Evaluatie ISIDOOR IV

April 2024

Inhoudsopgave

AFKORTINGENLIJST

CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
DCC	Departementaal Coördinatiecentrum Crisisbeheersing
DIVD	Dutch Institute for Vulnerability Disclosure
IAO	Interdepartementaal Afstemmingsoverleg
ICCb	Interdepartementale Commissie Crisisbeheersing
ISAC	Information Sharing & Analysis Center
LCMS	Landelijk Crisis Management Systeem
LCP-Digitaal	Landelijk Crisisplan Digitaal
LDS	Landelijk Dekkend Stelsel
LOCC	Landelijk Operationeel Coördinatiecentrum
NCC	Nationaal CrisisCentrum
NCO-T	Nationaal Continuïteitsoverleg Telecommunicatie
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorisme en Veiligheid
NKC	Nationaal Kernteam Crisiscommunicatie
OKTT	Een organisatie die ‘objectief kenbaar tot taak’ heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen
OL-call	Operationeel Leiders-call
OT	Operationele technologie
SOC	Security Operations Center
TCO	Tripartiet crisismanagement operationeel
Wbni	Wet beveiliging netwerk- en informatiesystemen

1. INLEIDING

1.1 Aanleiding

Het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) zetten zich dagelijks in om de cyberweerbaarheid in Nederland te versterken. Daarom initieerden zij de grootste cyberoefening ooit gehouden in Nederland: ISIDOOR IV. De oefening was verspreid over vier dagen. Van 13 t/m 15 november 2023 vond de hoofdoefening plaats en op 27 november 2023 oefende de Interdepartementale Commissie Crisisbeheersing (ICCb) met de input uit de hoofdoefening. Deze nationale cyberoefening biedt een platform om de digitale weerbaarheid, sectorale- en cross-sectorale samenwerking te verbeteren.

Het NCSC en de NCTV organiseerden ISIDOOR IV en lieten zich in het ontwikkelen van het scenario en het oefenleiderschap ondersteunen door het COT Instituut voor Veiligheids- en Crisismanagement (COT) en Fox-IT. In de voorbereiding werkten tal van deelnemende organisaties samen om tot een realistisch, grootschalig en uitdagend cyberscenario te komen. In aanvulling op de voorbereiding en uitvoer van de oefening, verzorgt het COT ook de overkoepelende leerevaluatie. In deze rapportage presenteren we onze observaties, leerpunten en aanbevelingen.

1.2 Over de oefening

Van 13 t/m 15 november 2023 namen meer dan 3.000 deelnemers van ruim 120 organisaties, verdeeld over twaalf verschillende sectoren, gelijktijdig deel aan de driedaagse hoofdoefening. Op 27 november 2023 vond aansluitend op de hoofdoefening de oefening plaats met de ICCb. Afsluitend werden op 30 november 2023 de eerste lessen met elkaar gedeeld tijdens een online-evaluatiebijeenkomst.

Om alle deelnemende organisaties zo goed mogelijk te kunnen bedienen tijdens de oefening waren de organisaties ingedeeld op deelnameniveau Goud of Zilver. Dit deelnameniveau werd vooral bepaald door de mate waarin de organisatie behoort tot de doelgroepen rijksoverheid en vitaal en de eigen oefenambitie. Ook is gekeken naar (relevante) betrokkenheid bij de crisisbeheersing ten aanzien van de nationale veiligheidsbelangen. De partners op niveau Goud waren nauw betrokken bij de voorbereiding van de oefening en dachten mee over het scenario in de scenariowerkgroep. De deelnemende organisaties op niveau Zilver waren niet betrokken bij de inhoudelijke voorbereiding van de oefening, maar konden tijdens ISIDOOR de informatie en berichten uit het scenario gebruiken om een deeloefening binnen de eigen organisatie te organiseren.

Het doel van ISIDOOR IV was het beoefenen van de nationale respons tijdens een grootschalige digitale crisis, zoals beschreven in het Landelijk Crisisplan Digitaal (LCP-Digitaal). Daarbij werd specifiek gekeken naar informatie-uitwisseling, samenwerking en de nationale opschaling bij een cybercrisis. Naast deelnemende organisaties uit de vitale sectoren oefenden ook ministeries, veiligheidsregio's, netwerkorganisaties, uitvoeringsorganisaties en andere crisispartners mee.

Oefendoelen ISIDOOR IV

1. **Informatie-uitwisseling –** Het beoefenen van informatie-uitwisseling en samenwerking (op alle niveaus) ten tijde van een cybercrisis.
2. **Opschaling** – Het beoefenen van de nationale opschalingsstructuur tijdens een cybercrisis, tot en met het niveau van een ICCb.
3. **Samenwerking** – Het versterken van de onderlinge samenwerking tussen de vitale en rijksoverheidsorganisaties.

Scenario

In het scenario neemt gedurende drie dagen de (dreiging van) uitval en het aantal verstoringen toe. Dit zorgt voor impact op de dienstverlening en maatschappelijke onrust.

Het scenario van ISIDOOR IV gaat uit van een statelijke actor, die al langere tijd bezig is met het ongezien verwerven van een kritieke positie in de leveringsketen van vitale- en overheidsorganisaties. De actor heeft

een kwetsbaarheid weten te bouwen in wijdverbreide netwerkmonitoring software. Bij de aanvang van de oefening komt de kwetsbaarheid bij de softwareleverancier aan het licht. Deze kwetsbaarheid in de software, waarvoor de leverancier nog geen oplossing heeft uitgebracht, kan misbruikt worden door geavanceerde kwaadwillende partijen.

De statelijke actor wil zijn sporen zoveel mogelijk wissen en maakt daarvoor slim gebruik van de reflex van organisaties om systemen preventief te isoleren. In de malafide software zit een *scheduled task* (een soort timer) verstopt die wordt getriggerd zodra organisaties de software preventief isoleren. Zodra de timer afloopt rolt er automatisch *wiperware* uit die alle data op de systemen van de desbetreffende organisaties vernietigt.

Dag 1
In het eerste deel van het scenario komt de kwetsbaarheid bij de softwareleverancier aan het licht. Technische teams zoeken uit of ze kwetsbaar zijn en zoeken naar sporen van misbruik van de kwetsbaarheid.

Dag 2
In de loop van dag twee groeit de dreiging. Organisaties ervaren verstoringen die mogelijk te relateren zijn aan de kwetsbaarheid. Dit vraagt om onderlinge samenwerking en intensiever onderzoek. De verstoringen krijgen steeds meer impact op de levering van diensten en zorgen voor maatschappelijke onrust. De actor en het motief achter de aanval zijn onduidelijk en bij het bekend raken van de kwetsbaarheid meldt ook een opportunistische en geavanceerde hackersgroep zich in het spel. Zij misbruiken de kwetsbaarheid en rollen ransomware uit bij verschillende organisaties.

Dag 3
Vitale processen komen onder druk te staan: delen van het betalingsverkeer vallen uit, containers stapelen zich op in de Rotterdamse haven en cruciale overheidssystemen zijn niet meer te vertrouwen. Ondertussen groeit de mediadynamiek en stijgt de maatschappelijke onrust. Dit leidt uiteindelijk tot nationale opschaling en twee keer een Interdepartementaal Afstemmingsoverleg (IAO).

Dag 4
Het laatste deel van de oefening betreft een bijeenkomst van de ICCb. In dit ICCb wordt onder meer gesproken over het gezamenlijk beeld en de inzet van schaarse middelen (waaronder forensische ondersteuning).

De oefening in cijfers

- ✓ **120** deelnemende organisaties en gremia, meer dan **3000** deelnemers
- ✓ 17 organisaties deden mee met ieder meer dan **40** deelnemers
- ✓ Één organisatie deed met **14 teams** mee aan de oefening
- ✓ **84%** van de organisaties heeft opgeschaald naar strategisch niveau
- ✓ **31%** van de organisaties heeft tijdens de oefening aangifte gedaan
- ✓ Er is tijdens de oefening minimaal **220 keer** contact opgenomen met het NCSC
- ✓ **65%** van de deelnemende organisaties heeft in een samenwerkingsverband sectoraal afgestemd
- ✓ **24%** van de organisaties deed tijdens de oefening een Wbni-melding

1.3 Evaluatieproces en -scope

Samen leren Leren van oefeningen gebeurt op verschillende manieren, niveaus en momenten. Niet alleen de ervaringen tijdens de oefening zelf en op de evaluatiedag op 30 november 2023 zijn leermomenten, maar ook de voorbereidingen zijn leerzaam. Veel deelnemers hebben elkaar in het voortraject leren kennen en hebben zich gebogen over inhoudelijke en organisatorische vraagstukken. Wie heeft welke rol? Hoe lopen informatielijnen? Wat zijn mogelijke sleutelbesluiten? Daarnaast wordt het reflecteren en leren versterkt door teamevaluaties en uitwisselingen tussen organisaties die met elkaar de oefening nabespreken. In deze rapportage ligt de focus op de overkoepelende leerpunten.

Evaluatieproces Elke deelnemende organisatie heeft voorafgaand aan de oefening een evaluator aangesteld. Daarnaast is in de voorbereiding per sector ook een sectorale evaluator aangesteld. Deze fungeert als schakel tussen de organisatie-evaluatoren binnen de sector en de centrale oefenleiding. Op basis van de vooraf opgestelde oefendoelen heeft het COT een online vragenlijst opgesteld. Deze vragenlijst is door de organisatie-evaluatoren tijdens en na de oefening ingevuld. In totaal is de vragenlijst ingevuld door 83 organisaties. De week na de oefening hebben de sectorale evaluatoren in korte online gesprekken met twee evaluatoren van het COT de belangrijkste en opvallendste uitkomsten besproken ter voorbereiding op de evaluatie-ochtend op 30 november. Tijdens de oefening hadden twee evaluatoren namens het COT en de NCTV een vrije evaluatierol; zij liepen rond en verzamelden gedurende de dag leerpunten. De NCTV-evaluator schrijft niet mee aan deze rapportage maar leverde enkel input tijdens de oefening.

Uitgangspunten evaluatie

- ✓ Het accent van de oefening ligt op leren, niet op testen. Deze insteek is nadrukkelijk gekozen om de diverse bij een cybercrisis betrokken teams en organisaties ervaring te laten opdoen en van die ervaring te laten leren. De oefening is dan ook géén (systeem)test en niet bedoeld om de kwaliteit van de afspraken of crisisparaatheid van de betrokkenen te beoordelen.
- ✓ De focus van de evaluatie ligt op de overkoepelende crisisstructuur en niet op individueel of organisatie-niveau.

Op 30 november 2023 vond de evaluatie-ochtend plaats. Onderdeel van deze ochtend was een gesprek per sector, waarin de sectorale evaluatoren samen met oefenleiders en organisatie-evaluatoren het gesprek voerden over de belangrijkste uitkomsten per sector. Hierbij de focus lag op de vragen ‘wat ging goed?’ en ‘waar vraag je aandacht voor?’. De notities van deze gesprekken zijn door ons meegenomen in deze evaluatie. Dit geldt ook voor de rode draden uit de ingevulde vragenlijsten, de observaties tijdens de oefendagen en de verdere input uit de evaluatie-ochtend.

1.4 Leeswijzer

Hoofdstuk 2 bevat het overkoepelend beeld van hoe deelnemers reflecteren op de oefening, op punten aangevuld met de reflectie van het COT, en de aanbevelingen voor de toekomst die hieruit volgen. In hoofdstuk 3 staan de observaties per oefendoel. In de bijlage staan de belangrijkste leerpunten uit ISIDOOR III.

NB: Waar wij in dit rapport verwijzen naar percentages en aantallen organisaties, betreft dit de organisaties die de vragenlijst hebben ingevuld.

2. OVERKOEPELEND BEELD EN AANBEVELINGEN

In dit hoofdstuk geven we een overkoepelend beeld van hoe deelnemers reflecteren op de oefening, op punten aangevuld met de reflectie van het COT. Daarnaast doen we in dit hoofdstuk enkele aanbevelingen voor versterking. Deze vloeien voort uit de oefening en de evaluatie.

2.1 Overkoepelend beeld

Zowel direct na de oefening als in de sectorale gesprekken en de evaluatiebijeenkomst is de overkoepelende afdronk na ISIDOOR IV: oefenen op deze schaal met zo veel partijen is waardevol. Het zorgt voor een grotere bewustwording van de brede impact van een cybercrisis. Ook de voorbereiding op de oefening droeg hieraan bij. In de voorbereiding zochten partijen elkaar op, bijvoorbeeld om af te stemmen over het scenario. Dit droeg bij aan elkaar (cross) sectoraal beter leren kennen en aan de aanscherping van informatielijnen tussen deelnemende organisaties.

Vergelijking met aandachtspunten uit ISIDOOR III (2021)

In de observaties van ISIDOOR III werd opgemerkt dat over de hele breedte van betrokken stakeholders groei werd gezien ten opzichte van ISIDOOR II en van eerdere grotere incidenten. Op basis van ISIDOOR IV kan geconcludeerd worden dat die groei zich na 2021 heeft voortgezet.
De behoefte aan informatie en duiding verschilt tussen organisaties (afhankelijk van eigen capaciteit en expertise) en komt, net als in 2021, ook tijdens ISIDOOR IV niet altijd overeen met de mogelijkheden van het NCSC.
Informatiedeling door het NCSC wordt tijdens ISIDOOR IV beter beoordeeld. Waar na ISIDOOR III ‘vertraagde informatiedeling’ als belemmerende factor wordt aangemerkt, wordt nu benoemd dat meer informatie op een duidelijke manier is gedeeld en meer informatie direct naar getroffen partijen is gegaan. Ook de beperkte mogelijkheid van organisaties om vroegtijdig veilig ruwe informatie uit te wisselen (zoals benoemd tijdens ISIDOOR III) was tijdens ISIDOOR IV geen struikelblok.

Deelnemers geven aan dat het scenario en de mediaomgeving realistisch waren en ervoor zorgden dat iedereen snel helemaal ‘in’ de oefening zat. Wel wordt opgemerkt dat zo’n grote oefening met zo veel partijen veel tijd en capaciteit vergt, zowel in de voorbereiding als tijdens de oefening zelf. Het maken van een eigen script en het (tijdig) op orde hebben van de interne (logistieke) organisatie leverden soms knelpunten op. Dit komt ook deels door het feit dat organisaties de voorbereiding onderschat hebben. Dit gold met name voor de Zilver deelnemers, die niet betrokken waren bij de inhoudelijke voorbereiding van de oefening maar de informatie en berichten uit het scenario gebruikten om een deeloefening binnen de eigen organisatie te organiseren.

Uit de oefening en de evaluatie blijkt dat organisaties en sectoren sinds ISIDOOR III (die plaatsvond in 2021) zijn gegroeid in cyber crisismanagement. Dit is bijvoorbeeld merkbaar op het gebied van het delen en verzamelen van zowel cyber gerelateerde informatie (over de techniek, aard van het probleem etc.) als informatie over de effecten van de cyber crisis (bijvoorbeeld op de (uitval van) vitale dienstverlening en daaruit voortkomende maatschappelijke onrust). Binnen de sectoren wisten partijen elkaar over het algemeen goed te vinden. Verschillende initiatieven om beelden bij elkaar te brengen, zoals Signal-groepen, Operationeel Leider-calls of via een brancheverenigingen droegen bij aan een betere onderlinge afstemming. Het lukte beter dan tijdens ISIDOOR III om een beeld te vormen van de situatie dan tijdens de vorige oefening. Dit past bij het niveau van voorbereiding waarin men nu zit en de ontwikkelingen die organisaties en sectoren hebben doorgemaakt. Waar voorheen de cyber kennis en -preparatie nog in de beginfase stond, zijn plannen en competenties nu vaak beter ontwikkeld. Overkoepelend kan worden geconcludeerd dat organisaties intern alles goed hebben geregeld op het gebied van cyber crisismanagement. Nu is het tijd om met de keten te oefenen. Wel is duidelijk dat er verschillen zijn tussen sectoren. In sommige sectoren bestaan sterke samenwerkingsverbanden en overlegstructuren. In die sectoren weet men elkaar daardoor snel te vinden. In andere sectoren vergt dit nog extra aandacht en ontwikkeling.

Het hoofd-oefendoel van de ISIDOOR oefening was het beoefenen van het LCP-Digitaal. 30% van de organisaties geeft aan dat het LCP-Digitaal de organisatie handvatten heeft gegeven bij de aanpak (of voorbereiding) van de digitale crisis tijdens ISIDOOR. Organisaties die aangeven dat het plan niet heeft

geholpen geven hiervoor onder andere als reden dat het plan te abstract is en te weinig concrete tools en handvatten biedt. Ook wordt door organisaties aangegeven dat het plan niet goed vindbaar is. De reden hiervoor is onduidelijk. Enkele organisaties geven aan dat ze het plan niet kennen.

Uit de vragenlijst blijkt dat tijdens de oefening 20 organisaties een Wbni-melding hebben gedaan. Wat opvalt is dat in werkelijkheid tijdens de oefening maar zeven Wbni-meldingen zijn binnengekomen. Het is achteraf niet met zekerheid vast te stellen waar die discrepantie door komt. Niet alle organisaties die een melding hadden moeten doen, hebben dit ook daadwerkelijk gedaan. Geconcludeerd kan worden dat in de oefening het doen van een Wbni-melding niet voor alle organisaties duidelijk was, zowel inhoudelijk (wanneer wel/niet melden en bekendheid met artikel 10b) als qua proces (hoe doe je een melding).

Zoals gezegd lukte het op beide informatiestromen (cyber gerelateerd (bron) en effect) beter om informatie te delen en te verzamelen, en op basis hiervan een beeld te vormen. Een aandachtspunt in een betere voorbereiding is het stroomlijnen van de informatiestromen vanuit de sectoren en zorgen dat informatie op sectoraal niveau beter samenkomt. De sectorale regie op het bundelen van informatie (zowel over de oorzaak als de impact) moet beter gecoördineerd worden. Op die manier kan het Interdepartementaal Afstemmingsoverleg (IAO) worden voorzien van een compleet en actueel beeld vanuit alle sectoren. De beeldvorming liep nu achter op de actualiteit. In veel sectoren wordt hier ook hard aan gewerkt, maar de aansluiting op de nationale crisisstructuur is onvoldoende. We zien dat de technische informatie en de informatie over de impact twee aparte lijnen volgen: sectorale Computer Emergency Response Teams (CERTS) vertegenwoordigen sectoren en zij hebben een lijn naar het NCSC. Vitale organisaties die getroffen zijn hebben op hun beurt (onder andere) contact met de betreffende veiligheidsregio. De veiligheidsregio's hebben een lijn met het Landelijk Operationeel Coördinatiecentrum (LOCC), het Nationaal CrisisCentrum (NCC) en het Nationaal Kernteam Crisiscommunicatie (NKC). Dit zijn als het ware twee kolommen, die nu pas op een laat moment samenkomen waardoor het complete en actuele beeld pas laat kan worden gevormd.

Met betrekking tot de rol van het NCSC kan worden geconcludeerd dat de deelnemende organisaties het NCSC zien als *de* organisatie die gevalideerde informatie levert tijdens een cyber crisis. Organisaties weten het NCSC te vinden en leveren informatie aan. Organisaties konden informatie en vragen echter niet altijd kwijt. De enorme stroom aan informatie zorgde voor druk op de bereikbaarheid van het NCSC. In vergelijking met eerdere ISIDOOR oefeningen ging dit nu wel veel beter. Het NCSC pakt een duidelijke rol en er is sprake van meer volwassenheid in de coördinerende rol in het cyberstelsel dan in 2021. Dat sommige organisaties meer verwachten heeft ook te maken met de verwachtingen die organisaties hebben van een 'nationaal' Computer Emergency Response Team (CERT). Het is belangrijk om de verwachtingen steeds af te stemmen op de werkelijke rol en vermogens van het NCSC. De verwachtingen die sommige organisaties hadden van het NCSC, sluiten niet aan op de verdeling van taken en verantwoordelijkheden in het cyberstelsel. De verantwoordelijkheid voor cyber veiligheid start bij elke organisatie die een verantwoordelijkheid heeft voor de eigen processen en continuïteit. Hieronder valt ook het kunnen voorzien in de eigen basisbehoefte van cyberveiligheid en het borgen van de 'crisisvolwassenheid' van de eigen organisatie.
Naast dat een organisatie in staat moet zijn een beeld te krijgen van de eigen situatie, bestaat een interdependentie tussen verschillende organisaties om informatie tijdig te delen. Alleen zo kan een werkbaar beeld van de totale situatie ontstaan. Dat kan binnen een sector nodig zijn maar ook voor een beeld dat sectoren overstijgt tot het nationale of internationale niveau. Deze informatiestroom is, voor organisaties zoals het NCSC met verantwoordelijkheden op het nationale niveau, een levensader om het bredere belang te kunnen dienen.

Organisaties geven aan dat de nationale opschaling een 'black box' is. Dit is deels te verklaren door de oefenopzet. Na een IAO is er geen terugkoppeling meer geweest vanuit dit overleg. Dat viel buiten de oefening. Het is wel aan te bevelen hier aandacht voor te houden. Deelnemende partijen zoeken houvast bij een landelijke strategie en duiding. Dat organisaties in de oefening weinig zicht hadden op de nationale opschaling hangt ook samen met het feit dat nationaal sneller opschaalt dan regionaal. Veiligheidsregio's handelen nu (vanuit hun gevolgbestrijdingsrol) vooral op basis van de impact van een cyberverstoring en komen daardoor bij een cybercrisis vaak pas later in actie. Ze zouden daar een nog meer proactieve (signalerende) rol in kunnen gaan spelen en bijvoorbeeld afspraken maken met bedrijven in regio om eerder

meldingen te krijgen als er iets speelt, zodat ze op basis daarvan potentiële impact beter kunnen monitoren. We bedoelen daarmee niet dat veiligheidsregio's een rol hebben in het bestrijden van het cyberincident. Zij kunnen zich op deze manier nog beter richten op de cybergevolgbestrijding. Het is van belang om nog eens goed te bekijken welke partijen een rol kunnen spelen bij het samenbrengen van cyber technische informatie en de impact van de verstoring. Daarmee hangt samen dat, hoewel de aansluiting van partijen als de sectorale CERTS op het digitaal stelsel sterk is verbeterd en bestaan van de partijen zorgt voor een betere afstemming binnen de sectoren, die rollen op verschillende manieren worden ingevuld. De één biedt actief cyberexpertise en monitoring, terwijl de ander alleen informatie verzamelt en deelt. De rolbeschrijvingen voor de verschillende partijen (ISAC's, OKTT's, etc.) kunnen nog beter uitgewerkt worden zodat sprake is van een meer eenduidige rolinvulling en deze partijen vanuit een gedeeld kader opereren en een bepaalde kwaliteitsstandaard kunnen leveren.

Gedurende de oefening kwam in verschillende gremia de vraag op over attributie, ofwel de vraag 'Wie zit hier achter?' De informatie die hier ten aanzien van de statelijke actor werd ingebracht in de oefening, betrof zeer gevoelige informatie uit het buitenland. Dit was bij een beperkt aantal deelnemers bekend. Partijen betrokken bij het onderzoek naar de kwaadwillende actoren, vroegen zich af waarom dit noodzakelijk was om te weten voor andere partijen. Anders gezegd, is er voor andere partijen een 'need to know'? Dit is een reële vraag en we zien hier het belang van beide zijden. Zo zien we aan de ene zijde de noodzaak tot geheimhouding om de acties van een kwaadwillende actor niet negatief te beïnvloeden. Aan de andere zijde zijn de potentiële gevolgen duidelijker als de intentie, motivatie en mogelijkheden van een actor bekend zijn. Ook wil men weten of acties tegen de actor kunnen leiden tot verergeren van de dreiging, stoppen van de aanval, het wegvallen van een dreiging etc. Deze informatie kan mogelijk ook gedeeld worden (voor zover bekend) zonder dat er specifieke informatie over de actor verstrekt hoeft te worden. Het is aan te bevelen om over en weer meer inzicht te krijgen over elkaars processen en belangen.

In de oefening werd de druk geleidelijk opgevoerd waardoor uiteindelijk (de kans op) schaarste van producten en diensten ontstond. Dit roept de vraag op welke organisaties als eerste geholpen moeten worden. De (verdeling van) schaarste is op het hoogste niveau besproken: voorbereid door het IAO en daarna voorgelegd aan de ICCb. In de oefening zijn hiervoor verdringingsreeksen[1] benut. Deze zijn echter individueel voorbereid en niet interdepartementaal besproken. Het opstellen van een standaard of absolute verdringingsreeks is onwenselijk en niet mogelijk. De factoren die bepalen welke sector of vitaal proces belangrijker is dan de ander, zijn in belangrijke mate situatie-afhankelijk (zie bijvoorbeeld ziekenhuizen tijdens de coronapandemie.) Dit vraagt om een scherp afwegingskader met een helder proces er omheen. Samen met een duidelijk beeld en advies vanuit de sectoren, kan het afwegingskader goed worden gevuld en toegepast in de besluitvorming.

2.2 Aanbevelingen

1. Grootschalig oefenen is waardevol gebleken, maar er kleven ook nadelen aan. Zorg voor een passend vervolg op ISIDOOR IV op basis van de ontwikkelingen binnen het cyberstelsel. Overweeg daarbij om een eventuele volgende keer als voorwaarde voor deelname aan organisaties mee te geven dat zij een interne crisisorganisatie hebben waarmee zij geoefend hebben en dat er sectoraal afspraken zijn op het gebied van informatiedeling, communicatielijnen en samenwerking die ook een keer beoefend zijn.

2. Sectoren moeten investeren in informatiedeling en zorgen dat zowel cyber gerelateerde informatie (technisch/inhoudelijk) als informatie over de impact samenkomt en aansluit op landelijke informatiestromen. Hoe de routing precies vormgegeven moet worden is ter nadere beoordeling. Uiteindelijk zal dit moeten leiden tot een beter geïnformeerde nationale crisisstructuur en actueler IAO.

3. Op rijksniveau is er een behoefte aan een scherp afwegingskader met een helder proces er omheen. Gecombineerd met een duidelijk beeld en advies vanuit de sectoren moet dit ertoe leiden dat het afwegingskader goed kan worden gevuld en benut.

[1] Verdringingsreeksen geven de rangorde van maatschappelijke behoeften aan, die bij de verdeling van schaarste in acht wordt genomen.

4. We zien een groot verschil in de mate waarin organisaties zelf zijn voorbereid op cybercrises. Vanuit een perspectief van nationale weerbaarheid zou het goed zijn als die partijen die nu een achterstand hebben prioriteit geven aan hun eigen voorbereiding. Hiermee kan ook het beroep op, en de verwachting van, het NCSC realistischer worden.

5. Werk de rolbeschrijving en werkwijzen van sectorale CERTS, ISAC's, OKTT's, etc. beter uit zodat sprake is van een meer eenduidige rolinvulling en deze partijen vanuit een gedeeld kader opereren en een bepaalde kwaliteitsstandaard kunnen leveren.

6. Zorg dat de bestaande overlegstructuren beter worden benut en eventueel uitgebreid met relevante partners. Dit kan worden bereikt door enerzijds de bekendheid met de bestaande structuur te vergroten en anderzijds te onderzoeken waarin de bestaande structuur op dit moment niet voorziet.

7. Zorg voor meer bekendheid van de Wbni criteria en de meldingsprocedure.

3. OBSERVATIES PER OEFENDOEL

3.1 Informatie-uitwisseling

Onder informatie-uitwisseling verstaan we de manier waarop informatie tussen verschillende partijen wordt verzameld, gevalideerd en gedeeld. Indicatoren[2] hiervoor zijn:

- De organisatie verzamelt informatie over het incident bij ketenpartijen
- De organisatie deelt op snelle en efficiënte wijze informatie over het incident binnen de sector
- De organisatie valideert binnenkomende informatie vanuit de sector
- De organisatie communiceert zelfstandig over de eigen aanpak aan andere partijen binnen de sector
- Er is een gezamenlijk, sectoraal en actueel beeld van de situatie

Overkoepelend kan geconcludeerd worden dat de informatie-uitwisseling tussen partijen tijdens ISIDOOR IV vele malen intensiever was dan tijdens ISIDOOR III (zie verder: *Informatie-uitwisseling binnen de sectoren*, pag. 11). Organisaties zijn beter voorbereid en kennen de route beter. Mede door de ontwikkeling van sectorale CERTS en sectorale oefeningen die plaatsvonden, weten partijen elkaar beter te vinden. Wel blijkt dat er behoefte is aan het formaliseren van informatieprocessen en -middelen. Er is, zeker tijdens een crisis van deze omvang, al snel sprake van (te) veel informatie en van verschillende informatiestromen. Sectoren moeten investeren in informatiedeling en zorgen dat zowel cyber gerelateerde (technisch/inhoudelijk) als informatie over de impact samenkomt en aansluit op landelijke informatiestromen. Uiteindelijk zal dat moeten leiden tot een beter geïnformeerde nationale crisisstructuur en een actueler IAO.

Over het algemeen is de communicatie vanuit het NCSC beter beoordeeld dan tijdens ISIDOOR III. Niet alleen is meer informatie op een duidelijke manier gedeeld, maar ook meer informatie direct naar getroffen partijen gegaan. Dit neemt niet weg dat bij een grootschalige aanval zoals gesimuleerd in ISIDOOR er altijd partijen zullen zijn die onvoldoende bediend of geïnformeerd zijn of die dit zo voelen. Dat vraagt enerzijds om verdere professionalisering van communicatie door het NCSC maar legt ook een verplichting bij alle ontvangende partijen om aan hun kant de verwerking van informatie beter te regelen.

Informatie-uitwisseling algemeen
Van de organisaties die de vragenlijst hebben ingevuld waardeert de meerderheid de informatie-uitwisseling als goed (49%) tot zeer goed (2%). 39% ervaart de informatie-uitwisseling als neutraal en 7% als slecht. Op 2% van de respondenten is deze vraag niet van toepassing.

Op de vraag wat men goed vond aan de informatie-uitwisseling komen de volgende drie punten naar voren:
- de berichtgeving en het handelingsperspectief vanuit het NCSC,
- de goede samenwerking binnen de eigen organisatie en tussen partijen onderling, en
- de echtheid van het technisch portaal en de mediaomgeving.

Veel organisaties waarderen het dat partners erg benaderbaar waren, dat partijen over en weer open en transparant waren en dat informatie snel met elkaar werd gedeeld. De berichten vanuit het NCSC werden als divers, duidelijk en fijn in gebruik ervaren. Het bood organisaties een duidelijk handelingsperspectief.

Wat betreft interne verbeterpunten noemen een aantal organisaties dat zij moeten werken aan hun vergaderstructuur en meer helderheid moeten creëren wat betreft rollen en mandaten. Zij liepen nu tegen verschillende struikelblokken aan, zoals het niet helder hebben hoe de communicatielijnen lopen, onduidelijkheid over taken en rollen en een chaotische interne overlegstructuur. Dit hinderde hen in het goed kunnen uitwisselen van informatie omdat belangrijke informatie (zowel over de oorzaak als over de effecten van de verstoring) werd gemist, op de verkeerde plek binnenkwam en zo niet tijdig kon worden geïnterpreteerd. Ook geven meerdere organisaties aan dat er betere coördinatie en afstemming mag komen tussen de partijen binnen een sector. Hoe wil je elkaar benaderen? En wanneer? En wie zijn de contactpersonen van elke organisatie? Ondanks dat er een deelnemerslijst was, was het niet altijd duidelijk welke persoon/functie gecontacteerd diende te worden. Dit is een intern leerpunt voor organisaties. Daarnaast blijkt uit de evaluatie dat informatie-uitwisseling soms lastig was doordat een aantal sleutelfiguren/stakeholders niet mee deden aan de oefening waardoor een belangrijke schakel werd gemist en het lastig was om goed te oefenen in de keten.

[2] Bij de uitwerking van de oefendoelen is ervoor gekozen aan te sluiten bij de meest relevante uitkomsten van de vragenlijst, gesprekken en evaluatie-ochtend. De indicatoren komen daardoor niet allemaal expliciet terug in de tussenkopjes.

Informatie-uitwisseling binnen de sectoren
Binnen alle sectoren heeft informatie-uitwisseling plaatsgevonden. Er werd actief gezocht naar informatie. Informatie die mogelijk relevant zou kunnen zijn voor andere partijen, zoals analyses en mogelijke oplossingen, werd proactief gedeeld. Deelnemers geven aan dat er op verschillende manieren informatie is uitgewisseld, zowel via bestaande processen en structuren (zoals de CISO-raad[3], Operationeel Leiders (OL)-call, Information Sharing & Analysis Centers (ISACs), het Landelijk Crisis Management Systeem (LCMS) en het Nationaal Continuïteitsoverleg Telecommunicatie (NCO-T)) als via nieuwe initiatieven (zoals het Teams-kanaal voor CISO's van getroffen gemeenten). Als kanttekening bij de overleggen binnen de sectoren wordt aangegeven dat deze overleggen soms structuur misten. Zo werd er niet altijd een standaard agenda gehanteerd en misten sommige partijen een informatiemanagement-omgeving. Nu werd bijvoorbeeld veel informatie gedeeld via chatomgevingen waardoor structuur ontbrak en informatie verloren kon gaan. Daarnaast is het, zeker bij een crisis van deze omvang waarbij veel verschillende partijen en organisaties betrokken zijn, belangrijk om afspraken te maken met betrekking tot informatie-uitwisseling. Welke informatie wordt gebracht? Via welke kanalen en wie heeft daar welke verantwoordelijkheid? Verschillende sectoren geven aan dat er behoefte is aan informatiedeling. Het ontbreekt soms echter nog aan een duidelijk proces en aan middelen om dit goed vorm te geven.

Op de vraag of de informatie-uitwisseling met andere partijen hielp bij het bestrijden van de crisis, geeft iets meer dan de helft van de respondenten (51%) aan dat zij dit inderdaad zo hebben ervaren. 36% geeft aan dat dit hen deels heeft geholpen in het bestrijden van de crisis. Een kleine groep (7%) geeft aan dat de informatie-uitwisseling met andere partijen niet heeft bijgedragen. Op 6% van de respondenten was deze vraag niet van toepassing.

Organisaties die aangeven dat het uitwisselen van informatie hen hielp met het bestrijden van de crisis, geven aan dan dit met name komt doordat dit bijdroeg aan de beeld- en besluitvorming. De informatie-uitwisseling hielp bij de duiding van de impact en ernst van de situatie en om zicht te krijgen op eventuele keteneffecten (de mogelijke gevolgen van de situatie voor bepaalde organisaties konden impact hebben op de continuïteit van andere partijen). Ook hielp het organisaties een beter inzicht te krijgen in het probleem dat voor hen lag en in de zoektocht naar welke systemen geïnfecteerd konden zijn. Het uitwisselen van informatie met andere partijen werd ten slotte als positief ervaren doordat het de eigen besluitvorming ondersteunde, de genomen acties bevestigde of discussies startte over het nemen van vervolgacties.

De 7% van organisaties die aangaven dat informatie-uitwisseling weinig tot geen impact heeft gehad in het bestrijden van de crisis, geven daar uiteenlopende redenen voor. Enkele organisaties noemen slechte bereikbaarheid van partners als een reden dat informatie-uitwisseling niet tot nauwelijks mogelijk is geweest. Sommige organisaties vonden dat informatie-uitwisseling beter gestimuleerd had mogen worden, anderen gaven juist aan dat hun organisatie de interne crisis boven contact met anderen partijen prioriteerde.

Informatie-uitwisseling met het NCSC
Op de vraag of de organisatie wist waar ze gevalideerde informatie over het incident kon halen heeft 64% van de organisaties 'ja' geantwoord en 34% 'deels'. Het NCSC wordt hierbij het meest genoemd als partij waar gevalideerde informatie werd gehaald over zowel de oorzaak als mogelijke oplossingen (handelingsperspectief).

Een les van ISIDOOR III was dat het NCSC voldoende capaciteit moet hebben in geval van een crisis met brede impact. Naar aanleiding hiervan is de capaciteit tijdens ISIDOOR IV uitgebreid.[4] Tijdens ISIDOOR IV is door veel partijen contact opgenomen met het NCSC. Het merendeel geeft aan tevreden te zijn over dit contact.
Uit de vragenlijst blijkt dat het grootste gedeelte van de organisaties (75%) tijdens de oefening minstens één keer contact heeft gehad met het NCSC. Daarvan heeft 27% meer dan vijf keer contact gehad.

[3] Interdepartementale adviesraad, bestaande uit de CISO's van de verschillende departementen, voorgezeten door de CISO-Rijk.
[4] Er is door het NCSC met een nieuwe werkwijze gewerkt. Deze is beproefd tijdens ISIDOOR IV en positief gewaardeerd. Over de permanente realisatie en borging hiervan in de dagelijkse praktijk moet nog besluitvorming plaatsvinden.

De meest toegevoegde waarde van het contact met het NCSC zat voor organisaties in het verkrijgen van informatie over de aard/ernst van de dreiging (70%) en in het verkrijgen van advies over hoe te handelen (61%). Door 26% van de organisaties wordt het verkrijgen van informatie over de verdachte(n) achter de dreiging/het incident als toegevoegde waarde van het contact met het NCSC genoemd.

Daarnaast wordt benoemd dat de overzichten van het NCSC vooral een samenvatting vormden van wat er gebeurde in de buitenwereld en een soort controlefunctie hadden voor de maatregelen die organisaties hadden getroffen: sluiten deze aan bij de adviezen die het NCSC geeft of zien we iets over het hoofd?

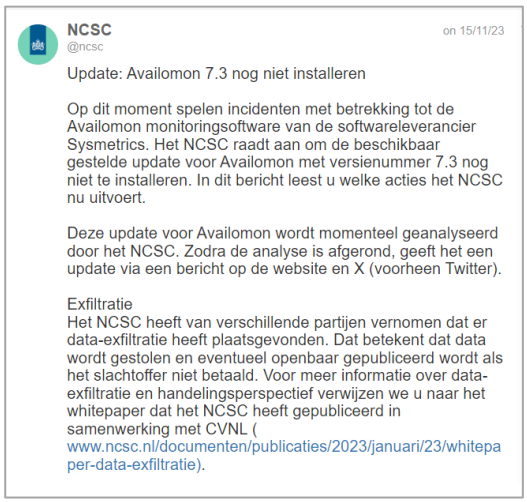

Fig. 1: Bericht van het NCSC verzonden tijdens de oefening, ter illustratie

Als kanalen voor informatie-uitwisseling wordt onder andere Mattermost genoemd. Men vindt dit een nuttig kanaal waar veel gebruik van wordt gemaakt. Omdat iedereen hier informatie op kan delen (die niet altijd geverifieerd is) wordt aangegeven dat men scherp moet blijven op ruis en (mogelijk) onjuiste informatie.

Gedeeld beeld

Dat er regelmatig informatie werd uitgewisseld betekent niet automatisch dat er ook sprake was van een gedeeld beeld binnen de sectoren. Onder een gedeeld beeld verstaan we een overkoepelend beeld van de situatie waarin technische informatie, cyber gerelateerde informatie en informatie over de effecten en de impact bij elkaar komen. Wat opvalt is dat de mate waarin het is gelukt om tot een gedeeld beeld te komen tussen de sectoren verschilt. De financiële sector heeft hier een positief beeld bij (onder andere door een goede werking van het Tripartiet Crisismanagement Operationeel, het TCO). Binnen de drinkwatersector werd het sectorbeeld gevormd door Vewin en doorgegeven aan het NCSC. Andere sectoren geven aan dat het maar beperkt is gelukt om tot een actueel gedeeld beeld van de situatie te komen, onder andere doordat het onduidelijk is waar alle beelden gekoppeld moeten worden. In de oefening was het onduidelijk waar partijen heen konden met hun informatie over de impact van alle gebeurtenissen teneinde het landelijk beeld compleet te maken. Idealiter gebeurt dat via de veiligheidsregio's en het Landelijk Crisis Management Systeem (LCMS) richting het Landelijk Operationeel Coördinatiecentrum (LOCC). Dat betreft echter alleen de impact op vitale voorzieningen en geeft geen compleet beeld waarin zowel de cyber gerelateerde problemen, leveringsproblemen en maatschappelijke impact samenkomen. Het NCC is uiteindelijk verantwoordelijk voor het nationale beeld ten behoeve van het IAO, waarin zowel oorzaak als impact samenkomen. Tijdens de oefening bleek dat deze beelden nog onvoldoende samen worden gebracht tot één product.

Sectoren geven aan een landelijk beeld en een beeld van andere sectoren (en mogelijke keteneffecten) te hebben gemist. Sectorale Computer Emergency Response Teams (CERTS) vertegenwoordigen sectoren, zij hebben een lijn naar het NCSC. Vitale organisaties die getroffen zijn hebben op hun beurt (onder andere) contact met de betreffende veiligheidsregio of in een aantal gevallen direct met hun DCC (denk aan de financiële sector en organisaties met een systeemverantwoordelijkheid). De veiligheidsregio's hebben een lijn met het Landelijk Operationeel Coördinatiecentrum (LOCC), het Nationaal CrisisCentrum (NCC) en het Nationaal Kernteam Crisiscommunicatie (NKC). Dit zijn als het ware twee kolommen. Alle informatie (technisch, cyber gerelateerd, operationeel en over de impact) komt nu pas samen op rijksniveau, tijdens het IAO, terwijl deze beelden op sectoraal niveau al gekoppeld zouden moeten zijn. Er is op dit moment echter geen logische plek waar dit gebeurt. Een mogelijkheid zijn de Departementale Coördinatie Centra (DCC's) maar uit de oefening blijkt dat hier informatiedeling niet op zo'n manier plaatsvindt dat hier overkoepelende sectorale beelden ontstaan. Wanneer op sectoraal niveau geen compleet beeld kan worden gemaakt, zal dat ook op nationaal niveau onmogelijk blijken. Daarnaast liep de beeldvorming in het IAO nu achter op de actualiteit. Zo was een deel van de aanvallen, waaronder het wissen van de systemen en daarmee de ernst van de situatie, niet volledig inzichtelijk.

3.2 Samenwerking

Onder samenwerking verstaan we de functionele interactie tussen vitale organisaties en rijksoverheidsorganisaties. Indicatoren hiervan zijn:

- De organisatie heeft een goed beeld van alle betrokken ketenpartijen bij het incident en hun rol en verantwoordelijkheid
- De organisatie heeft inzicht in het eigen sectorale relatienetwerk en weet elkaar daar te vinden
- De organisatie stemt de eigen aanpak af met die van andere partijen binnen de sector
- De organisatie schakelt expertise in van andere partijen binnen de sector wanneer nodig
- De organisatie formuleert een duidelijke behoefte aan ondersteuning van NCSC en NCTV

Er heeft op verschillende manieren samenwerking plaatsgevonden tussen organisaties en binnen sectoren. De samenwerking en onderlinge afstemming worden over het algemeen als zeer positief beoordeeld. Wel wordt hierbij, net als bij informatie-uitwisseling, de kanttekening geplaatst dat dit soms ad-hoc en ongestructureerd plaatsvond. Het formaliseren van afstemming en samenwerking en het vastleggen van een structuur en procedures die hiervoor gebruikt worden bespaart tijd en zorgt voor duidelijkheid.
De ervaringen met de samenwerking met het NCSC zijn over het algemeen zeer positief. Wat opvalt is dat er een verschil in verwachtingen zit tussen partijen met een hoog (cyber)crisis volwassenheidsniveau en organisaties die hierin nog minder ver zijn. Partijen die hierin wat minder ver zijn verwachten meer en sneller informatie van het NCSC terwijl het NCSC in de praktijk die informatie ook nog niet heeft. Het NCSC doet twee dingen met binnengekomen informatie: valideren en verrijken. Het vinden van een juiste balans tussen zorgvuldigheid en snelheid is hierbij uitdagend en mede afhankelijk van de situatie.

Samenwerking binnen de sector[5]
65% (van de 79 organisaties op wie samenwerken van toepassing was) van de organisaties werkte tijdens de oefening samen met andere partijen binnen de sector. Dit was rechtsreeks of bijvoorbeeld via een CSIRT, een OKTT of een ISAC. Organisaties maken daarnaast gebruikt van sectorale overlegorganen zoals de OL-call in de algemene kolom, het TCO (inclusief Advies en Consultatiegroepen) in de financiële sector, de Domeinraad van Netbeheer Nederland, Platform crisisbeheersing Waterschappen Midden Nederland, CERT-WM, Unie van Waterschappen en het NCO-T. Andere gremia waarmee organisaties hebben samengewerkt om de crisis te bestrijden zijn onder andere: ministeries, DCC's, DIVD, NKC, NCC (algemene kolom), de CISO-raad (departementen) en FERM (Rotterdamse haven).

43% van de organisaties waardeert de afstemming binnen de sector als goed en 4% als zeer goed. Sectorpartijen hebben elkaar goed kunnen vinden en waren doordrongen van nut en noodzaak voor sectorale afstemming en samenwerking. Organisaties geven aan dat gezamenlijk informatie is geanalyseerd en vertaald naar maatregelen. Overleggen hebben binnen de sector plaatsgevonden volgens de daarvoor afgesproken structuur zoals het TCO en het NCO-T.

26% van de partijen beoordeelt de afstemming neutraal. Als verklaring hiervoor wordt gegeven dat de afstemming informeel en ad hoc was, en afhing van personen (bijvoorbeeld wie initiatief neemt). Men weet elkaar uiteindelijk te vinden (en dan gaat de samenwerking goed) maar structuur en procedures ontbreken. Dit vergt nog verdere formalisering van afspraken. Ook wordt benoemd dat in het contact vooral het beeld werd gedeeld (informatief) maar dat er niet echt werd afgestemd. Zo wordt door de gemeenten aangegeven dat zeker gemeenten binnen dezelfde veiligheidsregio nog wat beter kunnen samenwerken door actiever af te stemmen en elkaar te informeren over impactvolle besluiten.

De partijen die de samenwerking binnen de sector als slecht beoordelen (15%) geven daarbij als redenen dat er geen totaaloverzicht was en er gefragmenteerd werd gewerkt, het voorzitterschap van de sector overleggen beter kon en de crisisorganisatie intern gericht was. Soms had het gebrek aan afstemming te maken met een beperkt aantal sectorale deelnemers, het ontbreken van een bepaalde schakel in de afstemming of het uiteenlopen van oefenscenario's.

[5] Voor de leesbaarheid van deze paragraaf hebben we de voluit geschreven versies van alle afkortingen opgenomen in een voetnoot: Computer Security Incident Response Team (CSIRT), een organisatie die 'objectief kenbaar tot taak' heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerken informatiesystemen (OKTT), Information Sharing & Analysis Center (ISAC), CERT Watermanagement (CERT-WM), Dutch Institute for Vulnerability Disclosure (DIVD).

Wel merken organisaties op dat de sectorale samenwerking over de drie dagen heen sterk is verbeterd, waarbij wordt benoemd dat de sector op dag 3 in staat was een gezamenlijk situationeel beeld, inclusief knelpunten, prioriteiten en oplosrichtingen, te vormen.

Een aantal keer wordt de kracht van community's genoemd: informele netwerken die hun bijdrage leveren ('community of trust'). Tijdens ISIDOOR III was hiervan minder sprake, maar tijdens ISIDOOR IV kwam het sterker naar voren. Vooral in de cyberrespons hebben die een belangrijke functie. Het zijn vaak de experts die hier (vertrouwelijke) kennis en informatie delen. Het gaat hierbij ook om het durven zeggen dat er kwetsbaarheden zijn en dat gaat vaak alleen in kleine setting. De kanalen waarlangs informatie gedeeld wordt zijn gesloten voor de 'niet-experts' en de duiding van informatie is niet gecentraliseerd. De community's zijn daarnaast niet altijd aangesloten op de reguliere informatielijnen. Het is mooi dat deze community's of trust er zijn want ze kunnen waarde hebben tijdens een crisis. Het NCSC zal zich hierbij wel moeten afvragen in hoeverre ze zicht wil blijven houden op de waarde van informatie die gedeeld wordt binnen community's en de vertrouwelijkheid en betrouwbaarheid van informatie.

Samenwerking met het NCSC
Van de organisaties waarop samenwerking met het NCSC van toepassing was, waardeert het grootste gedeelte samenwerking als goed of zeer goed (respectievelijk 46% en 12%). 30% van de organisaties is neutraal over de samenwerking en 12% beoordeelt deze als slecht.

Als positieve punten in de samenwerking benoemen partijen dat het NCSC tijdige en goede informatie verstrekt, waaronder meldingen over kwetsbaarheden, aanwijzingen om de aanwezigheid van een specifieke dreiging binnen het netwerk op te sporen (oftewel *Indicators of Compromise,* IoC's) en andere technische informatie. De aanwezigheid van het NCSC in gezamenlijke overleggen (zoals de OL-call) wordt gewaardeerd omdat op die manier rechtstreeks informatie kan worden uitgewisseld en geverifieerd.

Een ander aandachtspunt dat door partijen wordt benoemd is dat, ondanks dat dit veel beter ging dan tijdens eerdere ISIDOOR oefeningen, het NCSC niet altijd goed bereikbaar was en niet (of niet tijdig) reageerde op individuele informatieverzoeken. Daarnaast wordt door organisaties genoemd dat zij doelgroepberichten laat ontvingen omdat er door een technische oorzaak vertraging zat in het ontvangen van het bericht. Daarnaast hadden enkele organisaties op momenten sneller en meer proactief een handelingsperspectief verwacht vanuit het NCSC (bijvoorbeeld toen duidelijk werd dat er iets mis was met de oplossing die geboden werd door de leverancier) en een meer coördinerende en sturende rol. Dit heeft onder andere te maken met verkeerde verwachtingen of met de eigen crisisvolwassenheid van organisaties. In vergelijking met eerdere ISIDOOR oefeningen pakte het NCSC een duidelijke rol en was sprake van meer volwassenheid in de coördinerende rol in het cyberstelsel dan in 2021. Dat sommige organisaties meer verwachten heeft ook te maken met de verwachtingen die organisaties hebben van een 'nationaal' Computer Emergency Response Team (CERT). De verwachtingen die sommige organisaties hadden van het NCSC, sluiten niet aan op de verdeling van taken en verantwoordelijkheden in het cyberstelsel. Het is belangrijk om de verwachtingen steeds af te stemmen op de werkelijke rol en vermogens van het NCSC. De verantwoordelijkheid voor cyber veiligheid start bij elke organisatie die een verantwoordelijkheid heeft voor de eigen processen en continuïteit. Hieronder valt ook het kunnen voorzien in de eigen basisbehoefte van cyberveiligheid en het borgen van de 'crisisvolwassenheid' van de eigen organisatie.
Ook hier valt op dat in de reacties van partijen een onderscheid te maken is tussen partijen met een hoog (cyber)crisis volwassenheidsniveau en organisaties die hierin nog minder ver zijn en hoe zij berichten van het NCSC ontvangen, verwerken en benutten. Partijen met een lager (cyber)crisis volwassenheidsniveau verwachten meer en sneller informatie van het NCSC terwijl het NCSC in de praktijk die informatie ook nog niet heeft.

Naast dat een organisatie in staat moet zijn een beeld te krijgen van de eigen situatie, bestaat een interdependentie tussen verschillende organisaties om informatie tijdig te delen. Alleen zo kan een werkbaar beeld van de totale situatie ontstaan. Dat kan binnen een sector nodig zijn maar ook voor een beeld dat sectoren overstijgt tot het nationale of internationale niveau. Deze informatiestroom is, voor organisaties zoals het NCSC met verantwoordelijkheden op het nationale niveau, een levensader om het bredere belang te kunnen dienen. Via onder andere de relatiemanagers en doelgroepberichten heeft het NCSC vragen gesteld om zicht te krijgen op wat er speelde binnen organisaties en in sectoren. Met name in het begin was de respons hierop laag waardoor het NCSC moeite had de situatie te duiden en adviezen te formuleren. Het NCSC is op dit punt afhankelijk van de input van sectoren om vervolgens deze sectoren weer goed te kunnen

voorzien van de nodige informatie/situationeel beeld. Hiermee hangt samen dat het vormgeven van de aansluiting van de algemene kolom (gemeenten, veiligheidsregio's) op het nationale niveau een aandachtspunt is. Er is een OL-call maar die vervangt niet het informeren van en afstemmen met de voorzitters van de veiligheidsregio's en het Veiligheidsberaad. Daarnaast zijn er nog de CISO-lijn en de gemeentelijke lijn. Duidelijk in kaart brengen wie vanuit het cyberstelsel contact onderhoudt met welke functionarissen, vertegenwoordigers en/of overleggremia van de algemene kolom kan de samenwerking versterken.

Het TCO wordt genoemd als *best practice*. Voor het NCSC is het voordeel van het TCO dat de relatiemanagers van het NCSC op één plek een beeld van de sector kunnen ophalen en goede updates van organisaties krijgen. Tijdens het TCO stellen organisaties elkaar vragen en hebben ze een gesprek over oplossingen en impact.

3.3 Opschaling en besluitvorming

Onder opschaling en besluitvorming verstaan we het activeren van de relevante crisisteams en de manier waarop besluiten worden genomen, gedeeld en opgevolgd. Indicatoren hiervan zijn:

- De organisatie schaalt haar eigen crisisorganisatie op, passend bij de aard en de ernst van het incident
- De opschaling van de organisatie sluit aan bij de opschaling in de sector
- De organisatie geeft op efficiënte wijze leiding aan de crisis
- De organisatie vormt een oordeel over de situatie en de (mogelijk) consequenties, om vervolgens een weloverwogen besluit te nemen.
- De organisatie heeft kritieke momenten en besluiten in beeld
- De organisatie hanteert duidelijke doelen en uitgangspunten voor de crisisaanpak

Besluitvorming
Bij het nemen van lastige besluiten of het omgaan met dilemma's helpt het om als crisisteam te werken met uitgangspunten en leidende principes. Deze geven richting aan de crisismanagementaanpak. 81% van de organisaties geeft aan tijdens de oefening gebruik te hebben gemaakt van uitgangspunten en leidende principes, zoals 'veiligheid (van cliënten, medewerkers, klanten, etc.) staat voorop', 'continuïteit van dienstverlening/hulpverlening/organisatie waarborgen' en 'integriteit van data is leidend'. 16% heeft dit niet gedaan en voor 3% was het niet van toepassing. Organisaties die geen gebruik hebben gemaakt van uitgangspunten geven aan dit een volgende keer wel te willen doen en deze in de koude fase (de fase waarin er geen crisis is) - eventueel samen met ketenpartners - te willen voorbereiden zodat ze er tijdens een crisis gemakkelijk bij gepakt kunnen worden.

Op de vraag wat goed ging met betrekking tot de besluitvorming geven organisaties aan:

- het gebruik maken van vooraf opgestelde scenario's en het volgen van ingerichte processen en structuren (zoals de Beeldvorming, Oordeelsvorming, Besluitvorming-structuur (BOB-structuur);
- het valideren van informatie op basis waarvan besluiten werden genomen (door bijvoorbeeld Security Operations Center (SOC)-analisten);
- het expliciet meewegen van de impact van besluiten op burgers en ketenpartners in de besluitvorming en het stilstaan bij de vraag of een maatregel niet meer schade berokkent dan de oorzaak;
- en het betrekken van de juiste expertise.

Als individuele verbeterpunten op het gebied van besluitvorming wordt onder andere genoemd:

- Mandatering: er is duidelijkheid nodig over 'wie binnen de organisatie kan in geval van een cybercrisis waarover een besluit nemen?'
- Snelheid: een aantal besluiten duurden vrij lang. Als verbeterpunt wordt genoemd het vooraf vastleggen van een aantal voorspelbare besluiten, bijvoorbeeld in een uitgewerkt scenario.
- Bekendheid met gehanteerde procedures en werkwijzen, het maken van vlieguren als crisisteam (bijvoorbeeld door oefeningen, en dan specifieke cyberoefeningen) en het updaten/doorontwikkelen van plannen en draaiboeken.
- Aandacht voor overkoepelende regie en besluitvorming op strategisch niveau. De operationele besluitvorming verliep snel en soepel, onder andere door de duidelijke processen die hiervoor zijn ingebouwd.

Nationale opschaling
Met betrekking tot de nationale opschaling geeft ongeveer de helft van de organisaties (47%) aan dat zij iets hebben meegekregen van de nationale opschaling. 53% van de organisaties geeft aan dit niet te hebben meegekregen. 77% van de organisaties geeft aan van mening te zijn dat de gehele (sectorale en nationale) opschaling paste bij de aard en de ernst van de crisis. 4% geeft aan het hier niet mee eens te zijn en 12% is het hier deels mee eens.

Uit de vragenlijst blijkt dat wat er op landelijk niveau gebeurde tijdens de ISIDOOR oefening voor een deel van de betrokken partijen een black-box was. Diverse partijen geven aan niet gemerkt te hebben dat er sprake was van een nationale opschaling van de crisisstructuur. Dit is deels te wijten aan de oefenopzet: de oefening eindigde na het tweede IAO. Daardoor vond geen terugkoppeling plaats vanuit dit tweede IAO (en de latere ICCb) en is de nationale opschaling niet echt zichtbaar geworden voor partijen die normaal aanwijzingen zouden ontvangen vanuit de ICCb. Deelnemende partijen zoeken houvast bij een landelijke strategie en duiding dus het is belangrijk hier aandacht voor te hebben. Ook is dit voor organisaties van belang voor het eigen situationeel bewustzijn en beeldvorming.

Dat er weinig zicht was op de nationale opschaling hangt ook samen met het feit dat, in een scenario zoals tijdens ISIDOOR IV, nationaal sneller opschaalt dan regionaal. Veiligheidsregio's handelen nu vanuit hun gevolgbestrijdingsrol vooral op basis van de impact van een cyberverstoring en komen daardoor bij een cybercrisis vaak pas later in actie. OL-calls en andere overleggen zijn wanneer sprake is van nationale opschaling normaliter wederkerig ingestoken; er wordt verteld wat in de nationale opschaling plaatsvindt waarna gevraagd wordt aan de veiligheidsregio's om het eigen beeld te delen. Maar als zij nog niet opgeschaald zijn omdat er geen gevolgeffecten merkbaar zijn, hebben ze geen zicht op kwetsbare of getroffen aanbieders in de regio, tenzij die zich proactief melden. Veiligheidsregio's zouden daar een nog proactievere (signalerende) rol in kunnen gaan spelen en bijvoorbeeld afspraken maken met bedrijven in regio om eerder meldingen te krijgen als er iets speelt, zodat ze op basis daarvan potentiële impact beter kunnen monitoren. We bedoelen daarmee niet dat veiligheidsregio's een rol hebben in het bestrijden van het cyberincident. Zij kunnen zich op deze manier nog beter richten op de cybergevolgbestrijding. VR ISAC heeft hiervan tijdens de oefening een mooi voorbeeld gegeven door schematisch de impact per regio en per sector in kaart te brengen. Dit schema was niet volledig ingevuld en is niet breder gedeeld met andere partijen. Het zou mooi zijn om dit verder te ontwikkelen en te kijken hoe dit een plek kan krijgen, als aanvulling op de bestaande verantwoordelijkheden voor het in beeld brengen van de impact van het LOCC, NCC en DCC's en ter ondersteuning van de beeldvorming in het IAO.

Wbni-melding[6] / aangifte
Tijdens de oefening heeft 24% van de organisaties een Wbni-melding gedaan. 59% heeft geen melding gedaan en op 17% van de organisaties was dit niet van toepassing. Organisaties geven voor het doen van een Wbni-melding onder andere de volgende redenen: het overschrijden van de afgesproken drempelwaarde en het (tijdelijk) stilleggen van vitale dienstverlening door een security incident. Ook organisaties die hiertoe niet verplicht zijn hebben een Wbni-melding gedaan omdat het een ernstig incident betrof. Daarnaast hebben enkele organisaties wel een vooraankondiging gedaan maar geen officiële melding. Wat opvalt is dat 24% (20 organisaties) in de vragenlijst aangeeft een melding te hebben gedaan, terwijl in werkelijkheid zeven meldingen zijn binnengekomen. Het is achteraf niet met zekerheid vast te stellen waar die discrepantie door komt.

Als redenen om geen melding te doen geven organisaties onder andere aan: geen verplichting om dit te doen (organisatie valt niet onder de Wbni/is geen vitale aanbieder), geen daadwerkelijke overschrijding van de drempelwaarde, onduidelijkheid over of werd voldaan aan de criteria en onbekendheid met de meldprocedure Wbni.
Uit de analyse van deze redenen blijkt dat niet alle organisaties weten dat ze een vitale aanbieder zijn volgens de Wbni en het besluit en dus een meldingsplicht kunnen hebben. Daarnaast geven sommige organisaties aan dat de drempelwaarde niet is bereikt omdat er geen daadwerkelijke gevolgen zijn of verstoringen niet zijn vastgesteld. Het lijkt erop dat niet alle organisaties bekend zijn met artikel 10b van de Wbni. Dit artikel

[6] De Wet beveiliging netwerk- en informatiesystemen (Wbni) geldt sinds 9 november 2018 en is er op gericht om de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen. De Wbni verplicht aanbieders van essentiële diensten en digitale dienstverleners om maatregelen te nemen om hun ICT te beveiligen tegen incidenten. Voor ernstige incidenten geldt een meldplicht. De Wbni geldt voor de rijksoverheid, voor vitale aanbieders en voor digitale dienstverleners (online marktplaatsen, clouddiensten, zoekmachines).

geeft namelijk een ruimer begrip voor melden als bedreiging van continuïteit nog geen gegeven is (‘een inbreuk […] die ‘ aanzienlijke gevolgen *kan* hebben’).

Geconcludeerd kan worden dat in de oefening het doen van een Wbni-melding niet voor alle organisaties duidelijk was, zowel inhoudelijk (wanneer wel/niet melden en bekendheid met artikel 10b) als qua proces (hoe doe je een melding).

Iets meer dan de helft van de organisaties (51%) heeft besloten aangifte te doen. 31% heeft dit niet gedaan en voor 18% van de organisaties was dit niet van toepassing.

3.4 Crisiscommunicatie

Tijdens de oefening werd gebruik gemaakt van een interactieve mediaomgeving waarin de oefenstaf berichten plaatste en organisaties zelf berichten konden plaatsen.

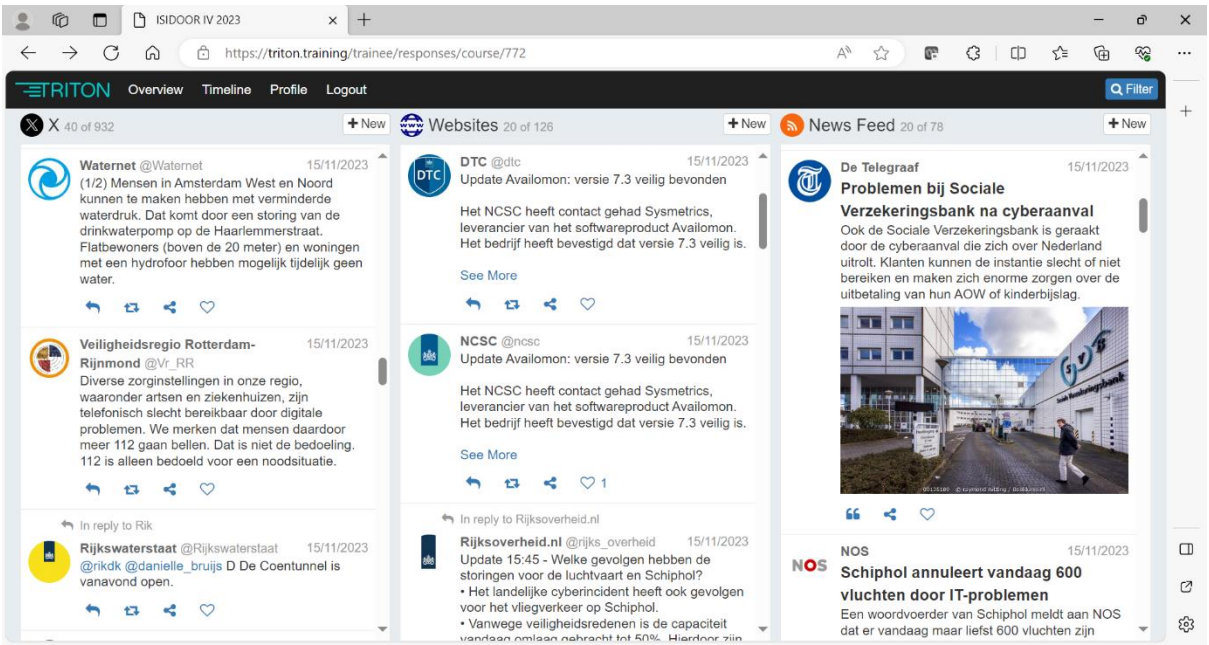

Fig.2: screenshot van de mediaomgeving tijdens de oefening

59% van de organisaties communiceerde zelf over het incident in de media. 34% deed dit niet, en 7% communiceerde deels zelf in de media. Meer dan de helft van de organisaties (55%) stemde de communicatie af met stelselpartijen of sectorale partijen. Zo is publieksinformatie afgestemd met het NKC, vonden woordvoerdersoverleggen plaats binnen sectoren en vond afstemming plaats met brancheorganisaties. 31% stemde de communicatie niet af en 13% deels.

Partijen beoordelen de communicatie vanuit het NCSC en NKC beter dan tijdens ISIDOOR III. Dit zat met name in het feit dat de vorige keer met name procesinformatie werd gedeeld (‘er is iets aan de hand en we zijn ermee bezig’) en dat er deze keer meer aandacht was voor het handelingsperspectief en de samenwerking (‘wat is er aan de hand, we zijn er mee bezig, we zijn aan het samenwerken.’) Ook waren de omgevingsanalyses kwalitatief goed.

In ISIDOOR I, II en III was er meer terughoudendheid in het communiceren over een cyberaanval. Dat was nu minder. Organisaties waren open en transparant over dat zij getroffen waren door een cyberaanval. Dit zegt iets over de tijdsgeest waarin cyberdreigingen en -aanvallen steeds meer aan de orde van de dag zijn en over de ontwikkeling dat cyber veel meer onderdeel geworden is van crisismanagement.

Wat opvalt zijn de verschillen in communicatie tussen organisaties. Er waren partijen die niks communiceerden (en dit bewust deden), er waren partijen die heel erg op hoofdlijnen bleven en partijen die er bovenop zaten, er meer van wisten en duidelijk communiceerden.

Een ander opvallend punt is dat partijen weinig aan elkaar refereerden en het met name bij zichzelf hielden. Aan de ene kant is dat logisch omdat organisaties communiceren over hun eigen impact en richting hun eigen doelgroep, maar aan de andere kant ondervindt bijna het hele land op de een of andere manier impact en voelt het vreemd als daar niet op wordt ingegaan in de communicatie uitingen. Sommige DCC's hebben een rol gespeeld in sectorale communicatie, maar de meesten niet. Het kan van meerwaarde zijn om hier de lijntjes bij elkaar te brengen en een breder beeld (inclusief duiding) naar buiten te communiceren. Dit helpt ook richting het NKC wanneer dat wordt opgeschaald omdat de informatie completer in het NKC kan worden ingebracht. Het is op dit moment voor het NKC niet mogelijk om een compleet, landelijk beeld te geven.

3.5 Landelijk Crisisplan Digitaal

Het hoofd-oefendoel van de ISIDOOR oefening was het beoefenen van het LCP-Digitaal. Op de vraag of het LCP-Digitaal de organisatie handvatten heeft gegeven bij de aanpak (of voorbereiding) van de digitale crisis tijdens ISIDOOR heeft 30% van de organisaties 'ja' geantwoord. 30% van de organisaties heeft geantwoord dat de organisatie onvoldoende kennis heeft van het plan. 17% van de organisaties geeft aan dat het plan niet heeft geholpen en voor 23% was het niet van toepassing.
Specifieke handvatten uit het LCP-Digitaal die worden genoemd zijn de netwerkkaart, informatie over meldpunten en opschalen, sleutelbesluiten, inzicht in de structuur en hoe bepaalde processen/ (communicatie)lijnen lopen en de beschrijving van de rollen en verantwoordelijkheden van de verschillende betrokken partijen. Ook is het LCP-Digitaal gebruikt in de voorbereiding en heeft het gezorgd voor het opfrissen van kennis. Daarnaast geven organisaties aan dat eigen crisisplannen en -handboeken zijn afgestemd/gebaseerd op het LCP-Digitaal en dat daarmee de lijnen zoals vastgesteld in het LCP-Digitaal dus ook worden gehanteerd. Organisaties die aangeven dat het plan niet heeft geholpen geven hiervoor onder andere als reden dat het plan te abstract is en te weinig concrete tools en handvatten biedt. Ook wordt door enkele organisaties aangegeven dat het plan niet goed vindbaar is. De reden hiervoor is onduidelijk, het plan is online makkelijk vindbaar.

Organisaties geven de volgende suggesties voor verbetering van het LCP-Digitaal:
- Een beknopte samenvatting/factsheet van het plan (bijvoorbeeld om mee te nemen in interne opleidingen en trainingen op het gebied van cyber-crisismanagement).
- Ontwikkelen van een beslistool met een scherp afwegingskader en heldere procesbeschrijving voor het gebruik.
- Meer aandacht voor operationele technologie (OT) systemen en processen.
- VR-ISAC opnemen in het Landelijk Dekkend Stelsel.
- Een meer heldere taakverdeling en -omschrijving van het LOCC i.r.t. het NCC.
- Concreter uitwerken hoe de veiligheidsregio's aansluiten in de nationale structuur (o.a. wie en hoe de vertegenwoordiger vanuit de sector veiligheidsregio's wordt geïnformeerd.)

3.6 De oefening

Uit de vragenlijst blijkt dat het grootste gedeelte van de deelnemers de oefening als 'goed' of 'zeer goed' waardeert. 6% beoordeelt de oefening 'neutraal'.

Organisaties geven aan dat het positief is dat het totale uitval scenario weer op het netvlies is komen te staan en dat dit de bewustwording van de effecten van een cybercrisis heeft vergroot. Ook het laten ervaren dat er binnen de sector andere crisestypen zijn (dan bijvoorbeeld alleen leveringsproblemen) heeft hierbij geholpen. Als andere positieve punten worden benoemd het integreren en leren vertrouwen op je IT organisatie en het feit dat door de oefening een betere brug tussen IT en beleid is geslagen. Tot slot is de voorbereiding door veel organisaties als prettig en positief ervaren. Er was veel commitment om het goed voor te bereiden en organisaties hebben elkaar door de intensieve voorbereiding beter leren kennen waardoor afstemming en samenwerking tijdens de oefening soepeler verliep.

De media responscel en algehele mediadynamiek wordt als een groot pluspunt benoemd. Het was een verrijking voor de oefening doordat het een belangrijke manier was om betrokken te blijven bij de oefening en zicht te krijgen op wat er speelde bij de andere sectoren.

Sommige organisaties benoemen dat zij meer tijd nodig hadden voor het voorbereiden van de eigen oefening. Dit is nu als krap ervaren, ook door de zomervakantie. Ook hebben sommige partijen behoefte aan meer duidelijkheid vooraf over wat er van deelnemende partijen gevraagd wordt. Voor partijen die voor het eerst deelnamen was dit lastig in te schatten en ze hadden daardoor moeite alles intern te regelen.

Een ander aandachtspunt dat door verschillende organisaties wordt benoemd heeft betrekking op het einde van de oefening. Deelnemers geven aan het jammer te vinden dat de oefening stopte bij de nationale opschaling. Idealiter hadden zij nog de terugkoppeling gekregen uit de ICCb omdat het belangrijke impact kan hebben en het input levert voor keuzes die bepaalde organisaties moeten maken. Nu stokten de communicatie en besluiten op een zeker niveau. Daarmee hangt samen dat organisaties behoefte hebben aan een iets meer inspirerende afsluiting van de oefening, bijvoorbeeld in de vorm van een epiloog waarin de afloop en eventueel nasleep wordt beschreven.

4. BIJLAGE

Belangrijkste leerpunten ISIDOOR III

Algemeen
- ✓ Attributie (wie zit er achter de aanval?) is belangrijk, maar kost tijd en vergt specifieke expertise.
- ✓ Het Nationaal Crisisplan Digitaal (NCP-Digitaal) is bij veel organisaties (nog) niet bekend.

Informatie-uitwisseling
- ✓ Sectorale uitdaging: het veilig en discreet uitwisselen van informatie.
- ✓ De behoeften van organisaties kwamen niet altijd overeen met de mogelijkheden van het NCSC.
- ✓ Duiding en de verbinding tussen cybersecurity/IT respons en breder crisismanagement niveau is een uitdaging.

Samenwerking
- ✓ Afstemming binnen sectoren heeft bijgedragen aan een gedeeld beeld.
- ✓ De oefening heeft belangrijke inzichten opgeleverd in de dynamiek van een grootschalige cyberaanval.

Opschaling
- ✓ In het dilemma tussen voorzichtigheid/proportionaliteit en benodigde snelheid overheerste veelal de voorzichtigheid.
- ✓ Het was zoeken naar de balans tussen informatiegestuurd en risicogestuurd werken.
- ✓ De nationale crisisorganisatie is benut, maar was niet voor alle organisaties zichtbaar.
- ✓ Rol van de nationale crisisorganisatie betreft vooral het samenbrengen van informatie en beperken van maatschappelijke impact en onrust.
- ✓ Het gerichter bij elkaar brengen – vroegtijdig – van cyber en (sectorspecifieke) crisisexpertise op nationaal niveau kan helpen bij het versnellen.

Disclaimer evaluatie

Deze evaluatie is gebaseerd op informatie die ter beschikking is gesteld, en verkregen, tijdens de periode waarin de evaluatie is uitgevoerd. Nieuwe of aanvullende informatie kan van invloed zijn op de inhoud en de geformuleerde conclusies en aanbevelingen. Het COT beschikt alleen over informatie waar het rechtswege toegang tot heeft. Rapporten worden in beginsel in opdracht van de opdrachtgever gemaakt en niet gepubliceerd. Eén kopie wordt bewaard voor juridische, IT- en wetgeving- en toezichtdoeleinden.

Over het COT

Het COT is een gespecialiseerd bureau op het gebied van veiligheids- en crisismanagement. Ons werkterrein strekt zich uit van vraagstukken over de vormgeving van veiligheidsbeleid tot de voorbereiding op crisissituaties. Met onze kennis en kunde helpen we opdrachtgevers in complexe situaties waarbij grote risico's worden gelopen, strategische belangen op het spel staan en vaak vele stakeholders zijn betrokken. Advies, onderzoek, en training en oefening vormen de basis van onze dienstverlening. Het COT is een volledige dochteronderneming van Aon Nederland.

Meer informatie: http:/www.cot.nl of cot@cot.nl.