GEDRAG

Verleiden tot samenwerking: interoperabiliteit en human factors

In het veiligheidsdomein is een gezamenlijk beeld van de situatie essentieel voor de besluitvorming. Dit kan alleen bereikt worden als partijen informatie met elkaar delen, oftewel interoperabel zijn. De welwillendheid tot delen van informatie is naast een technische, ook een organisatorische (beleid, vertrouwen) en juridische (privacy, vertrouwelijkheid) uitdaging.Een netcentrische werkwijze lijkt een belangrijke stap om organisaties bereid te krijgen om informatie te delen. Human Factors slaat hierbij een brug tussen technologie enerzijds en stakeholders/ gebruikers anderzijds. Een user-centric ontwerpproces is een beproefde benadering voor het ontwikkelen van platformen voor informatie-uitwisseling. Innovatieve technologie kan, mits afgestemd, eindgebruikers verleiden tot delen van informatie.

Michel Varkevisser en Wouter Hoogstra

Noodzaak tot samenwerken

In de informatieketens van organisaties die zich bezighouden met veiligheid, zoals politie, brandweer en defensie, draait alles om het op de juiste plek krijgen van de juiste informatie, bij de juiste persoon en op het juiste moment. Iedere stakeholder vervult een eigen rol en draagt daarom een stukje van de informatiepuzzel bij. Het is van belang dat die informatie vindbaar, toegankelijk, interpreteerbaar en deelbaar is. Dit blijkt heel lastig te zijn. Een complicerende factor in het veiligheidsdomein is dat informatie niet altijd direct voorhanden, vaak tegenstrijdig en van wisselende kwaliteit is of kan zijn. Samenwerken is dus essentieel om fouten te voorkomen. Partijen kunnen het zich simpelweg niet veroorloven informatie voor zichzelf te houden die van belang zou kunnen zijn voor een andere partij. Toch zien we in de praktijk dat samenwerking soms uiterst moeizaam verloopt. Gevolgen zijn onder andere miscommunicatie en een onvoldoende overzicht van de situatie.

Hobbels

In dit artikel bespreken we drie hindernissen voor efficiënt en effectief informatiedelen, te weten organisatie, privacy en security en technologie. Deze hobbels kunnen worden voorkomen, hetgeen besproken en geïllustreerd wordt met een use case. Human factors speelt hierin een essentiële rol.

Organisatie

Al meer dan vijftien jaar wordt er aan digitale transformatie en netcentrische oplossingen gewerkt. Toch slagen overheidsorganisaties er slechts moeizaam in om hier kwalitatieve slagen in te maken (zie Buul & Treurniet, 2015). Er zijn hier verschillende oorzaken voor aan te wijzen. We willen ons hier beperken tot drie factoren die we in de praktijk tegenkomen, te weten need to know, silovorming en beheersbaarheid van informatie.

Veel overheidsorganisaties, waaronder de politie, werken van oudsher vanuit een hiërarchische structuur en een ‘need to know’-principe (Scholten & Vlist, 2011). Men richt zich hierbij sterk op de eigen informatie en organisatiestructuur. Men heeft zich verschanst achter dikke virtuele muren. Deze houding staat netcentrisch werken in de weg. Een bijkomend probleem is dat er zich binnen de eigen organisatie een fenomeen voordoet dat ‘silovorming’ heet. Met name in grotere organisaties zijn er in de afgelopen decennia informatiesilo’s ontstaan binnen afdelingen. Afdelingen, zoals binnen grotere gemeenten, opereren autonoom en delen doorgaans weinig informatie met elkaar. Tevens is de beheersbaarheid van de informatie problematisch geworden. Door digitale transformatie is er zóveel informatie beschikbaar gekomen, dat werknemers bedolven raken onder informatie. Mentale overbelasting ligt dan op de loer, zéker als het om tijdkritische situaties gaat en de informatie niet adequaat

gemanaged kan worden. De drie genoemde factoren maken het uiterst lastig voor betrokkenen om de juiste informatie te vinden, er toegang toe te krijgen, resultaten inzichtelijk te maken en deze te delen.

Privacy en security

De genoemde 'need to know'-houding zit stevig verankerd in de wetgeving. Het delen en samenvoegen van informatie die tot personen herleidbaar is, roept privacyrechtelijke vragen op. Zowel de huidige Wet bescherming persoonsgegevens (Wbp) als de opvolgende Europese Algemene Verordening Gegevensbescherming zijn gebaseerd op onder meer de volgende beginselen:

- doelbinding (Wbp artikel 9.1): 'Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen';
- dataminimalisatie (Wbp artikel 11.1): 'Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn'.

Beide beginselen staan haaks op een netcentrische werkwijze waar informatie continue verzameld, gecombineerd en gedeeld wordt. Daarnaast weet je in een netcentrische omgeving nooit precies welke informatie met wie op welk moment gedeeld moet worden. Op de een of andere manier zullen privacy en netcentrisch werken toch met elkaar verenigd moeten worden.

Gerelateerd aan bovenstaande zijn er security-aspecten die bij interoperabiliteit een rol spelen. Met name access control – wie heeft toegang tot welke informatie – speelt een rol. We zien enerzijds dat er onduidelijke afspraken gemaakt worden over wie wat op welk moment zou mogen inzien. Hierdoor kan gevoelige informatie bij de verkeerde personen terecht komen. Anderzijds kunnen afspraken te rigide worden, door op casusniveau volledig uit te schrijven welke rollen er bestaan en op welke manier er wat gedeeld mag worden tussen partijen. Beide varianten staan structurele samenwerking in de weg, doordat het woud van afspraken stakeholders afschrikt informatie met elkaar te delen. Dit kan resulteren in een zichzelf voedende terughoudendheid in het informatiedelen.

Technologie

Technologische innovaties op het gebied van interoperabiliteit gaan nogal eens mank. Een belangrijke factor is dat huidige technologieën niet aansluiten op de dagelijkse routines van eindgebruikers. Hier ligt vaak een 'technopush' aan ten grondslag; technologie wordt opgedrongen aan eindgebruikers. Tevens blijken systemen van verschillende organisaties technisch veelal incompatibel te zijn en lukt het daarom niet om de juiste personen (dynamisch) met elkaar te koppelen. Daarnaast worden op human-machine interfaces verschillende termen, kleurstellingen

Afbeelding 1. Interoperabiliteit is in essentie het verbinden van verschillende partijen om informatiedelen en samenwerking mogelijk te maken.

en symbolen gebruikt. Dit leidt tot verwarring en fouten. Ten slotte geven huidige oplossingen doorgaans te weinig overzicht, te weinig middelen om informatie eenvoudig te delen, onvoldoende beslisondersteuning en helpen niet in fouten te vermijden. Met als gevolg een hoop frustratie en een afbreuk aan vertrouwen tussen partijen, hetgeen miscommunicatie en fouten in de hand werkt.

We zien bij overheidsinstanties en defensie ook vaak bottom-up gedreven oplossingen van knelpunten. Men ondervindt een specifiek probleem binnen de afdeling en probeert hier een technisch antwoord op te vinden. Er is dan weinig sturing van bovenaf. Zo ontstaat een wildgroei aan al dan niet aan elkaar geknoopte applicaties en informatieportalen. Op een gegeven moment bezwijken die (veelal tijdelijke en specifieke) oplossingen onder hun eigen gewicht. Met als gevolg dat men steeds argwanender ten opzichte van digitale middelen wordt.

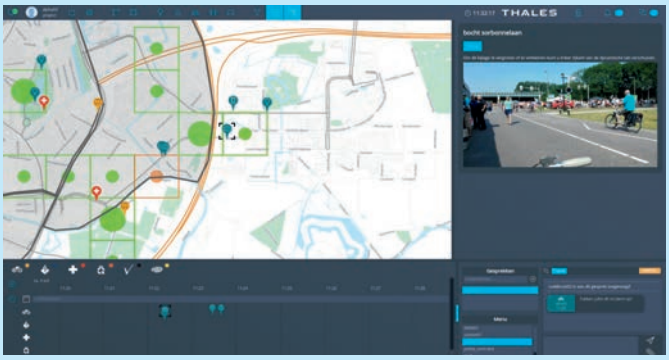
Mogelijke oplossingen

Vanuit een aantal projecten op het gebied van interoperabiliteit, zowel in het civiele als in het militaire domein, hebben we oplossingen proberen te bedenken voor eerder genoemde hobbels. Zie de casus (kader) van de Grand Départ (Tour de France) in Utrecht ter illustratie van een netcentrische oplossing. Voor dat project hebben we een informatie-uitwisselingsplatform ontwikkeld ter ondersteuning van de veiligheidsketen gedurende de Grand Départ.
Bij deelnemende organisaties uit de casus (zie kader) hebben we gezien dat een informatie-uitwisselingsplatform moet aansluiten op het dagelijkse werkproces. Een typisch human factors ontwikkelproces met de eindgebruiker als uitgangspunt, ook wel user-centric design genoemd (Abras, 2004), biedt hiervoor volop mogelijkheden. Een operationele analyse met alle betrokken partijen helpt om zicht te krijgen op de belangrijkste knelpunten. Wanneer stakeholders, gebruikers en ontwikkelaars

met ondersteuning van human factors-specialisten de huidige operaties onder de loep nemen, kan vastgesteld worden wat de knelpunten zijn en een verkenning gemaakt worden met betrekking tot de oplossingsrichting. In het daaropvolgende ontwerpproces kunnen stakeholders en gebruikers input leveren op de ontwerpen, zodat in een iteratief proces de concepten steeds meer toegespitst worden op de werkprocessen van de gebruiker. Door middel van gebruikersparticipatie tijdens het ontwerpproces wordt vertrouwen gecreëerd in elkaar en in de technologie. Men voelt zich meer verbonden met de oplossing, omdat men de eigen feedback verwerkt ziet in het ontwerp. Vertrouwen is sleutelfactor als het op samenwerken aankomt (Veiligheidsberaad IFV, 2013).

Casus Grand Départ

Voor de Grand Départ heeft Thales het Secure Shared Information Management Platform (SSIMP) ingezet dat beslisondersteuning moest geven op veiligheidsaspecten voor de betrokken organisaties. Dit zijn de gemeentelijke projectorganisatie, Politie Midden-Nederland, Veiligheidsregio Utrecht, etc. Primair hebben we ons gericht op een beveiligd, gebruikersvriendelijk platform, dat zowel horizontaal (tussen organisaties) als verticaal (binnen organisatie) informatie-uitwisseling faciliteert. Men moest in één oogopslag kunnen zien hoe de actuele situatie in de stad was. Het platform werd uitgerold in mobiele en desktopvorm, waarmee stakeholders op verschillende plekken in de stad informatie met elkaar konden delen. Ze hadden een aantal functionaliteiten tot hun beschikking, waaronder een geografische kaart en een taaktijdslijn (zie afbeelding 2). Men kon objecten op de kaart zetten en annoteren, en op de tijdslijn was te zien wie deze informatie wanneer had toegevoegd. Doordat er uniformiteit in symbolen en kleurstelling bestond, wist men direct wat de toegevoegde informatie voorstelde. Tevens kon ieder object verrijkt worden met actuele informatie, zodat er een gezamenlijk minidossier rond dat object gecreëerd werd. Verder was er de mogelijkheid met elkaar te chatten door een topic aan te maken en stakeholders in het netwerk uit te nodigen. Het gehele platform had een onderliggend security- en privacy-mechanisme waar op basis van rollen bepaalde rechten werden toegekend tot inzage van informatie. Zo mocht de politie alle informatie van het Rode Kruis zien, maar niet omgekeerd. Het platform hielp de projectorganisatie enorm in het bewaren van het overzicht. Momenteel wordt de oplossing in soortgelijke projecten ingezet.



Afbeelding 2. Voorbeeld van SSIMP (desktopversie) tijdens de Grand Départ waarop men informatie op de kaart kon toevoegen en inzien. Tevens was dit weergegeven op de tijdslijn. Rechtsboven konden details van het geselecteerde object worden ingezien en geüpdatet. Rechtsonder had men de mogelijkheid een chat met geselecteerde stakeholders te starten.

Een transparant, netcentrisch werkproces, waar iedere betrokkene in de informatieketen weet wat er van hem/haar verwacht wordt (met bijkomende rechten/plichten), leidt doorgaans tot meer vertrouwen. Ten slotte zullen mensen training moeten krijgen in netcentrisch werken, zodat men leert om van een 'need to know'- naar een 'need to share'-houding te gaan (Best, 2011). Genoemde zaken brengen veranderingen met zich in de organisatiestructuur, waar niet alleen juridisch toegestaan wordt om informatie te delen, maar waar structurele informatie-uitwisseling verankerd ligt in de organisatiecultuur. Met name waar netcentrische oplossingen raken aan internet-of-things-benaderingen liggen er nog veel mogelijkheden die in kaart moeten worden gebracht.

Eindgebruikers van een platform zouden zo min mogelijk geconfronteerd moeten worden met privacy- en security-vraagstukken. Ze zijn met de operationele taakuitvoer bezig en moeten minimaal belast worden met dergelijke zaken. Afspraken omtrent privacy en security dienen op hoger niveau met elkaar gemaakt te worden en vertaald naar beleid. In onze oplossing zijn deze 'policies' op de achtergrond actief en hinderen de eindgebruiker niet bij gebruik van het systeem. Men hoeft dus niet meer bij ieder gedeeld object continue na te denken of de informatie überhaupt gedeeld had mogen worden en wie dat dan had mogen zien.

Standaardisatie is voor interoperabiliteit noodzakelijk, waarbij met name open standaarden kansen bieden (Zwienink & Wisse, 2008). Open standaarden bieden de mogelijkheid om tools van verschillende organisaties eenvoudig met elkaar te koppelen. Ook kunnen rapid-prototyping oplossingen, zoals open webstandaarden, vroegtijdig inzichten geven in het uiteindelijke product. Verder is het van belang een 'common language', oftewel een uniforme semantiek aan te houden (Folmer & Verhoosel, 2011). Denk daarbij aan operationele terminologie, symbolen, kleurstelling, et cetera. Een top-down oplossing kan standaardisatie vereenvoudigen, aangezien er vanuit een bepaalde visie gedacht en ontwikkeld wordt. Een combinatie van top-down conceptualisatie en bottom-up gedreven ontwikkeling zal nog nader bekeken moeten worden.

Een innovatief informatie-uitwisselingsplatform dat voldoende is ingebed in de organisatie en stakeholders voldoende ondersteunt, kan mensen prikkelen om informatie met elkaar te delen. Zonder human factors-kennis is zo'n oplossing gedoemd te mislukken. De mens moet centraal staan in de ontwikkeling, niet de technologie. Een human factors-specialist is bij uitstek de persoon die een brug kan slaan tussen technologie en eindgebruiker. Er zal nog nader onderzocht moeten worden hoe een user-centric ontwerpproces naadloos kan aansluiten op (agile/lean1) ontwikkelprocessen.

1 Ontwikkelmethode met de filosofie van 'see-feel-change'. In de ICT staat het voor softwareontwikkeling in korte overzichtelijke perioden (sprints) van vaak niet meer dan een maand.

Een user-centric ontwikkelmethode, waarin zowel privacy als security in het ontwerp besloten ligt, verhoogt de kans op een optimale oplossing voor netcentrisch werken en informatiedelen. Met zo'n oplossing worden de stakeholders geprikkeld om in wisselende coalities en netwerken over sectoren en domeinen heen informatie uit te wisselen. Voorwaarde is en blijft dat men vertrouwen in elkaar en in de techniek heeft. Als eindgebruikers stapje voor stapje in dit proces meegenomen worden, kunnen ze daadwerkelijk verleid worden om middels technologische innovaties structureel met elkaar te gaan samenwerken.

Referenties

Abras, C., Maloney-Krichmar, D., an Preece, J. (2004) User-Centered Design. In Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications.

Best Jr., R.A. (2011). Intelligence Information: Need-to-Know vs. Need-to-Share. CRS Report for Congress. Congressional Research Service, Washington, D.C.

Buul, van, K., and Treurniet, W. (2015). De staat van netcentrisch werken - Update 2015. Rapport TNO R10627, Den Haag.

Folmer, E., and Verhoosel, J. (2011). State of the Art on Semantic IS Standardization, Interoperability and Quality. Gildeprint Drukkerijen, Enschede. Scholten, H. J., and Vlist, v.d., M. (2011). De inrichting van crisisbeheersing, de relatie tussen besluitvorming en informatievoorziening. Research Memorandum, 11.

Veiligheidsberaad IFV (2013). Netcentrisch Werken: nu en in de toekomst. Rapport programma Netcentrisch Werken. Instituut Fysieke Veiligheid, Zoetermeer.

Wolbers, J., Boersma, F.K., and Heer, de, J. (2012). Netcentrisch werken in ontwikkeling. Een cultuuronderzoek naar multidisciplinaire samenwerking en gezamenlijke operationele beelden in de Veiligheidsregio's. TNO en VU University, Amsterdam.

Zwienink, S., and Wisse, P.E. (2008). Eerlijk zullen we alles delen: verkenningen naar interoperabiliteit. Rapport Forum Standaardisatie, Den Haag.

Over de auteurs

Dr. M. Varkevisser, Engineering Psychologist, Thales Research & Technology, Thales NL, Delft
Michel.Varkevisser@nl.thalesgroup.com

Ir. W. Hoogstra, Industrieel Ontwerper, Thales Research & Technology, Thales NL, Delft