regelgevende en juridische hindernissen die voorkomen dat nieuwe technologieën worden opgeschaald. Hij benoemt de noodzaak tot meer investeringsmogelijkheden.

Sinds dit jaar heeft de Europese commissie een nieuw plan voor de duurzame welvaart en het concurrentievermogen van Europa. 'The Competitiveness Compass'12, is het eerste grote initiatief van de nieuwe Commissie, en vormt haar toekomstige werkzaamheden, voortbouwend op het Draghi rapport. Cruciale eerste stap is het gemakkelijker en sneller maken van zakendoen en het verdiepen van de Europese single-market.

Om te voorkomen dat innovatieve bedrijven uiteindelijk op zoek gaan naar financiering van Amerikaanse durfkapitalisten is het noodzakelijk dat er in Europa meer durfkapitaal is. Vanuit de nationale overheid en Europese entiteiten wordt door middel van subsidieprogramma's (Horizon Europe,

Digital, EDF) financiën beschikbaar gesteld. Maar dat is niet voldoende, meer Nederlands en Europees venture capital is noodzakelijk. Het Nederlandse durfkapitaallandschap groeide in 2024 sterk in vergelijking met de Europese markt, toch daalden de Nederlandse investeringen sterk. Ondanks deze veranderingen bleef Nederland met € 15 miljard de op drie na grootste durfkapitaalmarkt in Europa13. Er zijn meer middelen vanuit het bedrijfsleven nodig in Europa. Sinds 2019 werkt Capgemini bijvoorbeeld samen met ISAI14 en is het ISAI Cap Venture Fund15 opgericht. Samen met startups bouwen we aan hun go-to-market en helpen we nieuwe innovaties, ideeën en oplossingen te implementeren.



Conclusie

In Nederland moeten we de handschoen oppakken om niet afhankelijk te zijn van de 'Magnificent 7'. Dit vraagt niet alleen een proactief beleid op het gebied van innovatie en technologie. De focus moet liggen op het wegnemen van de hindernissen, het toegankelijk maken van kapitaal en het streven naar een duurzame super slimme samenleving. Door net als Defensie te coördineren hoe technologie wordt ingekocht, moet dat ook in andere industrieën mogelijk zijn. Deze coördinatie kan zowel in Nederland als in samenwerking met Europese landen en de NATO worden gevormd. Laten we streven naar het verwijderen van barrières op nationaal en Europees niveau. Voorkom nationalistische fragmentatie en creëer ruimte voor en stimuleer het toepassen van nieuwe technologie vanuit Europa. Cruciaal is de beschikbaarheid van kapitaal, daarom is het stimuleren van 'Venture Capital' op het Europese continent een must. Technologie speelt een onmisbare rol in de super slimme samenleving. Door te investeren in innovatie en strategische technologieën, kunnen Nederland en Europa hun positie claimen als regisseur van deze samenleving en bijdragen aan een duurzame en veilige toekomst. Van AI en robotisering tot quantum computing, de opkomst van nieuwe technologieën biedt ongekende mogelijkheden voor economische groei en maatschappelijke vooruitgang.

Over de auteur



Roeland de Koning

Director Public Security bij Capgemini Invent

Roeland heeft meer dan 20 jaar ervaring in het adviseren van nationale overheden en de Europese Commissie op het gebied van Digitalisering, Innovatie en Veiligheid. Afgelopen jaren is Roeland veelvuldig actief in het veiligheidsdomein op het gebied van kennis en innovatiemanagement.

[✉ roeland.de.koning@capgemini.com](mailto:roeland.de.koning@capgemini.com)

[in https://www.linkedin.com/in/roeland-de-koning-5536482/](https://www.linkedin.com/in/roeland-de-koning-5536482/)

Bronnen

1. 'De Magnificent Seven-aandelen zijn een groep goed presterende en invloedrijke bedrijven op de Amerikaanse aandelenmarkt: Alphabet, Amazon, Apple, Meta Platforms, Microsoft, NVIDIA en Tesla
2. <https://open.overheid.nl/documenten/67b0a9e1-135b-483f-9ed9-3aade270dbce/file>
3. <https://www.topsectoren.nl/>
4. <https://topsector-ict.nl/>
5. https://topsector-ict.nl/assets/images/default/KIA-Digitalisering-2024-2027_WEB.pdf
6. https://digitalekrant.ad.nl/algemeendagblad/45668/article/2196732/18/1/render/?token=08989533c01c21d053bdeac28d-30665d&v_l_platform=ios&v_l_app_id=be.persgroep.algemeendagblad&v_l_app_version=13.64.0
7. <https://open.overheid.nl/documenten/ronl-52ed0fc2-bddf-4792-9b95-6b13ac087e95/pdf>
8. <https://www.politie.nl/informatie/het-q-innovatorsprogramma.html>
9. <https://www.capgemini.com/au-en/insights/research-library/6g-for-the-hyperconnected-future>
10. <https://www.capgemini.com/news/press-releases/technovision-top-5-tech-trends-to-watch-in-2025/>
11. https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en
12. https://commission.europa.eu/priorities-2024-2029/competitiveness_en
13. <https://techleap.nl/wp-content/uploads/sites/2/2025/02/State-of-Dutch-Tech-report.pdf>
14. <https://www.isai.vc/>
15. <https://www.isai.vc/isai-cap-venture>

De AI-verordening: tijd voor actie voor een weerbare publieke sector

Hoe moeten organisaties binnen de publieke sector omgaan met de AI-verordening?



Highlights

- Achtergrond en overzicht van de AI-verordening.
- Verschillende rollen en een classificatie-mechanisme bepalen de zwaarte van de vereisten.
- De eerste vereisten zijn van kracht, publieke organisaties moeten maatregelen nemen.

De AI-verordening, die in augustus 2024 in werking is getreden, stelt geharmoniseerde regels vast voor de ontwikkeling, het in de handel brengen, en het gebruik van AI-systemen binnen de EU. Het doel is om een mensgerichte en betrouwbare AI te bevorderen, terwijl de gezondheid, veiligheid en grondrechten van burgers worden beschermd.

Society 5.0 heeft als doel een mensgerichte, superslimme samenleving te creëren, waarbij geavanceerde technologieën zoals AI, het Internet of Things, en big data geïntegreerd worden in alle aspecten van het dagelijks leven en de economie. Door duidelijke eisen en verplichtingen te stellen aan AI-toepassingen, helpt de verordening om potentiële risico's te beheersen en de maatschappelijke weerbaarheid te vergroten. In dit artikel geven we een beknopt overzicht van de AI-verordening. Ook beschrijven we wat er van publieke organisaties wordt verwacht.

Achtergrond en doel van de AI-verordening

De kansen voor AI zijn legio. De technologie draagt de belofte om allerlei activiteiten sneller en beter uit te voeren dan wij dit op dit moment als mensen kunnen. Zeker in de publieke sector waar overheidsorganisaties vaak interactie hebben met honderdduizenden burgers tegelijkertijd, kan (deels) geautomatiseerde communicatie en besluitvorming enorme productiviteitswinsten opleveren. Niet onbelangrijk in een vergrijzende samenleving met een krappe arbeidsmarkt. Tegelijkertijd hoef je de krant maar open te slaan om te lezen over de negatieve neveneffecten. Denk aan het toeslagenschandaal en recenter het discriminerende algoritme van DUO om studiefinanciering voor uitwonende studenten te controleren.

Society 5.0 is de mensgerichte superslimme samenleving waar technologie grondrechten respecteert en versterkt. Waar we AI inzetten ten goede van de samenleving en negatieve neveneffecten zoveel mogelijk beperken. De Europese AI-verordening tracht om de negatieve neveneffecten met behulp van de wet in te perken. De AI-verordening

is het allereerste wettelijke kader voor AI dat aan AI-ontwikkelaars en gebruikers eisen en verplichtingen oplegt met betrekking tot specifieke toepassingen van AI. Het is een EU-verordening en zodoende van toepassing in alle EU-lidstaten: rechtsgevolgen zijn automatisch en uniform bindend in alle nationale wetgevingen. In de volgende alinea's zetten we de vereisten nader uiteen.

Rollen en risico's binnen de AI-verordening

De AI-verordening maakt onderscheid tussen onder andere aanbieders, gebruiksverantwoordelijken, importeurs en distributeurs bij de inzet van AI-systemen. Twee rollen zijn hier voor de overheid bij uitstek relevant:

1. Aanbieders van AI-systemen, oftewel degene die het AI-systeem ontwikkelt om zelf te gebruiken of om aan te bieden aan andere organisaties, zullen aan de meeste regels moeten voldoen. In veel gevallen is de overheid zelf deze ontwikkelaar. En ook als overheidsorganisaties externe partijen (zoals consultancy) inhuren om hen te helpen bij het ontwikkelen, blijft de overheid voor de wet de aanbieder. Hierover moeten dus goede afspraken worden gemaakt.



De AI Act classificeert de volgende acht AI-systemen als hoog risico vanwege hun potentiële impact op fundamentele rechten en veiligheid



2. Gebruiksverantwoordelijken van AI-systemen, oftewel degene die een AI-systeem onder eigen verantwoordelijkheid gebruikt. Denk hierbij aan Microsoft Copilot, of andere systemen die de overheid inkoopt waarin gebruikt gemaakt wordt van AI.

De strengste verplichtingen van de AI-verordening gelden voor aanbieders van hoog-risico AI-systemen. Maar wanneer zijn AI-systemen eigenlijk hoog-risico? Er zijn verschillende redenen waardoor een AI-systeem als hoog-risico wordt beoordeeld.

1. De AI-systemen die als veiligheidscomponent dienen in specifieke eerdere Europese wetgeving (Annex II van de AI-verordening) waarbij een conformity assessment door een derde partij verplicht is. Denk aan kinderspeelgoed, boten, liften etc.
2. Of: als de AI-systemen gebruikt worden binnen een bepaalde context. Dit is vooral relevant voor de publieke sector, en in het bijzonder voor de toegang tot essentiële publieke diensten en rechtshandhaving. Onderstaande infographic toont welke type systemen nog meer hoog-risico zijn.

We beschouwen AI-systemen als hoog-risico als ze profielen van personen opstellen om verschillende aspecten van iemands leven te beoordelen, zoals werkprestaties, economische situatie, gezondheid, voorkeuren, interesses, betrouwbaarheid, gedrag of locatie. We beschouwen AI-systemen als geen hoog-risico als het AI-systeem een beperkte procedurele taak heeft, enkel menselijke activiteit beoordeelt of verbetert, beslissingspatronen opspoort of voorbereidende taken uitvoert.

Wat zijn de vereisten voor hoog-risico AI-systemen?

Ontwikkelaars van hoog-risico AI-systemen moeten aan verschillende vereisten voldoen voordat ze hun AI-systeem in gebruik mogen stellen. De onderstaande opsomming is niet volledig, maar geeft een goede impressie van die vereisten:

1. AI-systemen moeten een grondige risicobeoordeling en risicobeheer ondergaan om potentiële gevaren te identificeren en te beperken. Dit omvat het implementeren van passende risicobeheersmaatregelen gedurende de gehele levenscyclus van het systeem.
2. De datasets die worden gebruikt door AI-systemen moeten van hoge kwaliteit zijn, representatief en vrij van bias.
3. Voor hoog-risico AI-systemen moet technische documentatie worden bijgehouden en logs moeten automatisch worden opgeslagen.
4. AI-systemen moeten robuust, nauwkeurig en veilig zijn. Dit betekent dat ze bestand moeten zijn tegen fouten en eventuele aanvallen van buiten, en dat ze betrouwbare resultaten moeten leveren.
5. Er moeten procedures zijn voor het rapporteren en monitoren van AI-systemen om hun prestaties te waarborgen.

De eerste vereisten zijn al van kracht

Sinds 1 februari van dit jaar zijn de eerste vereisten voor organisaties van kracht: verboden AI-praktijken, zoals getoond in de infographic, moeten onmiddellijk worden stopgezet.

Ook moeten organisaties ervoor zorgen dat hun personeel voldoende AI-geletterd is, zie artikel 4 van de AI-verordening: 'zorgen voor een toereikend niveau van AI-geletterdheid bij hun personeel en andere personen die namens hen AI-systemen exploiteren en gebruiken'. Ook publieke organisaties moeten hierin dus investeren door bijvoorbeeld trainingen en educatieprogramma's op te zetten voor medewerkers, zodat zij de werking, risico's en ethische implicaties van AI begrijpen. Ook het opzetten van specifieke rol-specifieke trainingen is een belangrijke maatregel voor vooral ontwikkelaars bij publieke organisaties die hoog-risico AI-systemen gebruiken.

Hoe moeten overheidsorganisaties omgaan met de AI-verordening?

Om te voldoen aan de AI-verordening moeten publieke organisaties navigeren door een complex regelgevingskader. Verschillende vereisten moeten worden geïdentificeerd en geprioriteerd om hiervoor op organisatorisch- en op systeemniveau beleid en processen in te regelen. Afhankelijk van de context van de publieke organisatie en de classificatie van de gebruikte (of te ontwikkelen) AI-systemen, zal er een specifiek regime aan vereisten ingeregeld moeten worden. Organisaties die geen hoog-risico AI-systeem gebruiken zullen zodoende aan minder vereisten hoeven voldoen. Het is echter wel

essentieel voor alle organisaties om een duidelijke governance structuur te creëren, waarin heldere rollen en verantwoordelijkheden zijn bedeed en het binnen de organisatie duidelijk is wie verantwoordelijk is voor het toezicht op AI-implementatie en naleving van wet- en regelgeving. Daarnaast is samenwerking met privacy-, security-, IT- en data-afdelingen van belang om een holistische benadering van AI-projecten te waarborgen.

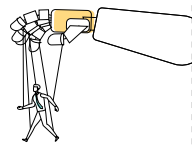




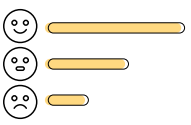


Het veilig en compliant ontwikkelen en/of inkopen en vervolgens gebruiken van AI-systemen is van groot belang. Dit omvat mede maatregelen om privacy te beschermen, discriminatie te voorkomen en de (cyber)veiligheid van AI-systemen te waarborgen. Hiervoor zullen processen moeten worden aangepast of worden opgesteld. Een ander belangrijk punt op organisatieniveau voor overheidsinstellingen is het bevorderen van transparantie en verantwoording door middel van volledige documentatie en uitlegbaarheid te waarborgen.

Voor publieke organisaties die zelf AI-systemen ontwikkelen is het van belang om op systeemniveau vereisten in te regelen. Specifiek als het om hoog-risico AI-systemen gaat. De AI-verordening volgt een modellevenscyclusaanpak voor elk individueel AI-systeem. Deze cyclus beschrijft de stappen waarin een model ontwikkeld wordt. In elk van deze stappen moeten specifieke vereisten vanuit de AI-verordening meegenomen worden. Ontwikkelteams zullen standaarden moeten implementeren die compliant zijn met de voorwaarden gesteld in de AI-verordening. Denk hierbij onder andere aan juiste standaarden voor data en datagovernance, het zoveel

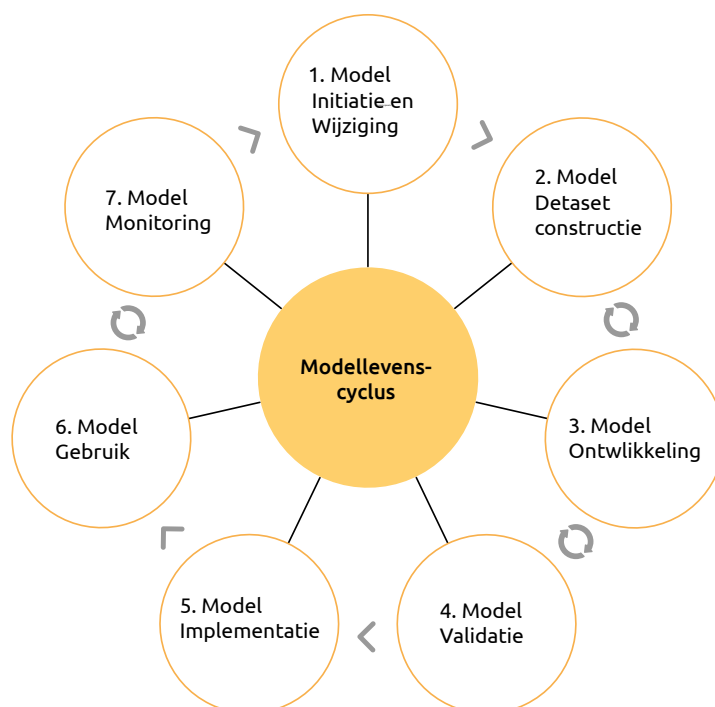
mogelijk voorkomen van aannames, het op de juiste manier bijhouden van technische documentatie, of het inregelen van menselijk toezicht. Ook de samenwerking met privacy - voor het doen van een Gegevensbescherming - seffectbeoordeling (GEB) - en een Impact Assessment Mensenrechten en Algoritmes (IAMA)) en informatiebeveiliging afdelingen zijn binnen deze aanpak van belang. Een sterke governance structuur met duidelijk belegde verantwoordelijkheden en toezicht is hier cruciaal.

Verboden AI-praktijken onder de AI Act: een kort overzicht

De AI Act verbiedt uw organisatie om deel te nemen aan de volgende AI-praktijken.

<p>Manipulatieve AI-systemen</p> <p>AI-systemen die gebruik maken van subliminale, manipulatieve of misleidende technieken, waardoor gedrag wordt verstoord, besluitvorming wordt beïnvloed en aanzienlijke schade wordt veroorzaakt.</p> 	<p>Uitbuiting van kwetsbaarheden</p> <p>AI-systemen die de kwetsbaarheden van individuen of groepen uitbuiten op basis van leeftijd, handicap of een specifieke sociale en economische omstandigheid, waardoor gedrag op een schadelijke manier wordt beïnvloed.</p> 	<p>Sociale profilering</p> <p>AI-systemen die individuen of groepen over een bepaalde periode evalueren of classificeren op basis van sociaal gedrag of persoonlijke kenmerken (bekend, afgeleid of voorspeld), en die leiden tot ongerechtvaardigde, onevenredige of context-vreemde nadelige behandeling.</p> 	<p>Voorspelling van crimineel gedrag</p> <p>AI-systemen die uitsluitend op basis van profilering of persoonlijkheidskenmerken het risico voorspellen dat een individu een strafbaar feit pleegt, zonder objectieve en verifieerbare feiten die direct verband houden met een misdaad.</p> 
<p>Ongecontroleerde gezichtsherkenning</p> <p>AI-systemen die gezichtsherkenningsdatabases aanleggen of uitbreiden door ongerichte scraping van internet of CCTV-beelden zijn verboden.</p> 	<p>Emotieherkenning op werk of in het onderwijs</p> <p>AI-systemen die emoties afleiden op de werkplek of in het onderwijs zijn verboden, behalve bij gebruik voor medische of veiligheidsdoelinden.</p> 	<p>Bitometrische categorisering</p> <p>AI-systemen die personen indelen op basis van biometrische gegevens om ras, politieke opvattingen, religie, vakbondslidmaatschap, seksleven of seksuele gerichtheid af te leiden, zijn verboden, behalve voor het labelen of filteren van rechtmatig verkregen biometrische datasets.</p> 	<p>Real-time biometrische identificatie in openbare ruimten</p> <p>Het gebruik van AI-systemen voor real-time biometrische identificatie in openbare ruimten voor rechtshandhaving is verboden, tenzij strikt noodzakelijk voor het opsporen van vermiste personen, het voorkomen van ernstige bedreigingen of de identificatie van verdachten bij zware misdrijven.</p> 

Figuur 1: Voorbeeld van de modellevenscyclus van een AI-systeem



Conclusie

De AI-verordening draagt bij aan het beschermen van grondrechten van burgers in een superslimme samenleving, waar technologieën zoals (generatieve) AI een grote rol spelen. Dat doet de verordening door verschillende essentiële maatregelen en principes te implementeren. Zoals hierboven beschreven stelt de AI-verordening strenge voorschriften vast voor zowel ontwikkelaars als gebruikers van AI. Dit omvat onder andere het voorkomen van discriminatie, het waarborgen van privacy en het beschermen van de veiligheid van individuen. Door duidelijke richtlijnen te stellen voor onaanvaardbare, hoog-, beperkt en minimaal risico AI, versterkt de AI-verordening de weerbaarheid van organisaties. Daarnaast bevordert de verordening transparantie en verantwoording, waardoor publieke organisaties verplicht zijn om duidelijk te communiceren over de werking en impact van hun AI-systemen. Dit verhoogt het vertrouwen van burgers in de technologieën die worden gebruikt en voorkomt dat menselijke belangen uit het zicht raken. Publieke organisaties moeten de voordelen van AI benutten terwijl ze de risico's minimaliseren en het vertrouwen van de samenleving behouden. Gezien de eerste vereisten al van kracht zijn, moeten publieke organisaties nu actie ondernemen en inzichtelijk maken wat voor veranderingen en aanpassingen op organisatie-, en mogelijk systeemniveau, moeten worden gedaan.

Over de auteurs



Jochem Dogger

Senior Manager in het Data Ethics & Regulations team van Capgemini Invent

Jochem zet zijn achtergrond in econometrie en politicologie in om organisaties te helpen verantwoord om te gaan met algoritmes en AI.

 <https://www.linkedin.com/in/jochem-dogger-90091254/>



Robert Kreuger

Senior Manager en Team Lead Data Strategy & Factory bij Capgemini Invent

Robert heeft een juridische achtergrond en helpt organisaties met vraagstukken rondom AI governance en Data Protectie.

 robert.kreuger@capgemini.com

Cbw: wetgeving maakt weerbaar, strategie houdt wendbaar

Welke rol speelt de Cbw bij het implementeren van een cybersecuritystrategie om organisaties wendbaar te houden?



Highlights

- Een effectieve cybersecuritystrategie verhoogt de wendbaarheid in het geval van dreigingen.
- De Cbw legt de nadruk op een risicogerichte aanpak van cybersecurity, waarbij organisaties verplicht zijn om significante incidenten tijdig te melden.
- Bewustwording en training van medewerkers is cruciaal, omdat menselijke fouten vaak de oorzaak zijn van cyberincidenten.
- Een goede cybersecuritystrategie zorgt ervoor dat initiatieven rondom cybersecurity in lijn zijn met de bedrijfsdoelen, waardoor middelen worden ingezet waar ze het hardst nodig zijn.
- De Cbw draagt bij aan de continuïteit van digitale diensten, wat cruciaal is voor het functioneren van de digitale samenleving. Het koppelen van cybersecurity aan bedrijfsdoelen versterkt de wendbaarheid en weerbaarheid van organisaties en daarmee de samenleving.

Een effectieve cybersecuritystrategie verhoogt de wendbaarheid en maakt organisaties weerbaar tegen dreigingen, de Cyberbeveiligingswet (Cbw) ondersteunt dit.

Het belang van een cybersecuritystrategie

Het hebben van een cybersecuritystrategie wordt steeds belangrijker. Het toenemend aantal cyber dreigingen, de potentiële financiële impact van een aanval, het beschermen van gevoelige data en de noodzaak om de continuïteit van kritieke bedrijfsprocessen te waarborgen onderschrijven dit belang. Dit jaar zal de Nederlandse implementatie van de Network and Information Security Directive 2 (NIS2) - de Cyberbeveiligingswet (Cbw) - zijn intrede maken. De Cbw verplicht organisaties niet om een cybersecuritystrategie te maken, maar wel om beleid te maken op het gebied van de beveiliging van netwerk- en informatiesystemen, risicomangement, incidentenbehandeling, bedrijfscontinuïteit en crisisbeheer. De Cbw stuurt aan op het beheer van cybersecurityrisico's, dat wil zeggen: een aanpak die middelen en initiatieven prioriteert op basis van dreigingen en hun potentiële impact. Voor iedere organisatie betekent deze aanpak dat risico's geïdentificeerd, geëvalueerd en waar mogelijk, gemitigeerd moeten worden. Hierbij is het onontkoombaar dat organisaties deze risico's zullen baseren op en koppelen aan hun kritieke bedrijfsprocessen. Deze zullen namelijk de grootste impact ervaren wanneer ze worden geraakt. Het is dus van belang dat de risico's voor deze processen geminimaliseerd worden.

Een effectieve cybersecuritystrategie bevat een overzicht van alle bedreigingen waarmee de industrie wordt geconfronteerd en de business impact van toekomstige wet- en regelgeving. De strategie koppelt risico's aan kritieke bedrijfsprocessen door een brug te slaan tussen cybersecurity en de business. Het is belangrijk om te identificeren waar de bedrijfsprocessen het meest kwetsbaar zijn bij een verstoring of security incident. Hierdoor wordt cybersecurity een onderwerp

in het uitvoeren van kritieke bedrijfsprocessen. Dit wordt gedaan door te kijken naar strategische security risico's, strategische security- en bedrijfsdoelen en strategische initiatieven. Deze worden vervolgens samengebracht tot één strategische richting voor cybersecurity die meerdere jaren vooruit kijkt en security onderwerpen in de gekozen prioriteit naar een hoger niveau tilt. Het doel van een cybersecuritystrategie is om ervoor te zorgen dat een organisatie voldoet aan wet- en regelgeving, data en systemen beschermd worden en de continuïteit van kritieke bedrijfsprocessen – oftewel de (digitale) diensten – gewaarborgd wordt.

Zonder een duidelijke cybersecuritystrategie kan een organisatie nog steeds voldoen aan de wetgeving, maar een strategie gaat verder dan compliance en zorgt voor de volgende belangrijke voordelen:

1. Proactief risicobeheer: anticiperen en mitigeren van risico's voordat het problemen worden. Het alleen hebben van een beleid op het gebied van cybersecurity biedt niet genoeg dynamiek om te kunnen reageren op voortdurende veranderingen in het cyberlandschap.
2. Holistische benadering: een strategie kijkt niet alleen naar documentatie van beleid, maar richt zich ook op het trainen van werknemers en senior management en het betrekken van de leveranciersketen in risicomangement (Third-Party Risk Management).
3. Afstemming met bedrijfsdoelen: een strategie zorgt ervoor dat cybersecurity initiatieven binnen de organisatie in lijn zijn met de bedrijfsdoelen en dat de juiste prioritering van risico's plaatvindt.





4. Voortdurende verbetering: een strategie plant voor de toekomst (bijvoorbeeld voor 2025-2028) en moet jaarlijks herzien worden zodat het overeenkomt met het dreigingslandschap. Dit bevordert de wendbaarheid van de organisatie.

Proactief risicobeheer in een flexibele cybersecuritystrategie

Zoals eerder benoemd wordt binnen de Cbw de nadruk gelegd op een op risico gebaseerde aanpak van cybersecurity. De wet stimuleert risicogericht werken. Enerzijds door organisaties te verplichten om zorg te dragen voor verplichte cybersecurity vereisten, zoals het tijdig melden van significante incidenten bij de toezichthouder. Anderzijds door ervoor te zorgen dat organisaties continu hun risicobeheerprocessen evalueren en verbeteren. Proactief risicobeheer als onderdeel van een cybersecuritystrategie helpt organisaties om potentiële dreigingen vroegtijdig te identificeren en te mitigeren. Dit risicobeheer omvat 4 aspecten: technisch, organisatorisch, financieel en sociaal. Vanuit een technisch perspectief ligt het belang bij het patchen voordat actoren kwetsbaarheden kunnen misbruiken,

het toepassen van preventieve maatregelen zoals multi-factor authenticatie (MFA) en firewalls. Maar óók bij het toepassen van monitoring en logging waarmee onregelmatige activiteiten gedetecteerd kunnen worden. Daarnaast zien we dat voortdurende risicobeoordelingen essentieel zijn om het risicoprofiel van de organisatie goed in te schatten en de potentiële impact van een dreiging op kritieke bedrijfsprocessen te evalueren. Hoe beter deze inschatting, hoe effectiever dreigingen kunnen worden voorkomen en verholpen. Het afstemmen van cybersecurityinitiatieven met bedrijfsdoelen zorgt er dan ook voor dat middelen worden ingezet waar ze het hardst nodig zijn.

Een belangrijk organisatorisch aspect is het hebben van incident respons plannen en draaiboeken. Deze zorgen ervoor dat, als er iets gebeurt, organisaties sneller kunnen reageren en de schade beperkt blijft. Dit helpt bedrijfsprocessen te continueren en voorkomt dat een incident onnodig uitdraait op een crisis. Ook vanuit de Europese Commissie wordt hier aandacht aan besteed. In 2025 brengt de commissie een herziene versie van de Cyber Blueprint uit. Het doel

hiervan is om op een toegankelijke manier het EU-raamwerk voor cyber crisismanagement toe te lichten en awareness te creëren voor de mechanisme die gebruikt kunnen worden tijdens een crisismanagement levenscyclus.¹ De aandacht van de Europese Commissie voor dit onderwerp benadrukt het belang van cybersecurity op tactisch niveau. Het is een duidelijke boodschap aan Europese organisaties om crisismanagement hoog op de agenda te plaatsen.

In het geval dat een incident of crisis toch plaatsvindt, ervaren organisaties vaak de grootste gevolgen door financiële verliezen, reputatieschade en eventuele juridische consequenties, zoals boetes of proceskosten. Dit maakt het behouden van het vertrouwen van burgers of klanten eveneens cruciaal. Een organisatie die haar cybersecurity goed op orde heeft met een duidelijke strategie, bevordert haar reputatie. Zo kan een slechte reputatie op haar beurt ook weer impact hebben op de wendbaarheid van een organisatie. Dit is duidelijk zichtbaar in cyberaanvallen zoals die bij SolarWinds. Dit bedrijf werd in december 2020 getroffen door

een supply chain-aanval. Meer dan 18.000 klanten, waaronder meerdere Amerikaanse overheidsinstanties en bedrijven zoals Microsoft, installeerden een geïnfecteerde update. Dit leidde tot ernstige reputatieschade, een daling van de aandelenkoers en een rechtszaak. Proactief risicobeheer helpt dus om kosten te besparen. Een incident is duur, zowel door de directe schade als door de nevenschade. Door betere besluitvorming kan de juiste kennis en kunde gealloceerd worden en kunnen organisaties efficiënter en effectiever opereren.

Het belang van bewustwording en training

Naast proactief risicobeheer zijn bewustwording en training van medewerkers van groot belang voor het succes van een cybersecuritystrategie en het behouden van organisatorische wendbaarheid. Medewerkers spelen een cruciale rol in het beschermen tegen cyberdreigingen, omdat de meeste cyberincidenten ontstaan

door menselijke fouten. Hun kennis en alertheid kunnen het verschil maken tussen een afgewend incident en een succesvolle aanval. Door medewerkers bewust te maken van de risico's en dreigingen omtrent cybersecurity en hen te trainen in hoe ze moeten reageren, kunnen organisaties een hoop schade voorkomen. Om het cybersecurity niveau binnen een organisatie te verhogen zou dit onderwerp gezien moeten worden als meer dan een compliance vinkje zetten. De Cbw draagt hieraan bij. De wet zorgt er niet alleen voor dat organisaties medewerkers betrekken bij het stellen van strategische prioriteiten en het identificeren van risico's, maar ook dat bewustwording en training hoog op de agenda komen te staan. Op deze manier worden werknemers zich bewust van de essentiële rol die zij spelen in het beschermen van de digitale infrastructuur van de organisatie. Werknemers die goed geïnformeerd en getraind zijn, kunnen potentiële dreigingen



sneller herkennen en adequaat reageren. Dit versterkt de algehele weerbaarheid van de organisatie. Naast aandacht voor de werknemer is een belangrijk aspect van de Cbw de nadruk op persoonlijke aansprakelijkheid van bestuurders. Hierbij moet specifiek het senior management getraind worden om de cybersecurityrisico's en mogelijke impact op de bedrijfsvoering te begrijpen. Dit is noodzakelijk omdat hun kennis van security grote invloed heeft op de sturing van de organisatie en omdat ze in het geval van bewezen nalatig handelen, aansprakelijk gesteld kunnen worden voor het cybersecurity incident. Regelmatige training en het creëren van bewustwording bevordert een proactieve houding en inzicht in cybersecurity bij zowel de werknemers als het senior management van een organisatie. Investeren hierin zorgt niet alleen een voor een veiligere organisatie, maar ook voor een veiligere samenleving. Society 5.0 zet aan tot het behoud

van de menselijk maat, publieke waarden, veiligheid, ethiek en het investeren in de digitale vaardigheden van burgers, werknemers en leiders van private en publieke organisaties.² Door deze benadering te integreren in hun cybersecuritystrategie, kunnen organisaties niet alleen voldoen aan de eisen van de Cbw, maar ook hun wendbaarheid en weerbaarheid behouden in een dynamisch dreigingslandschap.

Wendbaarheid en weerbaarheid in Society 5.0

Niet alleen het dreigingslandschap is tegenwoordig digitaal en dynamischer, maar ook de samenleving waarin burgers en bedrijven steeds meer berusten op digitale diensten en producten. Dit leidt ertoe dat de behoefte aan continuïteit van digitale diensten en producten groter is dan ooit. In sommige gevallen is deze continuïteit ook cruciaal voor het functioneren van de (digitale) samenleving. Hiervoor hoeven we niet verder te kijken dan de lokale supermarkt,

die door een storing problemen kan hebben met de toelevering van producten. Een voorbeeld hiervan is de ransomware-aanval die leidde tot lege kaasschappen in 2021.³ Een soortgelijk scenario zou zich kunnen afspelen in de toeleveringsketen van medicijnen of eerste levensbehoeftes, met potentieel verregaande gevolgen.

De NIS2 en daarmee de Cbw zijn een weerspiegeling van deze behoefte naar continuïteit van diensten en zorgen ervoor dat deze beter gewaarborgd wordt door het sturen op beheer van cybersecurity risico's. Door het beheren van risico's en het implementeren van alle daarbij horende initiatieven (awareness, crisisbeheer, incident respons, et cetera) stijgt de weerbaarheid van organisaties. Wanneer organisaties een cybersecuritystrategie implementeren en deze koppelen aan hun bedrijfsdoelen zal de weerbaarheid van digitale diensten voor de samenleving toenemen. Wendbare digitale diensten zijn voorbereid op de risico's van nu en van morgen. Dit heeft invloed op de weerbaarheid en daarmee de beschikbaarheid van de dienst voor de samenleving. In de samenleving van morgen, Society 5.0, is het van cruciaal belang dat de mens kan vertrouwen op technologie en er geïnvesteerd wordt in manieren om dit vertrouwen te verhogen. De Cbw biedt een kans om cybersecurity naar een hoger niveau te tillen. Organisaties kunnen deze grijpen door een strategie te implementeren.

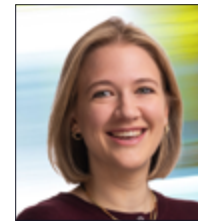


Conclusie

Een cybersecuritystrategie is essentieel om organisaties te beschermen tegen een toenemend aantal cyberdreigingen, financiële schade te voorkomen, gevoelige data te beschermen en de continuïteit van kritieke bedrijfsprocessen te waarborgen. Het biedt voordelen zoals proactief risicobeheer en ondersteunt de visie van Society 5.0. Proactief risicobeheer creëert immers een veilige en weerbare digitale omgeving die economische groei en maatschappelijke welzijn bevordert. De Cbw helpt organisaties om cybersecurity gestructureerd en systematisch te benaderen, waardoor ze beter voorbereid zijn op toekomstige dreigingen. In Society 5.0 staan naast proactief risicobeheer technologie en mens centraal. Daarom is het essentieel dat medewerkers zich bewust zijn van hun rol in het beschermen van hun organisatie. Regelmatige training en het creëren van bewustwording helpt om een proactieve houding binnen cybersecurity

te ondersteunen. Medewerkers die goed geïnformeerd en getraind zijn, kunnen potentiële dreigingen sneller herkennen en beter reageren. Dit versterkt de algehele weerbaarheid van de organisatie. Door training en bewustwording te integreren in hun cybersecuritystrategie, kunnen organisaties niet alleen voldoen aan de eisen van de Cbw, maar ook hun wendbaarheid en weerbaarheid behouden in een dynamisch dreigingslandschap. Dit is van groot belang, omdat door de digitalisering van de samenleving en de afhankelijkheid van digitale diensten, continuïteit cruciaal is. De NIS2 en Cbw bevorderen de weerbaarheid via onder andere risicobeheer en het creëren bewustwording. Een cybersecuritystrategie, gekoppeld aan bedrijfsdoelen, versterkt de wendbaarheid. Samen zorgen ze dat de burger kan vertrouwen op de continuïteit van onmisbare digitale diensten in Society 5.0.

Over de auteurs



Sasha Brouwer

Senior Management Consultant bij Capgemini Invent

Sasha is gespecialiseerd in cybersecurityvraagstukken binnen het publieke en commerciële domein en richt zich op organisatievraagstukken met betrekking tot EU-richtlijnen, cybersecuritystrategie en leveranciersmanagement.

✉ sasha.brouwer@capgemini.com

in <https://www.linkedin.com/in/sashabrouwer/>



Emir Hajduk

Senior Management Consultant bij Capgemini Invent

Emir richt zich op cybersecurityvraagstukken in het publieke en commerciële domein met een focus op cybersecuritystrategie, cybersecurity governance, Europese wet- en regelgeving en cybersecurity samenwerkingsverbanden.

✉ emir.hajduk@capgemini.com

in <https://www.linkedin.com/in/emir-hajduk-786146175/>

Bronnen

1. <https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation>
2. <https://www.capgemini.com/nl-nl/expertise/research/society-5-0-de-randvoorwaarden-voor-succes/>
3. <https://nos.nl/artikel/2376425-kaas-hack-opgelost-ging-om-gijzelsoftware>

Data Trust by Design: de sleutel tot vertrouwen, wendbaarheid en weerbaarheid

Hoe kunnen overheidsorganisaties door het toepassen van Data Trust by Design zowel vertrouwen opbouwen als wendbaar en weerbaar blijven in een steeds complexere digitale samenleving?



Highlights

- Digitale transformatie biedt ongekende kansen voor de publieke sector, maar brengt ook grote uitdagingen mee. Overheidsorganisaties moeten inspelen op voortdurende technologische en maatschappelijke veranderingen, terwijl ze ook moeten voldoen aan data-gerelateerde wetgeving.
- In de gedigitaliseerde samenleving gaat vertrouwen verder dan een ethisch uitgangspunt; het is een essentiële succesfactor voor overheidsorganisaties. Burgers en ketenpartners verwachten dat hun gegevens veilig en ethisch verantwoord worden verwerkt.
- Overheidsorganisaties moeten wendbaar zijn om tijdig in te spelen op wetgeving, technologische innovaties en maatschappelijke veranderingen, zonder concessies te doen aan gegevensbescherming. Tegelijkertijd is weerbaarheid noodzakelijk om bescherming te bieden tegen dreigingen zoals cyberdreigingen en datalekken.
- Data Trust by Design is een strategie die security, privacy, data-ethiek, datakwaliteit en interdisciplinaire samenwerking structureel verankert in systemen en processen. Organisaties kunnen zo uitdagingen die gepaard gaan met de naleving van wet- en regelgeving transformeren in strategische voordelen.

In Society 5.0 lopen de fysieke en digitale wereld naadloos in elkaar over. Burgers en ketenpartners verwachten in deze gedigitaliseerde samenleving dat hun gegevens veilig en ethisch verantwoord worden verwerkt. Vertrouwen gaat verder dan een ethisch uitgangspunt en is een essentiële succesfactor voor overheidsorganisaties. Om vertrouwen te verdienen van burgers en ketenpartners, is enkel de naleving van wetgeving zoals de AVG en de Europese AI Act niet voldoende. Organisaties moeten verder gaan dan compliance en digitale verantwoordelijkheid structureel verankeren in hun processen en diensten. Data Trust by Design biedt hiervoor een aanpak, waarin security, privacy, data-ethiek en datakwaliteit integraal centraal staan. Door deze principes integraal te benaderen, kunnen organisaties niet alleen vertrouwen opbouwen, maar ook flexibel inspelen op veranderingen en zich beschermen tegen digitale dreigingen. De sleutel tot succes ligt in een gezamenlijke aanpak waarin expertise uit verschillende disciplines wordt gecombineerd om data governance duurzaam en effectief vorm te geven.

De uitdagingen voor de publieke sector

Een cruciale uitdaging voor de publieke sector is het geven van vertrouwen, omdat burgers verwachten dat hun gegevens veilig, ethisch en verantwoord worden verwerkt. Deze verwachting groeit naarmate digitale technologieën een grotere rol spelen in het dagelijks leven. Wanneer dat vertrouwen ontbreekt, kan dit leiden tot weerstand tegen nieuwe digitale initiatieven. Daarom wordt het voor overheidsorganisaties steeds belangrijker om vertrouwen op te bouwen en te behouden.

Daarnaast vereist de steeds complexer wordende digitale omgeving dat overheidsorganisaties zowel wendbaar als weerbaar zijn.

Wendbaarheid is noodzakelijk om snel te kunnen inspelen op veranderingen in wet- en regelgeving, technologische innovaties en maatschappelijke verwachtingen, zonder concessies te doen aan gegevensbescherming of privacy. Tegelijkertijd is weerbaarheid essentieel om bescherming te bieden tegen dreigingen zoals cyberaanvallen en datalekken. Deze dreigingen nemen in frequentie en impact toe en kunnen niet alleen organisaties, maar ook de samenleving als geheel ontwrichten.

Om deze uitdagingen effectief aan te pakken, is het cruciaal om gegevensbeschermingsprincipes vanaf het begin in systemen en processen te verwerken. De AVG verplicht overheidsorganisaties om gegevensbeschermingsprincipes vanaf de ontwerpfase in systemen en diensten te integreren, zoals gegevensminimalisatie, opslagbeperking, en integriteit en vertrouwelijkheid. Tegelijkertijd legt de EU AI Act de nadruk op transparantie en verantwoordelijkheid in het gebruik van AI-systemen, wat cruciaal is voor het behoud van het vertrouwen van burgers. De Cyber Resilience Act (CRA), die in 2025 in werking zal treden, verplicht organisaties om cybersecurity als een integraal onderdeel van hun productontwikkeling te beschouwen, waardoor de weerbaarheid tegen dreigingen wordt versterkt. Deze wetgeving weerspiegelt een trend waarbij transparantie en veiligheid structureel verankerd worden in de kern van digitale innovatie.

Het succes van de publieke sector in het navigeren door deze uitdagingen hangt af van de strategieën die organisaties inzetten om te voldoen aan data-gerelateerde wetgeving en effectief om te gaan met de complexe uitdagingen binnen de digitalie samenleving. Ondanks de duidelijke wettelijke verplichtingen ervaren veel organisaties de naleving ervan als een afvinkoefening. Het aanpassen van bestaande systemen,



trainen van personeel en uitvoeren van regelmatige beoordelingen kan complex en uitdagend zijn, wat vaak tot weerstand leidt. Deze reactieve houding belemmert de kans om verder te kijken dan naleving en vertrouwen als onderscheidende factor te benutten.

Data Trust by Design: een strategie voor vertrouwen en innovatie

Data Trust by Design is een strategie gericht op samenwerking die organisaties ondersteunt bij het structureel toepassen van beginselen op het gebied van security, privacy, data-ethiek en datakwaliteit in hun processen en product- en dienstverlening. Interdisciplinaire samenwerking is hierbij essentieel. Het concept gaat verder dan naleving van wet- en regelgeving en richt zich op het creëren van een ecosysteem waarin deze principes centraal staan in elke interactie, beslissing en product. Het stelt organisaties in staat om vertrouwen op te bouwen en te onderhouden en tegelijkertijd wendbaar te blijven in het inspelen op veranderingen en weerbaar te zijn tegen potentiële dreigingen. Dit zijn de vijf kernpijlars van Data Trust by Design.

Security

Robuuste gegevensbeveiligingsmaatregelen vormen de basis voor een veilige digitale infrastructuur. Denk hierbij aan het gebruik van encryptie, regelmatige kwetsbaarheidsbeoordelingen en effectief toegangsbeheer. Deze maatregelen helpen organisaties om gevoelige gegevens te beschermen tegen datalekken en cyberaanvallen. Voor AI-systemen is het daarnaast essentieel om cyber resilience-mechanismen te integreren, zodat ze flexibel kunnen reageren op veranderende dreigingen. Door security vanaf de ontwerpfase in systemen te verankeren, kunnen organisaties een stevige bescherming bieden tegen huidige en toekomstige risico's.

Privacy

Het voldoen aan privacyregelgeving gaat verder dan compliance; het is ook een strategisch voordeel dat organisaties onderscheidend kan maken. Door transparantie in gegevensverzameling en -gebruik te prioriteren, kunnen organisaties vertrouwen opbouwen bij de burgers. Het bieden van deze transparantie zorgt ervoor dat burgers vertrouwen

hebben in de wijze waarop hun gegevens worden verwerkt. Door privacy principes te integreren, kunnen organisaties niet alleen voldoen aan wettelijke vereisten, maar ook een ethisch verantwoord databeleid voeren dat de relatie met de burger versterkt.

Data-ethiek

In een tijd waarin datagedreven besluitvorming en AI-toepassingen steeds prominenter worden, is het voorkomen van vooroordelen (bias) en het waarborgen van rechtvaardigheid en verantwoordelijkheid in besluitvorming essentieel. Organisaties moeten ervoor zorgen dat hun systemen geen onbedoeld discriminerende of oneerlijke resultaten opleveren. Proactieve ethische beoordelingen helpen hierbij: door risico's en controverses in een vroeg stadium te identificeren, kunnen problemen worden voorkomen. Dit versterkt niet alleen de acceptatie van technologieën, maar draagt ook bij aan het vertrouwen van burgers in de integriteit van de besluitvorming.

Datakwaliteit

De complexiteit van dataketens maakt inzicht in de herkomst en kwaliteit van gegevens onmisbaar. De oorsprong van data beïnvloedt direct de waarde, betrouwbaarheid en bruikbaarheid ervan. Lange en ondoorzichtige gegevensketens brengen risico's met zich mee, zoals onbetrouwbare informatie of fraude en misleidende analyses. Voor de publieke sector kan dit leiden tot onterechte besluitvorming en foutieve toekenning van middelen, zoals subsidies of uitkeringen. Het implementeren van data kwaliteitscontroles is daarom essentieel om zowel de authenticiteit van gegevens als betrouwbaarheid van uitkomsten te waarborgen. Dit voorkomt niet alleen fouten in de verwerking en interpretatie van data, maar creëert ook een solide basis voor effectieve en betrouwbare gegevensverwerking en besluitvorming, wat essentieel is voor transparantie en verantwoorde beleidskeuzes

Interdisciplinaire samenwerking

Expertise op het gebied van de hierboven genoemde pijlers is doorgaans wel aanwezig in organisaties. Wat vaak nog ontbreekt is een proactieve en structurele samenwerking tussen de verschillende vakdisciplines. Door kennis op het gebied van security, privacy, data-ethiek en datakwaliteit te combineren en toe te passen in de bedrijfsprocessen, wordt optimaal ingespeeld op actuele regelgeving en maatschappelijke en technologische ontwikkelingen. Continue samenwerking is hierbij van belang. Doorgaans werken deze vakdisciplines wel samen bij het ontwikkelen van processen en diensten maar verder niet. Juist door gedurende de gehele data levenscyclus kennis te combineren en toe te passen wordt een ijzersterke datastrategie neergezet.



Wendbaarheid en weerbaarheid door Data Trust by Design

Het concept Data Trust by Design draagt niet alleen bij aan het opbouwen en onderhouden van vertrouwen, maar stelt organisaties ook in staat om zowel wendbaar als weerbaar te zijn in een steeds complexer wordende digitale samenleving. Wendbaarheid wordt bereikt doordat privacy-, security-, datakwaliteit- en data-ethiekprincipes vanaf het begin geïntegreerd worden in systemen en processen. Voortdurende interdisciplinaire samenwerking maakt het mogelijk om snel en effectief in te spelen op veranderingen, zoals nieuwe wetgeving, technologische innovaties en verschuivingen in maatschappelijke verwachtingen. Organisaties kunnen zich daardoor flexibel aanpassen aan externe ontwikkelingen, zonder in te leveren op de bescherming van gegevens of de naleving van regelgeving.

Daarnaast helpt een sterke weerbaarheid organisaties tegen potentiële dreigingen, zoals cyberaanvallen, datalekken en misbruik van gegevens. Door robuuste beveiligingsmaatregelen zoals encryptie, regelmatige kwetsbaarheidsbeoordelingen en toegangscontroles te implementeren, kunnen organisaties hun systemen en gegevens beter beschermen tegen deze dreigingen. Het integreren van cyber resilience-mechanismen in systemen, zoals beschreven in de sectie Security in

de vorige paragraaf, stelt organisaties in staat om zich aan te passen aan veranderende dreigingen en risico's effectief te beheren. Data Trust by Design biedt niet alleen de tools en strategieën om risico's te minimaliseren, maar versterkt tegelijkertijd de weerbaarheid van organisaties tegen toekomstige bedreigingen in een dynamische digitale omgeving.

Aanpak voor Data Trust by Design

Cappgemini Invent ondersteunt organisaties bij het opzetten van een Data Trust by Design-raamwerk. Deze methodologie richt zich op:

1. Beoordeling van de huidige volwassenheid

- Uitvoeren van uitgebreide audits van bestaande systemen, processen en beleidsmaatregelen om hiaten te identificeren.
- Benchmarken tegen industriestandaarden en regelgeving.

2. Strategische afstemming

- Gegevensbeschermingsinitiatieven afstemmen op organisatiedoelen om waarde te genereren in plaats van als belemmering te fungeren.
- Ontwikkelen van een op privacy gerichte cultuur waarin medewerkers op alle niveaus het belang van vertrouwen in gegevensbeheer begrijpen.

3. Ontwerp en implementatie

- Privacy, security, data-ethiek, datakwaliteit en voortdurende interdisciplinaire samenwerking integreren in de data levenscyclus van producten en diensten. Door

bestaand beleid aan te vullen in plaats van nieuw beleid te creëren, wordt implementatie en blijvend gebruik effectiever.

- Gebruik maken van geavanceerde technologieën, zoals privacy-preserving computation en differentiële privacy, om naleving te verbeteren en datagedreven innovatie te ondersteunen.

4. Continue verbetering

- Mechanismen opzetten voor voortdurende monitoring, feedback en aanpassing aan veranderende bedreigingen en regelgeving.
- Een proactieve benadering van gegevensbescherming stimuleren in plaats van reactief te handelen.
- Stakeholders betrekken door gezamenlijke doelen na te streven, wat langdurige betrokkenheid en succes binnen de organisatie vergroot.

Conclusie

Data Trust by Design is meer dan een strategie om aan wet- en regelgeving te voldoen. Het is een toekomstgerichte benadering die organisaties in de publieke sector in staat stelt om digitaal vertrouwen op te bouwen en om de uitdagingen van wendbaarheid en weerbaarheid effectief aan te pakken.

Door security, privacy, data-ethiek, datakwaliteit en interdisciplinaire samenwerking te integreren in hun bedrijfsvoering, kunnen organisaties uitdagingen die gepaard gaan met de naleving van wet- en regelgeving transformeren in strategische voordelen.

De expertise van Capgemini Invent bij het opzetten van Data Trust by Design-raamwerken stelt organisaties in staat om succesvol te opereren in dit nieuwe tijdperk van innovatie gedreven door vertrouwen. Door vertrouwen te prioriteren, creëren organisaties blijvende waarde voor zichzelf en voor burgers en andere belanghebbenden. Ze laten zien dat verantwoord omgaan met gegevens niet alleen juist is, maar ook een slimme keuze. Dit stelt hen in staat niet alleen vandaag te innoveren, maar zich ook voor te bereiden op de uitdagingen van morgen, met de wendbaarheid om zich aan te passen en de weerbaarheid om zich te beschermen tegen de risico's van een dynamische digitale toekomst.

Over de auteurs



Albert Holl

Data Trust lead en als director werkzaam bij Capgemini Invent NL

Albert heeft uitgebreide consultancy ervaring en als Fellow of Information Privacy (FIP) heeft hij een sterke achtergrond en ervaring op het gebied van Privacy en de AVG. Albert heeft uitgebreide expertise in het creëren en verbeteren van Data Trust-frameworks in organisaties, cloudtransformatieprojecten en geavanceerde tools voor privacybeheer. Hierdoor heeft hij een sterke focus ontwikkeld op Data Trust by Design, de AI Act en risk management.

✉ albert.holl@capgemini.com

in <https://www.linkedin.com/in/albert-holl-fip-9041704/>



Jolie Sillevs

Consultant bij Capgemini Invent NL, gespecialiseerd in data privacy

Met een juridische achtergrond in privacy recht en ervaring als Privacy Officer in grote cloudtransformatieprojecten heeft Jolie zich gericht op het implementeren van Privacy by Design in complexe digitale omgevingen. Haar werk omvat het vertalen van wet- en regelgeving naar praktische en schaalbare oplossingen.

✉ Jolie.sillevis@capgemini.com

in <https://www.linkedin.com/in/jolie-sillevis/>



Prija Rambali

Data Privacy lead en senior manager bij Capgemini Invent NL

Prija heeft een sterke juridische achtergrond en is ruim 17 jaar werkzaam als advocaat en consultant. Haar expertise in privacy en de AVG combineert zij met een sterke focus op de AI Governance en Data Trust. Haar ervaring op het gebied van het implementeren van Privacy by Design-vereisten in grote softwaretransformatieprojecten kenmerkt zich door een pragmatische aanpak en het vertalen van wettelijke vereisten naar werkbare oplossingen.

✉ prija.rambali@capgemini.com

in <https://www.linkedin.com/in/prija-rambali/>

Autonomie uitbesteden? De rol van soevereine cloud

Hoe kunnen we digitale autonomie en zelfredzaamheid van Nederland waarborgen?

Geopolitieke onrust benadrukt de noodzaak van digitale autonomie en zelfredzaamheid voor de BV Nederland. Maar hoe voorkomen we dat de 'burger centrische digitalisering' hierdoor niet wordt geremd? En hoe zorgen we dat we snel met nieuwe wel autonome alternatieven komen? De politiek praat hierover, maar het is een vraagstuk dat onze industrie en dienstensector minstens zoveel raakt als de overheid.

Highlights

- Technologisch autonoom blijkt veel belangrijker dan we dachten.
- Een "stapel" problemen: overal in de stack zijn we (te) afhankelijk.
- Stappenplan naar een stack 5.0 die ons beter past.



Met de toename van geopolitieke onrust in de afgelopen jaren is de vraag hoe we de 'BV Nederland' beter kunnen beschermen boven aan onze agenda gekomen. Zeker ook in de digitale wereld. De nu geldende wet- en regelgeving en het rijkscloudbeleid 2022 zijn ontoereikend. Bovendien concludeert de Algemene Rekenkamer dat ook die niet serieus genoeg genomen zijn en soms ook niet in een goede kwalitatieve risicoafweging gevat zijn. In veel gevallen weten we niet goed genoeg hoe groot onze afhankelijkheid in het domein van big tech is. Heel recent zijn er nieuwe en vooral praktische risico's aan het licht gekomen die we eerder niet of niet volledig hebben onderkend. Met name dat een technologische afhankelijkheid gebruikt kan worden om ons onder druk te zetten in een handelsoorlog of bij het dreigen met sancties. Het sterk toegenomen aantal incidenten in de Noord- en Oostzee rond zeekabels toont de fysieke kant van onze afhankelijkheid. Allemaal aanleidingen om meer nadruk te leggen op zelfredzaamheid en autonomie van onze BV Nederland. En de noodzaak om dat voor de grote dingen als hyperscale datacenters en AI factories in Europa te concentreren.

Een "stapel" problemen: overal in de stack zijn we (te) afhankelijk

Het gaat om veel meer dan alleen de ICT-infrastructuur, hardware en netwerkkabels. Alles heeft software nodig en 'alle software zelf maken' zou ons snel terugwerpen in de jaren '70. Het zou ons namelijk afsluiten van alle innovatie op het gebied van hardware en software buiten Nederland. Juist de (veelal Amerikaanse) hyperscalers investeren stevig in vernieuwing en veiligheid. Hardware, energiegebruik in het kader van ESG, software en AI inclusief de daarin gebruikte data gaan hand in hand. We kunnen dus niet zonder toegang tot technologie van buiten, Amerikaanse technologie en wereldwijde technologie. Hoe brengen we dat in balans met het voorkomen van afhankelijkheid? Als we autonomie invullen met 'zorgen dat we alternatieven hebben' en 'snel genoeg kunnen switchen' en een fallback scenario, kunnen we aangesloten blijven op wereldwijde innovaties en toch voldoende sturen op onze eigen belangen. Naast



de harde IT-kant is uiteraard het hebben van de juiste kennis en talent essentieel. Zonder die kennis, gaat “snel genoeg switchen” niet lukken. Kennis is macht.

Het vanuit de overheid opzetten van één lokale Nederlandse Cloud infrastructuur vermindert de risico's niet zo goed als sommigen verwachten. Onderschatten van ICT-projecten is binnen de overheid al iets te vaak gebeurd. Het risico van single-point-of-failure is te groot. Eén is geen, ook in de wereld van Cloud. Zo'n overheids-only oplossing leidt niet tot de noodzakelijke kennisdeling met het bedrijfsleven. Bedrijven hebben net zo goed belang bij onafhankelijkheid en concurrentiepositie. De overheid is – zelfs als deze overheidsbreed als één geheel zou optreden – te klein om dit alleen te doen. Society 5.0 bestaat niet uit een overheid 5.0 en een bedrijfsleven 5.0, maar samen. Dat geldt bij uitstek rond onze digitale autonomie. Vanuit het Europese Draghi rapport is het daarom nodig dat we op het cloudterrein tot komen. Niet voor niets maakt het “EuroStack”¹ initiatief daarbij een knipoog naar de gezamenlijke munt. Er zijn wel degelijk Europese successen. Zijn we in staat de trend om te draaien en een bij de Society 5.0 passende stack 5.0 te realiseren?

Stappenplan naar een stack 5.0 die ons beter past

De impact die Cloud technologie als digitale katalysator kan brengen voor de burger - als klant van de overheid -, is onveranderd. En ook in industrie en diensteneconomie blijft Cloud technologie de hoofdstroom. Zonder cloud geen Society 5.0! Op alle lagen van “de stack”, van energie tot software tot data moeten we daarvoor stappen zetten. Het goede nieuws is ook dat we op heel veel onderwerpen top-research en experts

hebben, ook in Nederland. Waar we minder goed in zijn, is het “doen” en praktisch aan elkaar knopen van schaalbare oplossingen.

Iedere organisatie heeft daarin een verantwoordelijkheid. Als individuele overheidsorganisaties en bedrijven vanuit dat uitgangspunt aan de slag gaan, kan het snel gaan.

Veilig is subjectief en daarmee is het soms lastig om het in één strategie te vatten. Wat zijn dan wel de acties om zowel verantwoord vooruit te bewegen?

1. Denk vanuit de business-verantwoordelijkheid. Wat wil je zelf doen en wat niet. Voor wat je niet zelf wil doen, wil je kwalitatief goede ondersteuning. Weet wat essentieel is aan de diensten die je uitbesteedt, inbesteedt of op andere manier niet zelf doet. Maak een lijst van alle relaties waarvan je afhankelijk bent en doe op vrijdagmiddag de gedachtenoefening “wat als ik die dienst of partij moet inruilen voor een ander”. Ieder kan dit doen op zijn eigen niveau van verantwoordelijkheid, van productteam, tot afdeling, tot maatschappelijk domein.
2. Overlevingsvermogen (op langere en korte termijn): een ééndimensionale strategie, één infrastructuur, één Nederlandse Cloud is geen. Echte antwoorden en veerkrachtig liggen in bredere infrastructuur met meer aanbieders, keuzes en “common good”. Lokale infrastructuur is belangrijk, maar in onze tech-maatschappij zit dat letterlijk aan vanalles vast. Interoperabiliteit, standaarden en kunnen overstappen zijn in ieder probleemsценario relevant. Alternatieven voor de Amerikaanse hyperscalers en SaaS aanbieders met aantrekkelijk totaalaanbod

zijn nodig en tegelijk zullen we ze blijven gebruiken en blijft dat in veel omstandigheden met de juiste maatregelen een logische keuze.

3. Korte termijn risico's mitigeren door de kwaliteit van bestaande diensten op niveau te brengen en te proberen in de relatie met aanbieders van diensten voldoende waarborgen te krijgen. Binnen de overheid zal beter moeten worden samengewerkt om wat er wel is, bijvoorbeeld in de Overheids Data Centers (ODC's) slimmer te gebruiken en te combineren. Schaalgrootte is nodig en die ontstaat door bestaand aanbod te combineren. Het helpt enorm als je je basisbeveiliging op orde hebt en klaar bent om de NIS2 pro-actief te implementeren. Als je dat niet op orde brengt, is de afhankelijkheid van partijen je kleinere probleem. Daarnaast zijn brede investeringen nodig, in vervolg op het Draghi rapport. Bijvoorbeeld in de richting van het EuroStack initiatief. Voor de middellange termijn is

kennisdeling op Europees niveau cruciaal. Europese gezamenlijke oplossingen zijn politiek complex. Maar hergebruik van kennis en open standaarden is veel eenvoudiger. Zowel voor oplossingen binnen de overheid (ODCs) als voor aanbieders in de markt zal de middellange termijn afhangen van het vermogen de juiste keuzes te maken in het opvolgen en implementeren van deze en andere standaarden. Een voorbeeld is SECA, de The Sovereign European Cloud API2.

4. Voor de langere termijn gaat het om kennis. Society 5.0 heeft een industriepolitiek nodig die er aan bijdraagt dat kennis toegankelijk is en gedeeld wordt. Iedere organisatie in die Society. 5.0 is ook een kennisorganisatie. Kennis kun je nooit helemaal uitbesteden. Er is altijd een verantwoordelijkheid om genoeg kennis voorhanden te hebben om vooruit te kunnen, in huis of in samenwerking met anderen.

Kortom, 'never let a good crisis go to waste' en zorg dat ook de praktische stappen geborgd zijn. Dat is ieders eigen verantwoordelijkheid en kan niet worden uitbested. Cloud is daarin geen doel op zich. Wel is het nog steeds een kans voor veiligheid, onafhankelijkheid, duurzaamheid, innovatie en wendbaarheid.

De werkplek is een sleutelvoorbeeld en van nature complex vanwege de paraplu functie die het binnen een organisatie heeft. Iedereen heeft een "werkplek", van lagere school, naar werkplekken op kantoor, onderweg en op de device buiten. We gebruiken vrijwel allemaal Word en Teams omdat er weinig vergelijkbare, kwalitatieve alternatieven beschikbaar zijn. In een Society 5.0 heeft iedereen daarover nagedacht. Keuze en diversiteit zijn gezond en horen bij Society 5.0 en daarmee dus ook werkplek 5.0.



Conclusie

Samenvattend kunnen we opmaken dat we alle theoretische puzzelstukjes van 'de wat' en 'waarom' al hebben. Het gaat om 'de hoe' en het doen. Dat zal samen moeten, in Europees verband, vanwege schaalgrootte. Maar dat begint met iedere individuele organisatie in Nederland die zelf naar eigen inkoop van ICT-diensten kijkt. Aan de slag om daar waar afhankelijkheid echt pijn doet concrete alternatieven te maken en gebruiken. Met de juiste mix van Nederlandse, Europese en wereldwijde oplossingen kan de cloud van een bedreiging omgewerkt worden tot een kans: Een Cloud en technologiestack die overheid en bedrijven we samen gebruiken en doorontwikkelen.

Over de auteurs



Bart Turk

Bart Turk is werkzaam bij Capgemini Invent als Cloud lead

Bart heeft zowel hands-on ervaring met Cloud technologie als Architect als ook ervaring met Cloud transformaties, strategie en governance bij verschillende organisaties. Hij is de Cloud Business Transformation lead waar hij organisaties helpt met strategische vraagstukken en cloud transformaties.

✉ bart.turk@capgemini.com

🌐 <https://www.linkedin.com/in/bart-turk-39a6b8112/>



Jurjen Thie

Jurjen Thie is werkzaam bij Capgemini als Cloud strategist

Jurjen heeft een brede ervaring, variërend van Cloud Strategie advies tot Transitie- en Transformatieprojecten bij diverse grote bedrijven. Hij speelt een cruciale rol in het vergroten van de waarde van Cloud technologie, Cloud mindset en het toepassen ervan binnen verschillende organisaties. Als onderdeel van het Nederlandse Cloud CoE heeft hij als Cloud Strategist een passie voor complexe, holistische vraagstukken en probeert op een creatieve manier het juiste probleem op te lossen.

✉ jurjen.thie@capgemini.com

🌐 <https://www.linkedin.com/in/jurjenthie/>



COLOFON

Deze editie van society 5.0 is tot stand gekomen met medewerking van:

Roeland de Koning

Nanny Schoenmakers

Diederik Journée

Erik Hoorweg

Ernest – Jan Mutsaers

Marjolein Wenderich

Fokko Dijksterhuis

Advies, ontwerp en productie: Marketing & Communicatie, Capgemini Nederland B.V.

Duygu Mun

Runa Roychowdhury

Arindam Dey



Over Capgemini

Capgemini is een wereldwijde, maatschappelijk verantwoorde en multiculturele marktleider met 340,000 mensen in bijna 50 landen. Als strategisch partner ondersteunt Capgemini organisaties bij hun transformatie door gebruik te maken van de kracht van technologie. Hierbij laat de Group zich leiden door zijn bestaansreden: menselijke energie vrijmaken door middel van technologie voor een inclusieve en duurzame toekomst. Met meer dan 50 jaar ervaring en expertise in uiteenlopende sectoren, vertrouwen klanten de aanpak van hun zakelijke behoeften toe aan Capgemini: van strategie en ontwerp tot operationeel beheer. Dit gebeurt door gebruik te maken van innovaties in cloud, data, kunstmatige intelligentie, connectiviteit, software, digital engineering en platforms. De Group behaalde in 2023 een omzet van € 22.5 miljard.

Get the Future You Want | www.capgemini.nl

Capgemini Nederland B.V.
Postbus 2575 - 3500 GN Utrecht
Tel. + 31 30 203 05 00
www.capgemini.nl