Wereldcafé

Informatieveiligheid

Dit document is een initiatief van de Taskforce Bestuur en Informatieveiligheid Dienstverlening en vormt onderdeel van de coalitievorming tussen bestuurders uit de publieke en private sector, met als doel informatieveiligheid blijvend te verankeren.

12 maart 2014

Inhoud

Informatieveiligheid, samen aan de slag!

Nieuwe manier van denken… én sturen!

Onze samenleving digitaliseert, net als het openbaar bestuur. Onder de noemer ‘Digitaal 2017’ werkt de overheid hard aan het digitaliseren van alle overheidsdienstverlening voor het einde van 2017. Deze ontwikkeling vraagt om een denken en sturen waarbij leiderschap, risicoprioritering en -management en natuurlijk het beleggen van verantwoordelijkheden een cruciale plaats innemen. Het Ministerie van Binnenlandse Zaken (BZK) heeft de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) de opdracht gegeven om samen met koepelorganisaties en diverse samenwerkingspartners gericht bestuurlijke aandacht te vragen voor het onderwerp informatieveiligheid.
Hiertoe werkt de Taskforce BID niet alleen aan de realisatie van gerichtheid bij bestuurders en topambtenaren, maar ook aan het verankeren ervan op organisatie-, koepel- en stelselniveau.

Interbestuurlijke Coalitie Informatieveiligheid

De Taskforce BID is overtuigd van het belang van een blijvende coalitie om lopende en toekomstige ontwikkelingen effectief te laten landen en het onderwerp informatieveiligheid blijvend onder de aandacht te houden. De Taskforce BID werkt hiertoe samen met betrokken ministeries, koepelorganisaties en diverse partners aan een interbestuurlijke coalitie Informatieveiligheid. Een coalitie die gerichtheid stimuleert en ruimte biedt voor het borgen van resultaten en ontwikkelen van nieuwe perspectieven. Dit gebeurt op zo’n wijze dat informatieveiligheid concrete betekenis krijgt in mentaliteit en in toepasbare producten en diensten. Tijdens het eerste interbestuurlijk Diner Informatieveiligheid op 4 november 2013 is een start gemaakt met het bouwen van deze Interbestuurlijke Coalitie Informatieveiligheid. De basis van de coalitie bestaat uit de 120 bestuurders en topmanagers waarvan het merendeel aanwezig was tijdens het Diner. De resultaten van de tafeldialogen tijdens dit Diner hebben de basis gevormd voor de volgende stap in dit coalitievormende proces: het Wereldcafé Informatieveiligheid dat op 7 februari jl. heeft plaatsgevonden. Het Wereldcafé heeft als doel een eerste bestuurlijke Actie-Agenda op het gebied van informatieveiligheid op te stellen. In de maanden na 7 februari wordt deze informatieveiligheidsagenda stap voor stap gevuld met concrete afspraken en uitwerkingen van vraagstukken en handelingsperspectieven. Tijdens het volgende Interbestuurlijk Diner Informatieveiligheid eind 2014 worden de uitwerkingen plenair toegelicht en wordt een agenda voor het vervolg gepresenteerd.

Drie perspectieven

Uit de resultaten van het Diner van afgelopen november zijn drie perspectieven naar voren gekomen waarvan bestuurders hebben onderkend dat deze bestuurders voor een collectieve uitdaging stellen in het licht van informatieveiligheid. Centraal staat de behoefte om continu te leren van ervaringen op het

gebied van informatieveiligheid en deze te delen om zo proactief in te kunnen spelen op ICT-trends en ontwikkelingen, met bijbehorende ‘nieuwe’ risico’s.
Meer concreet waren tijdens het Diner drie perspectieven te onderscheiden:
(1) inspelen op informatisering door technologische ontwikkeling
(2) hoe verder te werken aan samenwerking
(3) hoe gerichtheid op informatieveiligheid lange termijn te verankeren

Een selectie van wetenschappers heeft hun visie gegeven op elk van deze drie perspectieven middels het schrijven van inspirerende essays. Essays die de basis vormen voor verdere gerichte gesprekken met betrokken ministeries, koepelorganisaties en diverse partners, en als input wordt gebruikt voor de vorming van de Actie-Agenda Informatieveiligheid. Eén van de punten die duidelijk naar voren komt, is dat informatieveiligheid een uitdaging van ons allemaal is. Kortom, samen aan de slag!

Essays

Bert Mulder

Lector Informatie, Technologie en Samenleving
Haagse Hogeschool

ICT: komende kansen en uitdagingen voor de overheid

Hoewel vaak gezegd wordt dat ICT-ontwikkelingen snel gaan, waren ze de laatste jaren toch ook vaak voorspelbaar: steeds meer rekenkracht, steeds kleiner, mobieler en goedkoper, betere databases, betere webontsluiting van informatie voor de klant. Die voorspelbaarheid verandert als de ICT-ontwikkelingen de komende jaren van een wezenlijk ander karakter zijn. De nadruk op de techniek zal verminderen terwijl de aandacht verschuift naar informatie en kennis.

De ontwikkelingen van ICT zullen in sterke mate bepaald worden door een externe factor: de demografie. Volgens schattingen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) (De Grote Uittocht herzien, 2013) zal het aantal overheidsmedewerkers de komende tien jaar met 40% afnemen en daarna mogelijk nog verder krimpen. Die ontwikkeling is bepalend, omdat de bijdrage van ICT aan belang wint. In het komende decennium zullen nieuwe oplossingen moeten worden gecreëerd, wil de overheid dezelfde kwaliteit kunnen leveren als zij vandaag doet. Nieuwe oplossingen richten zich niet op dingen beter doen of de dingen anders doen, maar op wezenlijk andere dingen doen. Binnen de overheid betekent het een andere inrichting van de organisatie met nieuwe en intensieve samenwerkingsrelaties met andere partners, zoals burgers. Niet alleen als afnemers van producten, maar als partners in het anders realiseren van oplossingen op het gebied van beleid en bestuur, diensten en uitvoering en de kwaliteit van leven in de samenleving. Buiten de overheid wordt ICT een essentieel element in het faciliteren van eigen regie en eigen verantwoordelijkheid van burgers. Dat ontwikkelen van de kracht van de samenleving – 'de participerende samenleving' – is essentieel om de kwaliteit van leven te kunnen blijven ondersteunen. Zoals twee decennia geleden het bezit van PC's en de toegang tot internet werden gestimuleerd, zal nu het strategisch gebruik van ICT-mogelijkheden om de kwaliteit van het eigen leven te verbeteren moeten worden gestimuleerd. Daarmee is het realiseren van de mogelijkheden van nieuwe ICT-trends die hierna worden beschreven essentieel voor zowel de transformatie van de eigen overheid als die van de samenleving.

Er zijn drie trends die de aandacht van de overheid vragen:

- **Slimme gegevens:**
  de toenemende hoeveelheid informatie en big data, open data en een transparante overheid.
- **Het slimme web:**
  web 3.0, web 4.0 en de overgang van informatie naar kennis.
- **De slimme wereld**:
  het internet der dingen, smart cities en 'the quantified self'.

Slimme gegevens: de toename van de hoeveelheid informatie en big data

De verwachting is dat de hoeveelheid informatie op het internet in 2020 veertig maal zo groot is als vandaag. Daarmee verschuift de aandacht van het genereren van meer informatie naar het ordenen en betekenisvol ontsluiten daarvan. Kwalitatief hoogwaardige informatie ontstaat door het selecteren, verbinden en presenteren van informatie zodat die betekenisvol wordt voor gebruikers, of die gebruikers nu eigen medewerkers zijn of burgers. In een participerende samenleving, waarin burgers afhankelijk zijn van die kwaliteit voor hun gezondheid, zal de zorg voor goede informatie de aandacht van overheden vragen.

Essay van Bert Mulder

Big data is de aanduiding voor een nieuwe klasse van gegevens die zich kenmerkt door drie eigenschappen: de omvang van de gegevens, de snelheid waarmee deze worden gegenereerd en de complexiteit ervan. Voorbeelden van big data zijn de reisgegevens van het openbaar vervoer, verkeersbewegingen, telecomdata, gebruiksgegevens van social media, metingen van lucht-, geluids- en waterkwaliteit. Het analyseren van big data kan leiden tot een beter inzicht in achterliggende factoren en een betere aanpak van problemen, de richting van ontwikkelingen voorspellen, inefficiënties in processen laten zien. Zo kan de griepdienst van Google op basis van analyse van de miljarden zoekopdrachten, eerder dan artsen voorspellen dat een griepepidemie in aantocht is. Hoewel big data kan leiden tot nieuwe inzichten, is er daarbij een duidelijk verschil tussen causaliteit en correlatie. Zo blijkt na analyse van alle data uit de verkeerslussen in Nederland, dat de verkeerbewegingen van één enkele verkeerslus op de A15 bij Rotterdam vrijwel één op één correleren met de stand van de Nederlandse economie. Het is duidelijk dat een dergelijk patroon in de data geen aanduiding geeft over de mogelijke causaliteit tussen verschillende factoren. Bij brede beschikbaarheid van dergelijke big data is er het gevaar van een te eenvoudige opvatting en toepassing van big data en het ontstaan van 'data driven government' waarbij er te veel vertrouwen in data ontstaat als basis voor sturing. Big data is een belangrijke ontwikkeling, maar op dit moment zijn het de nationale overheden, zoals de Amerikaanse regering, die beleid hebben geformuleerd en investeren in onderzoek naar big data omdat zij verwachten dat analyse hen uiteindelijk kan helpen bij het oplossen van problemen. Pas op langere termijn zal big data ook voor lagere overheden zelf van praktische betekenis worden.

Open data

Open data is het ter beschikking stellen van collecties basisgegevens aan derden voor (her)gebruik naar eigen inzicht. Het is een ontwikkeling waarbij de data worden losgekoppeld van de eigen dienstverlening en derden in staat gesteld worden zelf diensten te ontwikkelen. Voor de overheid krijgt de aandacht voor open data, al enkele jaren een belangrijk beleidsthema, een sterke stimulans bij het aantreden van de regering Obama. Hij verklaart 'open data' één van de centrale elementen in een transparante 'open overheid' die gebaseerd is op drie fundamentele principes:
Ten eerste moeten burgers in een goed functionerende democratische samenleving weten wat hun overheid doet: transparantie. Dat betekent niet alleen toegang tot gegevens, maar ook de mogelijkheid die gegevens zelf opnieuw te kunnen en mogen gebruiken voor nader onderzoek en analyse. Ten tweede zijn gegevens de sleutel tot het realiseren van sociale en commerciële waarde. Veel diensten vereisen toegang tot gegevens, die vaak in het bezit zijn van de overheid: zoals cijfers rond gezondheid in de samenleving of het kunnen vinden van gebouwen. Open data is de grondstof voor de innovatie van diensten met sociale en commerciële waarde. Ten derde kunnen burgers door de toegang tot en het werken met data makkelijker participeren in de overheid. Niet alleen omdat ze daardoor weten wat de overheid doet, maar ook omdat ze daaraan kunnen bijdragen. De Nederlandse overheid stelt vast dat open data openbaar zijn, bekostigd uit publieke middelen, bij voorkeur voldoet aan open standaarden en leesbaar moeten zijn door een computer.
Een goed voorbeeld van de mogelijkheden van open data is de trein app, die in 2008 door een student in twee weken gemaakt werd en gebruik maakt van de vertrek- en aankomsttijden gegevens van de NS. De gebruiksvriendelijke app wordt tienduizenden keren gedownload en is het eerste voorbeeld van een buitenstaander die op eigen

initiatief en onverwacht nieuwe digitale dienstverlening creëert op basis van data van anderen. De NS overweegt juridische stappen, maar houdt zich in. Diezelfde reactie ontstaat bij 'openkvk' een app die gratis toegang heeft tot de data van de Kamers van Koophandel. Misschien in het belang van burgers, maar ook op gespannen voet met het businessmodel van de organisatie. Toch kan het belang van dergelijke ontwikkelingen groot zijn, niet alleen in het creëren van betere en snellere dienstverlening. Wanneer de staat Californië financieel uitgeput is, vraagt zij haar inwoners om zelf apps te maken die diensten voor burgers kunnen realiseren.

Open data!

In de context van 'open data' is er de laatste jaren vraag uit de samenleving naar 'open spending', waarbij door het stimuleren van de ontsluiting van financiële informatie van overheden een transparantere en efficiëntere overheid zou kunnen ontstaan. Het beschikbaar stellen van deze gegevens is complexer en minder vanzelfsprekend. Er is internationaal aandacht voor deze trend: de website openspending.org stelt online 300 datasets uit 70 landen ter beschikking. Binnen Nederland is open spending nog niet sterk ontwikkeld en één van de relatief eenvoudige beschikbare voorbeelden is de begroting van het stadsdeel Centrum van Amsterdam. De politieke wens om open spending te realiseren blijft. En in de komende jaren zullen ongetwijfeld meer overheden hun begrotingen en uitgaven online presenteren.

Open data is een belangrijke en blijvende ontwikkeling voor overheden. Een aantal overheden formuleerden een actief 'open, tenzij...' beleid voor hun data, maar de uitwerking daarvan is weerbarstig. Terugkerende reserves van de beheerders van data collecties rond het beschikbaar stellen van hun bestanden betreffen de mogelijke gevolgen voor de privacy van burgers, de inspanningen die nodig zijn, het onderhoud, de rechten en soms het veranderende verdienmodel.

Andersom is de interesse bij de burger lang niet altijd aanwezig. Bij navraag blijken deze vaak niet in staat om aan te geven waarom en hoe zij gegevens zouden willen gebruiken. Het enkel beschikbaar stellen blijkt (nog) niet genoeg en vaak moeten betekenisvolle toepassingen voor burgers ontwikkeld worden om open data te laten gebruiken. Recent zijn verschillende gemeenten stimuleringsprogramma's gestart. Daarbij hoort het stimuleren van de ontwikkeling van open data binnen de eigen organisatie, in casu het ondersteunen van medewerkers om de door hen beheerde collecties openbaar te maken. Dat kan door organiseren van ondersteuning op de juridische, technische, organisatorische en inhoudelijke aspecten van open data. Deel daarvan vormt natuurlijk de toets op veiligheid voor personen of publieke belangen, maar bijvoorbeeld ook het creëren van een online platform waarop medewerkers datasets ter beschikking kunnen stellen, of gebruik maken van het landelijke platform data.overheid.nl om de eigen datasets ter beschikking te stellen.

Het gezamenlijk of afzonderlijk diensten ontwikkelen op dezelfde data zou burgers en overheden dichter bij elkaar kunnen brengen. Maar gegevens worden verzameld met een doel, en de aandacht van burgers kan elders liggen dan die van het openbaar bestuur. Het is de ontmoeting tussen de systeemwereld en de leefwereld, en de verbinding daartussen is niet altijd vanzelfsprekend. Daarbij komt dat het openstellen van data niet altijd leidt tot meer betekenis of meer transparantie: soms moeten data geïnterpreteerd worden op basis van ervaring of in relatie met andere gegevens. Voor een zinvolle toepassing moet die context dan beschikbaar gemaakt kunnen worden.

Essay van Bert Mulder

Het beschikbaar stellen van data en de ontwikkeling van apps om die te ontsluiten, zal de komende jaren nog een ontwikkeling moeten doormaken om te kunnen leiden tot transparantie, inzage in de doelmatigheid van het opereren van de overheid en effectieve participatie in besluitvorming.

Het intelligente web: web 3.0 – het semantisch web

Na de introductie van het eerste publieke internet in Nederland in 1994 kenmerkt het internet zich elk decennium door een nieuwe fase. In de eerste fase (web 1.0) richt het zich op het online presenteren van informatie terwijl in de tweede fase (web 2.0) de ontwikkeling is gericht op het verbinden van mensen en het online kunnen produceren en delen van informatie. Daarbij behoren Nederlanders tot de wereldtop in het gebruik van social media. Voor de overheid betekende die ontwikkeling aandacht voor de dialoog tussen burger en overheid, het digitaal betrekken van burgers bij beleid en in de participerende samenleving voor online gemeenschappen rond zorg, het uitwisselen van kleine diensten en vrijwilligers. Het komende decennium (web 3.0) worden computers in staat gesteld om de betekenis van teksten te kunnen definiëren, begrijpen en afleiden. Als daarmee de aandacht verschuift naar het verbinden van kennis en concepten ziet het internet zoektermen niet enkel meer als een reeks letters maar nu als een concept met omschreven eigenschappen. Dat maakt het mogelijk dat het internet niet langer documenten met elkaar verbindt, zoals webpagina's, maar individuele begrippen. Die verschuiving van informatie naar kennis zorgt ervoor dat de kwaliteit van online zoeken sterk kan verbeteren. Door de slimme analyse van de zoekvraag kunnen zoekresultaten beter op de vrager worden afgestemd, wat een groot voordeel kan zijn wanneer patiënten medische informatie zoeken, studenten opleidingen die zij kunnen gaan doen of burgers welke diensten zij het best kunnen gebruiken.

Waar overheid 2.0 zich richtte op 'gegevens' en 'dialoog' zal overheid 3.0 zich richten op het digitaal in kaart brengen van concepten en de basis leggen voor netwerken van kennis. Het is de ontwikkeling van een slimmere overheid die niet alleen data, maar nu ook kennis ter beschikking kan stellen. Het vereist wel dat de concepten die de processen en diensten van de overheid bepalen, zo beschreven moeten worden dat ze deel gaan vormen van het semantisch web. Het is een ontwikkeling die niet direct door overheden zelf plaatsvindt, maar die als nieuwe faciliteit in door haar gebruikte applicaties zal moeten worden geïmplementeerd.

Web 4.0

De netwerken van kennis, die in web 3.0 zijn gevormd, worden in web 4.0 actief bewerkbaar. Het kunnen werken met entiteiten legt de basis voor programmeren met concepten, soms 'concept computing' genoemd. Eerste voorbeelden van het programmeren met kennisconcepten, zoals de Wolfram language, verschijnen op dit moment. Daarbij kan de vraag 'ligt het totale bedrag aan uitkeringen van alle werklozen nog binnen de begrotingskaders' automatisch door de computer worden begrepen, om vervolgens ook automatisch vertaald te worden in een reeks zoekvragen en berekeningen die tot het antwoord leiden. Bij web 4.0 wordt het web voor gebruikers intelligent en lijkt het alsof een digitale butler diensten vormgeeft op basis van eerder digitaal gedrag. Hoewel deze ontwikkeling nog verder weg ligt,

ontstaan hier mogelijkheden voor 'model driven government'. Zo kan op dit moment het Nederlandse bedrijf Be Informed complexe vergunningsystemen realiseren enkel door het beschrijven van de verschillende constraints en voorwaarden zonder dat zij daarbij de gebruikte procedures uitputtend hoeven te beschrijven. Vanuit die definities wordt het totale systeem automatisch gegenereerd. Dergelijke constraint gebaseerde systemen schalen automatisch mee met groeiende belasting en kunnen nieuwe juridische en politieke ontwikkelingen direct en zonder verdere aanpassing volledig integreren. Bij het creëren van en werken met informatiesystemen werken gebruikers, maar ook ontwikkelaars, op een hoger niveau.

Het intelligente internet en de beschikbaarheid van slimme data creëert een nieuwe situatie. Burgers zijn in staat, door de combinatie van het intelligente web, door nieuwe op kennis gebaseerde programmeertalen en door het samenstellen van componenten, om zelf nieuwe toepassingen te maken met een relatief lage inspanning. Kennis is niet langer opgesloten in databases of in platformen, maar vrij beschikbaar. Systemen verzamelen zelf informatie over het gebruik door gebruikers en kunnen zo leren. Zij kunnen zich, anders dan nu, voortdurend aanpassen aan veranderende behoeften. De onderliggende technische infrastructuur is in toenemende mate in staat om zichzelf te beheren en aan te passen. Beveiliging is ingebouwd op elk niveau van systemen: het netwerk, de servers, alle verschillende apparaten, elke applicatie en elke dataverzameling. Dat geldt ook voor het beheer van eigendom en autorisatie. Voor overheden betekent het de aandacht voor 'de fabriek' verdwijnt: in de informatiehuishouding verschuift de aandacht van technische aspecten naar meer kennisgerelateerde en inhoudelijke aspecten. Ook kunnen complexe procesgangen makkelijker en meer automatisch door minder mensen worden ingericht en afgehandeld.

De intelligente wereld: the internet of things

'Internet of things' is het toevoegen van sensoren aan de fysieke werkelijkheid en die objecten verbinden met het internet. De trend is terug te herkennen in gebouwen als domotica, in transport als intelligente voertuigen en in de toekomst in de stad in parkeerplaatsen en –meters en vuilnisbakken. In de persoonlijke leefomgeving betekent het digitale intelligentie voor televisie, koffie apparaat, koelkast, thermostaat. In auto's, waarin het aantal digitale sensoren al jarenlang toeneemt, leidt deze ontwikkeling nu tot zelfsturende voertuigen. In supermarkten betekent het dynamische prijsaanduidingen op de schappen, beweegmelders in kratten die bij vervoer van fruit de beweging monitoren. En net zoals in de retail sector fruit weet wat het is en waar het is, weet in een kantooromgeving een ordner ook wat hij bevat en waar hij is.

Internet of things kan dienstverlening verbeteren, bijvoorbeeld wanneer vuilverzamelplaatsen zelf aan kunnen geven wanneer ze geleegd moeten worden, of parkeerplaatsen zelf dat zij onbezet zijn. De gemeente Eindhoven heeft recentelijk de enige snuffelpaal die zij rijk was vervangen door honderd nieuwe sensoren die 24 uur per dag verschillende elementen van luchtkwaliteit meten. De verwachting is dat verkeersborden zelf communiceren naar voertuigen over de op deze locatie geldende beperkingen. Mochten sensoren op grote schaal in de stedelijke omgeving gebruikt gaan worden, moet er een ondersteunende infrastructuur beschikbaar zijn. KPN heeft al enkele jaren geleden een concept ontwikkeld van een lantaarnpaal die naast licht

een communicatie- en informatiefunctie vervult. Daarbij is elke paal opgenomen in een glasvezelnetwerk. Overheden creëren met het thema 'smart city' een generiek beleidsthema waaronder een aantal van bovenstaande thema's worden verzameld. Het vestigt de aandacht en focust mogelijke investeringen, maar als zodanig voegt het inhoudelijk weinig toe aan al bekende ontwikkelingen. Het 'internet der dingen' zal zich sterk ontwikkelen en bij kunnen dragen aan betere dienstverlening en de kwaliteit van leven, zowel op stedelijk niveau als in organisaties en de persoonlijke leefomgeving.

Quantified self

Dezelfde sensor gebaseerde ontwikkeling zien we in de persoonlijke leefomgeving om vitale waarden te registreren en te verzamelen: bloeddruk, bloeddoorstroming, ECG, EMG, glucosegehalte. Fietsers kunnen alle lichaamsdata en de gegevens over de route, gereden snelheid en hellingshoek van hun rit op het internet verzamelen waarna speciale software analyses maakt van conditie en nieuwe oefenschema's suggereert. Individuele gebruikers verzamelen grote hoeveelheden data, op basis daarvan krijgen bewoners advies over hun gezondheidstoestand en de manier waarop zij die kunnen verbeteren.

Voor overheden is deze ontwikkeling interessant en van belang, omdat de komende jaren burgers steeds vaker zelf zorgen voor hun gezondheid en dat langer thuis zullen doen. Het betekent dat chronisch zieken, gehandicapten en ouderen in toenemende mate in hun ziekte en gezondheid ondersteund zullen worden door op hen gerichte oplossingen die gebruik maken van sensoren, apps en internetdiensten.

Digitalisering persoonlijke leefomgeving

Die ontwikkeling kent verschillende uitdagingen. De digitalisering van de persoonlijke leefomgeving is essentieel voor een samenleving waarin zelf thuis zorgen de basis vormt. De kwaliteit van die digitale omgeving is bepalend voor haar succes. Maar de huidige ontwikkelingen resulteren in een groot aantal verschillende individuele oplossingen, die niet met elkaar communiceren en gebruik maken van verschillende achterliggende diensten op het internet. Voor ouderen, die elk gemiddeld vier aandoeningen hebben, betekent het dat zij tientallen apparaten, toepassingen en webdiensten gebruiken om in hun gezondheid te voorzien. Op de schaal van 7 miljoen huishoudens betekent dit een geheel nieuwe complexiteit, schaal en kwaliteit, waarvoor op dit moment niet of nauwelijks aandacht is.

Slimme gegevens, het intelligente web en de intelligente wereld creëren nieuwe kansen maar ook nieuwe uitdagingen voor de overheid. Die nieuwe kansen zullen moeten worden gerealiseerd in de context van de demografische ontwikkelingen, waarin de overheid (en naar verwachting ook het onderwijs en de zorg) zal bestaan uit een sterk kleiner aantal medewerkers. De overheid zal bij al deze ontwikkelingen betrokken zijn en belang hebben, soms direct en soms indirect, omdat het haar eigen functioneren en de kwaliteit van leven in de samenleving sterk zal faciliteren. Er ontstaat een andere manier van leven en werken die meer dan nu gefaciliteerd wordt door digitale toepassingen en informatie, en die daarmee bepalend zal zijn voor de komende transformatie van de samenleving.


Feodale
veiligheid

Michel van Eeten

Professor
Technische Universiteit Delft

Elegant falen in het tijdperk van feodale veiligheid

1.

Wanneer heeft u voor het laatst iemand horen zeggen: 'Wij gaan een groot automatiseringsproject doen om de veiligheid van onze processen te verhogen'? Mijn vermoeden is: dat hoort u zelden of nooit.
Er zijn allerlei redenen waarom overheden informatiesystemen bouwen of uitbreiden, maar veiligheid is er zelden een van.[1] Veiligheid is geen doel op zich, behalve voor de veiligheidsdiensten. De overheid doet deze projecten met andere motieven. Innovatie, kwaliteit, transparantie, betere dienstverlening. En vaak, achter alle hoera-begrippen, is de ware drijvende kracht: bezuinigingen. In het beleidsjargon heet dat doorgaans 'efficiency'. Dat lijkt hetzelfde, maar is het niet. Bij efficiency ga je automatiseren in de hoop daarna geld te besparen, dat je dan elders kunt aanwenden. Maar bij bezuinigingen gaat de besparing vaak vooraf aan de automatisering. Daarna is het niet alleen afwachten of de efficiency werkelijk omhoog gaat, maar ook of het primaire proces überhaupt overeind blijft. Zie het geplaagde werk.nl. Maar dan is de bezuiniging al gerealiseerd. Op papier tenminste.
Deze context doet er toe. Sterker nog, hij is cruciaal voor elk gesprek over de veiligheid van bestuurlijke informatiediensten. Toch wordt hij veelal genegeerd, vooral door veiligheidsexperts. Die redeneren doorgaans via een eenvoudig sjabloon - een sjabloon dat prettig genoeg hun expertise de schijn van urgentie meegeeft en hun producten voorstelt als hoogst noodzakelijke investeringen. Het sjabloon kennen we in talloze variaties van hetzelfde betoog: 'Dienst X kent bepaalde kwetsbaarheden en is dus onveilig.' Of: 'Systeem Y introduceert nieuwe risico's en vereist daarom aanvullende investeringen.' Alsof dat nieuws is.
Natuurlijk kennen systemen kwetsbaarheden en introduceren ze nieuwe risico's. Een veilig systeem is een systeem dat niet gebouwd wordt.
(Tot voor kort zei ik altijd: 'een veilig systeem is een systeem dat uit staat', maar inmiddels weten we dat de NSA manieren heeft om systemen die uitgeschakeld zijn evengoed te infiltreren.) Veiligheid is altijd onvolkomen. Een systeem is nooit 'veilig', het is hoogstens minder of meer onveilig. Mantra's als 'security by design' zijn dan ook holle frases. De enige zinnige interpretatie ervan is een banaliteit: hou bij het ontwerp rekening met veiligheid. Tja. Alsof er iemand is die het tegendeel beweert.
Kortom, als we een systeem bouwen, nemen we altijd zekere risico's. God zij dank, zou ik zeggen. Je zou het haast vergeten in onze door risico's geobsedeerde maatschappij: we danken onze welvaart en gezondheid aan het nemen van risico's, niet het vermijden ervan. Voorkomen is op termijn vaak erger dan genezen.[2]
De vraag of iets veilig genoeg is, kan nooit alleen beantwoord worden op basis van inzicht in de technische risico's of het optreden van incidenten. Er liggen allerlei impliciete en expliciete afwegingen ten

1 Onder veiligheid verstaan we hier de conventionele triade van beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
2 Voor een diepgravende beschouwing hierover, zie de klassieker Searching for Safety van Aaron Wildavsky (Transaction Publishers, 1988).

grondslag aan veiligheidskeuzes. Veiligheid kost geld. Alleen al daarom is het economisch wenselijk een zekere mate van onveiligheid te tolereren. Of iets veilig genoeg is hangt af van de gevolgen van hogere of lagere veiligheid voor andere waarden, zoals efficiëntie, bruikbaarheid, toegankelijkheid, transparantie, vrijheid en innovatievermogen.

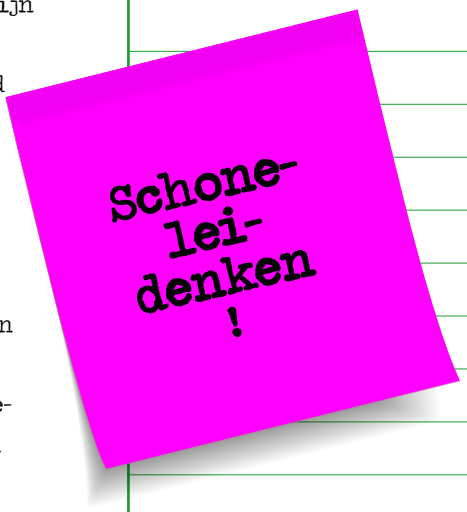
Het nemen van risico's is dus niet ten principale verkeerd, integendeel. Daarom zullen we ook moeten accepteren dat er zaken zullen misgaan. Toch is het soms te makkelijk wanneer overheden die veiligheidsproblemen afdoen met: 'Shit happens'. Of in de nette, eufemistische variant: 'Honderd procent veiligheid bestaat niet'. De gedachte dat we bepaalde risico's beter kunnen accepteren, is gebaseerd op in ieder geval twee cruciale aannames: de overheid heeft de risico's correct ingeschat en de risico's worden niet op derden afgewenteld.
De overheid zal steeds aangesproken kunnen worden op competente risico-inschattingen en op rechtvaardige risico-verdelingen. In veel van de recente problemen rondom grote ICT-projecten schiet de overheid tekort in een van deze opgaven, of in beide. We bespreken ze kort.

2.

Het correct inschatten, en vervolgens communiceren, van risico's van informatie- en communicatietechnologie is een notoir moeilijke opgave. Vaak weet de publieke instantie niet echt welke risico's ze neemt, ook al zijn er pakken papier vol risico-analyses gefabriceerd en hebben de leveranciers allerlei geruststellend bedoelde bezweringsformules afgescheiden. Denk aan: 'Deze kwetsbaarheid is volkomen theoretisch.' Of: 'Een dergelijk scenario is technisch onmogelijk.'
Risico-analyses kunnen, mits goed uitgevoerd, nuttig zijn. Maar de complexiteit van informatietechnologie is te groot om zich in dit keurslijf te laten dwingen. Om zich in welk keurslijf dan ook te laten dwingen. Grootschalige ICT is beperkt beheersbaar. Dat is de les van lijst van problematische ICT-projecten die extra parlementaire aandacht hebben weten te verwerven.
Een beetje systeem bestaat al snel uit tienduizenden onderdelen elk met tientallen miljoenen regels code. Tel uit je winst. Zoals een systeemanaliste ooit schreef: 'The chief manifestation of complexity is surprise.'[3] Wanneer die verrassingen optreden, leggen ze al snel de discrepantie bloot tussen de papieren realiteit of de beweringen van een leverancier en het daadwerkelijke functioneren van een systeem.
Ja maar, bij de banken en andere grote bedrijven lukt het toch wel om die complexiteit in de hand te houden? Nou nee. De paradox is dat die bedrijven veel incrementeler innoveren dan de overheid. Hun ICT-voorzieningen zijn lappendekens van verschillende systemen die in de afgelopen dertig jaar zijn gebouwd. Die functioneren allemaal naast elkaar. Daar zit geen grote ontwerpvisie achter, juist niet, eerder een

3 Zie C.C. Demchak, Military organizations, complex machines: Modernization in the U.S. armed services. (Ithaca, N.Y.: Cornell University Press, 1991), p. 3.

principe dat respect uitdrukt voor complexiteit: 'If it ain't broke, don't fix it.' Het duurt een poos voor je de reguliere fouten uit een systeem hebt gehaald. Daarna duurt het nog jaren voordat je de onregelmatige, vreemde fouten hebt ontdekt, begrepen en gerepareerd. En dan heb je eindelijk een complex systeem dat enigszins stabiel en voorspelbaar functioneert. Tegen die tijd heeft het technologische front zich allang weer verplaatst, natuurlijk. Maar deze organisaties weten dat het daar niet om gaat. Je blijft af van die zuurverdiende stabiliteit. Vernieuwingen bouw je vervolgens naast die oudere systemen, zelden in plaats ervan. Ja, het is rommelig. De nieuwe systemen, de meest recente lapjes in de deken, kunnen complexe interacties aangaan met de oudere systemen. Maar die zijn nog altijd beter te controleren dan de interacties in een grootschalig systeem dat met een schone lei is gebouwd. Schone-lei-denken is de vijand van beheersing. Overheden, daarentegen, zijn de gewillige slachtoffers gebleken van het schone-lei-denken en van de ICT-leveranciers die deze ontwerpen verkochten als oplossing: weg met de lappendeken, op naar de geïntegreerde, elegante totaal-ontwerpen. Telkens lag de verleiding op de loer om het dan ook maar in een keer goed te doen. Niet te klein denken, maar meteen een complete oplossing neerleggen. Deze verleidingen drukken een minachting uit voor lappendekens, voor complexiteit. En ze zijn de snelste routes naar grootschalige debacles. Ook op veiligheidsgebied. Dan hoort een bestuurder zichzelf ineens beweren dat het allemaal veilig is, dat de risico's onder controle zijn. Dat is een uitnodiging om in je hemd gezet te worden door wildvreemden die de krochten van je eigen technologie beter blijken te kennen dan jouw eigen mensen en je leveranciers.



Falen is inherent aan de complexiteit van systemen. Het verbluffende van werk.nl is niet dat het faalde, het verbluffende is dat het grotendeels lijkt te functioneren. Zodra je falen vooraf accepteert, kun je het beter organiseren. Niet voor niets praten softwareontwikkelaars over 'failing gracefully' - de vraag is niet of software faalt, maar hoe. Als je, door bezuinigingen voortgejaagd, een grootschalig primair proces in korte tijd naar een nieuwe online dienst moet overhevelen dan moet je meteen weten dat er grootschalig falen gaat optreden. UWV had dat falen eleganter kunnen organiseren door vooraf, in plaats van na maandenlange klachten, de extra mensen aan te nemen die burgers kunnen helpen waar het systeem faalt.

Hetzelfde zien we in andere gevallen. De Eerste Kamer had meer respect voor de complexiteit van het Elektronisch Patiëntendossier (EPD) dan het ministerie en de instanties die het ontwikkelden. Die weigerden oplossingen te creëren voor dat wat onvermijdelijk is, namelijk onbevoegd gebruik. Zo wilde men pas heel laat in het traject schoorvoetend overwegen of patiënten misschien een sms konden ontvangen wanneer hun dossier werd ingezien. Er zou immers geen onbevoegde toegang zijn, was de aanname. Die houding was niet alleen naïef, maar grensde aan nalatigheid. De Eerste Kamer trok de juiste conclusie: deze instanties kun je het EPD niet toevertrouwen.

Helaas maakte het sneuvelen van het EPD ook de weg vrij voor een private oplossing, waarvan het vooralsnog onduidelijk is welke waarborgen en

accountability daarbij zijn inbegrepen. Deze ontwikkeling onderstreept een ander punt: er is eigenlijk geen exit-optie meer. De krachten die onze samenleving deze kant op trekken zijn sterker dan formele besluitvormingsprocedures en collectieve wilsvorming.

3.

De problemen met werk.nl waren normaal, vond de minister. Er werd namelijk 'verbouwd terwijl de winkel open is', schreef hij aan de Kamer. Hij zegt dus eigenlijk: 'shit happens'. Daar is geen speld tussen te krijgen, maar het is ook ongelooflijk gratuit. Elders noemde ik dat: fatalisme op andermans rekening.[4]

Verdeling van risico's

Hier komt de tweede opgave voor de overheid om de hoek kijken: een rechtvaardige verdeling van risico's. Wie draait er op voor de gevolgen? Ook een beetje falen betekent op deze schaal meteen dat duizenden mensen in nare situaties terecht komen. Hier zien we een afwentelingsprobleem: de risicobeheerder is niet de risicodrager. De gevolgen van falen komen bij anderen terecht dan de beheerders van het systeem. Dat gebeurt ook in de markt. Daar noemen we het een externaliteit, een klassieke vorm van marktfalen. Het geeft partijen de verkeerde prikkels: omdat ze niet zelf de schade dragen, zijn ze te optimistisch of te laks om dat falen te voorkomen of adequaat af te handelen. Dat mechanisme geldt evenzeer voor overheden als voor bedrijven.

Er zijn verschillende antwoorden voorhanden om afwenteling te bestrijden, maar in de kern doen ze hetzelfde: ze proberen de schade terug te duwen naar de instantie die het risico genomen heeft. De instrumenten lopen uiteen. Denk aan wettelijke aansprakelijkheid, consumentenbescherming, normering, naming and shaming, meldplicht, administratieve boetes, of zelfs strafrechtelijke vervolging.

Soms gaat het zonder formeel mechanisme. Bij uitkeringsfraude met DigiD, waarbij criminelen het account overnemen van een burger en dan het rekeningnummer veranderen waardoor de uitkering op de rekening van een katvanger wordt gestort, wordt de schade doorgaans vergoed. Ik zeg doorgaans, omdat we alleen die gevallen kennen waar mensen met honderden tegelijk slachtoffer worden. Daar kunnen bureaucratische organisaties als de Sociale Verzekeringsbank of de Belastingdienst wel mee uit de voeten. Juist door de herhaling kunnen de incidenten correct herkend en geroutiniseerd worden. Maar wat als een individueel geval bij het loket staat en beweert dat hij dat rekeningnummer niet gewijzigd heeft? En dat hij zijn DigiD niet heeft afgegeven aan zijn gezinsleden? Ik vermoed dat je dan verbaal en procedureel tamelijk vaardig moet zijn om voorbij de eerste afwijzing aan het loket te komen. Niet iedereen is dat - en dat geldt wellicht in sterkere mate voor de mensen in deze groep. Hun schade kan onzichtbaar blijven, ook voor de instanties zelf. Daar kun je alleen iets aan doen door het formeel te regelen en de bewijslast om te draaien, bijvoorbeeld.

4 Van Eeten (2010). Techniek van de onmacht. Fatalisme in politiek en bestuur. Den Haag: NSOB.

4.

Na deze korte reflectie op de positie van overheden tegenover de risico's van ICT, doet zich de vraag voor: wat komt er aan nieuwe technologie op hen af? Die vraag verdient meer aandacht dan we hem hier kunnen geven. Het is belangrijk het antwoord niet in puur technische veranderingen te zoeken. Dat biedt weinig inzicht. Meer houvast is te vinden in het benoemen van de economische krachten die de evolutie van deze technologie sturen. Vier wil ik er hier noemen.

Economische krachten

Toenemende waarde van persoonlijke data

Naarmate ICT in alle primaire processen van de maatschappij doordringt, wordt er ook meer data geproduceerd. Dat is geen keuze, maar een gegeven. Data is een onvermijdelijk en essentieel product van elke transactie. Het kost geen moeite om data te produceren, het kost juist moeite om het desgewenst weer ongedaan te maken. Niet voor niets praat de Europese Commissie over het recht om vergeten te worden. Gegeven dat de data er hoe dan ook is, ontstaan er steeds daarna nieuwe manieren om die te gelde te maken. Je kunt die mooi zien bij Google. Ze lanceren aan de lopende band nieuwe diensten, zonder verdienmodel dat vooraf is bedacht. Bij veel van die diensten komt er geen expliciet verdienmodel, maar wordt het onderdeel van het conglomeraat aan diensten waarmee Google ons beter en beter leert kennen. Wij zijn niet de klanten van Google. We betalen geen cent. Probeer maar eens de klantenservice te bellen. Wij zijn deel van het product dat Google verkoopt aan haar werkelijke klanten, zoals adverteerders. Een ander voorbeeld is PayPal, onderdeel van eBay, net als Marktplaats. Als je op Marktplaats een product koopt, kun je meestal via PayPal betalen, waarna je aankoop verzekerd is tegen oplichting of niet-levering. Dat kan PayPal doen, omdat ze via Markplaats gedetailleerde profielen kent van verkopers. Met die data kan ze tegen lage risico's de facto een verzekering aanbieden. Dat onderscheid de betaaldienst van haar concurrenten en zo is de data die wij, al kopend en verkopend op Marktplaats, genereren, te gelde gemaakt. Overal waar data is, zullen partijen zijn die proberen hier waarde aan te onttrekken, niet in de laatste plaats degene die de informatie bijeenbrengt en beheert. Zie EPD. Het sneuvelen van het overheidsinitiatief betekende slechts dat de marktpartijen nu zelf die voordelen gaan najagen.

Krachtige nieuwe intermediairen

Ooit was het verhaal dat internet alles ging dis-intermediëren - dat wil zeggen: de tussenpersonen ging wegvagen. Inmiddels weten we dat het een illusie is. We hebben oude intermediairen ingeruild voor nieuwe. De grote internetbedrijven - Google, Apple, Microsoft, Facebook - blijken enorme machtsconcentraties op te bouwen. Dat komt mede doordat de markten voor informatiediensten hele sterke neiging

hebben tot "winner takes all": dominantie door een of enkele spelers die zulke grote schaalvoordelen opbouwen dat er geen concurrentie meer mogelijk is. Ook wordt concurrentie ondermijnt door 'lock-in' en informatie-asymmetrie. Deze mechanismen zijn inherent aan informatiediensten: het kost een enorme investering om een nieuw operating system of sociaal netwerk te bouwen, maar de kosten voor elke volgende kopie of gebruiker zijn nagenoeg nul (hoge vaste kosten, verwaarloosbare marginale kosten). Dat zie je ook in clouddiensten. De prijs daarvan is vele malen lager dan het zelf beheren van hardware en software. Dat heeft een enorme aanzuigende werking. Steeds meer van onze ICT - en dus onze veiligheid - komt in handen van een beperkte groep machtige intermediairen.

Overheden liften mee op hyper-transparantie

Doordat data als noodzakelijk en gratis bijproduct van ICT-transacties wordt gegenereerd en de kosten van opslag naar nul dalen, zien we een enorme data-obesitas in de private sector. Google weet inmiddels meer van elk van ons dan de staat. Een Oostenrijkse student vroeg ooit zijn dossier op bij Facebook. Hij kreeg enkele CD-roms toegestuurd met 1200 A4'tjes aan data. Een geheime dienst zou dit vroeger slechts voor een selecte groep burgers hebben kunnen verzamelen, vanwege de enorme kosten die ermee gepaard gaan. Facebook verzamelt het standaard voor elke gebruiker.
De overheid heeft een Januskop ten aanzien van de private data-obesitas. Aan de ene kant werpt ze zich op als de beschermer van burgers tegenover de private bedrijven. Aan de andere kant ontdekken overheden steeds meer dat de verschuiving van macht naar de intermediairen ook mogelijkheden biedt. Zie NSA. Veel van wat de NSA doet is zich toegang verschaffen tot informatie die private partijen al hadden. Op kleinere schaal zie je dit ook in Nederland. De informatie is er al. Leg dan maar eens uit dat de overheid die niet mag inzien om een of andere misstand aan te pakken. Het is in zekere zin het witwassen van data. De overheid kan langs deze weg informatie verkrijgen die ze zelf nooit zou mogen verzamelen.

Incentives en technologie van marktspelers zijn leidend

De huidige dominante spelers zullen ongetwijfeld weer door andere vervangen worden. Maar de kans dat die nieuwe spelers beter passen in de oude statelijke en supra-statelijke governance arrangementen is nihil. Wat betekent dit voor veiligheid? De opkomst van intermediairen is niet per se beter of slechter voor veiligheid, het is vooral anders. Het ondermijnt enerzijds de soevereiniteit van staten en lokt anderzijds juist uit dat staten zich extra-territoriale bevoegheden toe-eigenen, of dat nu de Patriot Act is of het Nederlandse wetsvoorstel om politie te laten inbreken op systemen in het buitenland. We hebben nog geen governance-arrangementen voor de omgang hiermee, zoals de nasleep van de NSA-onthullingen pijnlijk duidelijk maken. Overheden laten zich afschepen met bezweringsfor-

mules die hol klinken, zoals de belofte van cloudaanbieders dat ze alles conform Nederlands recht zullen afhandelen. Ik vermoed dat weinigen aan de kant van de overheid naïef genoeg zijn om hierop te vertrouwen. Het feit dat deze antwoorden getolereerd worden geeft vooral aan dat er geen beter arrangement voorhanden is.

5.

De optelsom van deze ontwikkelingen is moeilijk te overzien. Maar een manier om deze te benoemen is te zeggen dat we overgaan naar feodale veiligheid, om de term van Bruce Schneier te gebruiken. We gaan weg van het model waarin we zelf onze apparaten beheren. Niet voor niets hebben we in de de opmars gezien van tablets en smartphones met afgegrendelde software - in de consumentenmarkt en steeds meer ook in de zakelijke markt. Die apparaten vergen veel minder know-how en beheer om goed te functioneren. En als er al iets misgaat, kunnen je gegevens zo uit de cloud worden teruggezet. De tradeoff is dat Apple nu bepaalt wat je wel en niet mag doen op je apparaat. Talloze apps worden geweerd uit de App Store. Buiten de App Store om installeren is helemaal uit den boze.
Dit staat haaks op de voorafgaande periode. Het internet heeft juist zo'n innovatie kunnen veroorzaken doordat er aan het netwerk 'general purpose computing' apparaten hingen - lees: de vermaledijde PC. De vernieuwing was mogelijk omdat er geen poortwachters waren. Als je een obscuur programma wilde installeren, omdat je vrienden dat ook deden, zeg iets uit Estland genaamd Skype, dan hoefde je daarvoor bij niemand toestemming te vragen. Niet bij je internetprovider, niet bij Microsoft, niet bij je leverancier van de computer. En zo kon Skype binnen een paar jaar de telecommarkt op zijn kop zetten.
Natuurlijk: dezelfde vrijheid om welk programma dan ook te installeren, is tevens een groot veiligheidsrisico gebleken. Zo kom je aan virussen en andere ellende. Of je raakt gegevens kwijt bij het crashen van software. Veel consumenten willen die problemen niet meer en dragen graag een deel van hun soevereiniteit over aan de platformeigenaar (Apple, Google, Microsoft, Facebook) in ruil voor meer veiligheid en zekerheid. Dat is voor overheden niet veel anders. De complexiteit van ICT is groot en complexiteit betekent hoge beheerskosten. Deze en andere drivers maken dat we als samenleving steeds meer richting het feodale model gaan - vandaag heet dat de cloud, morgen ubiquitous computing, daarna weer anders. Alleen tegen hoge kosten kunnen we specifieke data en informatie-diensten buiten dit model houden. Dat zal dus alleen op selecte gebieden gebeuren, waar we dat geld er voor over hebben.
In het feodale model zijn we afhankelijk van de keuzes die de dominante intermediairen maken. Of gedwongen worden te maken. Kijk maar naar de knarsentandende reacties van de internetgiganten op de onthullingen van Snowden. Over veel van die keuzes weten we eigenlijk nauwelijks iets. Ook dat hebben de onthullingen voelbaar gemaakt. Deze informatie-asymmetrie tussen aanbieders en afnemers is altijd een probleem. Veel overheden weten eigenlijk niet wat ze inkopen en kunnen de claims van hun leveranciers

over veiligheid niet wezenlijk op waarheid toetsen. Maar dit vraagstuk wordt in het feodale model aanzienlijk urgenter.

6.

Welke handelingsrichtingen hebben overheden in het licht van dit alles?

Ze zijn terloops al benoemd in het voorafgaande. We zetten ze kort op een rij:

. Beteugel de neiging tot risicominimalisatie. Minder is niet altijd beter. Voorkomen is soms erger dan genezen.

. Vertrouw niet blind op formele beheersmechanismen. Standaarden à la ISO kunnen nuttig zijn om je huishouding op orde te krijgen, maar hebben weinig met daadwerkelijke veiligheid te maken en zuigen ondertussen wel veel aandacht en middelen op in de organisatie.

. Accepteer falen vooraf, wees daar eerlijk over en organiseer het falen zo elegant mogelijk. Het woord 'onvoorzien' moet op de zwarte lijst, net als de uitdrukkingen 'het is veilig' en 'honderd procent veiligheid bestaat niet'.

. Ondervang afwentelingsmechanismes voor falen, ook door je leveranciers. Te vaak zijn de risiconemers niet de risicodragers. Zie ook de vele datalekken bij publieke instanties à la het Groene Hart ziekenhuis.

. Ontwikkel een strategie voor overheidsdiensten in het feodale tijdperk. Ook de ICT van de overheid zal zich steeds meer buiten haar eigen beheer en eigendomsrechten afspelen. Welke gevolgen heeft dit? Zijn er diensten waarvoor dat onacceptabel is?

. Erken informatie-asymmetrie. Besef dat je ten diepste niet weet wat je geleverd krijgt. Zoek naar manieren om die asymmetrie te reduceren, bijvoorbeeld door derden te belonen voor het blootleggen van gaten (responsible disclosure) en meldplichten die openbare informatie genereren voor onderzoek.

. Onderken dat je zelf als publieke instantie ook een krachtige intermediair bent en bescherm de burgers tegen je eigen falen, in plaats van hen verantwoordelijk te maken voor informatiebeveiliging.


Agendeer
begrenzing
!!!

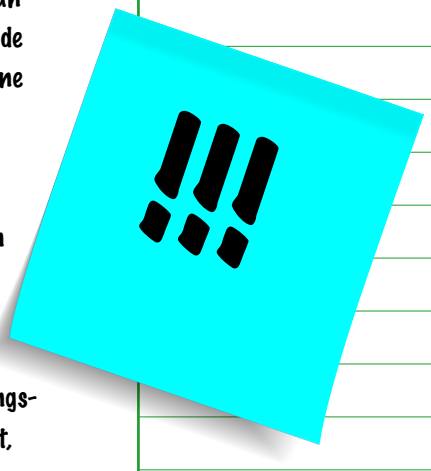
Corien Prins

Hoogleraar Recht en Informatisering en decaan
Universiteit van Tilburg

Toekomstbestendige informatiebeveiliging: agendeer begrenzing en systeemverantwoordelijkheid

1. Inleiding

Bij de voorbereidingen voor dit essay nam ik een willekeurige greep uit mijn doos 'Krantenknipsels 2011' over hacken, lekken van digitale informatie en andere al dan niet succesvolle pogingen om de informatiesamenleving te ontwrichten. Juni 2011 melden de ochtendbladen dat het kinderlijk eenvoudig is via de website van de Dienst Uitvoering Onderwijs (DUO) - voorheen de IB-groep – privégegevens van studenten te stelen. Ook blijkt het mogelijk - gebruik makend van het feit dat oud-studenten een studieschuld moeten aflossen – hen geld afhandig te maken via het betalingssysteem iDeal. Zoals eerder bij de ov-chipkaart, is ook hier een beveiligingslek de boosdoener. Het voorbeeld illustreert niet alleen de kwetsbare kanten van digitalisering, in dit geval het lekken van grote hoeveelheden persoonsgegevens. Evenzeer laat het zien hoe digitale diensten van de overheid (in dit geval die van DUO) zijn verweven met die van de private sector (het online betalingssysteem iDeal).



Het tweede krantenknipsel, nrc.next van 19 september 2011, maakt melding van omvangrijke fraude via authenticatie met DigiD. Onterecht bijgestelde toeslagen kunnen worden aangevraagd door ondertekening met de DigiD van anderen. Door opgegeven inkomsten naar beneden bij te stellen en bankrekeningnummers te veranderen, zijn toeslagen te innen op een rekeningnummer dat niet van diegene is die recht heeft op de toeslag. In de afweging tussen snelle dienstverlening enerzijds en omslachtige beveiligingsprocedures anderzijds zijn compromissen gesloten. In de woorden van de Belastingdienst, in de krant aan het woord: 'Een kwestie van snelle dienstverlening en van vertrouwen'. Om toeslagen bij zoveel mogelijk rechthebbenden terecht te laten komen, besloot de Belastingdienst de aanvraagprocedure te vereenvoudigen. Maar door toe te staan dat bij de aanvraag willekeurige DigiD-authenticatie viel te gebruiken, konden ook hulpverleners, vrienden of familie toeslagen aanvragen voor 'hulpbehoevenden'. Misbruik op grote schaal was het gevolg: 2010 kende 200 fraudegevallen en in 2011 waren dat er nog eens 2500[1].

De voorbeelden zijn illustratief voor de uitdagingen waar de overheid op het terrein van informatiebeveiliging momenteel voor staat: a. de verwevenheid van de informatiehuishouding in ketens en uitvoeringsprocessen, waarmee verantwoordelijkheid nemen voor het beveiligingsniveau van deze huishouding een diffuse aangelegenheid wordt. Verweesde verantwoordelijkheid ligt daarmee op de loer. b. de afweging die telkens weer dient te worden gemaakt tussen diverse – veelal ongelijksoortige – belangen. Zoals het wegen van beveiligingsbelangen en de wens tot een efficiëntie dienstverlening. Comprissen sluiten is noodzakelijk, maar telkens weer staan bepaalde belangen prominenter op het netvlies dan andere. En het belang van een adequate beveiliging blijkt dan nogal eens het onderspit te delven.

De constatering dat digitalisering een totaal andere - namelijk vernetwerkte - informatieomgeving heeft gecreëerd, geeft daarom alle aanleiding om de complexe uitdaging van een adequate informatiebeveiliging te doordenken en op zoek te gaan naar aanknopingspunten voor de wijze waarop actoren binnen de overheid zich hebben te verhouden tot de diversiteit aan belangen die in dit kader spelen. Hoe paradoxaal het ook moge klinken, deze aanknopingspunten moeten wat mij betreft gezocht worden in beredeneerde begrenzingen van digitalisering. Niet in de laatste plaats om actoren houvast te geven in het bepalen van

1 Zie: Privacy & Identity Lab, Eindrapport iOverheid, burger in beeld, TNO 2012 R11216, p. 9.

wat een juiste omgang is met het stellen van beveiligingsvoorwaarden aan partijen met wie ze in een vernetwerkte overheid samenwerken. Die omgang is nu vaak onvoldoende geëxpliciteerd en vervolgens uitgewerkt. Vermenging van informatiestromen, onder meer tussen publiek en privaat, is ongemerkt heel gewoon geworden. Maar bij nadere beschouwing (en zoals ik in paragraaf 2 nader zal bespreken), blijkt deze vermenging ook z'n problematische kanten te kennen als het aankomt op keuzes en verantwoordelijkheden voor adequate informatiebeveiliging. Vanuit deze constatering beoogt dit essay een aanzet te geven voor de wijze waarop de overheid zich zou moeten verhouden tot het belang en de inrichting van informatiebeveiliging. Centrale noemer is daarbij een tweeledige opdracht voor de overheid: **begrenzing** voor wat betreft haar eigen informatiehuishouding en **systeemverantwoordelijkheid** voor de informatiehuishouding van anderen.

Een toekomstbestendige omgang met informatiebeveiliging vraagt namelijk om een hernieuwde balans tussen informatievrijheid, geheimhouding en beveiliging van gegevens, en een revitalisering van de beginselen van doelspecificatie en doelbinding in een tijdperk van grootschalige informatievergaring, -opslag en -hergebruik. Sommige informatie wordt dan helemaal niet meer verzameld, opgeslagen of gebruikt, andere informatiebronnen zijn juist transparanter in plaats van vertrouwelijk en geheim en sommige informatie is veel beter beveiligd. En daar waar actoren buiten de publieke sector de verantwoordelijkheid voor het stellen van grenzen en daarmee het belang van informatiebeveiliging. onvoldoende oppakken, is het de overheid die vanuit haar systeemverantwoordelijkheid de grenzen soms alsnog zal moeten stellen. Dan moet het ook de overheid zijn die bereid is het overschrijden van deze grenzen te ontdekken en te sanctioneren met flinke boetes. Maar dan is het ook een overheid die zich inzet voor het ontwikkelen van objectieve maatstaven voor een zorgplicht op het terrein van informatiebeveiliging, om vervolgens actoren die gehoor geven aan deze zorgplicht de hand toe te steken wanneer ze alsnog het slachtoffer worden van de risico's die digitalisering onheroepelijk met zich meebrengt.

Wat exact zijn de motieven die noodzaken tot zowel begrenzen als inzetten op systeemverantwoordelijkheid? Nadat ik in paragraaf 2 allereerst kort de kwetsbare kanten van de toenemende verwevenheid voor informatiebeveiliging en daarmee het risico van een verweesde verantwoordelijkheid heb neergezet, zal paragraaf 3 het belang van begrenzing nader duiden en aanknopingspunten presenteren voor de weging van belangen met h et oog op begrenzen in het belang van informatiebeveiliging. Paragraaf 4 betoogt vervolgens dat de overheid vanuit een systeemverantwoordelijkheid initiatieven op het terrein van informatiebeveiliging ontplooit als andere actoren hun verantwoordelijkheid hiervoor niet of onvoldoende zelf oppakken. Paragraaf 5 sluit af met het agenderen van enkele concrete punten voor debat en verder beleid.

2. Kwetsbare verwevenheden

Het voorbeeld van fraude bij DUO laat zien dat in de informatiesamenleving schotten steeds diffuser worden. Op een organisatieniveau is sprake van een toenemende digitale verwevenheid tussen allerhande partijen en sectoren, waarmee op een informatieniveau de grens tussen de publieke sector en de private sector nauwelijks meer te ontwaren valt. Het is deze verwevenheid die de informatiehuishouding van de overheid inmiddels tot een uiterst complex samenstel van actoren met ieder hun rechten en plichten heeft

gemaakt. En die situatie heeft overduidelijk consequenties voor het belang van informatiebeveiliging[2]. Want juist in een dergelijk complex samenstel van verantwoordelijkheden blijkt het uitgangspunt van adequate beveiliging, zoals neergelegd in artikel 13 van de Wet bescherming persoonsgegevens (Wbp)[3], nogal eens een papieren tijger. Belangrijker nog, het risico van 'verweesde verantwoordelijkheid' voor het belang en de concrete invulling van informatiebeveiliging ligt overduidelijk op de loer. In technische zin en daarmee in 'technologische' kwetsbaarheid raken verschillende delen van de overheid meer en meer verweven. In juridische en organisatorische zin is echter nog immer sprake van verkaveling (wetgeving per beleidsdomein, verantwoordelijkheden per uitvoeringsinstantie, rijk-provincie-gemeente, etc.). Van een dossier- en institutioneeloverstijgende aanpak en het ontwikkelen van een breder kader is geen sprake.

Technologische kwetsbaarheid

Een eerste kenmerk van de huidige omgang met informatie die hier debet aan is, is de onterechte veronderstelling bij veel organisaties dat de eigen informatiehuishouding verschilt van een open systeem als het internet. Veel instanties – zowel binnen de overheid als in de private sector – gaan nog immer van de veronderstelling uit dat de eigen informatiehuishouding zich daarvan onderscheidt in de zin dat het om een semi-gesloten systeem van de eigen organisatie gaat en niet een veel meer open systeem als het internet, waar men nauwelijks meer zicht heeft op de aangesloten partijen. Anders gezegd, men handelt vanuit de assumptie zelf nog het heft in handen te hebben en voor 100% te kunnen sturen op de veiligheid en beveiliging van informatiestromen binnen de eigen organisatie dan wel de keten van partijen met wie men samenwerkt. De in de introductie tot dit essay genoemde voorbeelden laten echter goed zien dat die 'maakbaarheid' en 'stuurbaarheid' van informatieprocessen onder druk zijn komen te staan. Zowel het vernetwerken van informatie als het laten vervloeien van informatiestromen over de grenzen van het publiek-private heen, maken dat de semi-gesloten informatiehuishouding van individuele instanties intern steeds meer op het internet gaat lijken. Illustratief waren al eerder de informatieketens op het terrein van de sociale zekerheid, zorg of de jeugdhulpverlening waar een nauwelijks nog te overzien aantal instanties op is 'aangehaakt'. Meer recent is de vanzelfsprekendheid waarmee overheden, bedrijven maar ook burgers hun gegevens via clouddiensten opslaan, delen en bewaren een illustratief voorbeeld. Vele complexe vragen die raken aan informatiebeveiliging moeten hier nog worden beantwoord[4]. Vrijwel geen enkele betrokkene en daarmee ook verantwoordelijke voor informatiebeveiliging weet 'waar' de gegevens zich bevinden (welk land, welke jurisdictie en daarmee welke wettelijke beveiligingsvereisten), welke auditprocedures en andere checks het naleven van het geclaimde beveiligingsniveau moeten garanderen en wie verantwoordelijkheid neemt voor als het onverhoopt toch mis gaat. Informatie is kortom meer en meer een zaak van velen, in plaats van toebehorend aan één organisatie. En daarmee is het belang van de veiligheid van die informatie ook niet langer zaak van één organisatie. Doorredenerend betekent dit ook dat het definiëren van de standaarden voor informatiebeveiliging en het nemen van verantwoordelijkheid voor het naleven daarvan op grenzen stuit: naarmate organisaties in digitaal verband verknoopt raken wordt het immers problematischer voor de keten dan wel de (cloud)dienst als geheel om informatiebeveiliging te kanaliseren, te verifiëren en voor de betrouwbaar-

2 Zie al eerder hierover: B.J. Koops, S. van der Hof & V. Bekkers, "Risico's in de netwerksamenleving: over vervlochten netwerken en kwetsbare overheden", in: Lips, Bekkers & Zuurmond (red.), ICT en openbaar bestuur, Utrecht: Lemma 2005, pp. 671-70.

3 Artikel 13 Wbp luidt: "De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."

4 Nationaal Cyber Security Center, Whitepaper NCSC, Cloudcomputing & Security, Den Haag januari 2012.

heid in te staan. Zo hanteert de Wbp in artikel 1, onder d, het begrip verantwoordelijke als instrument voor de toedeling van bevoegdheden en verantwoordelijkheden die uit de wet voortvloeien. Daartoe behoren ook de beveiligingsplichten. De wet gaat daarbij uit van een concreet aan te duiden en aan te spreken organisatie, namelijk degene die doel en middelen van de verwerking bepaalt. Het is deze organisatie die verantwoordelijkheid draagt voor het naleven van de beveiligingsplicht, zoals neergelegd in art. 13 Wbp. De vraag is echter of bij breed samengestelde informatieketens en diffuse applicaties als clouddiensten[5], de concrete verantwoordelijken wel altijd helder te duiden zijn. Wie naar informatieketens kijkt, ziet dat de verantwoordelijkheid voor de technische uitvoering op de ene plaats wordt belegd, terwijl als het aankomt op zaken als informatiebeheer, informatiegebruik en daarbij behorende bevoegdheden, vele andere instanties wat betreft verantwoordelijkheid in beeld zijn. Deze opdeling heeft vervolgens repercussies voor de veiligheid en beveiliging van gegevens, omdat er bijvoorbeeld lang niet altijd helderheid bestaat of de noodzakelijke afspraken zijn gemaakt over: security audits, gewenste niveau van beschikbaarheid van de applicaties en digitale diensten alsmede het onderhoud daarvan, procedures voor interne melding van datalekken en andere incident-response procedures, backup en hersteldiensten, etc.

Een tweede kenmerk, dat tekenend wordt geïllustreerd met het genoemde voorbeeld van DUO, is dat informatieketens en andere (semi-)gesloten systemen ongewild deel worden van het internet. Illustratief zijn de Snowdon- en eerder de WikiLeaks-affaire. Beide kunnen als een voorbode gelden van wat in de toekomst ongetwijfeld vaker zal gaan gebeuren: de interne informatiehuishouding van overheden komt ineens op de digitale straten van het internet te liggen. Oncontroleerbaar door het vele kopiëren en de snelle migratie van de informatie van server naar server, van apparaat naar cloud naar apparaat. Voordat een dergelijk 'lek' van overheidsinformatie naar het internet realiteit wordt, wordt het risico veelal beschouwd als een kwestie van beveiliging van data en van techniek en beleid om dat te bewerkstelligen. Zodra een lek resulteert in het verspreiden van gevoelige informatie op het internet is er echter geen beleid meer voorhanden, gaan instanties improviseren om – vergeefs – de controle terug te winnen, wat uiteindelijk veelal een weinig verheffende aanblik biedt. Toch zijn dergelijke lekken juist door digitalisering nagenoeg onvermijdelijk (in feite inherent aan de technologie) en laat ook het voorbeeld van DUO zien hoe kinderlijk eenvoudig het blijkt te zijn om de interne informatiehuishouding van individuele organisaties ineens op de digitale straten van het internet te dumpen.

Een derde punt zien we in de (wellicht ogenschijnlijk) tegenstrijdige belangen die de overheid beoogt te beschermen. De overheid heeft een taak burgers te beschermen tegen digitale kwetsbaarheden, waaronder cyberaanvallen, wat ook een verantwoordelijkheid impliceert om cybercriminelen op te sporen en te vervolgen. Daartoe moet de overheid de informatiebeveiliging van verdachten van cyberaanvallen kunnen doorbreken, wat leidt tot wetsvoorstellen om te kunnen inbreken op computers van verdachten of verdachten te dwingen hun wachtwoorden af te geven. In de publieke discussie over dergelijke voorstellen valt op dat burgerrechtenorganisaties en computerbeveiligingsexperts vrezen dat de overheid, al dan niet bewust, belang heeft bij een niet al te hoog beveiligingsniveau van computergebruikers. Sommigen vrezen bijvoorbeeld dat de overheid een pas ontdekt beveiligingslek eerst zelf

5 Zie onder meer: Zienswijze CBP over cloud computing, Den Haag: 10 september 2012. Zie ook de beveiligingsraamwerken, zoals specifiek voor cloud ontwikkeld door de Open Security Architecture en de Cloud Security Alliance (deze incorporeren ISO 27002): <http://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/251-pattern-cloud-computing> en <https://cloudsecurityalliance.org/research/ccm/>.

zou willen exploiteren om binnen te dringen in de computer van een verdachte, alvorens het lek publiekelijk bekend te maken. Daargelaten of een dergelijke vrees terecht is, geeft het een spanningsveld aan waar de overheid vanuit de handhavingstaak mee te maken heeft: naarmate het beleid om burgers beter te beschermen tegen digitale kwetsbaarheden beter werkt, wordt potentieel ook het werk van opsporingsdiensten om sturings- en bewijsmateriaal te verzamelen moeilijker.

Wat achter dit spanningsveld schuilgaat, is een gerelateerd spanningsveld dat wordt veroorzaakt door de nadruk die in een risicomaatschappij ligt op preventief ingrijpen: wil men zoveel mogelijk misdaad of ander onwenselijk gedrag voorkomen, dan vraagt de logica van de databanksamenleving om zoveel mogelijk gegevens te verzamelen waarmee risicoprofielen kunnen worden gemaakt. Vanuit die rationaliteit wil men gegevens over grote groepen kunnen vergaren, wat een stuwend beginsel oplevert dat gegevens van burgers (en consumenten, werknemers, enzovoorts) niet te makkelijk afgeschermd zouden moeten worden. De grootschalige gegevensverzameling creëert echter kwetsbaarheden, niet alleen door de databanken van beleidsuitvoerders zelf, maar ook omdat de gegevens daardoor voor derden (door lekken of hacken) eenvoudiger toegankelijk zijn. Zo bijt de sleepnetaanpak van preventief beleid vaak met het beleidsdoel dat deze aanpak juist beoogt, namelijk om diezelfde burgers (consumenten, enzovoorts) te beschermen tegen het onwenselijke gedrag van de (vaak kleine) groep fraudeurs of misbruikers.

Evenals bij de vernetwerkte informatieverbanden zien we ook hier dat de overheid in de nodige beleidsdomeinen niet altijd expliciet en eenduidig inzet op een adequaat niveau van informatiebeveiliging in de maatschappij, omdat de innerlijk tegenstrijdige logica van het beleidsdoel verschillende kanten op wijst. Ook daardoor dreigt de verantwoordelijkheid voor informatiebeveiliging verweesd te raken.

3. Beveiliging en begrenzing: redeneren vanuit wegen van belangen

De centrale stelling van dit essay is dat serieus werk maken van informatiebeveiliging impliceert dat overheidinstanties en politiek bereid en in staat zijn grenzen te stellen aan het groeiende gebruik van informatie en aan de toenemende verwevenheid van informatiestromen. De noodzaak tot het stellen van dergelijke grenzen werd ook reeds in 2011 op de agenda gezet. In dat jaar bood de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) het rapport iOverheid aan de regering aan[6]. Het rapport handelde over de inzet van ICT-applicaties door de overheid en concludeerde dat met deze inzet een achterliggend complex geheel van informatiestromen is ontstaan waar politiek en bestuur zich ogenschijnlijk niet of nauwelijks van bewust lijken te zijn. Deze onbewuste iOverheid, die eerder in de praktijk is ontstaan dan dat deze door de overheid is ontworpen, heeft de natuurlijke neiging om onbekommerd door te groeien. 'Grenzen aan de groei' komen pas in zicht als er zich een bewustzijn ontwikkelt van wat die iOverheid is en doet. Zo ook ontwikkelt de samenleving zich met een grootschalige en welhaast allesomvattende inzet van ontelbare digitaliseringsinitiatieven tot een iSamenleving. In vergelijking met de iOverheid is deze iSamenleving nog veel grenzenlozer. De iSamenleving is een conglomeraat van ongelijksoortige actoren die met elkaar in vernetwerkte verhoudingen staan en waartussen informatie rijkelijk vloeit en vermengt: burgers, overheden, NGO's, media, bedrijven, social media, cybercriminelen etc.

6 Beschikbaar via: <www.wrr.nl>. Amsterdam University Press 2011.

Centrale regie is onmogelijk in de geïnformatiseerde netwerksamenleving. Maar het idee dat overheden niets meer vermogen in een informatiesamenleving is eveneens een naïef beeld. In het rapport iOverheid benadrukte de WRR een aantal punten waarop de overheid scherp zou moeten letten om de eigen informatiseringambities op een goede manier vorm te geven. Een aantal van deze punten zijn van ook groot belang om te bepalen wanneer begrenzingen aan informatiegebruik en vernetwerking in beeld komen met het oog op het belang van informatiebeveiliging. Uiteraard zijn de afwegingen voor de overheid intern enerzijds en de afwegingen voor de vrije markt en samenleving in brede zin anderzijds niet hetzelfde. Het gaat eerder om 'informatieordening' in de zin van marktordening; net als de markt is informatisering een autonome kracht en de informatiesamenleving een vrije sfeer die toch, en om goede redeneren, begrensd en bijgestuurd wordt door overheden.

In de eerste plaats moet bij nieuwe ontwikkelingen goed nagedacht worden of verschillende belangen en beginselen voldoende met elkaar in evenwicht zijn. De WRR introduceerde voor het zoeken naar dit evenwicht drie clusters van beginselen - stuwende, verankerende en procesmatige beginselen. Deze drie zullen niet alleen met elkaar in evenwicht gebracht dienen te worden als het gaat om overheidsinformatisering (de centrale thematiek van het WRR-rapport), maar meer specifiek ook ten aanzien van informatiebeveiliging. Daarbij zal de overheid niet alleen zichzelf, maar soms andere partijen de maat moeten nemen om burgers en bedrijven te beschermen tegen kwetsbaarheden ten gevolge van een onvoldoende aandacht voor beveiliging. Zo zijn efficiëntie van dienstverlening of bestrijding van fraude met publieke middelen stuwende krachten voor overheidsinstellingen. Daar is ook in een informatiesamenleving in het geheel niets mis mee, vooropgezet dat ook verankerende beginselen als privacy, non-discriminatie en informatieveiligheid voldoende gewaarborgd zijn.

Wie het scala aan beleidsdocumenten over technologiegestuurde beleidsinitiatieven leest, ontkomt niet aan de vele woorden die zijn gewijd aan de beoogde en te verwachten voordelen die het betreffende initiatief de overheid en burgers in het vooruitzicht stelt. Efficiënte dienstverlening, terugdringen van administratieve lasten, veiligheid, proactief (doelgroepen)beleid en dienstverlening-op-maat, om maar enkele van deze voordelen te noemen. Veel minder woorden worden veelal gewijd aan de kosten van het betreffende initiatief, waaronder de risico's verbonden aan digitale opslag en communicatie en de daarop gerichte criminaliteit en systeemaanvallen. Kortom, veelal blijft onvoldoende duidelijk wat de keerzijde van digitale innovatie is.

Als illustratie voor de wijze waarop de overheid de weging van de verschillende belangen vorm kan geven, kan het opschonen van de overheidsinformatiehuishouding worden genomen. De informatiesamenleving heeft een goed geheugen, soms tot onze schade en schande zelfs een te goed geheugen. En met een groeiend geheugen en daarmee uitdijende berg aan opgeslagen informatie nemen ook de risico's toe, zoals het risico op lekken van al die informatie of het vertrouwen op verouderde informatie. Wat de kwetsbaarheid verhoogt, is dat formele, wettelijk vastgelegde bewaartermijnen in de dagelijkse praktijk niet of nauwelijks in acht blijken te worden genomen. Nu opslagcapaciteit geen belemmering meer vormt, is een vaakgehoord argument als het op wel of niet wissen van gegevens aankomt: 'ze kunnen altijd nog wel eens van pas komen'. Ook staat de techniek zelf soms het vergeten in de weg: bepaalde technische systemen, zoals relationele databases, zijn zo ingericht dat absolute en volledige verwijdering van gegevens het systeem welhaast als een kaartenhuis in elkaar doet storten. Kortom, de aanpak van informatiekwetsbaarheid

hangt samen met een duidelijk en stringent gehanteerd opschoonbeleid. En een dergelijk opschoonbeleid is veel meer dan zo af en toe stilstaan bij het weggooien van gegevens. Het noodzaakt tot een heldere en tijdige weging van belangen (belangen die enerzijds bewaren en anderzijds verwijderen benadrukken) en het agenderen van de uitkomst van deze weging bij het ontwerpen en bouwen van systemen. In feite is het een kwestie van 'Security by Design' – het in de techniek verdisconteren van normen voor de veiligheid van gegevens. Dat betekent dat in het eerste stadium van een beleidscyclus al wordt nagedacht over de weging van de verschillende belangen (stuwende en verankerende belangen) met het oog op de keuze voor een concrete bewaartermijn van de gegevens. Vervolgens zal de uitkomst van deze weging onderdeel moeten zijn van het ontwerp van de architectuur van het informatiesysteem en wel zodanig dat de gegevens bij ommekomst van de betreffende termijn automatisch worden gewist.

Tot op heden is er in de praktijk nauwelijks aandacht voor de mogelijkheden van Security by Design, onder meer omdat de business case voor een dergelijke benadering en deze systemen ontbreekt. Zonder een politieke omarming van dergelijke oplossingen en de bereidheid om als overheid hierin als launching customer op te treden zullen dergelijke technologieën nooit de oplossingen worden die ze wellicht zouden kunnen zijn.

4. Systeemverantwoordelijkheid

Een belangrijke lijn waarlangs de discussie over de rol van de overheid voor informatieveiligheid zeker ook moet worden gevoerd, is die van systeemverantwoordelijkheid – een verantwoordelijkheid die vanwege het enorme publieke belang alleen bij de overheid kan liggen. Een nadrukkelijker bemoeienis van de overheid met het gehele 'systeem' van informatiebeveiliging - dus niet alleen die van de overheid zelf, maar ook de private sector - is om meerdere redenen aan de orde. Allereerst is dat het geval waar de overheid een rol als beschermer van de belangen van burgers en bedrijven moet spelen. Illustratief voor deze rol is de navolgende stellingname van het Ministerie van Veiligheid en Justitie over de toepassing van biometrie in de private sector: "De aspecten waar de overheid rekening mee houdt ten aanzien van biometrie in de publieke sector kan zij ook van toepassing verklaren op de private sector in haar rol als beschermer van de belangen van de burger en de maatschappij"[7]. Het gaat dan bijvoorbeeld om de informatiegiganten die hun businessmodel op de persoonsgegevens van burgers bouwen, maar onvoldoende oog hebben voor het beveiligen van die gegevens. De overheid heeft dan de positie en verantwoordelijkheid om (technologische) onveiligheid aan te pakken. De overheid kan digitale systemen net zomin als marktpartijen voor de volle 100 procent beveiligen, maar heeft wél, en hierin verschilt ze van marktpartijen, de doorzettingsmacht om de afwenteling van onveiligheid te reguleren. De overheid kan, met andere woorden, voorschrijven welke schouders bepaalde risico's moeten dragen. Binnen deze arrangementen kunnen de kosten en baten van onveiligheid worden afgewogen en verantwoordelijkheden aan de betrokken actoren worden toebedeeld.[8] Burgers zijn dan niet langer uitsluitend op zichzelf aangewezen om eventuele problemen die voortkomen uit de onveiligheid van digitale systemen en diensten op te lossen.

7 Ministerie van Justitie, Visie op biometrie in de identiteitsketen publieke sector, Den Haag, Programma VIPS, juli 2010, p. 33.
8 Eeten, M. van (2011) "Gedijen bij onveiligheid: afwegingen rond de risico's van informatietechnologie", in D. Broeders, C. Cuijpers & J.E.J. Prins, De staat van informatie, WRR verkenning nr.25, Amsterdam: Amsterdam University Press.

Een tweede aanleiding voor systeemverantwoordelijkheid van de overheid is er waar de effecten van een onvoldoende aandacht voor informatiebeveiliging over de grenzen van de private sector heen in het publieke domein gaan spelen. Illustratief is hier digitaal identiteitsmanagement. Momenteel is nauwelijks sprake van regulering of zelfs maar politieke aandacht voor het gebruik, de kwaliteit en daarmee de veiligheid van digitale identiteiten in de private sector. Zwembaden, supermarkten, werkgevers en computerfabrikanten experimenteren bijvoorbeeld volop met nieuwe toepassingen van biometrische identiteitsbepaling. Hoe het met garanties voor de kwaliteit en veiligheid hiervan is gesteld, blijft echter onduidelijk. Nu de praktijk laat zien dat bij het gebruik van identiteiten de grenzen tussen de publieke en private sector steeds diffuser worden, zijn er serieuze risico's dat ook de veiligheid van systemen voor de identiteitsbepaling door de publieke sector verwatert.

Interventie door de overheid kan ook voorbeeldstellend en richtinggevend voor andere sectoren zijn. Bijvoorbeeld door organisaties te stimuleren een minimumniveau van veiligheid te realiseren en aldus hun zorgplicht wat betreft de veiligheid van systemen en gegevens invulling te geven[9]. Stimulerend kan bijvoorbeeld werken wanneer het Openbaar Ministerie (OM) zegt een stap harder te gaan lopen voor partijen die hebben voldaan aan een bepaalde zorgplicht waar het informatiebeveiliging betreft. En tegelijkertijd bedrijven en organisaties hard aanpakt als ze daarin nalatig zijn, ook om ervoor te zorgen dat partijen die niet voldoen aan een zorgplicht onterecht economisch voordeel behalen. Een en ander betekent overigens wel dat nagedacht zal moeten worden over objectieve maatstaven voor de invulling en omvang van deze zorgplicht en de rol die alle partijen in een bepaalde keten (bijvoorbeeld de keten van financiële transacties, waarbij niet alleen banken maar ook webwinkels, ISP's en consumenten zijn betrokken) daarbij hebben te spelen, gegeven hun mogelijkheden tot interventie, verdienmodel en de lasten die ze kunnen dragen. Ook zal hier meer dan momenteel het geval is, nagedacht moeten worden over de back-upfaciliteiten van verzekerbaarheid en schadefondsen voor degenen die aan de vastgestelde zorgplichten hebben voldaan. Bij het totstandkomen van een level playing field voor verantwoordelijkheidsverdeling kan de overheid vanuit haar systeemverantwoordelijkheid stimulerend, initiërend en interveniërend optreden. In zo'n situatie ook, kan het OM een stap terug doen waar het strafrechtelijke handhaving en sanctionering betreft en alle capaciteiten koesteren voor die situaties waarin het strafrecht daadwerkelijk als ultimum remedium heeft te functioneren. In deze zin is interventie door de overheid vanuit systeemverantwoordelijkheid kan ook ingegeven door de prijs die de overheid betaalt voor de kosten van opsporing.

Dat de overheid in financiële zin een flinke prijs voor niet alleen de kosten van opsporing, maar ook informatiebeveiliging betaalt, is duidelijk. Dat doet de vraag rijzen of bedrijven en overheidsinstanties die onvoldoende aandacht hebben voor informatiebeveiliging, niet harder aangepakt moeten worden dan momenteel mogelijk is. Een optie is om het verontachtzamen van de beveiligingsplicht met een forse boete te sanctioneren, waarbij deze boetes aan een fonds ten goede komen. Dit fonds kan dan specifiek beogen informatiebeveiliging op een hoger plan te krijgen, bijvoorbeeld door met deze middelen op te treden als launching customer voor Security by Design.

9 Zie over de rol die civiel- en strafrechtelijke zorgplichten bij informatiebeveiliging kunnen vervullen: J.E.J. Prins, "Zorgplichten en Cybercrime", Nederlands Juristenblad, 2013, p. 1185. In reactie hierop: B. Jacobs, "De DDos Paradox", Nederlands Juristenblad, 2013 pp. 2191- ev; E. Tjong Tjin Tai, "Zorgplichten van banken tegen Ddos-aanvallen", Nederlands Juristenblad 2013, pp. 2196.

Ter toelichting het volgende. Het College Bescherming Persoonsgegevens (CBP) - de toezichthouder op de naleving van de regels van de Wet bescherming persoonsgegevens, waaronder de beveiligingsbepaling en de uitwerking daarvan via de Richtsnoeren Beveiliging van Persoonsgegevens[10] - kan momenteel alleen dreigen met een dwangsom als de beveiliging niet op orde blijkt. Het CBP vraagt al langer om de bevoegdheid ook boetes op te kunnen leggen, soortgelijk aan de bevoegdheid die de OPTA heeft. De laatstgenoemde heeft namelijk op grond van art. 15.4, vierde lid, Telecommunicatiewet de mogelijkheid om een bestuurlijke boete van ten hoogste € 450.000,- op te leggen bij overtreding van de beveiligingsplicht die conform art. 11.3 Telecommunicatiewet rust op aanbieders van openbare elektronische communicatienetwerken en -diensten. Inmiddels ziet het ernaar uit het sanctionerend instrumentarium van CBP wel wordt uitgebreid met het boete-instrument, maar de nieuwe bevoegdheid ziet echter op een heel specifieke situatie. Het Wetsvoorstel 'gebruik camerabeelden en meldplicht datalekken'[11] introduceert namelijk de plicht voor bedrijven en overheden die persoonsgegevens verzamelen en gebruiken om een datalek zo snel mogelijk te melden bij het CBP. Als een datalek niet wordt gemeld, kan de toezichthouder het bedrijf of de overheidsinstantie een boete van maximaal € 200.000,- opleggen. Het zal duidelijk zijn dat deze meldplicht voor datalekken in nauw verband staat met de eerdergenoemde beveiligingsverplichting van art. 13 Wbp. Juist ook gezien deze samenhang bepleitte het CBP twee jaar geleden dat inbreuken op art. 13 Wbp ook bestuurlijk door het CBP kunnen worden beboet[12].

Ook voor overheidsinstanties die de veiligheid van informatiesystemen en gegevens onvoldoende serieus nemen, is beboeting zeker geen ondenkbeeldig scenario. Zoals bekend zijn in het strafrecht handelingen van tot de centrale overheid behorende bestuursorganen (vooralsnog) niet strafbaar. Maar in het bestuursrecht zijn de handelingen van deze organen wel beboetbaar, aldus de Afdeling Bestuursrechtspraak van de Raad van State[13]. Met andere woorden: de Staat kan in principe worden beboet[14] en daarmee is er ruimte om het verontachtzamen van de wettelijke regels voor het beveiligen van persoonsgegevens, ook als dat binnen de overheid gebeurt, daadwerkelijk te sanctioneren. En als het aan de Europese wetgever ligt, gaan deze boetes in de toekomst flink omhoog[15]. De Ontwerpverordening gegevensbescherming bevat in art. 79 (6e) een maximale boete van € 1.000.000,- dan wel 2% van de jaarlijkse omzet wereldwijd voor schending van de beveiligingsverplichting. Van een actief gebruik door de toezichthouder (CBP) van de ruimte tot het beboeten van bestuursorganen zou een heldere signaalwerking uit kunnen gaan. Deze boetes zouden, zoals hiervoor al gesuggereerd, ten goede kunnen komen aan een fonds dat specifiek ten doel heeft informatiebeveiliging binnen de overheid op een hoger plan te krijgen.

10 http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx.
11 Wetsvoorstel tot wijziging van de Wet Bescherming Persoonsgegevens en enige andere wetten in verband met de verruiming van de mogelijkheid van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving en de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens, 33662, Kamerstukken II, 2011/12, nrs. 1-2.
12 Advies College Bescherming Persoonsgegevens over het wetsvoorstel "Meldplicht datalekken en camerabeelden", Den Haag 22 maart 2012.
13 Afdeling Bestuursrechtspraak Raad van State (ABRS) 12 mei 2010, ECLI:NL:RVS:2010:BM4168, AB 2010, 185.
14 Bij decentrale overheden lijkt voor beboeten overigens minder ruimte te bestaan. Zie: ABRS 23 april 2008, ECLI:NL:RVS:2008:BD0232, AB 2010, 180.
15 Zie de ontwerp-Verordening zoals gepresenteerd door de Europese Commissie op 27 januari 2012.

5. Ten slotte: een bestuurlijke agenda voor iVeiligheidszorg

Het voorgaande betoog levert een aantal concrete punten op voor een bestuurlijke agenda op het terrein van informatieveiligheid, die is ingezet vanuit de twee leidende motieven in dit essay: begrenzing en systeemverantwoordelijkheid. Kort samengevat zijn deze punten de volgende.

Informatiebeveiliging heeft weliswaar bij de meerderheid van de overheidsinstanties de aandacht, maar is onvoldoende meegegaan in de hedendaagse realiteit van een vernetwerkte overheid. De risico's die deze vernetwerking in zich draagt voor het belang van informatieveiligheid staan niet of nauwelijks op het netvlies van politiek en beleid. Juist daarom ook ontbreken de juiste verantwoordelijkheidsstructuren en het daartoe noodzakelijke beleidsinstrumentarium om een meer verknoopte aanpak van informatieveiligheid te doordenken en te ontwikkelen. Wil de overheid het pad van digitalisering met vertrouwen kunnen vervolgen, dan zal het op een veel meer geïntegreerde wijze met het belang van informatieveiligheid om moeten gaan.

Belangrijk is het om hier aansluiting te zoeken bij andere initiatieven die de rijksoverheid momenteel neemt op het terrein van veiligheid, risico's en verantwoordelijkheden. Het is immers belangrijk om ook te leren van de ervaringen op andere dossiers als het gaat om verwachtingen en mogelijkheden om veiligheid te garanderen. Aansluiting zal daarom gezocht moeten worden bij de Strategie Nationale Veiligheid, en de daaraan gekoppelde Nationale Risicobeoordeling, alsmede het BZK-programma Risico's en verantwoordelijkheden. Vanuit deze ambitie geldt eveneens dat aansluiting gezocht moet worden bij de initiatieven van andere departementen op het terrein van informatieveiligheid, waarbij in ieder geval genoemd moet worden het cybersecurity-programma van het ministerie van Veiligheid en Justitie.

Strategie
Nationale Veiligheid

Noodzakelijk is hierbij tevens te komen tot het opstellen van een overkoepelend kader voor de uitvoering en handhaving van informatiebeveiliging en zeker ook de wijze waarop de daarvoor noodzakelijke verantwoordelijkheidsstructuur moet worden ingericht. Tot voorbeeld kan hier dienen de door de staatssecretaris van Infrastructuur en Milieu (IenM) aangekondigde maatregelen op het terrein van IenM-veiligheid, die moeten resulteren in een dossieroverstijgend kader voor de veiligheidsvraagstukken op de beleidsterreinen van dit departement. Onderwerpen die – naar voorbeeld van IenM – in een dossieroverstijgend kader voor iVeiligheid aan de orde moeten komen zijn: uniform en deskundig toezicht met toezichthouders die zowel als één loket en daarmee vanuit deze gedeelde voorkant als één systeemtoezicht opereren als ook vanuit een bundeling van krachten beschikken over de noodzakelijke expertise en prioriteitsstelling ; uniforme, afgestemde en voorspelbare handhaving met meer en hogere sanctiemogelijkheden; transparantie als het gaat om toezicht- en handhavingsregels en -praktijken; doorzettingsmacht voor de verantwoordelijke bewindspersoon als doeltreffende handhaving in gedrang komt[16]. Het belang van een dergelijk kader is dat het zowel een baken als een sturingsinstrument kan zijn voor degenen die in de praktijk van alle dag verantwoordelijkheid nemen en dragen voor de wijze waarop i-veiligheidszorg vorm krijgt.

16 Zie: Magazine Nationale Veiligheid en Crisisbeheersing, nr. 5 2013, p. 15. Zie over de noodzaak tot doorzettingsmacht op het terrein van informatiebeleid ook het WRR-rapport iOverheid.

Een belangrijke opdracht is ook het expliciteren van informatieveiligheid als onderdeel van de toetsing en uiteindelijk wellicht ook sanctionering van overheidsbeleid. In de voorgaande paragraaf heb ik al gewezen op de mogelijkheid tot het beboeten van bestuursorganen wanneer deze het belang van informatiebeveiliging verontachtzamen. Hiernaast wil ik wijzen op de rol van de beginselen van behoorlijk bestuur. Zoals bekend nemen deze beginselen een centrale positie in bij het toetsen door de bestuursrechter maar ook de Nationale ombudsman van het handelen van overheidsinstanties. De behoorlijkheidsvereisten vormen voor de Nationale ombudsman het toetsingskader bij de beoordeling van het handelen van de overheid en daarmee ook het handelen met het oog op informatieveiligheid. Voldoet het optreden van een bestuursorgaan in de concrete context aan deze vereisten dan wordt dit optreden als behoorlijk aangemerkt. De behoorlijkheidsvereisten vormen, zoals de Nationale ombudsman het zelf formuleert, in zekere zin de gedragscode voor de overheid[17] Uiteindelijk moeten deze vereisten ook de noodzakelijke checks and balances kunnen garanderen voor de wijze waarop de overheid omgaat met informatieveiligheid en de keuzes die hieraan ten grondslag liggen (zoals het hiervoor besproken wegen van stuwendee, verankerende en procesmatige belangen). De afgelopen jaren heeft de Nationale ombudsman bij meerdere gelegenheden de aandacht gevraagd voor de kwetsbare kanten van digitalisering, zoals de betrouwbaarheid en veiligheid van DigiD[18].

Expliciteren van informatie-veiligheid

Een vierde opdracht betreft de noodzaak om informatieveiligheid prominent op de tekentafels van de overheid neer te leggen. Keuzes over informatieveiligheid zijn in essentie politieke en beleidsmatige keuzes en pas in het verlengde daarvan technische keuzes. En dit betekent dat een cruciale rol is weggelegd voor het opdrachtgeverschap van de overheid. Het uitwerken en vaststellen van de eisen aan en de functies van nieuwe systemen en applicaties is bepalend voor de veiligheid en de (toekomstige) risico's van nieuwe toepassingen. Het opdrachtgeverschap van de overheid zou daarom moeten investeren in kennis op het snijpunt van beleid, uitvoering en informatieveiligheid in plaats van investeren in technische kennis over deze veiligheid. Alleen door te investeren in kennis op dit snijpunt kan het wegen van (stuwende, verankerende en procesmatige) belangen en daarmee zorg voor de noodzakelijke beperking tot onderdeel van het opdrachtgeverschap van de overheid worden.

Ten slotte ligt er bij de overheid een verantwoordelijkheid om zich de ontwikkelingen in de informatiesamenleving aan te trekken, en waar noodzakelijk daarin te interveniëren. Paragraaf 4 bevat enkele suggesties voor een nadere concretisering van deze verantwoordelijkheid, waaronder de opdracht voor de overheid om objectieve maatstaven te ontwikkelen voor een zorgplicht op het terrein van informatiebeveiliging, om vervolgens actoren die gehoor geven aan deze zorgplicht de hand toe te steken en die actoren die deze plicht aan hun laars lappen hard aan te pakken. Uiteraard zijn dergelijke interventies altijd politiek gekleurd en omstreden. Toch zal er moeten worden geprobeerd een soort common ground te formuleren voor het niveau van informatieveiligheid waar de overheid garant voor staat. Het is de zoektocht naar deze common ground die politiek en beleid hebben te agenderen vanuit het besef dat er – zeker ook als het op zoiets cruciaals als informatieveiligheid aankomt - ten principale een eindverantwoordelijkheid bij de overheid ligt.

17 Nationale ombudsman, (2007), p. 112. De behoorlijkheidsvereisten zijn te vinden op de website van de Nationale ombudsman <www.nationaleombudsman.nl>.
18 Zie onder meer het rapport 'De burger gaat digitaal', Den Haag, december 2013 en de daarin opgenomen uitkomsten van een enquête, onder meer over (het gebrek aan) vertrouwen in informatiebeveiliging door de overheid.

Decaan en bestuurder
Nederlandse School voor Openbaar Bestuur (NSOB)

Mark van Twist en Martijn van der Steen

Adjunct-directeur en co-decaan
Nederlandse School voor Openbaar Bestuur (NSOB)

Strakke schakels, kwetsbare ketens: naar uitgebalanceerde samenwerking rond informatieveiligheid

1.

Urgenter en relevanter risico: toenemend belang

Niets nieuws onder de zon?

Informatieveiligheid is geen nieuwe kwestie. Sterker nog, het is een klassiek probleem van overheidsdiensten. Verloren stukken in de trein, een gestolen aktentas, een oudpapierbak met persoonlijke gegevens of een aan de straat gezette PC die vol staat met gevoelige data. Soms diefstal, vaak gewoon slordigheid. Allebei met belangrijke consequenties. In dat opzicht niet nieuw, maar toch zijn er zaken die het belang van de kwestie in onze tijd vergroten. Allereerst gaat het om schaal. Waar in de zoekgeraakte tas een beperkt aantal stukken zat, betekent een beveiligingslek nu dat niet alleen de tas zoek is maar dat de hele achterliggende kast open staat. Gegevens kunnen ook door 'kleine kieren' op grote schaal worden geëxporteerd, in heel korte tijd. Ten tweede is de informatie steeds minder direct gerelateerd aan één zaak, maar wordt vooral de bulk interessant. Een zoekgeraakt dossier was gevoelig en vervelend, maar vooral voor de betreffende betrokkene en de zaak waarover het ging. Tegenwoordig wordt informatie gebruikt voor commerciële of criminele doelen die anders werken. Geen chantage, maar identiteitsfraude. Niet één dossier uitmelken, maar de veelheid van data gebruiken voor commerciële doeleinden, bijvoorbeeld voor gerichte reclame op basis van gebruikersprofielen. Of, een stapje ernstiger, gericht verhoogde premies door zorgverzekeraars op basis van vertrouwelijke gegevens over de medische geschiedenis van een patiënt. Het gaat bij informatieveiligheid niet om zomaar een denkbaar risico, maar om concrete gevaren voor individuele burgers, bedrijven, overheidsinstellingen, openbare orde en fysieke veiligheid. Oud of niet, het doet er betrekkelijk weinig toe als er grote belangen en publieke basiswaarden op het spel staan.

Niet nieuw, wel anders

Dat informatieveiligheid en onveiligheid van alle tijden zijn, laat onverlet dat er nu wel veel zaken anders zijn. Zo is de informatie steeds meer gedeeld, wat naast gebruikersgemak voor extra kwetsbaarheid zorgt. Gedeelde informatie is handig en verhoogt de productiviteit en gebruiksvriendelijkheid van systemen, maar het zorgt ook voor nieuwe kwetsbaarheid. Informatie staat niet meer ergens lokaal op een server in het eigen gebouw, maar ergens virtueel in de Cloud. Het is overal toegankelijk, maar daarmee verliest de organisatie ook grip op de toegang. Mensen gebruiken onbeveiligde Wi-Fi-verbindingen op allerlei locaties en werken vanuit daar op de gemeentelijke bestanden. Heel prettig voor hen, maar het maakt het leven van wie kwaad wil ook gemakkelijker. Beveiliging helpt en hindert tegelijk. Een alarm vergroot de gevoelde veiligheid, maar zorgt ook voor nieuwe zorgen: weet je de code nog, net van huis het ongemakkelijke gevoel dat het misschien niet aan staat, op vakantie de

telefoon bij de hand omdat de centrale kan bellen, rechtop in bed als het per ongeluk af gaat. En net als de beveiliging voor ongemak zorgt, zijn juist de bronnen van gevaar zaken die het leven aangenamer maken. 'Bring your own' is voor individuele medewerkers heerlijk, net zoals het zelf zonder gedoe kunnen installeren van de apps en toepassingen die handig zijn. Eén wachtwoord voor alle programma's, liefst gemakkelijk te onthouden. En hoe handig is het om met goede koffie te kunnen inloggen op een public Wi-Fi in een koffiehuis ergens onder weg. Lekker en makkelijk voor de mens, zondig en fout vanuit het systeem. Gemakkelijk voor de mens, gemakkelijk voor het gemeentelijke netwerk. Welke malware, spyware en andere 'gevaarlijke' elementen brengen de thuiswerkers en hun zelf gekozen apparaten en programma's mee? Thuis wordt werk en werkt wordt thuis, maar wat als de gegevens van het werk thuis zoek raken? De klassieke principes van beveiliging gaan uit van begrenzing en juist die begrenzing raakt door de inzet van gebruiksvriendelijke technologie steeds meer zoek. En niet zoek in de zin van iets dat kwijt raakt en wat we maar niet terug kunnen vinden, maar als iets waar mensen juist van af willen en ze blij zijn dat ze het kwijt zijn. Bevrijd van de kaders van het systeem, maar daarmee ook los van de traditionele beveiligingsmechanismen. Als ze al werkten doen ze dat nu in ieder geval niet meer. En dus, los van of ze het ooit ook echt deden, de traditionele hekken, sloten en kaders om informatiesystemen en communicatietechnologie zeker te stellen doen het niet meer. Omdat de centrale controle op de informatiesystemen verdwijnt, raakt ook het systeem van gecentraliseerde beveiliging zoek.

Informatie is opgeteld gevoeliger

Belangrijker nog is dat de informatie niet alleen in zijn toepassing, maar ook in zijn aard gevoeliger is geworden. Gevoegd bij het feit dat de waarde van grootschalige informatiebestanden is ontdekt, zowel in de reguliere markt als door criminele organisatie, maakt de waarde van de straks door gemeenten beheerde informatie steeds groter. Door de decentralisaties komt er veel informatie in handen van de gemeente en die informatie vertegenwoordigt veel waarde voor grote en kleine partijen die zoeken naar mazen in het beveiligingsweb. De gemeente professionaliseren, maar de partijen waarmee ze strijden ook. Zo is er sprake van een wedloop tussen gemeenten die bewust of onbewust steeds méér en steeds gevoeligere informatie accumuleren, waar professionaliserende partijen (groot en klein) achteraan jagen.

De begroting wordt krapper: meer met minder

Beperkt budget voor beveiliging

En terwijl de datacenters groter worden, wordt de gemeentebegroting krapper. Informatiebeheer wordt door de toename in volume en gevoeligheid van informatie steeds belangrijker, maar moet vorm krijgen in een context van kleiner budget. Bezuinigingen op de begroting laten zich voelen in het budget voor informatiebeheer. Ook als dat 'ontzien' betekent dat er nog steeds maar beperkt budget is voor beveiliging. De ontwikkeling en de opbouw van een nieuw systeem kan nog als bijzonder project verkocht

worden, maar het ontbreekt aan structureel geld voor verder ontwikkelde beveiliging van informatie. Zo staat het vermogen tot beveiliging van informatie onder druk. Er zijn bezuinigingen, de taken van gemeenten nemen al toe, de buitenwereld wordt steeds slimmer, de technologie wordt ingewikkelder, en gebruiksvriendelijke toepassingen zorgen tevens voor toenemende kwetsbaarheid.

De wedloop tussen toenemend belang en afnemend vermogen

Er staat dus veel op het spel: het belang van informatieveiligheid neem toe, terwijl het vermogen om voor die informatieveiligheid te zorgen afneemt - of in ieder geval onder grote druk staat. Om goed te kunnen werken en operationele kwaliteit te kunnen leveren, moeten gemeenten de informatie kunnen laten stromen, maar tegelijkertijd moeten ze ook zorgen voor adequate beveiliging er van. En daarbij staan ze tegenover zich steeds verder professionaliserende partijen: soms internationaal opererende bendes, soms pubers vanaf een zolderkamer, soms bedrijven die meer of minder legaal proberen om door toegang tot informatie een commercieel voordeel te behalen. Hoe gaan gemeenten hier mee om? Welke strategieën kunnen ze hiervoor hanteren? Hoe geven ze invulling aan het spanningsveld dat ze zelf verantwoordelijk zijn voor veilige informatie én ze die veiligheid in samenwerking met andere partijen moeten realiseren?

Ja, maar: na het instemmend geknik

Het toenemende belang van informatieveiligheid en de ongemakkelijke spanning met het afnemende vermogen om er goed mee om te gaan wordt door bestuurders en professionals gedeeld. Er is discussie over de oplossing, maar de kwestie is onder de aandacht. Iedereen vindt veiligheid een wezenlijk onderdeel van informatiebeleid. Vraag er naar en er komt een bevestigend antwoord en instemmend geknik. "Ja, dat vinden wij hier van het grootste belang." Zelden pleit iemand voor onveilig informatiebeleid, net zoals een publiekelijk voorstel voor verbetering van de veiligheid nauwelijks tot expliciete tegenwerpingen leidt. Toch verbloemt die publiekelijke helderheid en het eensgezinde geluid een belangrijk aspect. Voorbij het instemmend geknik op de vraag naar veiligheid blijkt informatieveilighed een onderwerp waar weinig bestuurders uit zichzelf over beginnen. Ze knikken instemmend als je er naar vraagt, maar spreken er met enige terughoudendheid over. In gesprekken over de nieuwe aanpak van de decentralisaties snijden weinig lokale bestuurders (wethouders of burgemeesters) eerst het onderwerp informatieveiligheid aan. Ze spreken over de nieuwe taken, over de samenwerking in de praktijk, komen dan (soms) bij het belang van gedeelde informatie, en zeggen dan nog iets over dat het vanzelf spreekt dat die informatie veilig is. En heel vaak zeggen ze dat laatste niet. Informatieveiligheid is bij voorkeur vanzelfsprekend. Een belangrijke reden om niet steeds over informatieveiligheid te beginnen is dat het bespreken van deze kwestie vaak het gevoel van

Belangrijk

onveiligheid oproept. Veel mensen realiseren zich niet hoe gevoelig de informatie is die gemeenten van hen beheren en dat is misschien voor hen wel zo prettig ook. Zo zit informatieveiligheid weliswaar 'tussen de oren', maar wel een beetje achterin de aandacht. En voor het alledaagse comfort, of in gevoelige besluitvormingsprocessen, is dat ook wel zo gemakkelijk. Eén zorg minder.

2.

Dynamisch denken over veiligheid maken

Veilig is (niet) heilig

Vaak agendeert een essay of een traject van bijeenkomsten en sessies van bestuurders een nog onvoldoende onderkend probleem. De aandacht is beperkt, terwijl er meer nodig is. Het belang is niet gedeeld, terwijl dat wel zou moeten. Er is nog onvoldoende gebeurd, terwijl er nog zoveel moet. In dit geval is het volgens ons toch anders. Er wordt niet te weinig gedaan, integendeel. Er gebeurt heel veel, het vraagstuk van informatieveiligheid wordt met grote daadkracht aangepakt. Gemeenten werken er individueel met grote inzet aan en stellen wezenlijke middelen vrij voor het opbouwen van een beveiligde informatieomgeving. Daarnaast investeren partijen nadrukkelijk in hun samenwerking en in de onderlinge samenhang van hun inspanningen. Zo is er al veel bereikt, variërend van gemeenschappelijk of gedeelde structuren - zoals de baseline informatieveiligheid - en protocollen, tot de inspanningen om door diepgaande metingen en audits te speuren naar de gaten en kieren in de informatieveiligheid. Er wordt veel gedaan, er is veel bereikt en er staat nog het nodige te gebeuren. De veiligheid is nog niet af, maar er is al veel in beweging gebracht.

Toch leert nadere analyse van de tot nu toe ondernomen inspanningen dat zich daarin een belangrijke leemte bevindt. Niet op het niveau van een technisch gat in de systeembouw, maar meer op conceptueel niveau, in de manier waarop de beveiliging wordt benaderd. De aandacht is tot nu toe sterk gericht geweest op informatieveiligheid als opgave van organisatieontwerp: technische expertise, adequate organisatie, voldoende middelen en een uitgedachte balans in belangen die op het spel staan, zoals gebruiksvriendelijkheid en veiligheid. Informatieveiligheid wordt benaderd als een operatie die vooral gaat om aandacht, middelen, expertise en techniek. Dat zijn uiteraard cruciale onderwerpen, maar het is de vraag of ze de systemen uiteindelijk ook werkelijk veiliger maken.

Wij vragen hier aandacht voor een andere dimensie van informatieveiligheid, die niet gaat over hoe systemen technisch werken, maar hoe mensen met die technische systemen werken. Informatieveiligheid is een wisselwerking tussen techniek en gebruik, tussen toegang en

omgang. In het concrete gebruik, maar ook in de allocatie van aandacht. Protocollen kunnen er zijn, maar hebben alleen zin als mensen ze volgen. Een speciale medewerker belast met veiligheid werkt alleen als alle andere medewerkers de gevraagde discipline opbrengen. En krachtig programma informatieveiligheid is alleen sterk als het leidt tot inbedding in de staande organisatie en de alledaagse werkelijkheid van medewerkers. Veiligheid is geen product van voldoende stevige maar statische systemen, maar omvat het vermogen om intelligente structuren te bouwen die aansluiten bij de sociale werkelijkheid van mensen die ze moeten gebruiken. De systeembouwers maken het systeem, maar het zijn de gebruikers (medewerkers, managers, bestuurders, buitenstaanders) die uiteindelijk maken dat het al dan niet werkt. Het is technisch vaak problematisch als systemen naast elkaar bestaan die niet goed met elkaar kunnen communiceren, maar het is nog veel erger als de gebruikers van het systeem er niet mee kunnen of willen interacteren. En die interactie heeft nogal eens een paradoxaal karakter, met - voor wie er geen rekening mee houdt - onverwachte gevolgen. Let wel, het zijn geen ontwerpfouten of tekorten, maar de paradoxale gevolgen van te eenvoudig doordachte goede bedoelingen. Ze doen geen afbreuk aan de deels ondernomen en deels nog te ontwikkelen stappen in het Programma Informatieveiligheid; ze voegen er een dimensie aan toe die, mits geïntegreerd in de aanpak, maken dat het systeem straks niet alleen staat, maar het ook werkt en meebeweegt met de zich ontwikkelende praktijk.

1. Veilige systemen zorgen voor gevaarlijk gedrag

Gevaarlijk gedrag

We kennen allemaal de zogeheten gordelparadox. Een deel van het veiligheidseffect van het dragen van een autogordel gaat verloren doordat mensen met de gordel om gevaarlijker rijden. Hetzelfde geldt voor ABS en alle andere systemen. Mensen passen hun gedrag aan op de door hen gepercipieerde veiligheid van hun systemen. Zo gaat het ook met informatiebeveiliging. Juist daar waar de standaard van de veiligheid het grootst is, ligt het gevaar van gevaarlijk gedrag op de loer. Waar mensen zich bewust zijn van het gevaar en gedragen ze zich veiliger. Ze nemen voorzorg, kijken zelf actief uit, en signaleren mogelijke risico's. Soms worden systemen veiliger als mensen zich onbeschermd voelen. Het uitrollen van grootschalige beveiligingssystemen neemt veel van die prikkel tot waakzaamheid weg. Sterker nog, de introductie van het systeem maakt dat mensen hun leervermogen aanwenden om praktische workarounds en 'olifantenpaadjes' te ontwikkelen die in of rond het systeem de leefwereld vergemakkelijken. Het systeem is zo veilig, dat mensen menen zich wat handigheid en veraangenaming te kunnen veroorloven. Wie zich achter een onneembare muur waant, neemt ruimte voor wat afwijking van het protocol; 'van één bypass stort dit prachtige systeem vast niet in'. Wie zonder verdediging het gevaar recht in de ogen ziet, zal het nooit zo zeggen. Niet omdat de één laks is en de ander niet, eenvoudigweg omdat in beide situaties het bewustzijn van het gevaar heel anders is. Gevoeld gevaar zorgt voor veiliger gedrag; vermeende veiligheid vergroot de verleiding van gevaarlijk gedrag.

2. Een stevige aanpak leidt tot snel verslappende aandacht

Vergelijkbaar is het gedragseffect dat de lancering van een omvangrijke aanpak, met vaak een gespecialiseerde projectorganisatie er omheen, leidt tot externalisering van de opgave. De keuze voor de stevige aanpak heeft uiteraard als bedoeling om een aantal dingen snel en goed op orde te brengen, en alle partijen met het fenomeen in aanraking te laten komen: 'veiligheid is van ons allemaal'. Maar tegelijkertijd zorgt het grote programma er voor dat het gevoel ontstaat dat er ergens wel anderen zijn die er mee bezig zijn. En de stevige aanpak impliceert meestal een fasering, waarbij majeure aandacht aan het begin op een moment weer uitdooft en overgaat tot 'going concern'. Onbedoeld leidt het niet tot doorgaande en zichzelf versterkende aandacht, maar heeft de krachtige impuls als onbedoeld effect dat het een tijdelijke maatregel wordt. Een piek, die opgevolgd wordt door een periode van rust. Let wel, dat is nooit de taal van het programma en de betrokkenen. Het is een gedragseffect dat met de tijd optreedt: de aanpak kan eenvoudigweg niet altijd stevig zijn.

3. Het beeld van bouwen suggereert een afronding

Organisaties zijn druk bezig met opbouwen of uitbouwen van systemen voor de informatieveiligheid. Dat is een logisch beeld, maar het is tevens verraderlijk. Opbouw impliceert dat het op een moment 'staat' en zo goed als af is. Een beetje bijhouden, hier en daar aanpassen, maar het grote werk is dan gedaan. Ook in de bestuurlijke aandacht komt dit terug. Tijdens de bouw doen allerlei partijen mee en is het onderwerp van gesprek. Dan ontstaan ook vragen naar wanneer het klaar is en hoe ver men al is. Op een gegeven moment moet het dan klaar zijn, het bouwen kan niet altijd maar doorgaan. Informatiebeveiligingssystemen zijn niet eeuwig in aanbouw, zoals de Sagrada Familia, waarbij de continue bouw deel van de schoonheid. Het is eerder zoals de bouw van een kantorencomplex; er is een moment waarop het gereed en gebruiksklaar moet zijn. Op zich is er niets mis met een systeem dat af is, maar de realiteit van informatieveiligheid zal zijn dat door de snelheid van ontwikkelingen de 'bouw' veel meer een proces van continue aanpassing, uitbouw, herinrichting, verbouwing en gedeeltelijke afbraak is.

4. Door inpassing in lopende systemen verliest het zijn bijzonderheid

Informatieveiligheid is geen primair proces, in die zin dat het niet tot directe producten of diensten leidt. Het is een afgeleide, bijkomende zaak, hoewel daarmee, zoals eerder beschreven, niet minder belangrijk. Cruciaal is echter dat het door het secundaire karakter - in de zin van geen direct tastbaar product - het nooit vanzelfsprekend onder de aandacht van het strategisch management of het bestuur staat. Die aandacht moet geconstrueerd worden en dat gebeurt via systematisering en professionalisering. Er worden meetsystemen gemaakt die leiden tot rapportages aan het management. Er worden audits uitgevoerd die met stoplichten laten

zien waar men in control is en waar mogelijke risico's zich bevinden. Dat zijn technische analyses, maar tevens beeldende interventies om de aandacht van de leiding te mobiliseren. Het vraagstuk moet zichtbaar in beeld gebracht worden, om te voorkomen dat het via negatieve incidenten onder de aandacht komt. Betrokkenen verbeteren hun systemen steeds verder en maken ze steeds professioneler, waarbij langzaamaan de professionaliseringsparadox intreedt: de rapportages die urgentie moeten wekken raken geïnternaliseerd in de organisatie en worden beantwoord met evenzeer professionele antwoorden. Er wordt een proces voor gemaakt, het wordt een terugkerend punt op de agenda en er wordt een medewerker voor aangesteld. Dat lijkt 'aandacht', maar het is het niet; het onderwerp komt juist buiten de aandacht te liggen. Waar de eerste rapportages nog 'arousel' creëerden en voor ongemak zorgden, wordt met de professionalisering van de systematiek ook het antwoord steeds meer een formaliteit. Wat eerst een door de gehele leiding gevoelde splinter in de vinger was, is nu een splinter die op een schaaltje wordt gepresenteerd. Hij is beter zichtbaar dan ooit, maar wordt niet meer gevoeld - en leidt dus tot steeds minder reactie. Niet omdat het systeem niet goed is, maar juist omdat het te zeer geperfectioneerd is.

5. Beveiligingssystemen stichten zelf gevaar

Een terugkerend thema in de inrichting van veiligheid en preventieve systemen is de vraag hoe veilig het systeem uiteindelijk moet en kan zijn: hoeveel veiligheid kan een systeem verdragen. De paradox van het betonnen zwemvest is dat het vest zo zwaar wordt dat de drager naar de bodem zinkt. Informatiesystemen kunnen zo goed beveiligd worden dat mensen er amper meer gebruik van kunnen maken. Dat werkt onveilig gedrag in de hand. Mensen gaan zich om de beveiliging heen organiseren, maar het schaaft ook de primaire processen van de organisatie. Informatie kan zo veilig zijn dat letterlijk niemand er meer bij kan - ook niet de normale gebruikers.

6. Dringend alarm zorgt voor zuinige reactie

Er is in onder andere de auditliteratuur veel werk gedaan over de beste manier om een 'moeilijke boodschap' te brengen. Auditors waarschuwen voor problemen, maar hoe doen ze dat op een manier die ook maakt dat de ontvanger van die boodschap actie onderneemt. Als het probleem te groot wordt gemaakt, dan lijkt de oplossing onmogelijk en nodigt het eerder uit tot passiviteit. Er is toch niets aan te doen. Is de boodschap te klein, dan is de urgentie beperkt: het kan nog wel even zo, we zien het aan, er is iemand mee bezig. En achterblijvende prestaties zijn vaak ook wel ergens aan te wijten, maar moet de boodschap zelf ook schuld adresseren: je moet iemand aanspreken om gehoord te worden, maar het direct aanspreken leidt evengoed tot defensief gedrag. Zo is het steeds zoeken naar de beste manier om wel aandacht te generen voor het belang van informatieveiligheid, zonder daarmee al in de boodschap zelf de deur voor vervolg dicht te gooien.

Essay van Mark van Twist en Martijn van der Steen

7. Steeds beter, nooit goed genoeg

Wie eenmaal het pad van investering en aandacht voor veiligheid inslaat komt terecht op een hellend vlak. Elke stap vooruit maakt dat er eigenlijk geen argument is om niet ook de volgende stap nog te nemen. Zo wordt het steeds beter, maar is het nooit genoeg. Niet omdat het te weinig veilig is, maar omdat er eenvoudigweg geen argumenten zijn om niet nog een extra beetje veiligheid in te bouwen. Dat is meer dan onmatigheid van de gebruiker - of gulzigheid van het systeem. Bij elke uitbreiding van het systeem voor veiligheid ontstaat zicht op nieuwe onveiligheid. Een stresstest laat zien dat het systeem het goed doet bij een aantal risico's, maar toont ook kwetsbaarheid op andere elementen. Het laat zien hoe het gaat met wat er is, maar dat roept onvermijdelijk zorgen op over wat er allemaal nog ontbreekt. Het voorbeeld van een kleinere gemeente die met informatieveiligheid aan de slag gaat illustreert het sluipende maar amper te keren proces van steeds beter maar nooit genoeg. Eerst is er een medewerker voor informatieveiligheid. Maar heeft die wel voldoende gewicht? Dan schalen we op en is er een zwaardere medewerker, maar kan die het wel alleen? Vervolgens is er een klein team van mensen die zich er mee bezig houden, maar hebben die wel voldoende bevoegdheden?
Dan is er een directe lijn naar het MT en zijn er protocollen voor concrete noodsituaties, maar die dekken lang niet alle mogelijkheden af. Dan zijn er meer omvangrijke protocollen, maar die vereisen ook steeds verder gaande technische expertise die bijna niet meer in eigen huis te organiseren is. Dan is er externe inhuur, maar die is omwille van kosten beperkt en uit de nieuwe hoogwaardige analyses blijkt dat er toch nog belangrijke kwetsbaarheden zijn. Vervolgens ontwikkelt de organisatie daarvoor een nieuw systeem, dat echter dusdanig ingrijpend is dat het bestuur en ook de gemeenteraad er steeds meer aandacht voor ontwikkelen. Er komen vragen over de veiligheid en de wethouder maakt het zijn eerste prioriteit. Dat is voor de raad aanleiding om er een vast onderwerp van te maken en men maakt zich zorgen over de kwetsbaarheden die er ondanks jarenlange inzet nog steeds zijn. Moet er niet bijgeschakeld worden?

Paradoxale gevolgen

Paradoxale gevolgen van goede bedoelingen

Elk van de zeven paradoxale mechanismen maakt dat een interventie om de urgentie te vergroten, het systeem veiliger te maken en bestuurlijke kracht te mobiliseren er toe leidt dat de (aandacht voor) informatie-veiligheid kleiner wordt. De complexiteit van de techniek is één, de dynamiek van bestuurders, managers en gebruikers met informatiesyste-men is iets heel anders. Wie informatieveiligheid onder de aandacht wil brengen én houden, zal zich rekenschap moeten geven van deze dynamiek. Het vormt de constante van informatieveiligheid en moet daarom in de kern van de aanpak een plek krijgen, in plaats van als uitzondering te worden uitgebannen. Veiligheid is niet iets dat een projectorganisa-tie of programmateam door systeembouw maakt, maar is een coproductie waarin gebruikers, deskundigen, betrokkenen en belanghebbenden samen het systeem en de informatie veilig maken.

Essay van Mark van Twist en Martijn van der Steen

3.

Samenwerken als opgave: het geketende netwerk

De bovengenoemde inspanningen zijn bijna per definitie aan de orde in een contact waarin de veiligheid van de één een product is van de handelingen en systemen van de ander. Partijen die zichzelf los kunnen schakelen van het netwerk kunnen het zich misschien veroorloven om hun eigen veiligheid te organiseren, maar voor alle andere partijen geldt dat hun belangrijkste kwetsbaarheden voortkomen uit interacties met anderen. Informatieveiligheid is daarmee in belangrijke mate een vraagstuk van samenwerking tussen organisaties. Gemeenten kunnen individueel hun zaken op orde hebben, maar dat is van betrekkelijk weinig waarde als andere partijen dat niet hebben - of als tussenpartijen alsnog gaten ontstaan. Samenwerking is nodig om de eigen gaten te dichten, maar ook om nieuwe gaten tussen partijen samen op te pakken. Vanuit beide redenen hebben gemeenten elkaar nodig, net zoals ze samen moeten werken met private partijen en andere publieke partners.

Die noodzaak van samenwerking wordt door alle partijen ook wel onderkend. Sterker nog, partijen hebben stappen ondernomen om hun eigen informatieveiligheid als een coproductie op te pakken. Dat gebeurt bestuurlijk, door aldaar het commitment uit te spreken, maar ook operationeel. Partijen trekken samen op, spreken samen hun baseline af, en bouwen hun systemen zo dat ze op de ander zijn afgestemd. Informatieveiligheid is onverminderd een taak van iedere gemeente op zich, maar gemeenten pakken die taak steeds meer samenwerkend op. Die erkenning van de noodzaak tot samenwerking leidt tot platformorganisaties en nationaal georganiseerde samenwerkingsverbanden. Daarnaast zijn er regionale verbanden, van gemeenten die elkaar in algemene zin goed liggen of die gemeenschappelijke uitdagingen en kwetsbaarheden zien. De beweging is indrukwekkend. Partijen melden zich aan, ondertekenen intentieverklaringen en zetten op organisatieniveau stappen om aan de afgesproken baseline te voldoen. Dat zijn belangrijke signalen van voortgang, die tegelijkertijd niet betekenen dat het van hieruit vanzelf vooruit gaat.

Net als in op het niveau van systemen is ook op het niveau van de verschillende concrete platforms en vehikels voor samenwerking een reeks complexe en paradoxale beginselen te benoemen die voor onvoorspelbaarheid zorgen. Dat wil zeggen, wie de samenwerking en het proces beziet vanuit de enkelvoudige logica van het ontwerp ziet stevige constructies die het succes bijna wel moeten verzekeren. Borgen en verbeteren moet in die lijn van denken bovendien gezocht worden in het verder finetunen en strak trekken van de onderlinge verbanden, zodat partijen steeds dichter op elkaar georganiseerd worden. Als de doelen maar gedeeld zijn, de processen op elkaar geschakeld, de lucht uit de systemen geperst is en de belangen gelijk lopen komt de samenwerking vanzelf tot bloei. Vanuit dat beeld bezien gaat het goed en is helder hoe het nog beter kan: het

bestaande netwerk van samenwerkende partijen moet steeds meer, en meer gedisciplineerd, gaan samenwerken volgens het organisatiemodel van de keten. Gelijkvormig, gecoördineerd, helder en opgelijnd. Door het netwerk te ketenen - in strakke ketens te organiseren - wordt de basis voor informatieveiligheid gelegd. Een aantal van de ondernomen stappen en de voorstellen voor vervolg zijn in dat kader te begrijpen.

Afstemmen en coördineren zijn prima, maar de praktijk van interbestuurlijke samenwerking is ingewikkelder. Dat netwerken maar niet tot eenduidige richting komen is geen gevolg van afstemmingsproblemen of tekort aan mandaat, maar is een inherente eigenschap. Belangen verschillen, perspectieven zijn anders en versnelling en vertraging wisselen elkaar onvermijdelijk af. In dat proces kan de keuze voor 'verdergaande samenwerking' synoniem staan voor bewuste vertraging en kan het nemen van een besluit bedoeld zijn om de besluiteloosheid te markeren. Partijen doen mee om te hinderen, of stappen er uit om een impuls te geven. Ze spreken hun steun uit omdat ze daarmee tegenspreken, of zoeken juist de confrontatie met anderen om het zo oprecht beter te maken. Meedoen, tegenstribbelen, verzet tonen of steunen zijn in interbestuurlijke processen geen zaken die zich op oppervlakteniveau doen gelden. We werken samen en daarom doen we zelf nog even niets. We doen het met zijn allen en daarom maken wij nu nog even geen kosten. Het heeft prioriteit, maar die ligt wel vooral bij de regio. Het heeft onze aandacht, maar we gaan nu eenmaal maar zo snel als de langzaamste. Samenwerken en de uitdaging gemeenschappelijk aanpakken klinkt daadkrachtig, maar het kan evengoed leiden tot vertraging en steeds opnieuw stapelende belemmeringen. Zo is er, net als op het niveau van individuele organisaties, ook voor wat betreft de samenwerking tussen partijen een reeks paradoxale mechanismen te benoemen.

1. Samenwerken legt onbedoeld verschillen bloot

Partijen werken samen om tot één lijn te komen, maar samen betekent niet allemaal hetzelfde. In samenwerkingen draait het om wat partijen gemeen hebben, maar zijn de onderlinge verschillen minstens zo belangrijk. De ene gemeente is de andere niet, contexten en mogelijkheden verschillen, ook als de taken op papier ongeveer hetzelfde zijn. Dat geldt helemaal zodra de samenwerking ook andere bestuurslagen omvat. Provincies doen mee, maar zijn toch echt anders. Het Rijk zit aan tafel, maar opereert op een heel ander schaalniveau. Iedereen is welwillend, maar bij elke poging om dichterbij elkaar te komen hoort inherent de vaststelling dat partijen toch wel erg van elkaar verschillen. De intentie om samen te werken en tot één gemeenschappelijke standaard en werkwijze te komen neemt dat niet weg. Dat wordt scherper zichtbaar naarmate partijen pogingen ondernemen om juist meer samen te gaan doen. Dan wordt zichtbaar dat ondanks de goede intenties niet de overeenkomsten, maar de verschillen kenmerkend zijn. Samenwerken is niet het formuleren van het gemeenschappelijke doel of het afspraken van de gezamenlijke aanpak, maar evenzeer het productief omgaan met de onderliggende verschillen tussen partijen. Een

goede samenwerking maakt partijen niet allemaal gelijk, maar bouwt op de onderlinge verschillen.

2. Gedeelde doelen maar verschillende prioriteiten

Gedeelde doelen

Samenwerking legt bloot dat partijen andere prioriteiten stellen. Partijen zijn niet alleen verschillend, ze leggen ook andere accenten. De gemeenschappelijke afspraken maken altijd deel uit van een breder scala afwegingen en prioriteiten en daar maken partijen andere keuzes in. Ze onderschrijven het akkoord, maar het belang daarvan in relatie tot de vele andere eigen lokale prioriteiten ligt overal anders. Dat zorgt voor intense en soms tijdrovende discussies en zelfs conflicten over oorzaken en gevolgen en over de gewenste aanpak daarvan. Partijen willen hetzelfde, maar doen uiteindelijk toch net andere dingen, in een ander tempo. Dat is op zichzelf geen probleem, zo gaat het altijd, maar het wordt ingewikkeld zodra partijen zich expliciet verbinden aan doelen die alleen in samenwerking kunnen worden gehaald. Veel samenwerkingspogingen zijn erop gericht om dit soort verschillen te neutraliseren, bijvoorbeeld door partijen bindend te committeren aan afspraken en kritische deadlines. Daarmee kunnen partijen misschien deels wel gedisciplineerd worden, maar is het probleem van de verschillende prioriteiten niet opgelost. Die problemen zijn er, maar kunnen minder makkelijk invulling krijgen. Dat nodigt niet uit tot meer betrokken samenwerken, maar tot slimmere ontduiking of met minimale inspanning de afspraken halen. Duurzame samenwerking erkent de verschillende prioriteiten, geeft daaraan ruimte en bouwt op intrinsieke motivatie van partijen om gaandeweg het proces de prioriteiten dichter bij te brengen.

3. Belangen lopen langzaam uiteen

Samenwerkingsovereenkomsten maken expliciet dat er afspraken zijn waar alle partijen zich aan houden. Ze expliciteren het gedeelde belang en de gezamenlijke intentie. Toch moet niet worden vergeten dat die gedeelde belangen altijd een verbuiging zijn van wat uiteindelijk tegenstrijdige belangen zijn van betrokken partijen. Het Rijk wil andere dingen dan de gemeenten. Dat zij er op deelbelangen uit kunnen komen en samen een productieve samenwerking kunnen overeenkomen betekent niet dat hun verschillen weg zijn. In actieve samenwerking blijven die verschillen voortdurend opspelen en in de meeste processen worden ze gaandeweg het proces vordert langzaam weer groter. Het moment van ondertekening van het convenant was achteraf bezien vaak het toppunt van gemeenschappelijkheid, daarna komen rondom heel concrete kwesties en afwegingen steeds vaker de tegengestelde belangen op tafel. Niet altijd expliciet, maar wel altijd op de achtergrond. Zelfs al zijn alle partijen het eens over de urgentie van de kwestie, dan nog lopen hun belangen uiteen. Zo zijn samenwerkingsverbanden bundels van belangen die op hoofdlijnen een gemeenschappelijk doel onderschrijven, maar waar onder het oppervlak onverminderd de belangen uiteen lopen. Dat is geen probleem voor effectieve samenwerking, mits er in het ontwerp rekening mee wordt

gehouden. Vaak echter wordt het tegenovergestelde gedaan en is het 'not done' om in een overeengekomen samenwerkingsverband al te expliciet de eigen andere belangen in te brengen. Dat wordt opgevat als een breuk met het samenwerkingsverband, een niet-productieve interventie die daarmee ook meer is dan het melden van een tegenstrijdigheid. Het brengt de samenwerking zelf in gevaar, wordt daarmee groot, en lastig binnen het bedachte construct af te handelen. Partijen worden gedwongen te kiezen, de intenties te herbevestigen en kleur te bekennen. Daar staat tegenover dat het erkennen van de verschillen en daar ruimte voor te maken er voor zorgt dat partijen zich op termijn meer betrokken zullen voelen. Het gangbare beeld mag zijn dat juist door de gemeenschappelijkheid af te dwingen partijen op termijn nader tot elkaar komen, de praktijk is eerder tegenovergesteld. Partijen worden in het ongemak gedwongen en kunnen de spanning al snel niet meer goed in het arrangement kwijt.

4. Productie- en fexibiliteitsverlies

Samenwerking is een begrip waar iedereen voor is. Wie wil er nou niet samen optrekken, of in ieder geval een poging ondernemen. Alleen ga je sneller, samen kom je verder; uiteindelijk willen organisaties toch graag ver komen. Toch kent ook samenwerking keerzijdes, er is een 'dark side' aan het applausbegrip. Dat is geen kwestie van goede of slechte samenwerking, maar een inherente eigenschap van het niet alleen maar samen optrekken. Samen optrekken leidt op bepaalde aspecten misschien tot synergie, elders is het vooral productieverlies. Samenwerken kost tijd en verkleint de mogelijkheid om lokale oplossingen, die daar goed werken, te handhaven. Partijen leveren speelruime in, die ze goed zouden kunnen benutten om op onverwachte ontwikkelingen te reageren. Als ze in bepaalde primaire processen veranderingen willen aanbrengen, moeten ze steeds nagaan hoe die zich verhouden tot de gemeenschappelijke afspraken. Zo wordt wat bedoeld was als hefboom om de effectiviteit van de organisatie te vergroten tevens een beperking van de mogelijkheden.

5. Vrijwillige verstrikking

Partijen werken samen en kiezen daar zelf voor. Maar het is de vraag of waar ze in eerste instantie voor kiezen gelijk staat aan wat dat op langere termijn betekent. Samenwerking zorgt voor entrapment, voor verstrikking in processen. Partijen kiezen er voor om samen op te trekken, maar zodra ze dat eenmaal doen kunnen ze er niet goed meer uit stappen. En waar het samenwerkingsverband de neiging heeft om uit te dijen en te verbreden, is het steeds een grote stap om de uitbreiding niet te accepteren. Daarmee komt immers het geheel in gevaar en daar was men oorspronkelijk. Zo ontstaat langzaam het gevoel dat partijen niet meer terug kunnen, ook al zouden ze dat wel willen. Ze zijn gevangen in een arrangement, waar ze zich wel zelf vrijwillig deel van hebben gemaakt. Een variant op dit thema die zich eveneens vaak voordoet is capture. Partijen kopen diensten van een leverancier in, met op het eerste gezicht een goede deal, maar zitten dan vervolgens vast aan die leverancier. Het

Vrijwillige verstrikking

systeem draait nu eenmaal op hun techniek en overstappen betekent dat de investeringen voor niets zijn geweest. En de capture is zelfversterkend, want omdat partijen vast zitten aan het systeem kiezen ze voor hun uitbreidingen ook maar voor deze leverancier. Zo groeit het systeem waar ze niet van af kunnen verder aan, waarmee ze er nog moeilijk uit kunnen stappen.

6. Gebundelde kracht is geen gestapelde creativiteit

In samenwerkingsverbanden bundelen partijen de krachten. Ze trekken samen op, omdat ze 'samen sterker zijn'. De vraag is echter of sterker ook slimmer is? Dat partijen meer massa kunnen mobiliseren en daarmee sommige dingen beter kunnen staat vast, maar zijn ze ook in staat om beter te reageren op onverwachte ontwikkelingen? Of staan dan in eerste instantie de afgesproken protocollen centraal, waar alleen na consensus van afgeweken kan worden. Dat is van groot belang, omdat de uitdaging van informatieveiligheid er bij uitstek één van onverwachte wendingen en moeilijk te voorziene wendingen zal zijn. Een zekere massa is dan welkom, maar kan evengoed maken dat het reactievermogen kleiner wordt. Zolang de creativiteit geen expliciete plaats krijgt in de samenwerking is de kans groot dat deze in de pogingen om samen massa te maken verwatert.

4.

Als de basis op orde is: ruimte laten voor complexiteit

Het lijkt verleidelijk om in geval van een grote opgave, die meerdere partijen aangaat, voortvarend de samenwerking te zoeken. Een programma instellen, bestuurlijk draagvlak organiseren, acties in gang zetten en over de voortgang rapporteren. De verdeling over meer partijen betekent bovendien dat er samengewerkt moet worden. Daarop laten we het model van de keten los, wat betekent dat er regie op de samenwerking plaatsvindt en dat de schakels gesloten moeten worden. Straks organiseren en zorgen dat partijen niet uit de pas lopen. Met dat model is op zichzelf niets mis, zolang de opgave maar min of meer stabiel is. Niet voor niets reproduceert het ketenmodel een 'lopende band', waarbij partijen op lijn geschakeld worden. Dat werkt efficiënt, maar zorgt tevens voor problemen. De keten is zo sterk als de zwakste schakel, maar het tegenovergestelde is temidden van complexiteit ook waar: al te sterke schakels maken ketens die uiteindelijk zwak zijn als ze onder druk komen te staan. Zolang de problematiek zich keurig binnen de kaders beweegt gaat het goed, maar zodra de problematiek over de randen gaat en beweeglijk is wordt het lastiger. Dan zitten de sterke schakels in de weg, omdat ze een realiteit voorschrijven die er mogelijk niet is. Hoe strakker de afspraak, hoe lastiger het is om te improviseren en lokale betekenis te geven aan wat er aan de hand is. Als de omgeving onvoorspelbaar is, dan is juist ruimte voor

maatwerk, snel reageren en eigen initiatief nodig. De keten wordt sterker als de schakels meer ruimte laten voor variëteit.

We openden dit essay met de verwijzing naar vroeger: de romantiek van vergeten tas in de trein of de zoekgeraakte USB-stick met gevoelige informatie. Of het verbrandde archief, want informatieveiligheid gaat over bewaken maar ook over bewaren. Het lijkt bijna een romantisch verlangen naar toen, een tijd waarin het informatielek nog overzichtelijk was. Toen het nog mogelijk was om grenzen te stellen en met disciplinering de veiligheid te vergroten. Tegelijkertijd laat ons essay zien dat de huidige tijd zich dubbelzinning tot dat verleden verhoudt. In zekere mate zijn de veranderingen namelijk helemaal niet zo groot; er is niet zoveel verschil tussen de vergeten tas in de trein en de onveilige omgang met systemen. Zorgvuldigheid, goed opletten, veilig gedrag en risicobewust-zijn vormen nog net zo goed als eerst de basis voor een veilig systeem met goed beveiligde informatie. In die zin is ook het bewaren van stukken in een tas een interactie tussen mens en systeem; als die haper, de mens vergeet de tas, dan hapert het systeem. Los van alle waarmerken en borging die er mogelijk in zit. Daarnaast is het systeem van nu wezenlijk anders als toen, zowel vanwege de technische complexiteit ervan als door de veranderingen in de aard van de bedreigingen. De kunst is vervolgens om vanuit die ambivalentie de juiste elementen te nemen en daarop het nieuwe repertoire voor informatieveiligheid te bouwen. Gelijk blijft de essentie van veiligheid als product van interactie tussen mens en systeem, waarbij uiteindelijk de menselijke maat bepalend is. Ook, of misschien wel juist, als die interactie zich afspeelt binnen hoogwaardige technische systemen die nog maar een heel beperkt aantal mensen begrijpt en overziet. Het belang van interactie is geen afgeleide van de kennis van het systeem of het begrip er van. Dat zijn andere grootheden, die niets over elkaar zeggen. Daarnaast moet ook meegewogen worden dat de technologische én organisatorische context waarbinnen informatieveiligheid aan de orde is volstrekt anders is dan vroeger. De context kenmerkt door diepe complexiteit, waarin grenzen vervagen, in elkaar overlopen en processen elkaar voortdurend bedoeld én onbedoeld beïnvloeden. Technisch design vereist categorisering en afbakening van delen en domeinen, maar in werkelijkheid lopen die in elkaar over en werken ze op elkaar in. Dat betekent dat er een manier gevonden moet worden om binnen de technische mogelijkheden en noodzaak tot technische begrenzing juist gezocht moet worden naar manieren om met grensvervaging om te gaan. Dat is de realiteit van organiseren, dus is er behoefte aan systemen die de realiteit van grensvervaging en grensverwarring serieus nemen.

Basis op orde, verbazing voorbij

Op dit moment worden er belangrijke stappen gezet om de basis van informatieveiligheid op orde te brengen. Er is de baseline informatieveiligheid, certificering, control modellen en er worden afhankelijkheids- en kwetsbaarheidsanalyses uitgevoerd. Gemeenten zijn aan het werk, maar

veiligheid is meer dan alleen het inbouwen van meer waarborgen, het opwerpen van meer hindernissen en obstakels. Normen stellen en audits uitvoeren is niet hetzelfde als duurzaam borgen van veiligheid. Ze zorgen voor schijnzekerheid, die verankerd wordt in modellen, metingen, stoplichten en rapporten. Het risico dat daar bij hoort is onteigening van de thematiek, waarbij na een korte impuls tijdens het programma de aandacht van het bestuur en het management snel weer wegzakt. Het risico is ingekapseld in systematiek, uitgeplaatst bij deskundigen en mensen die er voor zijn vrijgesteld. Die dragen zorg voor de veiligheid, zodat anderen daar minder zorg voor hoeven te hebben. Niemand zal het expliciet zo zeggen, maar het is wel wat in de praktijk in veiligheidsdossiers gebeurt. Waarom zou het bij informatieveiligheid anders zijn?

Daarom moet het idee van de baseline meer letterlijk genomen worden dan nu het geval is. Het is een basis, een uitgangspunt van waaruit het echte werk begint. En dat werk moet niet liggen bij diegenen die vanuit hun professionaliteit bezig zijn met informatieveiligheid, maar bij allen die bezig zijn met informatie. Die urgentie wordt niet gewekt door de veiligheid in systemen onder te brengen die de gevaren steeds verder indammen - met bijbehorende rapportages van de auditors dat de organisatie steeds meer in control komt -, maar door juist de aandacht te vestigen op de continue onveiligheid van informatie. Dat werkt niet langs de weg van de rapportages, maar door betrokkenen 'gecontroleerd' in situaties van onveiligheid te brengen. Bijvoorbeeld door de onveiligheid te ondervinden in stresstests, waarbij recente incidenten elders op de eigen organisatie worden geprojecteerd. Kan de Sinterklaasactie in Amsterdam ook hier gebeuren? Zijn wij zelf de Pieter Hilhorst van de komende tijd? Wat als Diginotar nu plaatsvindt, hoe staan wij er dan op? Wat doen we? Wie belt wie? En zijn we dan bereid om maatregelen te nemen, die tegelijkertijd ook productieverlies betekenen en chagrijn en schade bij anderen opleveren. Achteraf zijn die analyses gemakkelijk gemaakt, maar wat als het echt zover is? Dan gaat het niet om een gestroomlijnd proces met rapportages en audits, maar om 'streetwise' bestuurders en managers die weten hoe ze moeten handelen en waar ze op moeten letten.

Genezen is niet altijd beter dan voorkomen

En de voorbereiding kan ook een stap verder gaan. Niet alleen oefenen met de crisissituatie, maar vooraf kijken hoe de crisis voorkomen kan worden. En dan niet door te toetsen aan de ideale situatie en de standaard, maar door een aantal ongebruikelijke paden te bewandelen. Social hackers inhuren, de kwetsbaarheden niet toedekken maar ze juist vergroten. De gaten opzoeken, zodat de organisatie zich er op kan voorbereiden. Niet door alles bij voorbaat op te lossen, maar door juist in te zetten op wendbaarheid; het vermogen om met onverwachte verstoringen om te gaan. Het beeld van wendbaarheid staat tegenover de weerbaarheid die organisaties zichzelf proberen aan te meten. Ze zoeken naar mogelijkheden

Essay van Mark van Twist en Martijn van der Steen

om de gevaren ofwel te voorkomen, ofwel reservecapaciteit, buffers en terugvalopties te ontwikkelen voor als het mis gaat. De organisatie maakt zich groot, dik, zwaar en stevig om op het moment dat het nodig is sterk genoeg te zijn. Wendbaarheid benadrukt juist de lichtheid, het vermogen om snel te zien waar de verstoring is, wat de oorzaak is en wat adequate eerste antwoorden kunnen zijn.

Strategisch improviseren

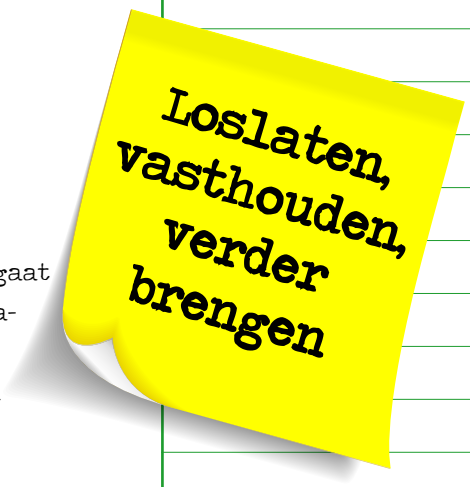
Juist omdat het onderwerp zo dynamisch is, is de strategie van wendbaarheid van groot belang. Niet als enige optie, maar als volgende laag bovenop de baseline die wordt aangelegd. De programma's die in ontwikkeling zorgen voor de basis, maar die heeft alleen zin als daar bovenop de mechanismen van wendbaarheid geborgd worden. Dat klinkt logisch, "natuurlijk doen we het allebei", maar datgene dat de baseline bouwt staat haaks op het vermogen tot veerkracht. Het voorkomen wordt de standaard, control is de norm. Er is geen ruimte meer voor twijfel en onzekerheid, terwijl dat aan de basis van veerkracht staat. Het moet allebei, maar het gaat maar zelden samen. Om die combinatie invulling te geven moeten organisaties leren om strategisch te improviseren. Wel doordacht en met een doel voor ogen, maar met maximale ruimte om steeds te signaleren welke veranderingen zich voordoen, wat er nodig lijkt, en daar dan vervolgens naar te handelen.

Het ontketende netwerk

Informatieveiligheid blijft ook in een improviserende en op veerkracht sturende vorm een zaak van samenwerken. Partijen moeten elkaar versterken, al was het alleen al omdat ze zonder elkaar onmogelijk het gewenste veiligheidsniveau kunnen realiseren. Dat kan vervolgens echter alleen, als in inrichting van het systeem én het proces de complexiteit van het netwerk recht gedaan wordt. Partijen die anders zijn, maar van daaruit samen dingen kunnen ondernemen. Gemeenschappelijke standaarden, als basis voor variëteit en onderling verschil. Een projectorganisatie die het proces laat bloeien, ook als dat van het projectplan afwijkt. Doelen die gesteld worden om dynamiek teweeg te brengen die de doelen overtreft of overbodig maakt. Waar de natuurlijke neiging in systeembouw steeds is om de complexiteit en variëteit in strak gekoppelde procedures in te dammen en in een keten onder te brengen, vereist het netwerk iets anders. Het is goed om een stevige keten te bouwen, als die toelaat dat de dynamiek van het netwerk van daaruit kan groeien. Het netwerk moet niet geketend worden; het systeem moet de kracht van het netwerk ontketenen.

5.

Vertaling in handelingsrepertoire: loslaten, vasthouden, verder brengen



De analyse in dit essay laat zien dat er voorbij de technische complexiteit van het vraagstuk een interactieve complexiteit is, die gaat over de interactie van mens en systeem, en van mensen onderling in samenwerkingsverbanden. Dat werpt licht op mogelijke handelingsopties die bestuurders (en andere betrokkenen) kunnen inzetten in hun eigen organisatie en de samenwerkingsverbanden waarin ze actief zijn. We benoemen er hier zeven.

1. Ruimte voor snelheid

Benut en beloon de wil van bepaalde partijen om het voortouw te nemen, nieuwe dingen te proberen en zodoende lessen te leren die uiteindelijk voor het collectief ook nuttig kunnen zijn. In de praktijk is dat vaak lastig, omdat samenwerkingsverbanden in gelijke tred willen optrekken en veel aandacht zich richt op het meekrijgen van de langzaamste. Dat vertraagt het geheel, maar haalt bovenal de energie voor de versnellers weg. Schep daarom in het arrangement ruimte voor overheden die een voor-uitstrevende en verkennende rol ambiëren in de samenwerking bij de aanpak van maatschappelijke vraagstukken. Hinder ze niet, maar eer ze juist, geef ze een podium om successen te vieren.

2. Zelfbinding zorgt voor eigenaarschap

In samenwerkingsverbanden is het van groot belang dat partijen dezelfde standaarden en regels hanteren. Die moeten ontwikkeld en afgesproken worden, waarbij vaak om redenen van efficiency en expertise voor centrale sturing. Iemand gaat namens het samenwerkingsverband aan de slag, om na enige tijd terug te rapporteren over 'de' afspraken die gemaakt moeten worden. Die worden dan namens het samenwerkingsverband aan individuele partijen opgelegd. Omdat zij zich er niet in herkennen, geen eigenaarschap voelen en misschien beperkte maar concrete problemen er mee hebben, gaan ze niet mee maar mobiliseren ze juist verzet. Wat snel leek - 'we ontwikkelen de afspraken centraal, zodat er geen gedoe over ontstaat' - zorgt alsnog voor vertraging. Het alternatief is eenvoudig. Vraag de overheden die bereid zijn om te participeren in de samenwerking om zelf aan te geven aan welke kaderstellende regels en afspraken ze wel én geen behoefte hebben, zonder zo de verantwoordelijkheid voor een eigen finale afweging uit handen te geven. Zelfbinding maakt eigenaarschap.

3. Coproduceer normen en indicatoren

Hetzelfde geldt voor de meer operationele normen en indicatoren voor evaluatie en verslaglegging. Die kan het samenwerkingsverband 'van buiten' opleggen, maar effectiever is het in gezamenlijkheid er van ontwikkelen. Laat de bij een samenwerking betrokken overheden zelf, in een goed geregisseerd proces van interactie via coproductie, de normen en indicatoren aangeven waarop ze via monitoring willen worden gevolgd en afgerekend. Zo wordt gebruik gemaakt van lokale expertise én ontstaat eigenaarschap voor de normen en indicatoren. Vervolgen kan de monitoring van normen en afspraken onderdeel van een individuele contractuele relatie zijn, waarbij de samenwerkende overheden zelf kunnen verklaren welke resultaten ze willen bereiken in de samenwerking. Zo ontstaat overeenstemming over de normen, maar is er ook ruimte voor individuele en verschillende afspraken over het tempo van deelnemers.

4. Kwaliteit als criterium

Voor veel samenwerkingsverbanden geldt dat 'dekking' van de doelgroep als eerst belangrijke criterium wordt gezien. De maat voor succes is dan of alle partijen meedoen. Dat is op zich natuurlijk ook goed, maar om partijen mee te laten doen, moet vaak afbreuk worden gedaan aan de kwaliteit. Partijen zijn nog niet ver genoeg en zijn eigenlijk nog niet klaar om mee te doen. Toch worden ze toegelaten; dat vergroot de dekking van de samenwerking en - zo is een veelgebruikt argument - het stimuleert die partijen om extra snel te leren en hun niveau op te trekken tot dat van de andere partners. Ze moeten ingroeien, maar mogen dat als volwaardig lid doen. Ervaring leert dat de effecten daarvan dikwijls anders dan bedoeld zijn. Eenmaal lid verdwijnt een belangrijke prikkel voor leren en vaak duren de aanpassingsprocessen ook gewoon lang, omdat problemen hardnekkig zijn. Selectiviteit (op grond van kwaliteit) zou een veel belangrijker criterium voor toelating moeten zijn, belangrijker dan de wens tot algehele dekking van de doelgroep. Laat overheden die ruimte willen bij samenwerking in betrekkingen zich daarvoor kwalificeren. Waarborging van een zekere kwaliteit kan als voorwaarde voor de overdracht van verantwoordelijkheden dienen.

5. Beloon verschil in plaats van gelijkvormigheid

Onbedoeld streven veel samenwerkingsverbanden naar gelijkvormigheid in prestaties en - als gevolg - naar gemiddelde kwaliteit. Dat is lastig voor de partijen onder het gemiddelde, die forse extra inspanningen moeten leveren. Het is ook vervelend voor de partijen die beter presteren, want zij zien hun kwaliteit vaak niet beloond. Interessant wordt het als de samenwerking variëteit toestaat in de mate waarin partijen worden gecontroleerd en beoordeeld, zodat verschil in prestatie maximaal gezien, herkend en beloond wordt. Wie voorop loopt krijgt minder controle en kan zichzelf monitoren, wie achter loopt wordt juist intensiever gevolgd en begeleid. Zo ontstaat ook meer ruimte voor verdiend vertrouwen in de

relatie en wordt excellentie gehonoreerd met minder lasten, grotere zelfstandigheid en positieve zichtbaarheid.

6. Helderheid over risico's en vertragende partijen

In lijn met het toelaten van verschil is dat er afspraken zijn over hoe gebrek aan samenwerkingsbereidheid wordt behandeld. In plaats van het gebrek te ontkennen, moet het expliciet en transparant worden gemaakt. Schep dus helderheid over de gevolgen die verbonden zijn aan een gebrek aan samenwerkingsbereidheid en onvoldoende transparantie: minder zelfstandigheid en meer bemoeienis met overheden die worden aangemerkt als risicocategorie. Laat het niet bij mooie woorden alleen. Handel er ook naar.

7. Verbreed de samenwerking en zorg voor externe druk

Voor een goed werkende samenwerking is scherpte van groot belang. Die komt deels van binnenuit, door elkaar kritisch te bevragen. Maar externe disciplinering kan ook erg helpen. Dat kan eenvoudig worden georganiseerd door bondgenootschappen aan te gaan met belanghebbende derden, om zo via druk van buitenaf op de voortgang in de samenwerking te bevorderen. Denk bij afspraken over veiligheid dan bijvoorbeeld aan verzekeraars die de verklaringen willen gebruiken als polisvoorwaarden. Maar denk ook aan publieke instanties als de brandweer, vakorganisaties op het gebied van de horeca en belangenverenigingen op het gebied van veilig uitgaan. Zo ontstaat externe druk, en een realiteitstoets, die het interne proces mede op gang houdt.

Geert Munnichs

Coördinator Technology Assessment
Rathenau Instituut

Linda Kool

Senior onderzoeker
Rathenau Instituut

Frans Brom

Hoofd Technology Assessment
Rathenau Instituut

ICT en burger empowerment - een pleidooi voor digitale autonomie

1. Inleiding

Onze samenleving digitaliseert in hoog tempo. Computers, tablets en smartphones zijn niet meer weg te denken uit ons leven. Dat geldt zeker voor een land als Nederland, waar het overgrote deel van de bevolking actief is op internet. De voordelen zijn legio: we zijn tegenwoordig alt-ijd en overal bereikbaar, informatie over willekeurig welk onderwerp ligt binnen ieders handbereik en ICT-toepassingen leiden op allerlei terreinen tot meer efficiëntie en gemak. Burgers, bedrijven en overheden maken dan ook volop gebruik van de mogelijkheden die ICT biedt.

De digitalisering van ons leven brengt ook risico's met zich mee. Beveiliging van ICT-systemen tegen ongeoorloofde toegang en bescherming van persoonsgegevens zijn belangrijke thema's, die voortdurend aandacht behoeven. Informatieveiligheid en privacy staan dan ook hoog op de agenda. Maar tegelijkertijd schort het in de praktijk nogal eens aan voldoende risicobesef. Nog te vaak zijn databestanden van overheden en bedrijven onvoldoende bestand tegen aanvallen van buitenaf of liggen door een slordige omgang met datagegevens van duizenden werknemers, patiënten of burgers op straat.

Maar er is meer aan de hand. De voortschrijdende digitalisering gaat veelal gepaard met een groeiende afhankelijkheid van burger en consument van overheid en bedrijfsleven. Informatie is de nieuwe grondstof van de hedendaagse samenleving. Zeggenschap over die informatie vormt dan ook een kernvraagstuk van de informatiesamenleving en zal in toenemende mate de maatschappelijke verhoudingen bepalen. Vaak zijn het overheden of bedrijven die bepalen welke informatie wordt verzameld, wie toegang krijgt tot die informatie en wat er vervolgens met die informatie gebeurt.

Het zijn de wensen en behoeften van de Googles, de Albert Heijns en de diverse overheden die leidend zijn voor de inrichting van ICT-systemen – en veelal niet de belangen van de internet-gebruiker, klant of burger. Maar het gebruik van ICT-systemen hoeft niet per se tot grotere afhankelijkheden te leiden. ICT is namelijk bij uitstek geschikt om de positie van de burger te versterken. Dit vergt echter een wisseling van perspectief, waarbij andere keuzes worden gemaakt bij de inrichting van ICT-systemen. Het vergt tevens dat relevante groeperingen en burgers worden betrokken in de discussie over de doelen die ICT-systemen moeten dienen.

Digitale afhankelijkheid

2. Digitale afhankelijkheid

De digitalisering van overheidsdiensten leidt ertoe dat de wijze waarop burgers geregistreerd staan in overheidsbestanden – hun virtuele identiteit – bepaalt hoe de overheid hen behandelt. Deze virtuele identiteit kan gebaseerd zijn op gegevens uit een enkel bestand, maar kan ook geconstrueerd zijn op basis van informatie afkomstig van diverse, aan elkaar gekoppelde bestanden. De persoon in kwestie hoeft geen weet te hebben van zijn of haar registratie of van het (geconstrueerde) beeld dat anderen op basis daarvan over hem of haar vormen.

De afhankelijkheid die daarmee gepaard gaat toont zich vooral zodra er fouten sluipen in gegevens of een daarop gebaseerd virtuele identiteit. Deze fouten kunnen het gevolg zijn van een incorrecte invoer van gegevens, verouderde data, identiteitsdiefstal of een verkeerde match van gegevens. Als gevolg hiervan kan iemand ten onrechte als 'probleemkind', 'wanbetaler' of 'drugscrimineel' worden beschouwd. Een bijkomend probleem is dat fouten voor

betrokken overheidsdienaren lang niet altijd te herkennen zijn. Naarmate meer instanties binnen een informatieketen gegevens aanleveren en naarmate die keten langer is, wordt het moeilijker om de juistheid van gegevens te verifiëren. Tegelijk hebben digitale gegevensbestanden vaak een dwingender karakter dan hun papieren voorgangers. 'Computers liegen niet' is een vaak voorkomende gedachte.

Het bovenstaande heeft tot gevolg dat eenmaal gemaakte fouten gemakkelijker een eigen leven gaan leiden. En die fouten laten zich moeilijker herstellen. Zo beschrijft de Nationale ombudsman in zijn jaarverslag De burger in de ketens (2009) het voorbeeld van een zakenman wiens identiteit werd gestolen door een oude bekende met een strafblad. Dit leidde ertoe dat de zakenman jarenlang in politieregisters te boek stond als drugscrimineel. Als gevolg daarvan kreeg hij te maken met herhaaldelijke aanhoudingen en huiszoekingen. Hoewel hij steeds kon aantonen dat hij niet diegene was die de politie zocht, bleek hij niet in staat om de identiteitsverwisseling in de registers gecorrigeerd te krijgen. De voortdurende verdachtmakingen aan zijn adres leidden tot ernstige schade aan zijn privé- en zakenleven.

Een groot probleem zijn de gebrekkige mogelijkheden van burgers om zich te verweren tegen fouten in hun virtuele identiteit. Het in de Wet Bescherming Persoonsgegevens (WBP) vastgelegde recht op inzage en correctie van gegevens blijkt in de praktijk vaak niet meer dan een papieren recht. Dit tast de rechtspositie van burgers aan en maakt hen verregaand afhankelijk van het naar behoren functioneren van ICT-systemen, zonder dat zij daarop veel invloed kunnen uitoefenen.

3. Digitale autonomie

Digitale autonomie

Kan het ook anders? De overheid en aan de overheid gelieerde organisaties passen uiteraard grote zorgvuldigheid bij de opslag en verwerking van persoonsgegevens toe, zeker als het om gevoelige gegevens gaat. Bovendien zouden alleen die gegevens moeten worden verzameld die strikt noodzakelijk zijn voor het bereiken van een bepaald doel. De commissie Brouwer heeft er eerder voor gepleit de verleiding te weerstaan om maar zoveel mogelijk gegevens te verzamelen. In plaats daarvan zou moeten worden uitgegaan van het principe van 'select before you collect' (Commissie Brouwer 2009).

Een zorgvuldige en selectieve omgang met gegevens komt ongetwijfeld ten goede aan de kwaliteit en betrouwbaarheid van verzamelde data. Maar fouten kunnen nooit worden uitgesloten. En omdat fouten in iemands virtuele identiteit grote gevolgen kunnen hebben, moet ook aandacht uitgaan naar de informatiepositie van de burger. Wat is nodig om afhankelijkheidsrelaties te doorbreken en ICT-systemen zodanig in te richten dat burgers meer mogelijkheden krijgen om controle uit te oefenen over de gegevens die over hen worden verzameld? Aan de hand van enkele voorbeelden gaan we hier dieper op in.

Kilometerheffing en OV-chipkaart

Enige jaren gelden werd overwogen een kilometerheffing in te voeren voor het autoverkeer. Hiervoor zijn verschillende varianten bedacht. Bij een daarvan – de 'dikke' variant – zouden de reisgegevens zodanig worden opgeslagen en versleuteld dat alleen de automobilist zijn reisbewegingen kon inzien. De innende instantie kon een factuur opstellen, maar de ritgeschiedenis niet nagaan. Tegelijkertijd beschikten beide partijen over bewijsmateriaal in geval van fouten of fraude. Deze dikke variant van de kilometerheffing, die gebruik maakt van

'zero-knowledge' cryptografie, zou minimaal inbreuk doen op de privacy van de reiziger, terwijl het beoogde doel – prijsdifferentiatie voor tijd, plaats en type voertuig – zou kunnen worden gerealiseerd. In deze variant werd het reizigersbelang vooropgesteld. Ironisch genoeg is juist wegens privacybezwaren indertijd afgezien van invoering van de kilometerheffing – waarbij moet aangetekend dat nog niet vaststond welke variant uiteindelijk de voorkeur zou krijgen.

Het voorbeeld van de kilometerheffing staat in schril contrast met de OV-chipkaart. Bij de invoering van deze kaart heeft de informatiebehoefte van de vervoersmaatschappijen voorop gestaan. De vervoerders wilden maximaal inzicht krijgen in reizigersbewegingen en deze informatie kunnen gebruiken voor commercieel interessante, op de individuele reiziger gerichte aanbiedingen. Hoewel dit laatste aan beperkingen onderhevig is gesteld, worden sinds de invoering van de kaart alle reizigersbewegingen centraal opgeslagen. Voor opsporingsdoeleinden kan daarvan gebruik worden gemaakt – hoewel dat vooraf nooit de bedoeling is geweest van de OV-chipkaart.

De belangen van de reiziger hebben in ieder geval niet voorop gestaan. Zo had nadrukkelijker kunnen worden gekeken naar het nut voor de reiziger van de verzamelde gegevens. Bijvoorbeeld door gebruik te maken van een 'best pricing'-systeem, waarbij de kaart bijhoudt of een reiziger vaak hetzelfde traject neemt en berekent of een abonnement voordeliger is. Ook zou met behulp van zero-knowledge cryptografie een anonieme variant van de OV-chipkaart kunnen worden ontwikkeld waarmee reizigers in aanmerking komen voor kortingsrechten, wat nu niet het geval is. Er staat in de huidige situatie een grote prijsdruk op anoniem reizen.

Elektronisch patiëntendossier

Digitale patiëntendossier

De beoogde invoering van het landelijk elektronisch patiëntendossier (EPD) vormt een tweede voorbeeld van hoe keuzes in de inrichting van een ICT-systeem van invloed zijn op de zeggenschap van burgers over hun gegevens. Het primaire doel van het EPD was een veilige uitwisseling van medische gegevens tussen zorgverleners. Toegang van de patiënt tot zijn medische gegevens kreeg pas in een later stadium aandacht, toen de Tweede Kamer daarop aandrong. Maar toen waren er al keuzes gemaakt over de inrichting van het systeem, met een landelijk schakelpunt dat uitwisseling van medische gegevens mogelijk moest maken. Enkele honderdduizenden zorgverleners zouden toegang krijgen tot die infrastructuur met een zogeheten UZI-pas.

Deze variant van het EPD functioneert alleen naar behoren als zorgverleners zorgvuldig omgaan met hun toegangspas. Dat betekent bijvoorbeeld dat ze hun pas niet delen met een collega en na ieder gebruik van het systeem direct weer uitloggen. Zo luidden ook de voorschriften. Maar het was de vraag of die voorschriften in de praktijk zouden worden nageleefd. De zorgsector stond – en staat – immers bekend om zijn gebrekkige risicobewustzijn als het gaat om gegevensbescherming. In combinatie met het grote aantal toegangspassen dat in omloop zou komen, maakte dat het systeem vanuit veiligheidsoogpunt kwetsbaar. Zorgen hierover waren voor de Eerste Kamer een belangrijke reden om de plannen voor invoering van het landelijk EPD af te wijzen.

Een alternatief hiervoor vormt een decentrale opslag van medische gegevens, waarbij de patiënt de gegevens beheert. In deze optie waarborgt de technische inrichting van het systeem dat alleen die zorgverleners toegang krijgen tot gegevens die daarvoor expliciet toestemming hebben gekregen van de patiënt. Dit alternatief is door het ministerie van VWS echter nooit

serieus overwogen. Ook aan deze optie zullen ongetwijfeld haken en ogen zitten. Maar het valt op voorhand niet in te zien waarom we wel accepteren dat burgers hun geldzaken via internet regelen, maar hen niet in staat achten hun medische gegevens te beheren. In ieder geval had het maatschappelijke en politieke debat over invoering van het landelijk EPD er baat bij gehad als de diverse varianten met hun voors en tegens met elkaar hadden kunnen worden vergeleken.

Decentralisatie jeugdzorg

Een derde voorbeeld heeft betrekking op de decentralisatie van de jeugdzorg naar de gemeenten. Volgens het kabinetsbeleid dient de jeugdzorg dichter bij de burger te worden georganiseerd. Door per gezin 'één behandelplan' door 'één regisseur' te laten opstellen, moet een goede afstemming worden gerealiseerd tussen de diverse hulpverlenende instanties die bij een gezin zijn betrokken. Het lijkt in dit verband niet meer dan logisch dat relevante gezinsgegevens met de betrokken instanties worden gedeeld. Volgens een advies van het Kwaliteitsinstituut Nederlandse Gemeenten (KING) moeten gegevens niet alleen tussen de partners binnen het sociaal domein worden gedeeld, maar bijvoorbeeld ook met school en justitie.

Hoewel de discussie hierover nog gaande is, is het gevaar niet denkbeeldig dat rond de jeugdzorg een digitaal bouwwerk wordt opgetuigd, waarbij uit het oogpunt van veiligheid en privacy grote vraagtekens kunnen worden geplaatst. Zeker omdat het hierbij vaak om privacygevoelige informatie gaat – bijvoorbeeld of kinderen in contact zijn geweest met de politie of ouders een psychiatrisch verleden hebben. Bovendien is het de vraag of gezinnen 'in regie' kunnen blijven – zoals een van de doelstellingen van het advies luidt. Zo blijft het in het advies onduidelijk welke mogelijkheden ouders hebben om foutieve gegevens of 'vroegsignaleringen' te corrigeren, of besluiten aan te vechten die de gezinsregisseur op basis van die gegevens neemt.

Er zijn uiteraard goede redenen te geven om bij gezinnen die met meerdere problemen kampen, gegevens tussen betrokken hulpverleners te delen. Maar is het de vraag hoe dat het beste kan worden georganiseerd. Koppeling van diverse gegevensbestanden mag uit efficiëntieoverwegingen aantrekkelijk lijken, maar maakt het systeem kwetsbaar voor ongeoorloofde toegang – vergelijkbaar met de bezwaren tegen het landelijk EPD. Wellicht kan ook bij informatieverzameling binnen de jeugdzorg gebruik worden gemaakt van versleuteling van gegevens, waardoor bijvoorbeeld NAW-gegevens niet zomaar kunnen worden gekoppeld aan privacygevoelige data en gezinnen meer controle kunnen houden op wie toegang krijgt tot welke gegevens.

4. Systeemvarianten

Versterking van de positie van de burger vereist reflectie op de inrichting van ICT-systemen. In de ontwerpfase moet worden nagegaan welke doelen een systeem moet dienen, welke gegevens daarvoor nodig zijn, hoe privacy- en veiligheidswaarborgen kunnen worden ingebouwd en welke mate van zeggenschap van burgers over hun gegevens wenselijk is.

Deze ontwerpeisen zullen niet altijd verenigbaar zijn. Zo kan gebruiksvriendelijkheid op gespannen voet staan met veiligheidsvereisten; kan versleuteling van gegevens moeilijk te verenigen zijn met het gebruik van die gegevens voor opsporingsdoeleinden; of kan het streven kindermishandeling te voorkomen leiden tot inperking van de controle van ouders op de uitwisseling van gegevens. Afhankelijk van de weging van de diverse ontwerpeisen en de precieze doelen die een systeem moet dienen, zullen andere systeemvarianten de voorkeur

verdienen. Deze weging kan er overigens ook toe leiden dat het oorspronkelijke doel dat een systeem moet dienen nog eens kritisch tegen het licht wordt gehouden.

De te maken keuzes zijn complex van aard, zowel technisch als maatschappelijk gezien. De discussie over de weging van ontwerpeisen en de meest geschikte systeemvariant vergt dan ook inbreng van zowel onafhankelijke ICT-experts als betrokken burgers, gebruikers en maatschappelijke organisaties.

5. Maatschappelijke dialoog

Versterking van de positie van burgers vereist dat ze betrokken worden in de discussie over de inrichting van ICT-systemen en de doelen die daarmee gediend zijn. Het gaat immers ook om hun belangen. De burger kan zowel indirect als direct in de discussie worden betrokken: door een dialoog aan te gaan met relevante maatschappelijke groeperingen, die een publiek perspectief op de zaak verwoorden; respectievelijk door de burger zelf aan het woord te laten. Met beide vormen heeft het Rathenau Instituut de afgelopen jaren goede ervaringen opgedaan.

In 2009 heeft het Rathenau Instituut in samenwerking met de commissie voor Volksgezondheid, Welzijn en Sport/Jeugd en Gezin van de Eerste Kamer een expertmeeting georganiseerd over de kabinetsplannen voor invoering van het landelijk EPD. Behalve Eerste Kamerleden, namen aan deze bijeenkomst ruim twintig ICT-deskundigen, woordvoerders van medische beroepsgroepen en vertegenwoordigers van patiënten- en consumentenorganisaties deel. Het bijeenbrengen van deskundigheid op het gebied van ICT met een brede vertegenwoordiging van maatschappelijke belangen en opvattingen vormde een belangrijke voorwaarde voor een geslaagd debat. Zoals hierboven opgemerkt zijn beide nodig voor het maken van een doordachte weging van ontwerpeisen: zowel technische mogelijkheden en onmogelijkheden als maatschappelijke consequenties moeten hiervoor in ogenschouw worden genomen.

Expertmeeting

Tijdens de bijeenkomst in de Eerste Kamer zijn tevens de resultaten gepresenteerd van een door het Rathenau Instituut en Veldkamp gehouden onderzoek naar opvattingen van burgers over het landelijk EPD. Door middel van focusgroepen is met 38 deelnemers gesproken over hun kennis van het EPD, de doelen die het EPD in hun ogen moet dienen en de mogelijke voor- en nadelen ervan. Focusgroepen zijn een kwalitatieve onderzoeksmethode die inzicht geeft in de diversiteit aan opvattingen onder burgers en in de achterliggende redenen en motivaties voor die opvattingen. De methode geeft daarmee dieper inzicht dan bijvoorbeeld een kwantitatieve publieksenquête.

Het zal niet verbazen dat kennis over het EPD van de deelnemers aan de focusgroepen beperkt was. Dat valt bij een complex onderwerp als het EPD ook niet anders te verwachten. Tegelijkertijd waren de deelnemers wel degelijk in staat om aan te geven wat ze verwachten van het EPD, welke zorgen ze hebben en aan welke voorwaarden moet worden voldaan om die zorgen weg te nemen. De gesprekken maakten duidelijk hoe gevoelig de toegang tot medische gegevens ligt en hoe belangrijk de beveiliging van gegevens is. Tevens maakten ze duidelijk dat veel deelnemers belang hechten aan het voeren van (een bepaalde mate van) regie over de eigen gegevens – en de mogelijkheden voor die regie doorslaggevend vinden voor hun vertrouwen in het EPD.

Alleen door de dialoog aan te gaan met betrokken maatschappelijke groeperingen en door burgers een stem te geven, kunnen we erachter komen wat er in de samenleving leeft en aan welke voorwaarden de inrichting en het functioneren van ICT-systemen moeten voldoen om tegemoet te komen aan de wensen en noden van de burger.

Literatuur-lijst

LITERATUUR

J. ter Berg & Y. Schothorst (2010), Het EPD: opvattingen van burgers – Verslag van een focus-groeponderzoek, Rathenau Instituut, Den Haag.

Ch. Van 't Hof, R. van Est & F. Daemen (red.) (2010), Check in/check uit – De digitalisering van de openbare ruimte, NAI Uitgevers & Rathenau Instituut, Rotterdam.

Ch. Van 't Hof, J. Timmer & R. van Est (red.) (2012), Voorgeprogrammeerd – Hoe internet ons leven leidt, Rathenau Instituut & Boom Lemma Uitgevers, Den Haag.

Commissie Brouwer (2009), Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer, Rijksoverheid, Den Haag.

Eerste Kamer (2009-2010a), Verslag van een rondetafelgesprek, Vergaderjaar 2009-2010, 31 466, F.

A. Jacobi , M. Lund Jensen, L. Kool, G. Munnichs & A. Weber (2013), Security of eGovernment Systems – Final Report, Science and Technology Options Assessment, Europees Parlement.

H. van Kempen & G. Munnichs (red.) (2010), Privacy, ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag.

KING (2013), Eindadvies Verkenning Informatievoorziening Sociaal Domein (VISD), Den Haag.

L. Kool, G. Munnichs & C. Boland (2013), Voer haalbaarheidstoets op ICT-projecten in, Het Bericht, Rathenau Instituut, 2013, nr. 6.

G. Munnichs, M. Schuijff & M. Besters (red.) (2010), Databases – Over ICT-beloftes, informatiehonger en digitale autonomie, Rathenau Instituut, Den Haag.

G. Munnichs & L. Kool (2013), De autonome burger in de informatiesamenleving – Hand-out inwerkprogramma tijdelijke commissie ICT-projecten bij de overheid, Rathenau Instituut, Den Haag.

G. Munnichs & L. Kool (2013), De autonome burger in de informatiesamenleving – Aanvulling op hand-out inwerkprogramma tijdelijke commissie ICT-projecten bij de overheid, Rathenau Instituut, Den Haag.

Nationale ombudsman (2009), De burger in de ketens. Verslag van de Nationale ombudsman over 2008, Nationale ombudsman, Den Haag.


Zero-
knowledge
cryptografie

Ira Helsloot

Hoogleraar Besturen van Veiligheid
Radboud Universiteit Nijmegen

Leren voor de bühne of voor de goede zaak?

Abstract

Het belang van informatieveiligheid is (ook) in het openbaar bestuur onomstreden. Net zo boven elke twijfel verheven lijkt de wens om consequent en institutioneel te leren van eerdere fouten en nieuwe inzichten. Toch blijkt bij een nadere beschouwing dat binnen het openbaar bestuur het leren over informatieveiligheid niet de hoogste prioriteit heeft. In dit essay beschrijven we het 'ist' en het 'soll' van institutioneel en bestuurlijk leren in hun onderlinge samenhang.
In zekere zin is de 'soll' situatie het meest eenvoudig: we weten al veel over eerste-orde (aanpassingen binnen bestaande structuren) en tweede-orde-leren (fundamentele verandering van bestaande structuren is noodzakelijk). Bij de twee leeropgaven horen eigen verschillende leerstrategieën passend bij de niveaus 'bestuur', 'bestuurlijke omgeving' en 'organisatie'. Onderscheid moet bovendien gemaakt worden tussen vier leerstappen: intuïtie, interpretatie, integratie en institutionalisatie. In het daadwerkelijke leerproces vergen deze stappen verschillende werkvormen.
De weerbarstige praktijk van het 'ist' laat echter een heel andere leervorm zien: symbolisch leren is een aantrekkelijke optie voor wie een risico eigenlijk niet erg serieus neemt en daarom niet wil investeren. Zo kan een bestuurlijke tweede-orde leeropgave opeens gereduceerd worden tot een eerste-orde ambtelijk 'probleempje'.
Voor wie hecht aan betere informatieveiligheid is daarmee de eerste leeropgave om het hart van het bestuur te veroveren dat wil zeggen om het belang van informatieveiligheid werkelijk begrepen te krijgen.

1. Inleiding: de informatieveiligheidsopgave

Er is, tenminste op het eerste gezicht, iets bijzonders met het leren over informatie(on) veiligheid: feitelijke voorbeelden van onveiligheid lijken niet tot een grote urgentie te leiden binnen het openbaar bestuur.

Ter herinnering, de meest directe aanleiding voor het instellen van de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID) was de DigiNotar affaire. De Onderzoeksraad voor Veiligheid was indertijd hard in haar oordeel over wat zij zag als de gebrekkige onderkenning van het belang van informatieveiligheid binnen het openbaar bestuur.

> **Directe aanleiding rapport Onderzoeksraad**
> De Onderzoeksraad voor Veiligheid spreekt in haar DigiNotar-rapport over 'gebrekkig zicht op risico's bij bestuurders en ambtelijke opdrachtgevers' en daardoor over 'bestuurlijk onvermogen tot het nemen van verantwoordelijkheid'.

Is dat nu echt veranderd sindsdien? Daar is twijfel over mogelijk: tenminste in gesprekken met de auteur van dit essay blijken bestuurders nog steeds niet scherp te hebben wat het DigiNotar risico nu überhaupt was. Natuurlijk hoeft een bestuurder niet alle technische details te beheersen van alle dossiers die hij bestuurt, maar zoals we later in dit essay zullen betogen begint bestuurlijke belangstelling met begrip.

Gebrekkige aandacht niet uniek voor openbaar bestuur

Hoogleraar Financial information security Eric Verheul stelt dat de gebrekkige aandacht voor informatiebeveiliging niet uniek is voor het openbaar bestuur: 'As a mildly amusing anecdote on management awareness; in 2003 I thought that the so-called vulnerability exploit in Internet Explorer was a convincing demonstration of the pitiful state of security in commonly used IT. This exploit implies that any website has access to the information in a user's clipboard through Internet Explorer (the internal memory buffer you fill when you use copy-paste in Word, Outlook and the like). Just think of the implications: any text you copy and paste is readable on the Internet. That could be passwords, parts of sensitive emails, privileged stock exchange information enabling trading with prior knowledge et cetera. And of course by using automatic refreshing webpages, an attacker could continuously monitor the contents of a user's clipboard! I demonstrated the vulnerability to senior management of several organizations but nobody seemed to be really impressed and I finally gave up. Their response would typically be that it was a 'techie' thing and 'who could seriously be interested in my information?'. Baffling. But it explains why security professionals currently still might have a hard time explaining the seriousness of possible targeted attacks at their organization. They might get the same reaction: 'it is a "techie" thing' and 'who could seriously be interested in my information?' Just wait, I guess, and finally you will see who was interested.'[1]

Semantiek is vaak veelbetekenend binnen het openbaar bestuur. De Taskforce BID heeft gekozen voor het woord 'informatieveiligheid' in plaats van het woord 'informatiebeveiliging'. Dat is verstandig want het woord 'beveiliging' heeft vooral een technische connotatie. Het is daarom jammer dat de minister van Binnenlandse Zaken in zijn reactie op het DigiNotar consequent over informatiebeveiliging spreekt [2] terwijl de Onderzoeksraad wel over informatieveiligheid spreekt,

De discussie is echter meer dan semantisch: het is een essentiële vraag of informatieveiligheid een technische of een bestuurlijke opgave is. De al dan niet noodzakelijke energie die in de noodzakelijke verbeteringen moet worden gestoken, hangt van die inschtting af. Bij veranderingen moet immers een onderscheid worden gemaakt tussen twee typen veranderingen:

- Eerste-orde-veranderingen zijn beperkte aanpassingen binnen de bestaande structuren en werkwijzen(organisaties, procedures, middelenstromen etc.)
- Tweede-orde-veranderingen zijn fundamentele veranderingen van de bestaande structuren en werkwijze in een nieuwe aanpak.

Voorbeelden eerste- en tweede-orde-veranderingen

We geven enkele tentatieve voorbeelden van denkbare eerste- en tweede-orde-veranderingen relevant voor informatieveiligheid. Op deze plaats dienen deze voorbeelden slechts als illustratie niet als aanbeveling!

1 Hoogleraar Financial information security Eric Verheul op zijn website www.keycontrols.nl.
2 Reactie op het onderzoeksrapport van de Onderzoeksraad voor de Veiligheid inzake 'Het DigiNotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt', ministerie van BZK, 12 november 2012.

Eerste-orde-verandering:

- invoeren en verplichten van opleidingen informatieveiligheid voor een relevante groep medewerkers;
- expliciet benoemen van informatieveiligheid in portefeuille lid college van B en W;
- verplicht stellen van paragraaf 'informatieveiligheid' in (gemeentelijke) begroting en jaarverslag;
- het houden van informatie-veiligheidsoefeningen.

Tweede-orde-verandering:

- instellen van functie Chief Information Officer (CIO) met de juiste bevoegdheden;
- inrichten nieuwe functie 'audit dienst informatieveiligheid' bij Rijk, VNG of elders;
- wettelijke normering voor niveau informatieveiligheid.

De rapportage van de Onderzoeksraad voor Veiligheid (OVV) stelt natuurlijk dat voor de noodzakelijke verbetering van de informatieveiligheid niet volstaan kan worden met eerste-orde-veranderingen alleen. Met andere woorden er zullen in de visie van de Onderzoeksraad zeker (ingrijpende) tweede-orde-oplossingen noodzakelijk blijken die daarmee bestuurlijke aandacht vergen. De mening van de Onderzoeksraad alleen zal echter geen bestuurder verbazen en daarmee overtuigen want de Onderzoeksraad hecht immers altijd aan tweede-orde-veranderingen.

Bedacht moet worden dat tweede-orde-veranderingen veel meer energie vergen dan eerste orde veranderingen. Wanneer derhalve kan worden volstaan met de 'kracht van incrementele verandering' verdient dat de voorkeur ook al is dan minder groots en meeslepend.

In het geval van informatiebeveiliging geldt echter dat wie zelf iets beter nadenkt, ook tot de conclusie komt dat informatieveiligheid evident breder is dan alleen het nemen van computer-technische beveiligingsmaatregelen. De maatschappelijke risico's van onvoldoende informatiebeveiligingsmaatregelen maken een bredere oriëntatie noodzakelijk op de niet computer-technische facetten van informatieveiligheid. Het gaat ook om zaken als maatschappelijke impactanalyses, daaruit al dan niet volgende inzet op (digitale) weerbaarheid, daarmee samenhangende bestuurlijk verwachtingenmanagement en bestuurlijke keuzes over de aard en omvang van de voorbereiding op de uiteindelijk tot altijd aanwezige kans op informatiecrises.

Informatieveiligheid vergt derhalve bestuurlijke aandacht en daarmee een tweede-orde-verandering, al zou het het alleen maar zijn om bewust en transparant te besluiten dat er niet verder geïnvesteerd zou moeten worden in informatieveiligheid. Een optie die op onderdelen verfrissend en efficiënt zou zijn (zo is er geen reden om exceptioneel veel te investeren in de informatieveiligheid van de OV-chipkaart wanneer we die veiligheid daarvan vergelijken met die van de strippenkaart) maar die zeker ook minder voor de hand liggend is als het gaat om de informatieveiligheid van vitale diensten.

2. De theorie van het leren

Laten we derhalve als uitgangspunt nemen in dit essay dat er tweede-orde-veranderingen gewenst zijn in de informatieveiligheid. Er moet dus door de bestuurlijk en ambtelijk betrokkenen op een passende wijze geleerd worden van de incidenten van afgelopen jaren.

In theorie weten we aardig hoe optimale leerstrategieën vorm moeten krijgen. We zullen de theoretische stappen om tot zo'n leerstrategie te komen hierna doorlopen.

In de eerste plaats moet een bij de orde van verandering passende onderscheid gemaakt worden tussen 'lower-order-learning' en 'higher-order-learning':

- 'Lower-order-learning' wordt ook wel 'single-loop-learning' genoemd. Het gaat hier over activiteiten die iets toevoegen aan kennis, competenties of routines zonder daarbij de fundamentele natuur van de organisatie te veranderen. Mason (1996)[3] noemt deze vorm van organisatieleer ook wel non-strategic-learning, waarmee bedoeld wordt dat deze leer meer aan de oppervlakte blijft en niet de strategie van een organisatie aanpast.
- 'Higher-order-learning' wordt ook wel 'double-loop-learning' genoemd. Hier gaat het om de situatie waarin, naast het detecteren en corrigeren van fouten, de organisatie wordt betrokken bij het ter discussie stellen van bestaande normen, procedures, beleid en doelen. Mason (1996) noemt dit: strategic-learning.

Het ideaalbeeldbeeld van higher-orde-leren

In veel theoretische beschrijvingen wordt aan higher-order-learning als vanzelfsprekend een hogere waarde toegekend dan lower-order-learning. Zo'n positieve insteek inzake higher-order-learning zien we terug in Bloom's klassieke taxonomie van het leren.[4 5] Het maken van analyses, het creëren van nieuwe kennis en het evolueren van een organisatie, is in zijn ogen van een andere orde dan enkel het aanleren van feiten en concepten. Higher-order-thinking kost, zo stelt Bloom, meer moeite, vereist meer competenties, maar is uiteindelijk wel waardevoller omdat de capaciteiten die daarmee worden aangeleerd beter van pas komen in nieuwe situaties. Het stelt individuen én organisaties beter in staat zich aan te passen aan veranderende situaties. Maar, daartegenover staat dat het in de harde werkelijkheid wel noodzakelijk is om telkens de vraag te stellen of de energie die moet worden gemobiliseerd voor higher-orde-leren wel noodzakelijk is om de geformuleerde doelstellingen te bereiken. Er zijn veel situaties denkbaar waarin voor bepaalde doelgroepen volstaan kan worden met een eerste-orde-leerproces.

Ten behoeve van het kunnen ontwikkelen van een leerstrategie is het verder noodzakelijk onderscheid te maken tussen de drie niveaus die betrokken zijn bij de veranderopgave op het terrein van de informatieveiligheid:

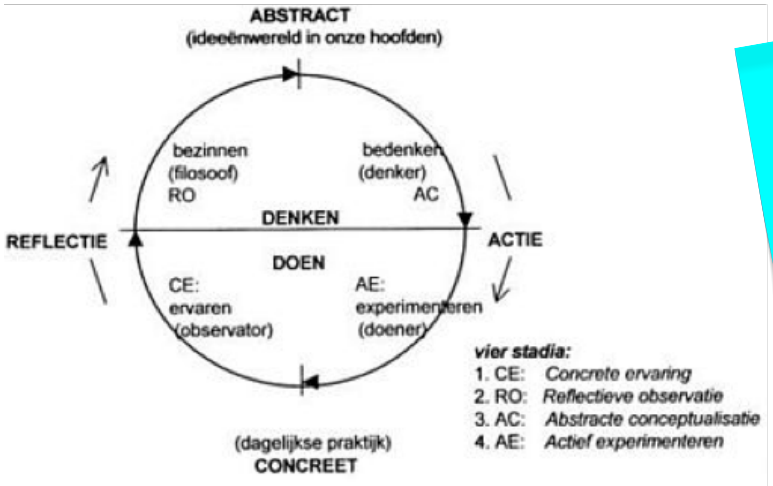
- Bestuurders: eindverantwoordelijk;

3 Mason, D. (1996). Leading and managing the expressive dimension: Harnessing the hidden power source of the nonprofit sector. San Francisco: Jossey-Bass.
4 Bloom, B.S. e.a. (1956). Taxonomy of educational objectives: the classification of educational goals; Handbook I: Cognitive Domain. New York: Longman.
5 Anderson, L. & Krathwohl, D.A. (2001). Taxonomy for Learning, Teaching and Assessing: A Revi-sion of Bloom's Taxonomy of Eductional Objectives. New York: Longman.

- Bestuurlijke omgeving: collega bestuurders en topambtenaren;
- Overheidsorganisatie: de ambtelijke uitvoerende organisatie.

Als voorbeeld: eerste-orde-veranderopgaven vergen vaak een kleinere bestuurlijke component. Het zal dan veelal voldoende zijn om het hoger management in de bestuurlijke omgeving te adresseren. Significante veranderingen die tot stand moeten komen in interactie met de directe omgeving en afstemming met andere partners, belanghebbenden en direct betrokkenen vragen meer om bestuurlijke aansturing van het tweede-orde-veranderproces.

Bij elk van de twee leerstrategieën maakt de klassieke leerliteratuur dan weer onderscheid in vier leerstappen, te weten ervaren, interpretatie, integratie en institutionalisatie.[6]



Figuur 1: De klassieke leercirkel van Kolb[7]

- Concrete ervaring als startpunt

Concrete ervaring

De literatuur gaat uit van het ervaren van een probleem als eerste stap in het leerproces. Wanneer een individuele actor, met invloed of (doorzettings)macht op basis van ervaring tot een bepaald inzicht komt, kan het zijn dat hij de rest van de organisatie daarin mee wil krijgen. In het geval van informatieveiligheid kunnen bestuurders in deze eerste stap bewust worden gemaakt van het belang ervan. Wanneer het over leren in de eerste orde gaat, zal dit niet tot nauwelijks nodig zijn. Pas als ook echt de structuur van en de denkpatronen binnen de organisatie moeten worden aangepast, moet van buitenaf worden geïnvesteerd in het krijgen van ervaring. Dit kan op individueel niveau bijvoorbeeld worden gedaan door het organiseren van serious games of peergroepen van elkaar te laten leren. Geen betere ervaring echter dan de eigen ervaring met echte crises.

De zegening van crises

Klassiek is het gezegde binnen de wereld van waterschappen: 'geef ons heden ons dagelijks brood en zo nu en dan een watersnood'. Concrete ervaringen als die van de watersnoodramp in 1953 of het bewust breed uitgesponnen gevaar van het hoge water in 1995 zijn de beste aanleiding voor bestuurlijk leren.

6 Lawrence, T., Mauws, M., Dyck, B., & Kleysen, R. (2005). The politics of organizational learning. In Academy of Management Review. 30(1), p. 180-191.
7 Kolb, D., (1981). Learning styles and disciplinary differences. In A. Chickering. The Modern Ame-rican College (pp. 232-255). San Francisco: Jossey-Bass Inc.

Op institutioneel niveau helpen hier verplichting tot audits en rapportage die dwingen tot confrontatie met de werkelijkheid.

- Interpretatie: nadenken over onze ervaringen

Ervaring geeft aanleiding tot reflectie, dat wil zeggen het nadenken over wat er is waargenomen en wat er moet gebeuren. Dit is de fase van interpretatie waarin de oordeelsvorming plaats vindt volgens Crossan e.a. (1999)[8]: 'Het interpreteren is het uitleggen, door woorden en/of acties, van een inzicht of een idee aan zichzelf of anderen.' In de praktijk vindt dit plaats door conversaties en dialogen. Wat bij een individu begint, belandt dan beoogd uiteindelijk binnen een groter geheel. Net zoals in de leerstap intuïtie bestaat ook hier verschil tussen eerste- en tweede-orde-leren. Wanneer het niet nodig is de organisatie grondig te vernieuwen, zal het aandragen van kennis voor de interpretatie al gauw voldoende zijn. Indien eerst ook begrip en bewustzijn moet worden aangebracht, zijn interactieve sessies als workshops, debatten en discussies echter een veel betere manier om het gewenste doel te bereiken. Interpretatie wordt gefaciliteerd door onafhankelijke experts die individuen behulpzaam kunnen zijn bij de analyse van de ervaring. Op institutioneel niveau kan dan iets als een planbureau of rijkscommissaris daarbij behulpzaam zijn.

Integratie

- Integratie: bedenken van oplossingen

Bewust zijn van en kennis hebben over problemen is evident niet voldoende om ze op te lossen. Het stadium van denken gericht op het ontwikkelen van een antwoord of een plan om het probleem op te lossen heet de integratiefase. Om dat te bewerkstelligen gaat het om het bedenken van alternatieve oplossingen en het maken van keuzes. Kennis wordt omgezet in handelingen, instructies en opdrachten. Het integreren gaat over het ontwikkelen van een gezamenlijk, gemeenschappelijk begrip tussen individuen. Alternatieve oplossingen die worden bedacht, worden geconfronteerd met bestaande kennis (geabstraheerde conclusies uit eerdere ervaringen). Uiteindelijk ligt de focus op het creëren van nieuwe situaties en coherente en gezamenlijke acties, bijvoorbeeld uitgevoerd door de individuen in de organisatie. Bij het bedenken ontstaan nieuwe ideeën, concepten en plannen, die verandering moeten brengen in de bestaande situatie. Dit zal over het algemeen gemakkelijker gaan in het eerste-orde-leren dan in het tweede-orde-leren. Waar andere actoren binnen de organisatie bij de simpelste variant met workshops en discussies kunnen worden geactiveerd, zal bij het tweede-orde-leren dieper op de aard van de organisatie moeten worden ingegaan. Ook in deze stap geldt dat integratie wordt gefaciliteerd door onafhankelijke experts die individuen behulpzaam kunnen zijn bij het bedenken van oplossingen. Op institutioneel niveau kan dan iets als een planbureau of rijkscommissaris daarbij behulpzaam zijn.

Maar pas op voor de woekerende professional

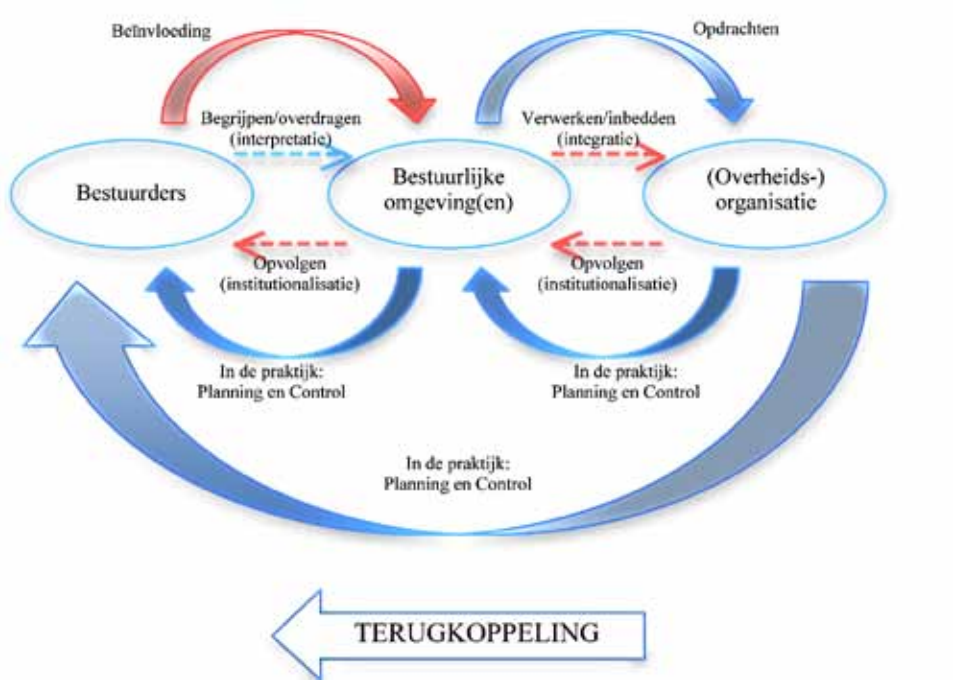
De wet van de woekerend professionaliteit wijst erop dat professionals hun werk altijd beter willen doen, ook al gaat dat ten koste van de effectiviteit en efficiency van het primaire werk van hun organisatie.

- Institutionalisatie: actie ondernemen

Problemen moeten uiteindelijk ook daadwerkelijk worden opgelost. Dit vergt implementatie of institutionalisatie van de bedachte oplossingen. Er is dan een nieuwe

8 Crossan, M., Lane, H. & White, R. (1999). An organizational learning framework: From institution to institution. In Academy of Management Review. 24(3), p.522-537.

situatie gecreëerd waarmee de geconstateerde problemen naar verwachting zijn opgelost. De cirkel is daarmee rond. Zolang er echter geen sprake is van verankering in de organisatie, is de verandering niet gewaarborgd voor de toekomst. Tijdens de institutionalisatie wordt de geleerde kennis verankerd in 'systemen, structuren, procedures en strategie' (Crossan, 1999). Deze vierde stap onderscheidt zich van het individuele of groepsleren doordat er instituties binnen de organisatie ontstaan die uiteindelijk ook voor alle nieuwe leden van de organisatie van toepassing zijn ook al hebben ze het leerproces niet doorlopen. Indien individuen vervolgens binnen die organisatie, vanuit hun ervaring van problemen, tot nieuwe ideeën of gedachten komen, begint de weergegeven leercirkel eigenlijk weer van voren af aan.



Figuur 2: Een theoretisch model dat leren in het openbaar bestuur beschrijft (merk op dat het model nadrukkelijk in beeld brengt dat de relatie in de praktijk tussen bestuurder en topambtenaren er een is van beïnvloeding niet van commanderen).

Theoretisch is dus niet zo ingewikkeld om te leren over informatieveiligheid: bestuurders hebben met DigiNotar en Lektober wel ervaren wat de problemen zijn, zij en hun bestuurlijke omgeving willen daarom graag geholpen worden bij de interpretatie ervan. Je zou zeggen dat de Taskforce BID weet wat haar te doen staat: ondersteun bij de interpretatie en integratie richting de organisatie en faciliteer bij de institutionalisatie.[9]

Wel, ik benoemde al dat bestuurders die ik spreek meestal nog weinig concrete ervaring hebben en daarmee niet erg genegen zijn om hard te sturen op betere informatieveiligheid binnen hun organisatie. Het kan dan ook niet verrassen dat informatieveiligheidsprofessionals nog weinig enthousiast zijn over de werkelijk gemaakt stappen ter verbetering van de informatieveiligheid. De werkelijkheid verschilt blijkbaar nogal van wat de theorie suggereert.

9 Theoretisch gesproken worden specifiek voor gemeenten ook die twee laatste stappen al deels geregeld. Immers het Kwaliteitsinstituut Nederlandse Gemeenten (KING) heeft een Informatiebeveiligingsdienst (IBD) opgericht dat als drie 'concrete doelen' heeft benoemd 'kennisontwikkeling, kennisdeling en kennisvermeerdering'. De IBD richt zich echter primair op een andere doelgroep: (ICT-) professionals. Het spreekt voor zich dat het belangrijk is om de inspanningen van de Taskforce BID en de IBD goed op elkaar te laten aansluiten.

3. De harde werkelijkheid van bestuurlijke (non-)keuzes

In de harde werkelijk moeten bestuurders altijd prioriteren. En dat is lastig. Het is derhalve aantrekkelijk om vooral symbolisch te veranderen en te leren: vele auteurs hebben al gewezen op de neiging van beleidsmakers om zich liever te concentreren op de verkoopbaarheid van beleid dan op de weerbarstige werkelijkheid.

De Amerikaanse politicoloog Edelman geldt als de grondlegger van de kritische studie naar het gebruik van symboliek door politici. In 1964 al betoogt hij dat de materie die aan politieke besluitvorming onderhevig is soms te ingewikkeld is om door betrokken partijen volledig begrepen te worden of door betrokkenen als te confronterend jegens de eigen overtuigingen wordt ervaren. In die gevallen wordt de discussie middels symbolen gevoerd die als metaforen fungeren. Hij noemt dan als voorbeelden ingewikkelde discussies over macro-economisch beleid; wie begrijpt nu werkelijk de economische pro's en contra's van de vrijemarkteconomie versus allerhande protectionistische maatregelen? Onder de betrokkenen die symbolische strohalmen omarmen zijn ook de bestuurders zelf die de materie eigenlijk niet begrijpen Edelman had het zomaar over informatieveiligheid kunnen hebben.

In Nederland zijn Ringeling, Frissen en Noordergraaf vertegenwoordigers van de stroming die met dergelijk begrip het ge- en misbruik van symboliek beschouwt.

Ringeling wijst erop dat het bij beleid veel meer gaat om de toekenning van betekenis aan begrippen en verschijnselen dan om te onderzoeken feiten. Noordergraaf heeft daar begrip voor op een Edelmaniaanse wijze:

> *Wanneer issues technisch en ethisch complex zijn, rest er weinig meer dan symboolpolitiek. Dan wordt de indruk gewekt dat 'eraan gewerkt wordt' en dat 'maatregelen worden genomen', teneinde burgers en bedrijven het gevoel te geven dat het probleem serieus en de oplossing nabij is. De aanpak van het WAO-vraagstuk in de afgelopen jaren is daar een goed voorbeeld van. Dat betekent niet dat er helemaal niets gebeurt. Door de symbolische aandacht kunnen betrokkenen zich bewust worden van het feit dat 'het zo niet langer kan'. Naarmate er meer incidenten plaatsvinden, zoals in de landbouw, of er zorgwekkender cijfers, zoals bij de WAO of tijdens Parlementaire Enquêtes, naar buiten komen, is de kans op 'doorbraken' groter. Het blijft dan de vraag of de bereikte doorbraak tot daadwerkelijke 'oplossingen' leidt, want 'wicked issues' laten zich eigenlijk nooit echt oplossen. En als er 'oplossingen' zijn, dan zijn ze instabiel en tijdelijk.*[12]

Frissen stelt dat de overheid zich in haar beleidsvorming bedient van taboes, metaforen en mythen en dat zij bol staat van de retoriek en rituele uitspraken.[13]

10 M. Edelman 1964.
11 Ringeling 1993, p. 249.
12 Noordegraaf 2002.
13 Geciteerd in Boutellier 2003 , p. 221

Maar de crisis in betekenisgeving en zingeving uit zich ook geheel contrair. Vaak zien we dat de gevoelde noodzaak tot transformatie tot uiting komt in een repertoire van beheersing en controle. Van de antropologie weten we dat een samenleving mythes kent en dat deze van tijd tot tijd door rituelen bevestiging moeten krijgen. Als een samenleving cultureel in verwarring, of sterker nog in crisis is, dan zien we dat mythes aan betekenis verliezen en dat in reactie daarop de rituelen intensiveren. Naarmate de overtuiging dat het opperwezen de regen zendt sterker ondermijnd raakt, neemt het aantal regendansen toe. Naarmate het politieke primaat meer wordt gerelativeerd, neemt de roep om het herstel ervan toe. Naarmate we beter beseffen dat de samenleving complexer wordt en het beleid zijn greep op de samenleving verliest, introduceren we VBTB en andere 'planning en control' rituelen. De semantiek is veelzeggend. We spreken van afrekenen en introduceren daarmee een begrip uit maffia-kringen waar het een liquidatie betekent. We koesteren transparantie en oogsten formulieren en bureaucratie.[14]

Juist na incidenten wordt die neiging tot symbolisch leren verstrekt door de risico-regelreflex: er moet meteen na een incident gehandeld worden om de maatschappij (feitelijk media en volksvertegenwoordiging) gerust te stellen.[15]

Geschiedenis van een taskforce

De geschiedenis van een Taskforce als illustratie

Nadat in 2005 onderzocht was dat de voorbereiding van Nederland op de gevolgen van overstromingen zwak was, werd besloten tot het instellen van de Taskforce Management Overstromingen. Deze Taskforce is met enthousiasme, maar met een beperkte analyse van haar takenpakket aan de gang gegaan. Startpunt was het creëren van bestuurlijke bewustwording door onder andere bestuurlijke bijeenkomsten en het maken van simulaties van de effecten van overstromingen.[16] De opbrengst van deze activiteit leek geslaagd in de zin dat bestuurders vaak zeer onder de indruk waren van de effecten van overstromingen die zij niet eerder zo onderkend hadden. Het zetten van een volgende stap bleek echter lastig: het treffen van werkelijk effectieve maatregelen om de enorme materiële schade te voorkomen was zeer, zeer kostbaar en voor een groot deel de discretie van externe partijen. Een complicerende factor was verder dat de verantwoordelijk staatssecretaris om politieke redenen niet kon meegaan met het bevorderen van de zelfredzaamheid van burgers, die noodzakelijk is om mensenlevens effectief te redden; in haar beleving was het aan de overheid om voor veiligheid van haar burgers zorg te dragen. Er was met andere woorden niet tijdig onderkend dat voor het slagen van het project essentieel tweede-orde-veranderingen moesten worden doorgevoerd, zoals verandering van de bouwwijze van vitale infrastructuur in Nederland en een paradigmashift van de rampenbestrijding waarbij zelfredzaamheid de basis zou moeten worden. Omdat geen draagvlak was bij de opdrachtgevers op rijksniveau voor deze tweede-orde-veranderingen had de Taskforce een onmogelijke opdracht om deze wel elders binnen het

14 Frissen in zijn afscheidsrede voor Roel in 't Veld als decaan van de NSOB (www.nsob.nl).
15 Van Tol, Helsloot en Meertens, Veiligheid boven alles? Beschouwingen over de risico-regelreflex, Boom Juridische uitgevers, 2011.
16 Kabinetsreactie Taskforce Management Overstromingen, 3 juni 2009.

openbaar bestuur te bewerkstelligen. Uiteindelijk werd halverwege de looptijd van de Taskforce impliciet besloten tot het bijstellen van de doelstelling; het eindresultaat was niet meer een betere voorbereiding, maar het opleveren van overheidsplannen en een eindoefening passend bij de bestaande rampenbestrijdingsorgansatie. Het eindresultaat was met andere woorden teruggebracht tot een eerste-orde-veranderopgave. De plannen en de eindoefening zijn opgeleverd, maar tot een werkelijke verbetering van de voorbereiding op overstromingen heeft de Taskforce niet kunnen bijdragen. Het tweede-orde-niveau van veranderen is niet bereikt, omdat de direct betrokken organisaties weliswaar meer inzicht hebben gekregen in de overstromingsrisico's en maatregelen, maar deze kennis en ervaring niet hebben verwerkt in een nieuwe aanpak en werkwijze. Na de Taskforce zijn deze organisaties weer overgegaan tot de gebruikelijke 'orde van de dag', ofwel de werkwijze die voor deze Taskforce van toepassing was.

Kijkend naar eerdere opgaven gericht op bestuurlijk ervaringsleren is het grote gevaar dat bewuste besluitvorming over de verbetering van de informatieveiligheid vervalt tot het snel en symbolisch wegzetten van verbetertrajecten op ambtelijk niveau. De nadrukkelijke opdracht die de Minister aan de Taskforce BID heeft meegegeven om informatieveiligheid bestuurlijk op de agenda te brengen en daar te behouden is daarmee een lastige.[17]

4. De agenda voor een beter leervermogen op het gebied van informatieveiligheid

Het bovenstaande maakt duidelijk dat een agenda voor een beter leervermogen tenminste twee hoofdstappen kent:

Niets zal er werkelijk gebeuren zolang bestuurders en hun omgeving niet werkelijk het risico van informatieonveiligheid inzien.

Over de relatie tussen bestuurlijk en ambtelijk leren

De Taskforce gaat uit van de gedachte dat het creëren van draagvlak voor nieuwe kennis bij bestuurders essentieel is om de rest van de organisatie mee te krijgen in de gewenste richting. Dit idee wordt onderstreept door bestuurskundig onderzoek van Eva M. Witesman en Charles R. Wise (2012).[18] Trainingen op het gebied van democratische processen, zo blijkt uit de daarop gerichte studie, hebben pas echt effect en rendement als bestuurders dit proces ondersteunen en medewerkers (lees: ambtenaren) voor die trainingen motiveren. Overigens heeft het niet alleen met motivatie te maken. Ook geld speelt hierin een rol. Het zijn, zo bleek al uit onderzoek van Kettl et al (1996)[19] en Wise et al (2007)[20], de bestuurders in het openbaar bestuur die verantwoordelijk zijn voor het

17 Ook omdat de brief van de minister veel geruststellende technische maatregelen belooft.
18 Witesman, E., Wise, C. (2012). The Reformer's Spirit: How Public Administration Fuel Training in the Skills of Good Governance. In Public Administration Review 72(5). pp. 710-720.
19 Kettl, D., Ingraham, P., Sanders, R. & Horner, C. (1996). Civil Service Reform: Building a Government That Works. Washington DC: Brookings Institution Press.
20 Wise, C. et al (2007). Strategic Assessment of the Present State of Public Administration Education and Training in Ukraine and Prospects for Launching a Capacity Building Institution for Public Offi-cials (http.glennschool.osu.edu/faculty/brown/home/FinalReport.pdf (accessed June 15, 2012).

maken van belangrijke beslissingen over 'trainingsprioriteiten' die gefinancierd, geïnitieerd of aangemoedigd worden. Zonder de trainingen of opleidingen van medewerkers (individueel leren) is echte verandering niet haalbaar, zo schrijven Witesman en Wise in hun artikel (pagina 711): 'Training van ambtenaren is een noodzakelijke voorwaarde om een effectieve overheidshervorming te bewerkstelligen'.

Het onuitgesproken standpunt 'Het is hier veilig, mij kan niets gebeuren, ik voldoe aan het veiligheidsvoorschriften' is één van de grootste valkuilen voor bestuurlijke besluitvorming over veiligheidsbeleid. Het leidt enerzijds tot disproportionele eerste-orde-verandering (nieuw veiligheidsbeleid kost meestal niet ontzettend veel meer maar levert meestal helemaal niets op zodat de balans negatief is) en anderzijds tot het vermijden van werkelijke transparante keuzes die meer veiligheid tegen verrassend vaak minder kosten opleveren.

Veiligheidsleren

In algemene zin is uniek voor 'veiligheidsleren' dat de dagelijkse werkpraktijk geen of niet voldoende prikkels bevat die de noodzaak van het tweede-orde-leren duidelijk maken. Veiligheidsrisico's zijn immers verborgen. Voorschriften leveren wel een bijdrage aan de veiligheid, maar kunnen (zeker op de langere termijn) niet waarborgen dat er geen onveilige situaties ontstaan. Veiligheid start met het te onderhouden besef welke risico's en gevaren er zijn, het zien en onderkennen hoe gevaarlijke situaties kunnen ontstaan, welke omstandigheden niet gewenste ontwikkelingen beïnvloeden en hoe moet worden opgetreden om de gewenste condities te kunnen beheersen. Veiligheid impliceert daarmee kennis en inzicht in de aanwezige omstandigheden en het vermogen om zelfstandig en adequaat in deze omgeving te kunnen ingrijpen of dat bewust en transparant niet te doen.

Diegenen die informatieveiligheid een warm hart toedragen moeten derhalve eerst echt duidelijk maken wat er nu mis kan gaan. En wel op een wijze die burgers, buitenlui en bestuurders begrijpen.

- Ten tweede zal de integratiestap concreet in beeld moeten worden gebracht. Als er geen realistische oplossing voorhanden is of lijkt, zal het openbaar bestuur snel vluchten in symbolisch handelen.

Het voorbeeld van de Taskforce Management Overstromingen hierboven laat zien dat zelfs als bestuurders overtuigd raken van de impact van een veiligheidsrisico zij wanneer er geen realistische oplossing voorhanden is toch weer terugvallen op symbolisch leren. Het is terecht dat bestuurders de afweging maken dat er grenzen aan de voorbereiding op zeldzame incidenten is. Idealiter wordt dat besluit echter wel transparant genomen zodat de maatschappij zelf kan kiezen voor eigen voorbereiding.

De opgave (voor bijvoorbeeld de Taskforce BID) is daarmee om de discussie over de voorbereiding op informatie-incidenten zo te voeren dat er ruimte is voor een bewuste en transparante afweging op welke punten er wel en niet door het openbaar bestuur verbeterinitiatieven genomen worden.

Opgave: Discussie voeren!

TASKFORCE

Bestuur & Informatieveiligheid Dienstverlening

www.taskforcebid.nl

Vragen?
De Taskforce BID beantwoordt deze graag
via info@taskforcebid.nl