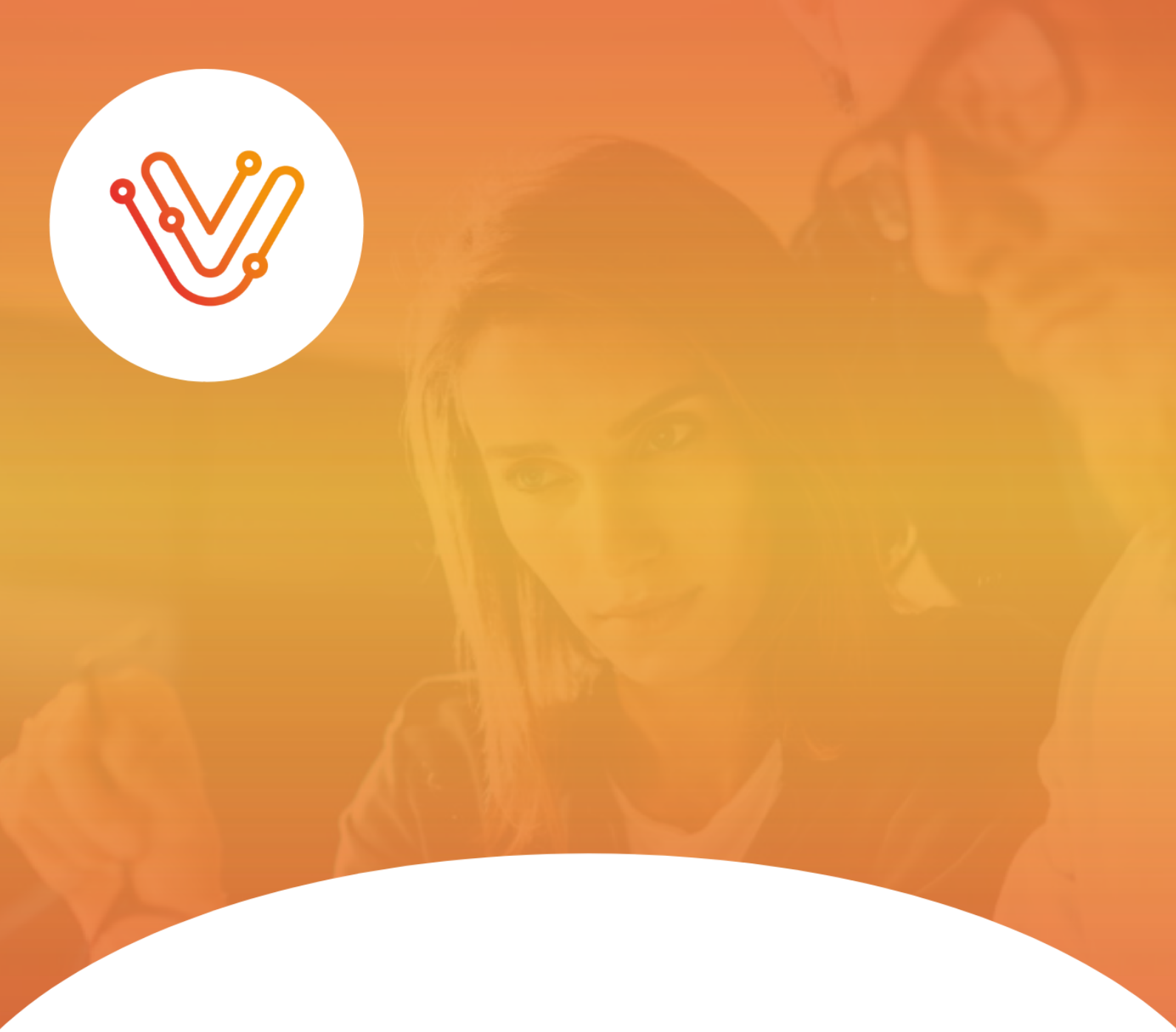

IJmond Werkt! gehackt

In opdracht van:

Veiligheidsbureau Kennemerland
Gemeente Heemskerk
Gemeente Uitgeest
Gemeente Beverwijk
Gemeente Velsen
IJmond Werkt!

VEILIGHEIDSPROF

Evaluatierapport IJmond Werkt! gehackt

Datum : 01-03-2022

Auteurs : Peter Lokker en Sjoerd Nugteren, Veiligheidsprof

Inhoudsopgave

Samenvatting

Als gevolg van een ransomware-aanval bij het leerbedrijf IJmond Werkt! heeft er gedurende een periode van september tot oktober 2021 een crisisteam gefunctioneerd. Dit crisisteam is opgeschaald naar behoefte, waarbij er niet conform de reguliere procedures van rampenbestrijding en crisismanagement is opgeschaald. De vier betrokken gemeenten bij IJmond Werkt! en de directie van het bedrijf zijn bij het bestrijden van de gevolgen van het incident ondersteund door functionarissen vanuit de Veiligheidsregio Kennemerland. Deze evaluatie heeft tot doel gehad dit functioneren te evalueren. Enerzijds omdat het hierbij ging om een bijzondere samenwerking tussen de getroffen organisatie, gemeenten en de Veiligheidsregio. Anderzijds om de casus een cyberincident betreft; een type incident wat steeds vaker voorkomt en waar de regulier opschalingsprocedures minder toepasbaar op zijn. Hierbij zijn vijf thema's behandeld aan de hand van een enquête en interviews met betrokken personen: (1) Melding en Alarmering, (2) Op- en afschaling, (3) Leiding en Coördinatie, (4) Informatiemanagement, en (5) Crisiscommunicatie.

Uit de evaluatie is gebleken dat de faciliterende rol van de functionarissen vanuit de Veiligheidsregio van meerwaarde is geweest voor het gehele proces. Vooral met betrekking tot de processen omtrent leiding en coördinatie en informatiemanagement hebben de ervaring en kennis van deze functionarissen een positief effect gehad op het functioneren en de samenwerking binnen het crisisteam. Daarbij zijn vanuit de vier gemeenten verschillende personen met relevante kennis en expertise die nodig waren voor het bestrijden van het incident toegevoegd aan het crisisteam, zoals FG's, CISO's en communicatieadviseurs. Wat daarnaast opvalt is de inzet die alle betrokkenen hebben getoond en de waardering voor deze inzet die uit de afgenomen enquête en interviews blijkt.
Gedurende het incident is het Regionaal Actiecentrum Communicatie (RAC) en een individuele communicatieadviseur OT gealarmeerd als gevolg van het onverwacht lekken van de gestolen data van IJmond Werkt!. Door verschillende omstandigheden hebben in deze situatie de behoefte om extra capaciteit bij het bestaande crisisteam en de bereidheid om bijstand te verlenen bij het RAC en de communicatieadviseur OT elkaar onvoldoende gevonden.

Informatiemanagement en het netcentrisch werken is in deze crisis opgepakt door functionarissen vanuit de Veiligheidsregio Kennemerland, waarbij zij creatief zijn omgegaan met de beschikbare middelen. Het kostte in beginsel moeite om de feiten te valideren en zo het beeld compleet te maken en alle teamleden van het crisisteam in dezelfde film te plaatsen. De relatief kleine hoeveelheid ervaring met crisismanagement van de meeste teamleden en de wisselende samenstelling binnen het crisisteam kunnen aangewezen worden als redenen hiervoor. Op langere termijn heeft aandacht hiervoor de effectiviteit van en de samenwerking binnen het crisisteam echter goed gedaan.

Het proces crisiscommunicatie nam een belangrijke plek in bij de bestrijding van dit incident. Door middel van een communicatiestrategie en een doelgroepanalyse zijn verschillende doelgroepen op verschillende manieren bereikt, waarbij kennis en middelen vanuit de gemeente, regio en IJmond Werkt! zelf zijn ingezet. Door bewust te kiezen voor de controle te nemen over het brengen van het nieuws van het lekken van de data aan een lokale nieuwszender is de maatschappelijke impact van het incident beperkt gebleven.

Het moment van afschalen van het crisisteam is een onderwerp waarover de meningen van de respondenten van deze evaluatie verdeeld zijn. Deze complexiteit ligt in lijn met een algemeen kenmerk van cyberincidenten; de relatief lange duurloop vergeleken met meer reguliere incidenten. Door deze lange duurloop is het lastig te bepalen wanneer een crisis op zijn eind is. In de casus van het incident bij IJmond Werkt! is er voor gekozen om het crisisteam in acute vorm af te schalen, maar tot op heden vindt er nog steeds samenwerking en coördinatie plaats tussen IJmond Werkt! en de vier deelnemende gemeenten met betrekking tot het informeren van getroffen personen.

Inleiding

1.1 Aanleiding

Op 6 september 2021 is het leerbedrijf IJmond Werkt! slachtoffer geworden van gijzelsoftware. Hackers wisten binnen te dringen in de systemen van het bedrijf en vergrendelden alle bestaande data. Daarnaast werd ook een deel van de data gestolen, en deze werd achttien dagen later online op het 'darkweb' gezet.
IJmond Werkt! is het participatiebedrijf van vier gemeenten (Heemskerk, Uitgeest, Velsen en Beverwijk) verantwoordelijk voor de uitvoering van de Participatiewet. Hierbij gaat het vaak om personen met een bepaalde afstand tot de arbeidsmarkt. Het cyberincident kende verschillende gevolgen en risico's, en om deze te bestrijden werd door het bedrijf en de vier deelnemende gemeenten een crisisteam opgezet, waarbij de Veiligheidsregio Kennemerland op verzoek van de vier gemeenten een faciliterende rol op zich nam.

Het incident kan ten eerste aangemerkt worden als een cyberincident, een type incident dat de laatste jaren steeds vaker voorkomt. Dit soort incidenten zijn anders dan de 'reguliere' incidenten waar Veiligheidsregio's en gemeenten doorgaans mee te maken krijgen, zoals branden, verstoringen van de openbare orde of andere soorten flitsrampen waarbij er indien nodig volgens de GRIP-structuur wordt opgeschaald.
Ten tweede is de aanpak van het cyberincident bij IJmond Werkt! uitzonderlijk te noemen gezien het buiten de reguliere regionale (GRIP-)structuur van rampenbestrijding en crisisbeheersing valt, maar waarbij actoren vanuit die structuur wel betrokken zijn geweest bij de bestrijding van de gevolgen van het incident.

Gezien deze twee redenen is het waardevol om het verloop van de crisis en het functioneren van het crisisteam te evalueren. Het doel van deze evaluatie is om zowel positieve factoren als knelpunten bij de bestrijding van deze crisis aan te wijzen en uit te lichten. Dit rapport sluit af met een aantal aanbevelingen per thema, op basis van uitgelichte knelpunten. Deze aanbevelingen verdienen aandacht, zodat men kan leren van de aanpak van dit incident en men beter voorbereid is op soortgelijke incidenten in de toekomst.

1.2 Methode en aanpak

Inzake deze evaluatie zijn alle betrokken personen bij deze crisis benaderd voor het invullen van een enquête. Hierbij gaat het om personen die minimaal eenmalig hebben plaatsgenomen in het gevormde crisisteam, of extern een positie hadden waardoor hij of zij veelvuldig te maken kreeg met het crisisteam. Daarnaast is er voor gekozen om met een aantal personen een interview te houden om zo aanvullende informatie op te halen. De keuze voor deze personen is gedaan op basis van hun betrokkenheid bij de crisis en in samenspraak met de eerder genoemde opdrachtgevers.

Om tot de gewenste resultaten te komen is voorafgaand aan deze evaluatie een evaluatiekader opgesteld. Binnen dit kader zijn vragen opgesteld aan de hand van vijf thema's te weten:

- Melding & Alarmering
- Op- & Afschaling
- Leiding & Coördinatie
- Informatiemanagement
- Crisiscommunicatie

Deze thema's staan in verhouding tot hoofdprocessen binnen crisismanagement. Ook zijn voor de totstandkoming van het evaluatiekader vragen opgehaald bij de vier gemeenten, Veiligheidsregio Kennemerland en IJmond Werkt!. Deze vragen zijn in sommige gevallen één-op-één overgenomen in het evaluatiekader. Daarnaast zijn extra vragen geformuleerd om zo een compleet mogelijk beeld te krijgen van het verloop van de crisis en aan de hand daarvan kritisch te kijken naar de bestrijding van de crisis en deze te plaatsen in de context van de bovengenoemde vijf thema's.

Het opgestelde evaluatiekader met daarin de opgenomen vragen voor zowel de enquête als de interviews is vooraf ingezien en goedgekeurd door vertegenwoordigers van het Veiligheidsbureau Kennemerland en de eerder vermelde vier gemeenten.

1.3 Leeswijzer voor dit rapport

Dit rapport beschrijft aan de hand van bovengenoemde thema's het feitelijke verloop van de crisis en de acties die zijn ondernomen om de crisis te bestrijden. Daarnaast zet het rapport bevindingen met betrekking tot de bovengenoemde thema's die aan het licht zijn gekomen middels de enquête en de interviews uiteen. Hierbij zijn positieve factoren en knelpunten per thema weergegeven. Het rapport rondt af met een aantal aanbevelingen betreffende deze positieve factoren en knelpunten.

Resultaten

2.1 Melding en alarmering

Beschrijving van gebeurtenissen

IJmond Werkt! merkte op de ochtend van 6 september 2021 dat de bedrijfssystemen niet meer werkten. Na onderzoek van de ICT-afdeling bleken er inbraaksporen aanwezig te zijn. Alle bestaande bestanden waren vergrendeld. Als reactie hierop heeft de directie Fox-IT ingeschakeld om het incident te onderzoeken. Na anderhalve week bleek dat er meer hulp vanuit de deelnemende gemeenten nodig was bij het bestrijden van de gevolgen van de hack. Ook omdat een meer gecoördineerde aanpak van de crisis nodig was. Met dit gegeven is er contact geweest tussen de directie van IJmond Werkt!, het dagelijks bestuur (DB) van IJmond Werkt! bestaande uit wethouders van de deelnemende gemeenten, en de gemeentesecretarissen van deze gemeenten. In samenspraak hebben deze partijen besloten een crisisteam op te zetten. Hierbij stapte de gemeentesecretaris (GS) van de gemeente Heemskerk naar voren om dit crisisteam te gaan leiden, gesteund door het DB. Vanuit dit overleg werd ook besloten om contact op te nemen met de Veiligheidsregio Kennemerland om de nodige kennis en ervaring met betrekking tot crisismanagement binnen het team te halen. Deze noodzaak om extra kennis op dit gebied binnen te halen werd gedeeld binnen het Dagelijks Bestuur en de directie van IJmond Werkt!. Bij de gemeentesecretaris van Heemskerk heeft er geen twijfel bestaan om de hulpvraag bij de Veiligheidsregio neer te leggen, de analyse van de uitdagingen die er op dat moment lagen was duidelijk; hulp was nodig om de gevolgen van het incident goed te beheersen. Daarnaast heeft de directie van IJmond Werkt! in de beginperiode van de crisis contact gehad met de Informatiebeveiligingsdienst (IBD). De IBD heeft IJmond Werkt! geadviseerd om naar de Veiligheidsregio te kijken als mogelijke partner voor ondersteuning. Met betrekking tot de keuze om de Veiligheidsregio Kennemerland te betrekken bij het te vormen crisisteam kan dit advies van de IBD ook aangewezen worden als meespelende factor.

De GS van Heemskerk heeft contact opgenomen met de directeur van de GGD Kennemerland, die de hulpvraag via de directie van de Veiligheidsregio Kennemerland naar verschillende crisisfunctionarissen heeft gebracht. Het contact tussen deze GS en directeur is te verklaren door de persoonlijke relatie die is ontstaan door eerder gedeelde werkzaamheden.

De resultaten van de enquête laten zien dat de alarmering op persoonlijk niveau bij ieder persoon anders is verlopen. Veel is via persoonlijke (informele) lijnen van de vier betrokken gemeentesecretarissen gelopen. De leden van het team die bij aanvang van de bestrijding van de crisis aan tafel zaten waren grotendeels afkomstig uit de interne bestuurlijke organisatie van de gemeente Heemskerk. Later zijn aan dit team bestuurs-, communicatieadviseurs en medewerkers van de andere gemeenten toegevoegd. Hun betrokkenheid is ook gestart via een vraag afkomstig van hun eigen gemeentesecretaris die hen gevraagd heeft aan te sluiten bij het crisisteam.

In een later stadium van de crisis is het Regionaal Actiecentrum Communicatie (RAC) gealarmeerd en opgeschaald. Deze opschaling is via de meldkamer verlopen, waarna verschillende crisisfunctionarissen fysiek opgekomen zijn in Haarlem. Niet het gehele RAC is als groep gealarmeerd. Leden van het RAC zijn als persoon, los van elkaar gealarmeerd via de pager. Daarnaast is een communicatieadviseur OT opgekomen die ook een melding via de pager heeft gekregen.

Positieve factoren

Het besef en de keuze bij IJmond Werkt! om extra hulp in te roepen via de vier gemeenten en de Veiligheidsregio is een goed en moedig besluit geweest. Dankzij de melding die gedaan is bij de gemeenten is er een concrete hulpvraag ontstaan die uitgezet kon worden bij de Veiligheidsregio, die op haar beurt de nodige ervaring op het gebied van crisismanagement kon inbrengen. De daadkracht van de het Dagelijks Bestuur en de gemeentesecretarissen van de vier gemeenten om de juiste personen binnen de gemeenten met de benodigde kennis en ervaring in het team te vragen moet hier ook genoemd worden. Ondanks dat de alarmering niet via een bestaande structuur van alarmering is gegaan, hebben de inspanningen toch geleid tot een goede basis van specifieke kennis die nodig was bij dit incident.

Knelpunten

Met betrekking tot de alarmering van het RAC blijkt dat de melding die verscheen op de pagers van de RAC-functionarissen die op piket stonden niet duidelijk genoeg beschreven was. Als gevolg hiervan wisten de functionarissen die opkwamen niet exact waarvoor zij opkwamen. Bij aankomst op locatie was er bij de opgekomen RAC-functionarissen de nodige verwarring over de alarmering en de noodzaak hiervoor ontstaan. Het feit dat het bij aankomst bleek te gaan om een crisis die al een significante periode liep was ook van invloed op deze verwarring. Dit rapport gaat later verder in op de opschaling van het RAC en op basis van welke behoefte dit heeft plaatsgevonden.

2.2 Opschaling

Beschrijving van gebeurtenissen

Om de crisis te bestrijden zijn als reactie op de hulpvraag vanuit de gemeenten en IJmond Werkt! een operationeel leider en een informatiemanager ingezet. Voor beide rollen zijn in totaal vier personen ingezet, waarbij een operationeel leider en informatiemanager in een beginnend stadium hun werkzaamheden hebben overgedragen aan een ander die hun rol overnam voor langere tijd.
De eerste informatiemanager heeft na het eerste overleg op vrijdag 17 september zijn taken overgedragen aan de informatiemanager die op piket stond voor de week daarna. In het overleg op maandag 20 september sloot deze tweede informatiemanager aan. Ook de operationeel leider van het team is gewijzigd na twee overleggen.
Deze rollen met bijkomende taken en bevoegdheden zijn binnen de GRIP-structuur vastgelegd, waardoor het bij het aantreden van een gevormd crisisteam voor iedereen duidelijk is wat de rol- en taakverdeling is. Bij de totstandkoming van dit crisisteam was deze bestaande structuur er niet. Als gevolg daarvan hebben de operationeel leider en informatiemanager moeten zoeken naar hun rol en bevoegdheden binnen het crisisteam, en deze ook moeten afstemmen met de andere leden.

Personen uit de gemeentelijke kolom en IJmond Werkt! die aansloten bij het crisisteam zijn opgeroepen vanwege hun kennis, expertise en affiniteit met verschillende belangrijke knelpunten binnen de bestrijding van deze crisis. Met betrekking tot communicatie zijn er verschillende communicatieadviseurs vanuit zowel de regionale crisisorganisatie, gemeenten, als IJmond Werkt! opgekomen. Gezien het feit dat het bij deze crisis om gestolen data met mogelijk privacy-gevoelige inhoud ging, is er besloten om de vier functionarissen gegevensbescherming (FG) van de vier gemeenten bij de crisis te betrekken. Namens deze functionarissen nam één FG plaats in het crisisteam. Een soortgelijke constructie bestond met betrekking tot de Chief Information Security Officers (CISO's) van de betrokken gemeenten. Namens deze CISO's nam één CISO plaats in het crisisteam.
Daarnaast zijn na twee overleggen per gemeente liaisons aangesloten met als doel de informatielijnen richting de besturen van deze gemeenten kort te houden. Deze vier liaisons waren afkomstig uit hun respectievelijke gemeenten.

Zoals eerder vermeld zijn in de nacht van 24 op 25 september het RAC in beperkte vorm en een Communicatieadviseur OT kort ingezet. Deze functionarissen zijn fysiek opgekomen op een locatie in Haarlem. De reden om deze extra communicatie-functionarissen op dat moment in te zetten was een onverwachte wending in de crisis.
De hackgroep verantwoordelijk voor het vergrendelen en stelen van de data van IJmond Werkt! kondigde online aan dat de data openbaar en te downloaden was. Het gehele crisisteam is hierop ongepland bij elkaar gekomen en hierbij sloten de bovengenoemde regionale functionarissen aan. Deze extra opgeroepen functionarissen hebben ter plekke niet veel concrete acties kunnen uitvoeren, ook omdat al veel nodige acties inmiddels liepen. Het gevoel bij deze functionarissen wat nu achteraf heerst is dat er vooral een beroep werd gedaan op extra communicatiecapaciteit in combinatie met de behoefte om te sparren over de stand van zaken en de strategie die genomen diende te worden om de gevolgen te beperken. Na het overleg is de coördinator pers en publieksvoorlichting gedurende de ochtend kort betrokken geweest bij het crisisteam om de directeur van IJmond Werkt! te ondersteunen bij de voorbereiding op eventuele persvragen. Naast de korte inzet van deze individuele functionaris is het RAC na de nacht van 24 op 25 september weer afgeschaald.

Positieve factoren

De rollen van de operationeel leider en informatiemanager hebben van het begin direct een positief effect gehad op de structuur binnen het crisisteam. Ondanks dat het voor hen zoeken was naar hun rol, taak en bevoegdheid in het begin is er met de keuze om hen als facilitator in het crisismanagementproces te betrekken structuur ontstaan in dit proces. Het aanbrengen van structuur in de overleggen en het uitwisselen van informatie tussen de grote verscheidenheid aan partijen heeft op lange termijn veel opgeleverd bij de andere leden van het crisisteam die een wisselende hoeveelheid ervaring met crisismanagement hadden.
Toen deze processen goed liepen, hebben de regionale functionarissen een stap terug kunnen zetten en deze taken bij de leider van het crisisteam, de GS van gemeente Heemskerk, kunnen beleggen.

De inzet van de coördinator pers en publieksvoorlichting vanuit het RAC volgend op het lekken van de data is enorm gewaardeerd door het crisisteam en de directeur van IJmond Werkt!. De coördinator heeft de directeur kunnen voorbereiden op mogelijke persvragen. Mede dankzij die inzet is het interview van de directeur met een lokale nieuwszender prettig verlopen.

Knelpunten

Verschillende factoren hebben ertoe geleid dat het RAC niet direct van waarde kon zijn voor het proces toen de daaraan verbonden functionarissen opkwamen. Zoals hierboven vermeld kwam de behoefte om op te schalen vooral uit de vraag om extra communicatiecapaciteit te verkrijgen en te sparren over de communicatiestrategie en de te nemen stappen hierbij. Vooral deze tweede behoefte sluit beperkt aan bij de rol van het RAC in de crisismanagementstructuur. Het RAC zorgt er normaliter voor dat de bevolking zo snel mogelijk via de media geïnformeerd wordt over de situatie, en kan ook betrokken worden bij het proces van het informeren van verwanten en familie wanneer er sprake is van slachtoffers. In de fase van deze crisis waarin het RAC betrokken werd was er geen sprake van deze acute behoefte om communicatie-slagkracht. Met betrekking tot deze reguliere rol van het RAC bestond er een verschil in verwachting van wat het crisisteam op dat moment nodig had van het RAC en wat het RAC normaliter uitvoert.

Daarnaast dienden de opgekomen functionarissen die niet eerder betrokken waren geweest bij deze crisis bijgepraat te worden over de stand van zaken. Het crisisteam lijkt zich op dat moment onvoldoende te hebben beseft wat een beroep op extra capaciteit zou betekenen voor het proces. Namelijk het opnieuw stilstaan bij de feiten (beeldvorming) en de uitdagingen waarvoor het crisisteam stond (oordeelsvorming). De bereidheid om te helpen bij de opgekomen functionarissen en de behoefte om extra hulp en advies bij het crisisteam waren beide aanwezig, maar deze bereidheid en behoefte hebben elkaar in beginsel onvoldoende gevonden. Achteraf kan de conclusie getrokken worden dat de inzet van het RAC en de communicatieadviseur OT in deze vorm niet nodig is geweest. Vanuit bovenstaand beschreven behoefte was een kort overleg buiten het formele overleg om met daarin de mogelijkheid om te sparren over de te nemen strategie voldoende geweest. Crisisfunctionarissen van het RAC geven aan dat ze achteraf het gevoel hebben op het moment van opkomen niet veel te hebben kunnen bijdragen aan het proces. Desondanks geven verschillende betrokkenen aan van mening te zijn dat de behoefte aan extra capaciteit op het moment van publicatie van de data op dat moment het beste ingevuld kon worden door het RAC in beperkte vorm te alarmeren.

2.3 Leiding en coördinatie

Beschrijving van gebeurtenissen

De bevoegdheid om beslissingen te nemen in deze crisis lag formeel bij het Dagelijks Bestuur van IJmond Werkt!, bestaande uit wethouders van de vier deelnemende gemeenten. Het Dagelijks Bestuur heeft de gemeentesecretaris van Heemskerk erkend als leider van het crisisteam.
De rol van de operationeel leider in deze crisis en de bijkomende taken en bevoegdheden waren (deels) anders dan deze zijn in de bestaande crisisstructuren. Hij nam in deze crisis de rol van technisch voorzitter op zich, waarbij hij de BOB-structuur heeft gebruikt om de vergaderingen op een gestructureerde manier te laten verlopen. Deze manier van vergaderen was voor een groot aantal leden van het crisisteam nieuw.

Het crisisteam heeft zichzelf tijdens één van de eerste overleggen drie doelen gesteld:

1. Het beperken van de impact voor de kwetsbare groep van cliënten van IJmond Werkt!
2. De bedrijfscontinuïteit van IJmond Werkt! bewaken
3. Het beperken van de maatschappelijke impact van het incident

Positieve factoren

De inzet die getoond is door alle leden van het crisisteam naast hun reguliere werkzaamheden en de waardering daarvoor is een terugkerende factor in alle antwoorden op zowel de enquête als in de interviews. Daarnaast is de inbreng van de BOB-structuur door de operationeel leider unaniem als fijn en constructief beoordeeld, ook door hen met relatief weinig ervaring met crisismanagement. De inzet die de operationeel leider heeft getoond om deze structuur vast in het proces te krijgen kostte in beginsel moeite, maar heeft op langere termijn als effect gehad dat de overleggen gestructureerd verliepen en er concrete actiepunten ontstonden. Dit heeft er tevens aan bijgedragen dat een gedeelte van de vooraf gestelde doelen gehaald zijn en dat acties en samenwerkingen nu goed zijn georganiseerd om volledige afhandeling van de doelen te bewerkstelligen.

Knelpunten

Dat de leiding van het crisisteam bij de gemeentesecretaris lag was voorafgaand aan het eerste overleg niet duidelijk voor IJmond Werkt!; zij waren in de veronderstelling dat de operationeel leider vanuit de Veiligheidsregio de leiding zou hebben. Deze onduidelijkheid leidde tot spanningen bij IJmond Werkt! tijdens het overleg en met name over wie nu precies de leiding had. IJmond Werkt! veronderstelde dat er een GRIP-constructie gaande was, waarbij de operationeel leider de crisis leidde. Deze operationeel leider vulde alleen de rol van technisch voorzitter in bij het overleg, om zo de overleggen en andere processen te stroomlijnen. IJmond Werkt! voelde zich daarnaast als getroffen organisatie tot in bepaalde mate bedreigd omdat vanuit hun perceptie geopperde mogelijke risico's gerelateerd aan het incident werden vertaald naar een directie schuldvraag en persoonlijke consequenties.

Naast de eerder beschreven melding bij het RAC die niet de gewenste duidelijkheid had en het knelpunt met betrekking tot de keuze om op te schalen is er een knelpunt aan te wijzen op het gebied van leiding. Met de opkomst van de RAC-functionarissen kwam ook het hoofd van het RAC op. Hierbij ontstond een situatie waarin het hoofd RAC, de operationeel leider en de informatiemanager fysiek in één ruimte bij elkaar zaten. Normaliter geeft het hoofd RAC leiding aan de opgekomen RAC-functionarissen in een apart ingerichte ruimte. Dit werkte voor de opgekomen RAC-functionarissen en het hoofd RAC verwarrend. Deze factor heeft ook meegespeeld bij de verwarring en onduidelijkheid bij het RAC over wat zij konden betekenen op het moment van opkomen.

2.4 Informatiemanagement

Beschrijving van gebeurtenissen

Om ervoor te zorgen dat informatie op een efficiënte manier werd gedeeld tussen de verschillende actoren van de verschillende partijen die aansloten bij het crisisteam is er een informatiemanager aangesteld. Zoals eerder beschreven waren de rol, taken en bevoegdheden van de informatiemanager in beginsel niet volledig duidelijk en omlijnd, zeker in vergelijking met een situatie waarin een informatiemanager opkomt in GRIP-situatie waarbij rollen, taken en bevoegdheden vastliggen. Met betrekking tot middelen die tot de informatiemanagers hun beschikking stonden om de informatie op een centraal punt vast te leggen is Microsoft Teams gebruikt. Normaliter wordt bij een GRIP opschaling het programma LCMS gebruikt, wat een belangrijk element vormt voor het netcentrisch werken bij crisismanagement binnen de gemeenten en Veiligheidsregio. De mogelijkheid om LCMS te gebruiken om het netcentrisch werken vorm te geven was er niet in deze crisis, waarna er gekozen is om Microsoft Teams als middel hiervoor in te zetten.

Positieve factoren

De ervaring van de informatiemanagers met het netcentrisch werken hebben de structuur van het proces een boost gegeven. De informatiemanagers hebben onderscheid tussen feiten en aannames aangebracht, om zo het beeld duidelijk te krijgen en iedereen in dezelfde film te plaatsen. Gezien het feit dat de crisis al twee weken gaande was waarbij IJmond Werkt! zelf acties heeft ondernomen om de crisis te bestrijden, bestond er een informatieachterstand tussen IJmond Werkt! en de andere actoren van verschillende partijen. De informatiemanagers hebben in beginsel focus gelegd op het verkleinen van deze achterstand.

Toen de voorzieningen omtrent het netcentrisch werken stonden, bewoog de rol van informatiemanager steeds meer richting de rol van verslaglegger van de overleggen. Naarmate er steeds meer sprake was van deze verschuiving heeft de informatiemanager van dienst een stapje terug gedaan en zijn taak overgedragen aan iemand die goede en duidelijke notulen kon maken. De opzet voor de notulen die stond werd ook door de nieuwe informatiemanager vastgehouden,

Knelpunten

Tijdens de crisis is de samenstelling van het crisisteam soms gewijzigd, waarbij vertegenwoordigers van partijen tussen overleggen veranderden. Voor de informatiemanager was het daardoor lastig te valideren wie tot welke informatie toegang diende te krijgen. Veel communicatie over de crisis verliep via e-mail en whatsapp, waarbij een whatsappgroep steeds voller dreigde te raken. Het gebrek aan afspraken over deze informatievoorziening aan de voorkant en de moeite om dit aspect op de agenda te krijgen binnen het crisisteam vormde een knelpunt. De wil om snel aan de slag te gaan met de uitdagingen die optraden als gevolg van het incident zorgde kan ervoor gezorgd hebben dat de noodzaak van het scheppen van een duidelijk beeld niet breed gevoeld werd binnen het crisisteam. De kleine hoeveelheid ervaring met crisismanagement kan hierbij ook meegespeeld hebben. Het heeft als gevolg even geduurd om de noodzaak om hier afspraken over te maken kenbaar te maken binnen het crisisteam. Uiteindelijk is er een centraal informatiepunt in Microsoft Teams opgezet, waar ieder lid van het crisisteam toegang tot had.

Daarnaast zorgde de wisselende samenstelling van het crisisteam ook voor nieuwe leden die niet op de hoogte waren van de stand van zaken op het moment van hun eerste overleg. Het belang om conform de BOB-structuur bij ieder nieuw lid kort opnieuw bij het beeld stil te staan zorgde voor wrijving met leden van het crisisteam die al bekend waren met alle details, en door wilden schakelen naar lopende zaken en concrete acties. Met het aansluiten van de vier bestuursadviseurs afkomstig van de vier deelnemende gemeenten werd dit proces meer gestroomlijnd. Hun toevoeging en rol in het crisisteam is door verschillende betrokkenen aangewezen als kantelpunt omtrent dit knelpunt.

Zoals eerder beschreven bij het thema leiding en coördinatie zorgde de onduidelijkheid over rollen en bevoegdheden bij IJmond Werkt! tot een terughoudende opstelling in het proces. Deze opstelling had ook effect op de bereidheid om informatie uit te wisselen. Verschillende betrokkenen hebben aangegeven dat de transparantie bij IJmond Werkt! niet op een niveau was die zij wensten.

Een voorbeeld hiervan is dat het lang duurde voordat alle partijen binnen het crisisteam toegang kregen tot belangrijke informatie zoals het rapport van Fox-IT over de gestolen data. Met betrekking tot deze transparantie geeft IJmond Werkt! echter aan zich niet te herkennen in dit beeld. Wat een mogelijke verklaring kan zijn voor dit verschil in perceptie is de keuze van IJmond Werkt! om een (begrijpelijke) samenvatting te maken van het rapport voordat deze gedeeld werd met het team.

Het vertrouwen om breed informatie te delen en dat men bij deze crisis was aangehaakt om de gevolgen zo goed mogelijk te bestrijden was niet op een gewenst niveau. Aan de voorkant van het proces is te weinig aandacht besteed aan het bouwen van vertrouwen tussen het crisisteam en de getroffen organisatie, alsook tussen de leden van het crisisteam.

2.5 Crisiscommunicatie

Beschrijving van de gebeurtenissen
Het communicatieproces was van essentieel belang in deze crisis en vormde een rode draad in de actiepunten van het crisisteam. De communicatie richting (oud-)medewerkers, cliënten en gemeenten stond centraal bij het behalen van de doelen van het crisisteam. Daarnaast is gerichte communicatie richting de pers ook steeds meer in beeld gekomen naar aanleiding van het lekken van de gestolen data door de hackgroep. Verschillende communicatiekanalen zijn ingezet om personen te bereiken: Q&A, raadsbrieven, persberichten en een callcenter.

Positieve factoren
Binnen het crisisteam is er nagedacht over een communicatiestrategie en heeft er een doelgroepanalyse plaatsgevonden. Men heeft nagedacht over de manieren waarop personen uit verschillende doelgroepen het beste bereikt konden worden, wat geleid heeft tot verschillende communicatiekanalen. Verschillende leden met een verscheidenheid aan kennis konden deze inzetten om berichten duidelijk, bestuurlijk en conform de AVG-wetgeving te krijgen. Hierbij moet gedacht worden aan communicatieadviseurs, bestuursadviseurs, CISO’s en Functionarissen Gegevensbescherming vanuit de vier gemeenten.

Het opschalen van het RAC en de communicatieadviseur OT heeft uiteindelijk geleid tot het meedenken en bijschaven aan de bestaande communicatiestrategie. Hieruit is het besluit genomen om actief te communiceren en de lokale pers hierbij de primeur van het nieuws van het lekken van de data te geven. De rol van de IBD mag hierbij ook niet vergeten worden. Deze strategie heeft goed gewerkt met betrekking tot het 'klein' houden van het nieuws. De lokale zender besloot het opgestelde persbericht één-op-één over te nemen en los van een bericht op nu.nl is het nieuws niet ver verspreid op landelijk niveau.

Het crisisteam heeft daarnaast goed beseft dat communicatie altijd tot reacties leidt. Om hier oog voor te hebben is er besloten om via de regionale crisisorganisatie en gemeenten omgevingsanalisten in te zetten, specifiek na het publiceren van het persbericht waarin het nieuws van het lekken van de data werd bevestigd.

Knelpunten

Bij het opstellen van de communicatieberichten richting de vastgestelde doelgroepen en conform de opgestelde communicatiestrategie was het lastig om de NAW-gegevens van alle personen van wie mogelijk data gestolen was te achterhalen. Dit betreft vooral oud-medewerkers die nu mogelijk een ander adres hebben. Deze uitdaging heeft de berichtgeving richting de getroffen personen vertraagd.

Het moment waarop de gestolen data gepubliceerd werd heeft het crisisteam verrast. Toch is er in een beginnend stadium aan scenariodenken gedaan; leden van het crisisteam hebben mogelijke scenario's waarnaar de crisis zich kon bewegen proberen te voorspellen. Het scenario dat er op korte termijn data gelekt zou worden is in bepaalde mate uitgewerkt en er is altijd rekening mee gehouden dat er data gelekt zou worden. Deze mogelijkheid is één van de redenen waarom er besloten is op te schalen naar een crisisteam in samenwerking met de gemeenten en met de Veiligheidsregio Kennemerland als ondersteunende crisisorganisatie en de daarbij betrokken functionarissen.. Desondanks leidde het lekken van de data uiteindelijk tot een behoefte aan extra communicatiecapaciteit en om te sparren, waarop het RAC werd opgeschaald.

Uit de enquête en interviews is gebleken dat er een communicatiestrategie lag voor het geval data gelekt zou worden. Hier had achteraf meer op vertrouwd en teruggevallen kunnen worden. De gehele opschaling van het RAC en de communicatieadviseur OT zoals het heeft plaatsgevonden in deze crisis waren dan niet nodig geweest.

2.6 Afschaling

Beschrijving van gebeurtenissen

Het crisisteam is uiteindelijk op 13 oktober afgeschaald. Op dat moment waren de acties omtrent het informeren van (oud-)medewerkers, cliënten en de vier gemeenten afgerond of goed onderweg. Ook was er gestart met het heropbouwen van de systemen van IJmond Werkt!. Het analyseren van de data vroeg nog samenwerking tussen de gemeenten en IJmond Werkt! op de langere termijn. Daarom is er voor gekozen om een regionaal afstemmingsoverleg in stand te houden, waarbij FG's en CISO's uit de gemeenten en IJmond Werkt! nog na het afschalen van het crisisteam samenwerken. Daarnaast werd er afgesproken om weer bij elkaar te komen wanneer de situatie hierom vroeg. Leden van het crisisteam hadden elkaars contactgegevens om zo het team naar wens weer bij elkaar te roepen.

Knelpunten

Uit de enquête en interviews is gebleken dat het moment van afschalen van het crisisteam een onderwerp is waar verdeeldheid over bestaat. Sommigen menen dat het moment van afschalen op het juiste moment kwam, omdat het acute element van de crisis niet meer speelde. Anderen menen dat er pas afgeschaald kon worden als alle door de datalek getroffen personen geïnformeerd waren over welke bestanden van hen mogelijk in handen van derden zijn. Hierbij werd in de enquête en interviews ook verwezen naar twee van de gestelde doelen van het crisisteam: het beperken van de impact op de kwetsbare cliënten van IJmond Werkt! en het bewaken van de bedrijfscontinuïteit van IJmond Werkt!.

Bij een strenge interpretatie van deze twee doelen, kan beargumenteerd worden dat het crisisteam nog niet afgeschaald diende te worden. Desondanks kan ook beargumenteerd worden dat de crisis niet meer acuut was op het moment van afschalen: voor beide van bovengestelde doelen waren acties belegd en werden inspanningen verricht. Daarnaast is er nagedacht over de nodige samenwerking tussen gemeenten en IJmond Werkt! en is er met die reden het eerder genoemde afstemmingsoverleg in het leven geroepen.

Juist de samenwerking tussen gemeenten en IJmond Werkt! die nog nodig was zorgde er ook voor dat het afschalen van het crisisteam lastig op de agenda te krijgen was binnen het crisisteam. Sommige respondenten menen dat het afschalen eerder had gekund, maar dat het lastig was deze mening op de agenda te krijgen vanwege die noodzaak om te blijven samenwerken. Dit knelpunt omtrent het bepalen van het einde van een crisis en de lange duurloop is kenmerkend voor cyberincidenten. Dit soort incidenten hebben vaak een relatief lange duurloop, waarbij het heropbouwen van gehackte systemen veel tijd kost. Vergeleken met ‘traditionele’ flitsrampen zoals branden en verstoringen van de openbare orde is het aanwijzen van een einde van de crisis en de nodige inspanning en coördinatie zoals die op dat moment plaatsvindt lastiger te doen.

Aanbevelingen

In dit laatste deel schetst dit rapport aanbevelingen zodat men kan leren van dit incident en de wijze waarop het is bestreden. Dit kan helpen bij de voorbereiding op en bestrijding van soortgelijke incidenten in de toekomst.

3.1 Samenstelling crisisteam

Het crisisteam wat is samengesteld in deze casus toont aan welke processen en de daarbij betrokken personen van toegevoegde waarde zijn in incidenten van deze aard. In dit geval heeft deze samenstelling betrekking op specifiek cyberincidenten en de bestrijding daarvan. Maar aan de hand van dit incident kunnen er ook aanbevelingen worden gedaan voor incidenten die buiten de reguliere procedures van rampenbestrijding en crisismanagement worden bestreden in het algemeen, waarbij de Veiligheidsregio en de daaraan verbonden functionarissen een meer faciliterende rol aannemen.

Aanbeveling:
Bij cyberincidenten is het belangrijk het vermogen te hebben om flexibel op te kunnen schalen, buiten de reguliere procedures van rampenbestrijding en crisisbeheersing om. Actoren die normaliter een grote rol spelen bij reguliere structuren van rampenbestrijding en crisismanagement zoals de GHOR, politie en brandweer zijn niet perse van toegevoegde waarde voor het proces. Desondanks kunnen als gevolg van het cyberincident wel fysieke en maatschappelijke gevolgen ontstaan waarbij de kennis van die actoren relevant zijn. Het uitgangspunt hierbij is daarom om flexibel op te kunnen schalen naar behoefte, waarbij er aandacht dient te zijn voor een vast aantal rollen, taken en bevoegdheden die nodig zijn bij de bestrijding van een incident.

Aanbeveling:
In het geval van een cyberincident is het belangrijk dat er bij de vaststelling van de samenstelling van het crisisteam oog is voor de meer technische kant van de crisis, zoals ICT en informatiebeveiliging. Daarnaast is het belangrijk dat er een rol is weggelegd voor iemand die het effect van het incident ook kan vertalen naar maatschappelijke en economische effecten..

Aanbeveling:
Leg de focus als crisisorganisatie op het bestrijden van de fysieke, sociale en maatschappelijke gevolgen bij een cyberincident. Voorbeelden hiervan zijn uitval van infrastructuur, maatschappelijke onrust of cybercrime op persoonlijk niveau zoals phishing. Dit is ook in lijn met eerder gevormde planvorming zoals het Nationaal Crisisplan-Digitaal. Deze focus op cybergevolgbestrijding ligt in lijn met de processen binnen rampenbestrijding en crisismanagement waar gemeenten en Veiligheidsregio's zich normaliter ook mee bezig houden. De getroffen organisatie blijft hierbij zelf verantwoordelijk voor haar bedrijfscontinuïteit, eventueel met ondersteuning van kennis binnen gemeenten en regio's.

Aanbeveling:
Zoals hierboven beschreven is er ervaring en kennis op het gebied van ICT nodig bij cyberincidenten. Personen die met betrekking tot deze behoefte aansluiten bij een potentieel crisisteam hebben vaak relatief weinig tot geen ervaring met crisismanagement, waar ook sprake van was in de casus bij IJmond Werkt!.
Om de belangrijke crisismanagement processen te waarborgen en efficiënt te laten verlopen zijn functionarissen die de rollen van operationeel leider en informatiemanager op zich nemen belangrijk om toe te voegen aan het crisisteam. Leiding en coördinatie en informatiemanagement zijn belangrijke processen om te waarborgen. Het waarborgen van deze processen is relevant voor alle bestrijding van incidenten die buiten de reguliere opschalingsprocedures verlopen. De samenstellingen die juist dan ontstaan zijn flexibel van aard, waarbij partners op een relatief grotere afstand staan van de regionale crisisorganisatie en met die oorzaak minder ervaring hebben met crisismanagement en het opereren binnen de context van een crisis. Zorg dat er aandacht is voor deze processen en het mogelijke gebrek aan kennis op dit gebied. Om dit op te lossen kan er een beroep gedaan wordt op de regionale crisisorganisatie waar de nodige ervaring en kennis op het gebied van deze processen al aanwezig zijn.

3.2 Opschalen

Aanbeveling:
Zoals boven geschetst is het flexibel opschalen naar behoefte gerelateerd aan het opschalen buiten de reguliere opschalingsprocedure. Het is belangrijk om vooraf aan het inzetten van meer of een ander soort capaciteit met betrekking tot het bestrijden van de crisis een goede afweging te maken wat dit doet voor het proces in zijn geheel. Meer dan bij reguliere opschalingsprocedures dienen er vooraf vragen beantwoord te worden, zodat er een duidelijk en concreet beeld ontstaat van waar behoefte aan is. Men dient de vraag te stellen wie aan deze behoefte tegemoet kan komen, in welke vorm dat dient te gebeuren en wat voor verdere consequenties het heeft wanneer extra slagkracht wordt toegevoegd aan een al bestaand en functionerend crisisteam.

Aanbeveling:
Zorg dat er aandacht is voor hoe de besluitvorming en leiding en coördinatie op dat moment zijn vastgelegd en of deze aan verandering onderhevig zijn wanneer er besloten wordt rollen die normaliter acteren binnen de reguliere procedure van rampenbestrijding en crisismanagement toe te voegen.
Binnen deze reguliere procedure liggen taken en bevoegdheden mogelijk anders dan hoe deze belegd zijn in de flexibele opschaling waarvoor is gekozen in beginsel. Zorg dat er in het geval van flexibel opschalen voor het opschalen al oog is voor het spanningsveld wat hier kan ontstaan met betrekking tot taken, rollen en bevoegdheden.

3.3 Leiding & Coördinatie

Aanbeveling:
Zorg voor duidelijke afspraken omtrent de rollen, taken en bevoegdheden wanneer er opgeschaald wordt buiten de reguliere procedures van de rampenbestrijding en crisisbeheersing. Zorg dat hierbij oog is voor waar de relevante kennis en expertise zit waar op dat moment behoefte aan is, en durf hier flexibel in te zijn om zo tot de meest efficiënte samenwerking te komen.

3.4 Informatiemanagement

Aanbeveling:
Het is goed als Veiligheidsregio's en gemeenten gaan nadenken over tools voor netcentrisch werken buiten LCMS.
Informatiemanagement en het netcentrisch werken tijdens een crisis zijn belangrijke processen om zo alle betrokken leden binnen een flexibel gevormd crisisteam in dezelfde film te plaatsen. De rol van een informatiemanager bij deze processen en de manier waarop dit vanuit de regionale crisisorganisatie ingevuld kan worden is al eerder besproken. Daarnaast zijn de tools die ter beschikking staan voor de informatiemanager belangrijk bij het netcentrisch werken. Vanuit de reguliere regionale crisisstructuur wordt LCMS gebruikt om dit proces vorm te geven. In de casus bij IJmond Werkt! heeft LCMS geen rol gespeeld op dit gebied, gezien het feit dat het merendeel van de leden van het crisisteam geen toegang hadden tot LCMS. Een soortgelijke situatie kan zich eenvoudig herhalen wanneer er weer buiten de reguliere procedures van rampenbestrijding en crisisbeheersing wordt opgeschaald en er partners aansluiten die bij hun dagelijkse werkzaamheden relatief ver van de regionale crisisorganisatie en haar werkzaamheden staan.

Vanwege die uitdaging is het goed als er buiten LCMS om wordt gedacht en er afspraken gemaakt worden welk programma gebruik dient te worden om het netcentrisch werken te borgen. In de casus bij IJmond Werkt! is hiervoor Microsoft Teams gebruikt.

Aanbeveling:
Wees bewust van de inzet en de tijd die in beginsel gestoken moet worden in het opzetten van een netcentrisch netwerk om zo iedereen in dezelfde film te plaatsen. Dit kost altijd tijd en energie, maar als gevolg van het flexibel opschalen waarbij samenwerkingen met relatief onbekende partners ontstaan kan het voorkomen dat personen te maken krijgen met systemen waar zij onbekend mee zijn. Op langere termijn zal deze inzet altijd zorgen voor een meer gestroomlijnde samenwerking tussen partners.

3.5 Crisiscommunicatie

Het informeren van de mogelijk getroffen personen is belangrijk tijdens cyberincidenten. Het kan soms lang duren totdat duidelijk is wat er heeft plaatsgevonden en wat het mogelijke effect kan zijn bij cyberincidenten. Met deze reden is het verstrekken van volledige informatie lastig.

Aanbeveling:
Stel vooraf vast wat de communicatiestrategie is, met daarbij doelgroepen en manieren om die doelgroepen te bereiken. Denk hierbij in verschillende mogelijke scenario's en de mogelijke consequenties van die scenario's.

Aanbeveling:
Durf het scenario van pro-actief communiceren naar betrokkenen en pers te overdenken en uit te werken. Het verstrekken van procesinformatie aan mogelijk getroffen personen kan al in een vroeg stadium, zonder dat het duidelijk is op welk detailniveau persoonlijke informatie gestolen is en mogelijk gepubliceerd kan worden. In de casus bij IJmond Werkt! heeft pro-actieve communicatie uiteindelijk goed uitgepakt met betrekking tot het beperken van de maatschappelijke impact.

3.6 Afschaling

Aanbeveling:
Stem het moment van afschalen goed af met alle betrokken partijen. De keuze van het moment van afschalen is lastiger te bepalen bij cyberincidenten en andere crises met een relatief lange duurloop. Bij het vaststellen van het moment van afschalen dient er aandacht te zijn voor de doelen die aan het begin van de crisis gesteld zijn, en te beoordelen tot in welke mate deze behaald zijn.

Aanbeveling:
Heb aandacht voor de vooraf gestelde doelen en tot in welke mate deze behaald zijn. Bij specifiek cyberincidenten duurt het vaak lang voordat de getroffen organisatie weer op een vergelijkbaar niveau als voor het incident operationeel kan zijn, waardoor het lastig is om een doel gerelateerd aan de bedrijfscontinuïteit van de getroffen organisatie volledig te halen. Dit hoeft echter niet te betekenen dat het opgezette crisisteam in acute en volledig opgeschaalde vorm bijeen dient te blijven. Zorg dat er bij een mogelijk gedeeltelijke afschaling oog is voor de relevante kennis en expertise die bij elkaar is gekomen in de vorm van partners. Deze partners kunnen de getroffen organisatie mogelijk over een langere periode bijstaan. Zorg dat er richting het einde van de crisis oog is voor de behoeftes die er op dat moment nog zijn. De samenwerking binnen het crisisteam kan dan eventueel voortgezet worden in een minder acute en verkleinde vorm totdat de gevolgen van het incident maximaal beperkt zijn.

Aanbeveling:
In de afrondende fase en na afloop van het incident dient er oog te zijn voor nazorg voor de betrokken functionarissen. Dit proces is normaliter belegd in de reguliere procedures van rampenbestrijding en crisismanagement. Dit proces dient niet vergeten te worden wanneer er buiten die reguliere procedures wordt opgeschaald en geöpereerd. Belangrijk hierbij is dat ook de getroffen organisatie en diens personeel meegenomen worden in dit proces. Vanuit deze en ook andere evaluaties is gebleken dat cyberincidenten een groot effect hebben op de getroffen organisaties.