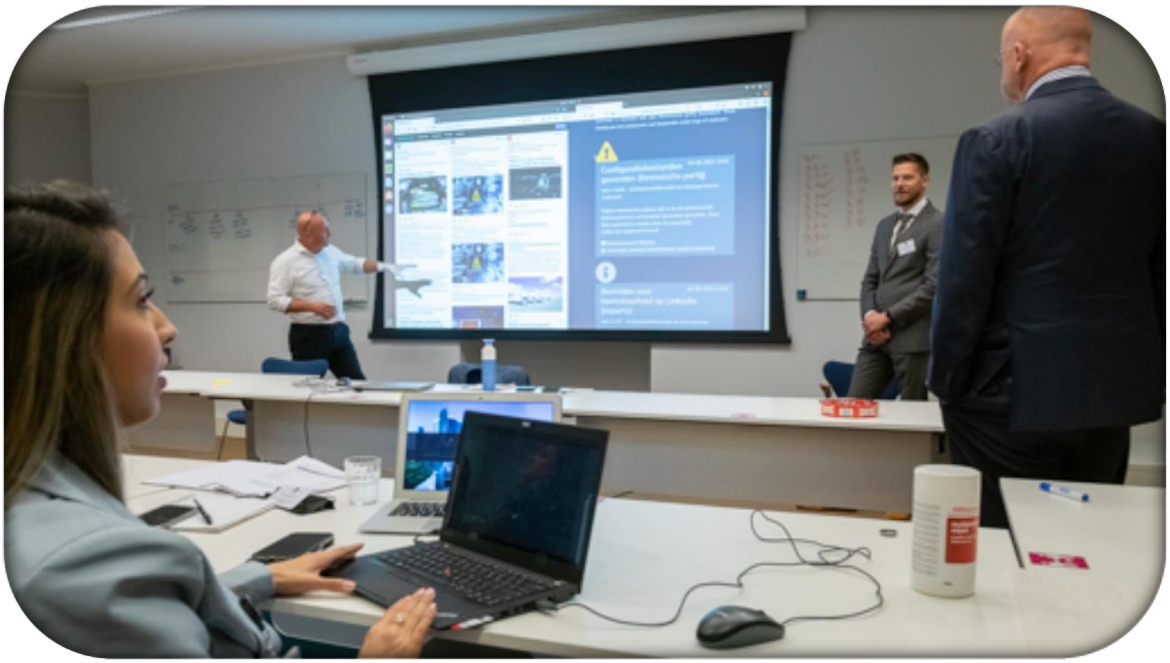
Leerpunten cyberoefening ISIDOOR 2021

Snelheid maken & impact beperken

17 augustus 2021

Inhoudsopgave



Toelichting foto: de centrale oefenleiding toont minister Grapperhaus de online media- en technische oefenomgeving.

1 Inleiding

1.1 Aanleiding

Nederland bereidt zich op verschillende manieren voor op een mogelijke cyberaanval met landelijke impact. Op 1, 2 en 10 juni 2021 vond in het kader van deze voorbereidingen de grootste cybercrisisoefening ooit in Nederland plaats: ISIDOOR 2021. De oefening werd georganiseerd door het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorisme en Veiligheid (NCTV). Centraal stond het beoefenen van het NCP-Digitaal. In de voorbereiding hebben tal van partners samengewerkt aan het scenario onder begeleiding van het COT Instituut voor Veiligheids- en Crisismanagement, in samenwerking met Fox-IT voor de IT-security aspecten. Naast de rol van oefenleider verzorgde het COT ook de overkoepelende leerevaluatie. In deze rapportage presenteren we onze observaties, leerpunten en aanbevelingen.

Tips voor gebruik evaluatie

Deze evaluatie kan worden benut door alle deelnemende organisaties, maar ook door organisaties die niet hebben deelgenomen. De uitdagingen, dilemma's en leerpunten kunnen immers breder relevant zijn. Ons advies is het volgende:

- ✓ Agendeer de rapportage voor bespreking in directie/MT met hierbij een toelichting vanuit experts vanuit de eigen organisatie.
- ✓ Benoem de drie belangrijkste inzichten voor de eigen organisatie.
- ✓ Ga na welke aanbevelingen uit deze rapportage relevant zijn voor de eigen organisatie.

1.2 Over de oefening

Bij de oefening op 1 en 2 juni waren 96 organisaties en gremia en ruim 1.500 deelnemers betrokken. Op 3 juni is uitgebreid stilgestaan bij de eerste ervaringen en leerpunten. Op donderdag 10 juni 2021 vond volgend op de eerdere oefendagen de (deel)oefening plaats met de Interdepartementale Commissie Crisisbeheersing (ICCb).

Het doel van ISIDOOR 2021 was het beoefenen van de crisisprocedures zoals beschreven in het NCP-Digitaal en het versterken van de onderlinge informatie-uitwisseling en samenwerking. Naast alle operationele diensten en netwerkorganisaties[1] op het gebied van cybersecurity, oefenden ook departementen, uitvoeringsorganisaties, bedrijven, veiligheidsregio's en andere crisispartners mee.

Oefendoelen ISIDOOR 2021

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

ISIDOOR 2021 was de derde ISIDOOR-cyberoefening voor organisaties binnen de rijksoverheid en in alle vitale sectoren van Nederland. De ISIDOOR-oefeningen hebben tweemaal eerder in 2015 en 2017 plaatsgevonden en zijn als succesvol ervaren door de deelnemers. De oefening was eerder uitgesteld, onder andere vanwege de coronacrisis. Geleidelijk aan werd de oefening steeds omvangrijker, zowel wat betreft het aantal deelnemers als de voorziene opbouw en invulling. Daarmee werd de oefening ook steeds realistischer. ISIDOOR 2021 was, net als eerder ISIDOOR I en II, een oefening op operationeel, technisch/operationeel, tactisch en strategisch niveau. Individuele organisaties moesten reageren op een cyberincident waarbij geleidelijk aan duidelijk werd wat de aard en de omvang was. Er werd afgestemd en samengewerkt met andere organisaties in eenzelfde sector en bij departementen en uitvoeringsorganisaties en tot slot binnen de nationale crisisorganisatie. In de oefening werd zoveel als mogelijk gewerkt conform het Nationaal Crisisplan Digitaal (NCP-Digitaal) en het Nationaal Handboek Crisisbesluitvorming (NHC).

[1] Denk hierbij aan het Incident Response Board (IRB), het Nationaal Respons Netwerk (NRN), de organisaties binnen het Landelijk Dekkend Stelsel (LDS), etc.

De oefening in cijfers

- ✓ **96** deelnemende organisaties en gremia (grootste sector Energie met **14** deelnemende organisaties)
- ✓ Meer dan **1500** deelnemers. Acht organisaties hadden ieder meer dan **40** deelnemers
- ✓ Één organisatie deed met **10** teams mee aan de oefening
- ✓ **Driekwart** van de organisaties heeft opgeschaald naar strategisch niveau
- ✓ **40%** van de organisaties heeft tijdens de oefening aangifte gedaan
- ✓ Er is tijdens de oefening minimaal **170 keer** contact opgenomen met het NCSC
- ✓ **60%** van de deelnemende organisaties heeft in een samenwerkingsverband sectoraal afgestemd
- ✓ Door **15** organisaties werd namens hun sector een teamlid afgevaardigd naar de IRB
- ✓ **70%** van de organisaties heeft niet overwogen om een Wbni-melding te doen

Organisatorisch & technisch oefenen Vrijwel alle organisaties oefenden ook 'technisch' mee: cybersecurity specialisten moesten daadwerkelijk malware identificeren, het aanvalspad van de aanvaller nagaan en onderzoeken welke data mogelijk was 'onttrokken'. Deelnemende organisaties konden contact opnemen met een gesimuleerde forensisch cyberexpert voor ondersteuning. Ook bredere crisisteams en communicatiespecialisten deden mee. Er was een interactieve communicatie-omgeving waarin media en sociale media werden nagebootst en organisaties zelf konden reageren en/of informatie konden geven. Ook kon er aangifte worden gedaan in een hiervoor ontwikkeld portaal en konden meldingen worden gedaan in het kader van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

Verloop van de oefening Het scenario van ISIDOOR 2021 ging uit van een complexe aanval door een (fictieve) statelijk actor. De aanval was gericht op kantoorautomatisering en grootschalige datadiefstal. De oefening begon vanuit een technische omgeving en werd vervolgens aan de hand van vijf dagdelen opgebouwd naar een eerste opschaling binnen de nationale crisisorganisatie. Hieronder schetsen we kort het scenario en de focus per dagdeel.

Dagdeel 1 - Technisch onderzoek

Het eerste dagdeel richtte zich voornamelijk op de cyberteams. Meerdere bedrijven hadden last van een phishing mail en IT-teams richtten zich op het intern technisch onderzoek. Bedrijven worstelden met eigen aanvallen en storingen. Klanten en burgers ervaarden beperkte impact, en het was nog onduidelijk dat verschillende cyberevents met elkaar te maken konden hebben.

Dagdeel 2 - Sectorale samenwerking

Meerdere organisaties bleken getroffen door de aanval. De dreiging van uitval van systemen werd steeds groter, en het was nog onduidelijk waar de aanvallers op uit waren. In de loop van de middag ontstonden de eerste bredere afstemmingsmomenten binnen de sectoren en departementen. Ook het NCSC schaalde op.

Dagdeel 3 - Coördinatie overheid

In de loop van de ochtend op de tweede dag werd voor steeds meer organisaties duidelijk dat er sprake is van een grotere aanval die al langer duurde en dat de aanvaller uit was op data-exfiltratie. Ook de maatschappelijke dynamiek werd steeds groter. Strategische teams schaalden op en op nationaal niveau werd de IRB bijeengeroepen door het NCSC.

Dagdeel 4 - Nationale duiding en afstemming

De vermoedens dat een (fictieve) statelijke actor achter de gecoördineerde aanval zit werden zeer groot. In het laatste dagdeel ontstond steeds meer behoefte aan nationale duiding en afstemming. Ook waren er zorgen over de impact van getroffen maatregelen en de kans dat meer bedrijven vergaande maatregelen moesten treffen met maatschappelijke gevolgen. 's Middags vond een Interdepartementaal Afstemmingsoverleg (IAO) plaats, gevolgd door een diplomatiek responsoverleg.

Dagdeel 5 - ICCb

Het laatste deel van de oefening betrof een bijeenkomst van de ICCb. Dit ICCb vond plaats nadat een fictief tweede IAO had plaatsgevonden. In dit ICCb werd onder meer gesproken over schaarste, over de communicatie en over mogelijke verdere opschaling in de veiligheidsregio's ter voorbereiding op mogelijke geleidelijke uitval van diensten bij organisaties.

Oefenbeperkingen Iedere oefening kent beperkingen. Dit geldt ook voor ISIDOOR 2021. Deze beperkingen zijn mede van invloed op het verloop en daarmee ook op de leerpunten. Een voorbeeld hiervan is dat organisaties tijdens een oefening niet alle capaciteit kunnen inzetten die zij in werkelijkheid wel zouden vrijmaken. De normale werkzaamheden gaan immers door. Ook merken we soms in een oefening dat organisaties het 'goed' willen doen en bijvoorbeeld vooral de formele lijnen volgen en er minder informeel contact is. In een oefening ervaren deelnemers niet de werkelijke druk en zeer grote hoeveelheid reacties, telefoontjes, appjes en dergelijke. Een laatste beperking is dat in de oefening sommige teams bijvoorbeeld maar één crisisoverleg hebben gehad en de dynamiek tussen overleggen niet is beoefend. Naast deze beperkingen zijn er ook 'voordelen' bij een oefening, die het crisismanagement bevorderen en die in een werkelijke situatie anders zullen lopen. Voordelen zijn onder meer het feit dat de oefening is voorbereid, de betrokken functionarissen weten wanneer deze plaatsvindt en 'klaar staan' om direct in actie te komen. In werkelijkheid kost het meer tijd om op te starten. Daarnaast is tijdens de oefening een deelnemerslijst beschikbaar met contactgegevens. In werkelijkheid zullen niet alle contacten direct bekend zijn.

1.3 De voorbereiding

Het voorbereidingstraject voor ISIDOOR 2021 bestond uit verschillende (online) bijeenkomsten met sectorale scenariowerkgroepen, waarin het overkoepelende scenario door de deelnemers zelf werd ingevuld. Daarnaast konden deelnemende partijen eigen doelstellingen formuleren. De oefening bood ruimte aan deelnemende partijen om, binnen de kaders van de centrale oefening, een eigen deeloefening te houden. Deze deeloefeningen sloten op een passende manier aan op het algemene scenario van ISIDOOR 2021.

De aanloop naar ISIDOOR 2021 was meerjarig omdat de oefening werd uitgesteld. Dit bracht voor de werksessies o.a. een wisseling van fysiek naar digitaal, van een algemene naar een gerichte sectorale aanpak en van fysieke werksessies van een dagdeel naar online deelsessies per sector van 1,5 uur met zich mee. Hierbij stond centraal dat ISIDOOR 2021 een oefening is voor en door deelnemers. Na het uitstel werden de eerdere oefenvoorbereidingen geborgd. Het scenario is steeds gelijk gebleven met enkele kleine aanscherpingen. De focus in de werksessies lag op de totstandkoming van het technische scenario. In de werksessies was vertegenwoordiging vanuit tientallen deelnemers uit de vitale sector, stelselpartijen en de betrokken Departementale Coördinatiecentrum Crisisbeheersing (DCC's). Elke sector had een eigen sectorale oefenleider die de informatie naar de sector uitzette en eerste aanspreekpunt was voor de kerngroep. Deelnemers van de werksessies toonden veel betrokkenheid en expertise en leverden een cruciale bijdrage aan de totstandkoming van de oefening.

Het kernteam (NCTV/NCSC/COT/Fox-IT) had wekelijkse - soms dagelijkse - afstemmingsmomenten. Maandelijks was er afstemming met de stuurgroep. De kerngroep stelde het technische en het generieke scenario samen en was verantwoordelijk voor het draaiboek, het evaluatiekader, de inhoud van de briefingsmomenten, de evaluatiedag, de bestuurlijke sessie en de ICCb-oefening. De communicatie in de oefening werd geregisseerd door het Nationaal Kernteam Crisiscommunicatie (NKC). De communicatie over de oefening kwam vanuit de communicatieteams van het NCSC en de NCTV. De deelnemers werden door nieuwsbrieven op de hoogte gehouden van het proces en kregen documenten toegestuurd via een afgeschermde portal.

Toelichting foto: in gesprek over de eerste leerpunten.

Toelichting foto: koers bepalen in de algemene responscel.

Leerpunten voorbereiding

De sectorale scenario-werksessies zorgden voor gerichte input voor het scenario en brachten meer verbinding tussen de sectorale partners. Voor elke sector was bovendien een sectorale oefenleider aangewezen, die de schakel was tussen de oefenorganisatie en de sector, maar ook de sector goed kende en op die manier input kon leveren. Ook de digitale werkwijze verliep effectief en was toegankelijk. Het werken met een technisch portal heeft goed gewerkt; technische dry-runs waren wel belangrijk om onverwachte struikelblokken tijdens de uitvoer te voorkomen. Verbeterpunten zaten in het eerder aanhaken van communicatieprofessionals in de voorbereiding van het scenario. Nu lag in de werksessies de focus voornamelijk op de technische injects. Wel zorgde de mediasimulatie met echte communicatie-professionals, vertegenwoordigd door specialisten vanuit de sectoren, tijdens de oefening voor een realistische mediadynamiek. Tot slot is een vaste kerngroep/oefenboard cruciaal. De wisseling van projectleiders (o.a. door uitstel van de oefening) zorgde herhaaldelijk voor een extra investering op afstemming (intern) en het verbinden met deelnemers (extern).

Een belangrijk, groeiend inzicht in de voorbereiding was hoe gescheiden de werelden van de functionele cyber kolom en de algemene kolom zijn. Voor de algemene kolom zijn de indicatoren afgestemd op maatschappelijke impact, en vooral informatie gestuurd, waar de cyberkolom juist weer nauwelijks rekening houdt met maatschappelijke effecten maar zich meer richt op de technische impact. Het beoefenen van een scenario met een dreiging op de nationale veiligheid en potentiële maatschappelijke ontwrichting zonder dat daar al effecten van voelbaar zijn, was voor een aantal partijen lastig inleven.

1.4 Aanpak evaluatie

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 3 juni 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, 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. Direct na de oefening hebben de sectorale evaluatoren de ingevulde vragenlijsten binnen hun sector doorgenomen en de belangrijkste en opvallendste uitkomsten genoteerd ter voorbereiding op 3 juni. 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, en 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.

De derde dag van de oefening bestond uit reflecteren en evalueren. Onderdeel van de derde dag was het gesprek per sector, waarin de sectorale evaluatoren samen met oefenleiders en organisatie-evaluatoren het gesprek voerden over de belangrijkste uitkomsten per sector. De notities van deze gesprekken namen we mee in deze evaluatie, evenals de rode draden uit de ingevulde vragenlijsten, de observaties tijdens de oefendagen en de verdere input vanuit de derde dag.

1.5 Opbouw rapportage

In hoofdstuk 2 beschrijven we onze observaties. Op basis hiervan geven we in hoofdstuk 3 ons overkoepelende beeld, benoemen we bevorderende en belemmerende factoren en doen wij gerichte aanbevelingen. In de bijlage schetsen we recente ontwikkelingen en incidenten in het cybersecurityveld; waar stonden we aan het begin van ISIDOOR 2021? Dit is relevante context bij het lezen van de observaties en leerpunten in het volgende hoofdstuk.

Toelichting foto: in de interactieve communicatie-omgeving worden media en sociale media nagebootst en kunnen organisaties zelf reageren en/of informatie geven.

2 Observaties en leerpunten

2.1 Inleiding

In dit hoofdstuk presenteren we eerst algemene observaties, gevolgd door een aantal indrukken per oefendoel. Daarvoor benoemen we kort een aantal terugkerende uitdagingen bij cyberincidenten en -crisis. Deze hebben we ook teruggezien in de oefening. We benadrukken dat de focus van de evaluatie ligt op de overkoepelende crisisstructuur, en niet op individueel of organisatieniveau.

2.2 Context: terugkerende uitdagingen

Uit onze eigen ervaring met cyberincidenten en cybercrisisoefeningen weten we dat er terugkerende uitdagingen zijn. We vatten deze hier kort samen als context bij de observaties die volgen.

Enkele terugkerende uitdagingen

- ✓ **Verschillende talen IT/crisismanagement** Het blijkt niet eenvoudig om de verschillende betrokken 'werelden' bij elkaar te brengen, mede vanwege de verschillende talen. Specialisten op het gebied van IT en cybersecurity moeten samenwerken met specialisten op het gebied van continuïteitsmanagement, communicatie, crisismanagement, juridische zaken, privacy, beleid en operatie. Een uitdaging, zeker aangezien de kern van het crisismanagement is dat er gezamenlijke duiding plaatsvindt, gewerkt wordt vanuit duidelijke doelstellingen en uitgangspunten, er daadkrachtig wordt besloten, en dat er snelheid wordt gemaakt.
- ✓ **Onbedoeld alerteren kwaadwillenden** Mogelijk is de insluiper/aanvaller al langere tijd 'binnen' voordat deze wordt gedetecteerd. In de respons moet rekening worden gehouden met het onbedoeld alerteren van de kwaadwillenden.
- ✓ **Communiceren over kwetsbaarheden** Het communiceren over kwetsbaarheden kent ook risico's: andere kwaadwillen kunnen worden getriggerd om deze kwetsbaarheid ook te misbruiken. Dit kan reden zijn om een kwetsbaarheid pas te communiceren als er een 'oplossing' is (bijvoorbeeld een patch). Echter, hoe sneller een kwetsbaarheid bekend is bij specialisten, hoe eerder zij hier alert op kunnen zijn en maatregelen kunnen treffen (ook preventief).
- ✓ **Voorbereiding om maatregelen te treffen** Afhankelijk van de voorbereiding/inrichting van het systeem zijn er meer of minder mogelijkheden om na detectie snel mitigerende maatregelen te treffen (zoals isolatie of quarantaine). Deze en andere voorbereidingen zijn direct van invloed op de mogelijkheden voor en snelheid van mitigatie.
- ✓ **Mogelijkheid van verschillende aanvallers** Er kunnen meerdere kwaadwillenden betrokken zijn die ieder een deel van een aanval voor hun rekening nemen, dan wel op meerdere manieren proberen misbruik te maken van dezelfde kwetsbaarheid.
- ✓ **Impact van genomen maatregelen** Naast de impact die een aanval direct kan hebben (bijvoorbeeld gestolen data of gegijzelde servers) wordt de impact in belangrijke mate ook bepaald door de respons vanuit de organisatie. Dit geldt bijvoorbeeld voor het uit voorzorg (deels) offline halen van systemen of het niet meer gebruiken van applicaties. Ook het grootschalig wijzigen van wachtwoorden kan grote impact hebben voor gebruikers. Hierbij speelt het dilemma tussen zorgvuldigheid en snelheid.

2.3 Algemene observaties

ISIDOOR 2021 was een geslaagde oefening. Deelnemers waren positief over de inhoud en het verloop van de oefening.

De genoemde oefenbeperkingen en -invloed spelen vanzelfsprekend een rol maar waren niet doorslaggevend: er zitten voor- en nadelen aan de oefensetting. Het scenario werd door de deelnemers als realistisch ervaren. De opzet met de vele (stelsel) partijen en sectorale partners maakte dat er ook echt geoefend kon worden met informatie-uitwisseling. Het mee kunnen oefenen van de technische respons had duidelijke toegevoegde waarde. Hierdoor moesten op alle niveaus 'werelden' bij elkaar komen die elkaar niet vaak treffen: IT security, crisismanagement, continuïteitsmanagement en (crisis)communicatie.

Over de hele breedte van betrokken stakeholders zien wij groei ten opzicht van ISIDOOR II en van eerdere grotere incidenten.

Tijdens ISIDOOR 2021 zien we groei zowel wat betreft expertise als in de bereidheid informatie te delen en samen te werken. Verschillende stakeholders weten elkaar in de basis te vinden. We zien terug dat zij zich specifiek op de respons op een cyberincident hebben voorbereid. De voorbereiding van de oefening heeft hierin ons inziens ook geholpen. Er is in de voorbereiding (maar ook tijdens de oefening) meer inzicht ontstaan in zowel de werkwijze binnen de eigen organisatie, als in de rol van anderen bij een cybercrisis, zowel op sectoraal als nationaal niveau.

Een deel van de observaties en leerpunten komt overeen met ISIDOOR II.

Er zijn duidelijk stappen gezet in de doorontwikkeling van de sectorale afstemming en bijvoorbeeld binnen het Landelijk Dekkend Stelsel (LDS).[2] Een terugkerend punt is de vraag wat de coördinerende rol vanuit het NCSC precies betekent en wat hierin wel/niet mogelijk is. Vragen van organisaties gingen bijvoorbeeld over het aantal mogelijke contactmomenten en de mogelijkheid van gericht advies plus een specifiek handelingsperspectief van het NCSC. Er was bij veel deelnemers begrip voor de beperkte capaciteit of mogelijkheden van het NCSC, maar er lijkt behoefte aan een grotere rol voor het NCSC. Kennis van organisaties over het eigen netwerk lijkt groter dan bij de eerdere oefening. De voorbereiding op de landelijke crisisoverleggen was nu steviger en ook lijkt er nu meer rekening te zijn gehouden met de mogelijke impact van maatregelen op anderen en vond actieve afstemming plaats. Zie voor de hoofdpunten van ISIDOOR II de bijlage.

[2] Zie voor informatie over het Landelijk Dekkend Stelsel, dit artikel: Aansluiting op het Landelijk Dekkend Stelsel (LDS) | Samenwerkingspartner worden | Nationaal Cyber Security Centrum (ncsc.nl)

Attributie (wie zit er achter de aanval?) is belangrijk maar kost tijd en vergt specifieke expertise.

In de balans tussen zorgvuldigheid en snelheid en tussen risico- en informatiegestuurd is het van groot belang om een inschatting te kunnen maken van wie er achter de aanval zit. Hoe geavanceerd zijn de aanvallers? Waar zijn zij toe in staat? Wat kan het doel zijn? Een overkoepelende duiding is cruciaal: is het motief van de aanvaller ontwrichting? Geld? Spionage? Hoe 'erg' is het? Antwoorden op deze vragen zijn direct van belang voor het kunnen inschatten van het risico en daarmee van de proportionaliteit van maatregelen en de benodigde snelheid van handelen. Deze duiding bleef lange tijd uit.

Een terugkerende vraag is of er een statelijke actor achter een aanval zit. Echter, ook criminele groepen kunnen zeer geavanceerd zijn. Bovendien is het onderscheid minder 'hard' dan soms wordt gedacht. Er is verwevenheid tussen verschillende actoren. Zeker als er meerdere aanvallers zijn die ieder een deel van het probleem vormen of juist gelijktijdig dezelfde kwetsbaarheid proberen te gebruiken. Attributie bij een cyberaanval is dan ook niet altijd eenvoudig: dit vergt specifieke expertise die snel gemobiliseerd moet worden. Deze kennis zit bij de overheid maar ook bij security specialisten bij bedrijven.

Het Nationaal Crisisplan Digitaal (NCP-Digitaal) is bij veel organisaties (nog) niet bekend.

Dit hoeft niet per se erg te zijn, maar het risico is wel dat dit ook betekent dat bij veel organisaties de werkwijze vanuit de overheid beperkt bekend is, dan wel dat informatielijnen en afstemmingsplaatsen niet duidelijk genoeg zijn. Uit de reacties van deelnemers blijkt dat meerdere organisaties het NCP-Digitaal actief hebben benut, onder andere voor scenario's en om rollen scherp te krijgen. Ook op nationaal niveau is het plan benut voor het maken van eerste mogelijke scenario's. Het plan is beperkt benut voor het vroegtijdig signaleren van mogelijke sleutelbesluiten of voor het identificeren van mogelijke dilemma's en bijbehorende uitgangspunten.

Een veelgenoemde behoefte is een factsheet met daarin een overzicht van de betrokken organisaties, de rolverdeling en de verschillende informatie- en coördinatielijnen. Dit overzicht betreft de betrokken overheidspartijen maar ook de koppelvlakken met publiek-private samenwerkingsverbanden en sectorale/branche voorzieningen. Het advies vanuit deelnemers is om het plan nog actiever uit te dragen: het is aan organisaties – en soms sectoren –om de implicaties voor het eigen handelen te doordenken.

In de oefening was er specifieke aandacht voor de pers- en publiekscommunicatie.

Het meenemen van het publiek over wat er aan de hand is, is van belang. Zeker op momenten waarop de mediadynamiek steeds groter wordt, is externe communicatie belangrijk. De uitdaging zit in het communiceren wat op dat moment bekend is, zonder onderzoek of opsporing in de weg te zitten. Het verstrekken van nieuwe informatie vanuit stelselpartijen duurde lang. De Rijksoverheid was voor het Nederlandse publiek vrij onzichtbaar, ondanks de groeiende mediadynamiek tijdens de oefening. Het uitspreken dat gewerkt wordt aan zaken op de achtergrond (procesinformatie) is beter dan stilte. Door lang stil te blijven als Rijksoverheid (het algemene publiek kent het onderscheid tussen het NCSC, het NKC en andere organisaties niet), krijgen speculaties en fake news alle ruimte om de overhand te nemen. Ook vanuit organisaties was er behoefte aan landelijke regie op externe communicatie toen duidelijk werd dat de situatie landelijke speelde, bijvoorbeeld een landelijke woordvoeringslijn of een bericht vanuit de Rijksoverheid dat partijen kunnen delen.

Toen de nationale crisisorganisatie werd opgeschaald, heeft het NKC een duidelijke rol gepakt en kwam met een overkoepelende strategie.[3] Echter, lang niet alle betrokken organisaties zijn aangesloten op het NKC. Voor veel organisaties kan het prettig en slim zijn om te kunnen verwijzen naar updates/boodschappen van 'de Rijksoverheid', zodat de aandacht (communicatief) vooral uit kan gaan naar eigen medewerkers/klanten die veel impact ervaren in plaats van naar het algemene publiek. Het kiezen voor een eerlijke en transparante communicatiestrategie is makkelijker als een organisatie (mogelijk) een van de vele getroffenen is, dan wanneer een organisatie een van de weinigen is, waardoor het lijkt alsof die organisatie de beveiliging slecht op orde heeft. De meeste organisaties kozen er nu voor om niet te communiceren, ook toen het in de media overduidelijk was dat er landelijk iets aan de hand was. Dit draagt (zeker op de lange termijn) niet bij aan het vertrouwen van de burger in de overheid en het bedrijfsleven. Een vroegtijdige opschaling van het NKC bij toenemende maatschappelijke vragen, discussie en zorgen is verstandig als het gaat om cyber.

Op sectorniveau was er in veel sectoren onderling regelmatig afstemming over woordvoeringslijn en communicatiestrategie. Intersectoraal was minder zicht op de informatievoorziening van andere sectoren.

2.4 Oefendoel: informatie-uitwisseling

Sectorale uitdaging: het veilig en discreet uitwisselen van informatie

Ondanks de bereidheid van organisaties om informatie met elkaar te delen, blijft een terugkerende uitdaging in de sectorale afstemming het op een veilige en discrete manier uitwisselen van die informatie. Dit speelt vooral binnen de sectoren. Vooral op het moment dat het om gevoelige data gaat, blijkt het een obstakel voor organisaties om dit met elkaar te delen. Enkele sectoren geven aan behoefte te hebben aan een middel om deze informatie op een veilige manier binnen de sector uit te kunnen wisselen. Het is goed om te beseffen dat uitgewisselde informatie vaak een mix van feiten, geruchten en aannames is. Zo bleek in de oefening dat meerdere organisaties aangifte hadden gedaan van vermeende ransomware, waar daar feitelijk geen sprake van was.

De behoeften van organisaties kwamen niet altijd overeen met de mogelijkheden van het NCSC.

De uitdaging voor het NCSC is het zo snel mogelijk delen van risico-informatie zodat organisaties hier hun voordeel mee kunnen doen. En vervolgens het komen tot landelijke duiding van de cyberaspecten en het geven van advies waar mogelijk. Ook is er een bredere, overkoepelende duiding nodig vanuit crisisperspectief. Het gaat hierbij om het duiden van de situatie (oorzaak en impact), het benoemen van de risico's en de dreiging en het schetsen van de mogelijke en reeds lopende aanpak (inclusief doelen en uitgangspunten). Hier ligt logischerwijs een rol voor de NCTV mede namens alle betrokken crisispartners.

[3] In werkelijkheid zou het NKC al eerder zijn opgestart, maar vanwege oefenbeperkingen gebeurde dit nu niet.

De behoefte van organisaties aan informatie en duiding verschilt. Sommige organisaties hadden vooral behoefte aan meer procesinformatie: wat is de stand van zaken? Wat gebeurt er landelijk? Andere organisaties hadden behoefte aan specifieke informatie voor de eigen organisatie. 1-op-1 contact en advies vanuit het NCSC met de getroffen organisatie kan alleen in prioritaire situaties. Dit vanwege onder meer de beschikbare tijd en capaciteit. De informatie- en adviesbehoefte hangt ook af van de eigen capaciteit en expertise van bedrijven en sectoren:

- Juist sectoren die minder volwassen zijn op het gebied van cybersecurity hebben behoefte aan informatie en advies over wat te doen. Hierbij is wel van belang dat een organisatie actief de vraag om informatie en advies stelt.
- Bedrijven die al wel meer 'volwassen' zijn, hebben vooral behoefte aan snelle en onderliggende data om te kunnen duiden en minder aan – latere – duidingsinformatie vanuit de overheid. Daarbij geldt ook een verantwoordelijkheid van organisaties om informatie te (blijven) verschaffen aan sectorale en sector-overstijgende samenwerkingsverbanden, zodat ook op nationaal niveau een goed beeld ontstaat.

Een leerpunt is dat bij een grootschalige cyberaanval met impact, er een proces moet ontstaan van het gezamenlijk, periodiek, in beeld brengen van de situatie en de resterende risico's en dreiging. Het gaat hierbij om zowel informatie over de mogelijke oorzaak als over het eventuele handelingsperspectief en de aanpak in het kader van continuïteits- en crisismanagement.

Duiding en de verbinding tussen cybersecurity/IT respons en breder crisismanagement niveau is een uitdaging.

Dit is een uitdaging die speelde op alle niveaus. De focus bij deelnemers lag voornamelijk op gebeurtenissen en veel minder op mogelijke impact, scenario's en vervolgdreiging. De vraag is wie de mogelijke impact duidt. Dit moet nationaal gebeuren.

Deze duiding is niet enkelvoudig, maar gebaseerd op een combinatie van indicaties vanuit de technische expertise (wat is er feitelijk aan de hand?), de impact analyse (welke effecten heeft dit?), de forensische expertise (wat is de oorzaak en wie zit er achter?) en inlichtingen (wat is het motief?). Elk van deze disciplines is voorzichtig in het duiden omdat ze de informatie van de andere partijen (nog) niet kennen. Hierbij komt de noodzaak van het benutten van sectorspecifieke kennis om ook de (on)bedoelde impact van eventuele maatregelen in te kunnen schatten. Hier ligt ook een (beperkte) rol voor de ICT Response Board (IRB) als het gaat om de mogelijke intersectorale impact en het mogelijke handelingsperspectief. Dit aanvullend op wat er direct vanuit de sectoren zelf komt in de contacten met onder andere departementen en wat er vanuit andere samenwerkingsverbanden komt (zoals vanuit het LDS).

Duiding zit deels in het overleg waar intelligence wordt gedeeld maar ook bij het NCSC, in het informatieteam dat input levert voor de nationale crisisorganisatie en in de voorbereiding vanuit de NCTV voor het IAO (in een situatie- en dreigingsanalyse). De duiding is versnipperd en overlapt soms. De vraag is of de duiding van impact nu integraal genoeg is.

2.5 Oefendoel: samenwerking

Afstemming binnen sectoren heeft bijgedragen aan een gedeeld beeld.

Op het moment dat duidelijk werd dat de phishing aanval meerdere organisaties in het hele land trof, werd ook sectoraal afgestemd over de aanpak. Verschillende CERT's, ISAC's (als professionele community zonder veelal een specifieke responsrol) en andere sectorale samenwerkingsverbanden werden geactiveerd. De mate van ervaring en volwassenheid van de afstemming verschilt per sector. Daarnaast werd ook op persoonlijk niveau de afstemming gevonden binnen de sector; onderlinge contacten uit de koude fase werden vaak benut. Deelnemers geven aan sectorale afstemming vooral nuttig te vinden voor het verifiëren van (technische) informatie, het ophalen van informatie ten behoeve van de beeldvorming voor het eigen interne crisisteam, het delen van kennis en informatie en het vaststellen van het urgentiebesef. Daarnaast is er in een aantal sectoren ook op sectoraal niveau afstemming gezocht m.b.t. gezamenlijke externe communicatie.

De oefening heeft belangrijke inzichten opgeleverd in de dynamiek van een grootschalige cyberaanval.

En ook in de uitdagingen die dit meebrengt voor het samenspel tussen betrokken organisaties. Er zijn zeer veel organisaties betrokken. Dit maakt coördinatie en het komen tot een gedeeld beeld zeker niet eenvoudig. Organisaties en teams op elk niveau hebben behoefte aan informatie, duiding en handelingsperspectief. Maar tegelijkertijd is iedereen druk om eerst tot eigen acties en duiding te komen. En duiding kost tijd. De grootste uitdaging – en het grootste knelpunt – tijdens de oefening was dan ook het komen tot een balans tussen zorgvuldigheid/proportionaliteit en benodigde snelheid.

2.6 Oefendoel: opschaling

Organisaties troffen belangrijke mitigerende maatregelen om de impact van de aanval te beperken.

Mitigerende maatregelen zijn veel bedoeld om de aanvaller/de besmetting de pas af te snijden en te zorgen dat er niet meer schade ontstaat (zoals het isoleren van een deel van de technische omgeving of het wijzigen van wachtwoorden). Dit gebeurt in combinatie met forensisch onderzoek om na te gaan waar de aanvaller is of is geweest en wat de mogelijke schade/gevolgen zijn. Hierin zitten grote verschillen tussen organisaties, zo bleek

ook tijdens de oefening. De ene organisatie beschikt zelf over genoeg expertise om te onderzoeken en te duiden en treft relatief snelle mitigerende maatregelen terwijl de ander afhankelijk is van de duiding van derden.

In het dilemma tussen voorzichtigheid/ proportionaliteit en benodigde snelheid overheerste veelal de voorzichtigheid.

Eerst meer duidelijkheid en inzicht en dan pas handelen: cyber is vooral een 'onzekerheidscrisis'. Immers, eigen maatregelen kunnen de impact onbedoeld nog groter maken. Op alle niveaus zagen we voorzichtigheid. Deze gestapelde voorzichtigheid zorgt opgeteld voor vertraging in de respons: in het informeren, duiden, waarschuwen, het opstellen van scenario's en het nemen van besluiten. Een belangrijk leerpunt voor de nationale crisisorganisatie is om laagdrempelig op te schalen en direct te starten met het opstellen van mogelijke scenario's. Hierbij ligt de nadruk vooral op de impact: van de aanvallen zelf en van de maatregelen die hierop volgen.

Het was zoeken naar de balans tussen informatiegestuurd en risicogestuurd werken.

De oefening begon met een grootschalige phishing aanval. Deelnemers waren een groot deel van de eerste dag bezig met het interne technisch onderzoek naar de phishing aanval. Op de eerste dag rond 11 uur werden de eerste (informele) meldingen gedaan bij de DCC's en het NCSC. In de media was wat onrust te zien vanwege haperende dienstverlening bij verschillende organisaties. De situatie zorgde voor grote verschillen in snelheid en mate van opschalen bij organisaties. In enkele sectoren werd er meer nadrukkelijk "snel" opgeschaald vanuit onzekerheid (risicogestuurd). In – de meeste – andere sectoren vond een rustige opschaling op basis van de feiten en de situatie plaats (informatiegestuurd). Dat geldt ook voor de duiding van de data extractie. Een aantal organisaties hield er al snel rekening mee dat dit wel eens een groot probleem zou kunnen worden terwijl anderen zich daar nog niet op richtten omdat daar geen feitelijke informatie over beschikbaar was. In zijn algemeenheid lag de focus tijdens de oefening voornamelijk op ransomware en 'uitval'. Dat er veel minder oog was voor datadiefstal, en voor de consequenties hiervan, werkte ook door op het nationale niveau.

De nationale crisisorganisatie is benut, maar was niet voor alle organisaties zichtbaar.

Het NCSC schaalde op de eerste dag op. Vanwege de opeenstapeling van calamiteiten werd op de tweede dag ook de IRB geactiveerd.[4] 's Middags vond vervolgens een IAO plaats. Aanvullend op de sectorale afstemming, wordt ook in de cyberwereld op steeds meer plekken afgestemd. Door het groeiend aantal gremia binnen deze cyberwereld waarin informatie wordt gedeeld en wordt afgestemd, is het steeds belangrijker om een heldere rolverdeling vast te stellen. Dit heeft ook effect op de crisisstructuur. Zo waren er veel vragen over de rol en toegevoegde waarde van de IRB (mede gelet op de gewenste snelheid van communiceren en duiding).

Het Nationale Crisisplan is benut. Er is nagedacht over scenario's. Tijdens het eerste IAO was er nog beperkte duiding, waren er eerste ruwe scenario's en was er beperkt zicht op mogelijke dilemma's en sleutelbesluiten. De oefening eindigde bij het eerste IAO: in een tweede IAO zou er meer duidelijkheid zijn geweest. De vraag hierbij is wel of er in werkelijkheid ook genoeg tijd is, of dat er ook in een eerste IAO al meer moet zijn uitgewerkt, waarschijnlijk op basis van inschattingen van experts. In werkelijkheid zal het ook enige tijd duren voordat er meer feitelijke informatie is.

[4] Zie voor een toelichting op de IRB https://www.ncsc.nl/over-ncsc/crisisbeheersing

Organisaties geven aan weinig zicht te hebben gehad op de opschaling en de motivatie daarachter: op basis van welke informatie wordt opgeschaald? Welk gedeeld beeld wordt ingebracht? Wat komt er uit de overleggen? Wat is het handelingsperspectief? Dit is voor organisaties van belang voor het eigen situationeel bewustzijn en beeldvorming.

Rol van de nationale crisisorganisatie betreft vooral samenbrengen informatie en beperken maatschappelijke impact en onrust

De overheid komt vooral in beeld daar waar er schaarste heerst of daar waar er bijzondere middelen moeten worden ingezet waarover alleen de overheid beschikt. Ook het beperken van maatschappelijke onrust en het bevorderen van gedrag dat de impact beperkt zijn taken voor de overheid.

Het is belangrijk dat vroegtijdig wordt nagedacht over de mogelijke impact en mogelijke sleutelbesluiten op nationaal niveau. Hierbij komt de opgave om ook als overheid zelf om te kunnen gaan met een cyberaanval. In deze oefening kwam dit samen: overheden die zelf een probleem hadden en de overheid met een rol richting de samenleving.

In de nationale crisisorganisatie kwamen beide componenten aan bod. Iedere crisispartner heeft informatie ingebracht om te komen tot een gedeeld beeld. Departementen hebben in de eigen sectoren afstemming gezocht en inzicht proberen te krijgen in de (mogelijke) impact. Het NCSC en de NCTV hebben intensief samengewerkt om zaken bij elkaar te brengen en de interdepartementale afstemming en besluitvorming voor te bereiden.

Het duurde enige tijd voordat een beeld met de duiding erbij tot stand kwam. De opschaling van de crisisorganisatie landelijk droeg wel bij aan een beeld met duiding. Een aandachtspunt is het moment waarop er tot opschaling wordt besloten. In een oefening is het bekend dat er een opschaling zal komen, maar in de werkelijkheid zullen er situaties zijn met potentieel 'grote impact', maar waarbij het ook kan meevallen en/of vooral organisaties zelf aan zet zijn. Een vroegtijdige, multidisciplinaire impactanalyse is cruciaal.

Het gerichter bij elkaar brengen – vroegtijdig – van cyber en (sectorspecifieke) crisisexpertise op nationaal niveau kan helpen bij het versnellen.

De rol van partijen binnen het LDS is vol in ontwikkeling. Deze lijkt nog beperkt tot het doorgeven van informatie, mogelijk met een enkel sectorspecifiek advies. Dit is volgend op de communicatie vanuit het NCSC. Hoe langer die communicatie duurt, hoe langer het ook duurt om sectorspecifieke informatie te kunnen delen. Hier ligt een kans voor het herijken van de rolverdeling nu de sectorale CERT's bijvoorbeeld meer volwassen zijn. De rol van de CERT's in duiden en adviseren kan mogelijk worden vergroot. Ook de samenwerking met het bedrijfsleven is in ontwikkeling.

Het is een terugkerend aandachtspunt betreft de rol van partijen binnen het LDS: wat mag/kan er wel en mag/kan er niet met betrekking tot het delen van informatie en het duiden van de situatie. Bij sectorale partijen bestaat de behoefte om de eigen sector gericht te informeren, maar ook het gevoel te moeten wachten op duiding en communicatie vanuit het NCSC. Ruwe info kan ook helpen zodat partners binnen het LDS hun eigen achterban kunnen helpen met duiden en eerder kunnen starten met het bepalen van de mogelijke impact op de eigen achterban. Met het oog op de benodigde snelheid, het belang van vroegtijdig delen van informatie en schaarste in benodigde expertise en capaciteit, is het cruciaal dat juist op het koppelvlak publiek-privaat maximaal kan worden samengewerkt.

3 Overkoepelend beeld en aanbevelingen

3.1 Overkoepelend beeld

In deze rapportage hebben we onze observaties gedeeld van de meerdaagse crisisoefening ISIDOOR 2021: een omvangrijke cyberaanval bij bedrijven en overheden. Tijdens de oefening hebben tientallen organisaties zelf, per sector en in interactie met landelijke partners geacteerd om de impact van de fictieve aanval zoveel als mogelijk te beperken. De observaties zijn gebaseerd op door de deelnemers benoemde ervaringen en leerpunten uit de ontvangen vragenlijsten, de bespreking tijdens de derde oefendag (die volledig in het teken stond van leren) en onze eigen observaties tijdens de oefening. In dit afsluitende hoofdstuk geven wij ons overkoepelende beeld. Ook schetsen we de bevorderende en belemmerende factoren die van invloed waren op de dynamiek en de respons. We sluiten af met enkele aanbevelingen. Wij hopen met deze rapportage bij te dragen aan het leren, ook na de oefening.

Overkoepelend beeld

ISIDOOR 2021 was een geslaagde oefening die breed werd gewaardeerd door de deelnemers. Het was vooral ook een ontwikkelstap: de voorbereiding en de oefening zelf hebben de voorbereiding van afzonderlijke organisaties, samenwerkende partijen binnen een sector en coördinerende teams op een mogelijke cyberaanval versterkt. Er is veel ervaren en geleerd. De grootste uitdaging zit in het maken van snelheid en tegelijkertijd het betrachten van zorgvuldigheid, ook om disproportionele maatregelen te voorkomen. In een groeiend spelersveld wordt het komen tot een gedeeld beeld, duiding en coördinatie alleen maar belangrijker, maar ook moeilijker. Het gezamenlijk benutten van expertise en ervaring om tot duiding te komen is cruciaal om vervolgens als betrokken crisispartners een bijdrage te kunnen leveren.

De verwachtingen van organisaties nemen toe: van elkaar maar ook van de nationale overheid en van het NCSC in het bijzonder. De toenemende volwassenheid van tal van partijen biedt een belangrijke kans om de rol- en werkverdeling zo in te richten dat ieder zijn of haar rol kan pakken en schaarse capaciteit optimaal kan worden benut. Dat vergt verdere stappen in het mogelijk maken van het vroegtijdig delen van (ruwe) data/informatie. Ook het versnellen van de crisisrespons nationaal is een belangrijke te zetten stap. Hierbij kan de doorontwikkeling van het Nationaal Crisisplan Digitaal helpen met bijpassende werkwijze en de toevoeging van cyberexpertise in de crisisteams. Hierbij is een combinatie van informatiegestuurd en risicogestuurd werken nodig met vroegtijdig aandacht voor de mogelijke impact (scenariodenken). Nu lag de aandacht nog te veel op het technische probleem en nog te weinig op de impact. Dit was een terugkerend punt voor zowel individuele organisaties als voor de multidisciplinaire crisisteams. Het vergt ook een meer continu proces van het delen van informatie over de situatie, de impact en de voorziene aanpak en het – als onderdeel hiervan – periodiek delen van updates. Hierin kunnen zowel sectorale als andere coördinerende gremia een belangrijke rol vervullen zodat de ‘cyberwereld’ en de ‘crisiswereld’ dichter bij elkaar komen.

3.2 Bevorderende en belemmerende factoren

In het onderstaande overzicht vatten we de eerder genoemde observaties samen. We maken een onderscheid tussen bevorderende en belemmerende factoren in de respons op de (dreigende) cybercrisis die is beoefend.

Bevorderend	Belemmerend
✓ **Voorbereiding** Merkbare voorbereidingen bij alle deelnemende organisaties bevorderden het handelen in de respons. ✓ **Technische mitigerende maatregelen** Organisaties troffen mitigerende technische maatregelen om de risico's te beperken. ✓ **Bereidheid informatie delen** Organisaties bleken bereid informatie te delen binnen de sector en met het NCSC. Ook waren er relatief veel aangiftes. Alle informatie helpt bij het duiden van wat er aan de hand is en van de mogelijke impact. Dit vergt wel dat er ook meer terugmeldingen worden gedaan vanuit organisaties richting het NCSC over (verwachte) impact en de ontwikkeling van de situatie. ✓ **Opstellen scenario's** Het Nationaal Crisisplan Digitaal bood houvast bij het opstellen van scenario's binnen de nationale crisisorganisatie. Er zijn in korte tijd eerste scenario's opgesteld. ✓ **Samenwerking diensten** Afstemming rond intelligence en respons werkte goed en gaf inzicht in mogelijkheden. ✓ **Strategie communicatie** Er was een duidelijke aanpak/strategie vanuit het Nationaal Kernteam Communicatie (NKC). ✓ **Voorbereiding ICCb** De ICCb bleek daadkrachtig in de besluitvorming. Intensieve voorbereiding van de vergadering loonde (onder andere uitgebreide agenda en concept adviezen). ✓ **Internationale afstemming** Er is gerichte internationale afstemming gezocht om gezamenlijk op te trekken richting de waarschijnlijk betrokken statelijke actor. ✓ **Afstemming sleutelbesluiten** Op nationaal niveau zijn impactvolle (sleutel)besluiten op elkaar afgestemd: dit voorkomt verrassingen en onbedoelde negatieve impact.	× **Gestapelde voorzichtigheid** Bij iedere stap/schakel wordt voorzichtigheid betracht. Opgeteld kost dit veel tijd. × **Onbekendheid risico data-exfiltratie** De begrijpelijke focus op de mogelijkheid van uitval leidt af van aandacht voor andere risico's. Bekendheid met risico's van data-exfiltratie bleek beperkt bij veel van de deelnemers. Dit werd aanvankelijk niet als risico herkend. Vermeende ransomware kreeg daarentegen veel aandacht, ook als dit in werkelijkheid niet overal speelde. Berichtgeving en 'ruis' in de communicatie lijken hier mede op van invloed. × **Vertraagde informatiedeling** Informatie over wat er speelt vanuit het NCSC richting doelgroepen is informatie op hoofdlijnen. Ook kost het relatief veel tijd voordat er een bericht uitgaat. Dit beperkt de ervaren meerwaarde van deze informatie bij ontvangers. × **Beperkte ruwe informatie uitwisseling** Al willen organisaties soms informatie delen, de middelen om dit op veilige manier te kunnen doen zijn niet altijd toereikend. Door deze beperkte mogelijkheid om vroegtijdig ruwe informatie en expert inschattingen te delen tussen specialisten van de overheid en van bedrijven, vindt op veel plaatsen dezelfde inspanning plaats op duiding. × **Verwachtingen NCSC** De verwachtingen bij een deel van de organisaties van de rol van het NCSC (snel duiden, soms 1-op-1 contact en advies) zijn niet realistisch bij een zeer omvangrijke cyberaanval: dan moeten er prioriteiten worden gesteld. Meerdere respondenten benoemden dat zij wel informatie deelden maar weinig informatie terugkregen. × **Verschillende talen** Beperkte kennis over/inzicht in cybersecurity aspecten bij crisisfunctionarissen bemoeilijken het komen tot inschattingen van impact en maatregelen. Sowieso is er de uitdaging van 'taal': specifieke technische materie die inzichtelijk moet worden gemaakt. × **Rol IRB** De rol van de ICT Respons Board (IRB) is niet voor iedereen duidelijk. In de oefening is er weinig met de output gedaan mede omdat op het moment van vergaderen er nog beperkte duiding was en er nog veel onzekerheden waren over wat precies de situatie was.

3.3 Aanbevelingen

Tot slot doen we een aantal overkoepelende aanbevelingen. Wij zien vier lijnen voor versterking:

1. Vergroten inzicht in rollen en routes
2. Zorgvuldig zijn & snelheid maken
3. Capaciteit en expertise optimaal benutten
4. Blijven werken aan de voorbereiding samen met partners

Op de volgende pagina lichten we de aanbevelingen verder toe.

Aanbeveling 1

Vergroten inzicht in rollen en routes

Blijf het NCP Digitaal actief uitdragen. Overweeg het ontwikkelen van een bijpassende basismodule/e-learning voor sleutelfunctionarissen landelijk en bij partners.

Kom tot een beknopt overzicht van betrokken organisaties en samenwerkingsverbanden/coördinatiepunten en geef beknopt weer welke partijen hierbij aansluiten en wat de rol is. Actualiseer dit periodiek.

Maak expliciete keuzes in de beoogde rol van de IRB. Met een groeiend aantal vormen van samenwerking en aansluiting op sectoren is de vraag wat de toegevoegde waarde van de IRB is, mede gelet op de beoogde snelheid.

Denk na over een meer cyber-specifieke invulling van de verschillende crisisteams in de nationale crisisorganisatie (van informatieteam tot ICCb) waarbij vooral inzicht in de mogelijke impact op het eigen beleidsterrein en het mogelijke handelingsperspectief wordt versterkt. Het gaat er om dat de vertegenwoordigers in de crisisteams voldoende basis-cyberkennis hebben om die mogelijke impact te doorzien.

Aanbeveling 2

Zorgvuldig zijn & snelheid maken

Informeer organisaties die melding kunnen doen bij het NCSC over de gewenste informatie die deze melding moet bevatten. Hoe meer en makkelijker (cruciale) informatie er in een vroeg stadium wordt gedeeld hoe beter.

Het NCSC wordt geadviseerd te onderzoeken of en op welke wijze eerder (ruwe) informatie en eerste expert-inschattingen van de mogelijke situatie kunnen worden gedeeld. Niet als formeel advies, maar als input voor de security experts binnen de achterban en breder binnen cybersecurity in Nederland. Dit vergt wel dat het juridisch kan en organisaties weten dat het gaat om eerste inschattingen en niet meer dan dat. Vervolgens kunnen de experts bijdragen aan duiding en nader onderzoek en op hun beurt ook het NCSC voeden.

Stel het vroegtijdig inschatten van de mogelijke impact (vanuit inzicht in risico's) meer centraal in de landelijke respons. Start in een vroeg stadium met het ontwikkelen van eerste scenario's vanuit crisisperspectief. Benut deze scenario's om mogelijke sleutelmomenten en -besluiten en de benodigde informatie en expertise te identificeren. Dit om vervolgens gerichte voorbereidingen te kunnen treffen of besluitvorming naar voren te halen. Start hier mee zodra de inzet van de nationale crisisorganisatie wordt verwacht.

Kies parallel aan het duiden en onderzoeken voor een scenario dat – voorlopig – als centraal scenario wordt benut voor het handelen. Dit is een sleutelbesluit binnen de nationale crisisorganisatie dat in een vroeg stadium moet worden genomen om houvast te geven.

Aanbeveling 3

Capaciteit & expertise optimaal benutten

Bij een grootschalige/impactvolle cyberaanval zal de beschikbare capaciteit van het NCSC een aandachtspunt. Tegelijkertijd zijn er steeds meer partijen binnen het Landelijk Dekkend Stelsel die meer 'volwassen' zijn geworden of vol in ontwikkeling zijn. Hun rol is veelal beperkt tot het verstrekken van informatie. Verken de mogelijkheid voor een grotere rol (in duiding, onderzoek, verkennen mogelijke oplossingen), waardoor het NCSC ontlast kan worden.

Kom tot een adviserend kader over hoe om te gaan met schaarste op het gebied van cybersecurity expertise in Nederland. Hoe kunnen overheid en bedrijven in zo'n situatie tot prioriteiten komen wat betreft de verdeling van de schaarse expertise die bijdragen aan het voorkomen of beperken van maatschappelijke ontwrichting?

Aanbeveling 4

Blijven werken aan de voorbereiding samen met partners

Overweeg het organiseren van ISIDOOR IV, waarbij een grotere rol voor sectorale CERTS/het Landelijk Dekkend Stelsel (LDS) en een intensiever samenwerking tussen overheid en bedrijfsleven (in het maken van snelheid in duiden, waarschuwen en adviseren) voor de hand liggende thema's zijn.

Werk in de tussentijd met kleinere, specifieke oefeningen en trainingen gericht op in ieder geval de volgende thema's: inschatten impact, scenario's opstellen, voorbereiding landelijke crisisteams en samenwerking in het duiden (publiek-privaat).

Kom tot een cyber-specifieke voorbereiding voor het NKC en ga na hoe ook afstemming op de communicatie kan worden bevorderd parallel aan het delen van technische waarschuwingen en bijbehorend handelingsperspectief.

Bijlage - Achtergrondinformatie: grote dynamiek in het cyberdomein

Digitale veiligheid blijft een groeiend aandachtspunt waar veel ontwikkelingen plaatsvinden, zowel op het gebied van weerbaarheid als het soort aanvallen dat wordt uitgevoerd. In dit achtergrondhoofdstuk schetsen we kort een aantal recente ontwikkelingen in het cybersecurityveld en benoemen we een viertal typen cyberaanval die in de afgelopen jaren heeft plaatsgevonden. Tot slot blikken we kort terug op de leerpunten uit de ISIDOOR II oefening. De hoofdvraag: "Waar stonden we op het moment dat ISIDOOR 2021 van start ging?". Dit is relevante achtergrond bij de observaties in hoofdstuk 2 en de aanbevelingen in hoofdstuk 3. Elementen van de recente ontwikkelingen en eerdere impactvolle incidenten komen terug in het scenario.

A. Ontwikkelingen in het cybersecurityveld

Bouwen aan het Landelijk Dekkend Stelsel Het LDS heeft als doel om Nederland weerbaarder te maken tegen cyberaanvallen. Binnen de structuur werken publieke en private partijen samen om informatie en kennis uit te wisselen. Denk hierbij aan CERTs, sectorale en regionale samenwerkingsverbanden. Het NCSC en het Digital Trust Center (DTC) spelen hierin een belangrijke rol, waarbij het NCSC fungeert als centraal informatieknooppunt. Het NCSC kan vanuit haar (wettelijke) taken en bevoegdheden informatie ook delen met schakelorganisaties die door het NCSC zijn aangewezen. Deze schakelorganisaties bestaan uit samenwerkingsverbanden (OKTT's) en computercrisisteams (CERTs of CSIRTs) . Deze OKTT's maken dat het speelveld steeds ruimer en meer georganiseerd raakt. De afgelopen jaren wordt hard gewerkt aan het LDS; een toenemend aantal samenwerkingsverbanden sluit aan en ontvangt informatie van het NCSC over dreigingen en kwetsbaarheden.

Nationaal Crisisplan Digitaal In februari 2020 is het herziene Nationaal Crisisplan Digitaal (NCP-Digitaal) gepubliceerd. Het plan biedt handvatten voor vitale en niet-vitale organisaties om in het geval van een cyberaanval snel schade te beperken en te herstellen. ISIDOOR 2021 beoefende de crisisprocedures zoals beschreven in het NCP-Digitaal.

Cybersecuritybeeld 2021 De NCTV brengt samen met het NCSC jaarlijks de digitale dreiging en de gevolgen daarvan in beeld in het Cybersecuritybeeld (CSBN). Het beeld van 2021 laat zien dat de digitale dreiging zich blijft ontwikkelen en dat de samenleving alleen maar afhankelijker wordt van digitale processen. De COVID-19 crisis heeft daar aan bijgedragen: in het afgelopen jaar werd nog meer via digitale middelen gedaan dan daarvoor. De digitale en fysieke wereld raken steeds meer verweven: verstoorde digitale processen kunnen hierdoor een enorme impact hebben op het functioneren van de maatschappij. Er worden stappen gezet in de voorbereiding op cyberincidenten, maar in het CSBN wordt ook geconstateerd dat de weerbaarheid in Nederland nog niet voldoende ontwikkeld is.

Wetenschappelijke Raad voor het Regeringsbeleid (WRR) rapport 'Voorbereiden op digitale ontwrichting' In 2019 brengt de WRR het rapport 'Voorbereiden op digitale ontwrichting' uit, waarin zij de aanbeveling doet om de voorbereiding op cyberincidenten nadrukkelijk onderdeel te laten zijn van het nationale veiligheidsbeleid. De WRR geeft aan dat de overheid op dit moment nog onvoldoende voorbereid is op digitale ontwrichting. In een reactie geeft het kabinet aan zich o.a. voor te bereiden met behulp van het NCP-Digitaal en nationale oefeningen zoals ISIDOOR. Daarnaast nemen zij o.a. aanbevelingen over om het uitwisselen van informatie over dreigingen meer te stroomlijnen.

B. Recente incidenten

Kwetsbaarheden in servers en systemen In de afgelopen twee jaar was er sprake van meerdere kwetsbaarheden bij grote bedrijven. Het bekendste incident is de kwetsbaarheid bij Citrix, die eind 2019 werd ontdekt. In de evaluatie van de Citrix-crisis kwamen een aantal aandachtspunten naar voren. Zo leefde bij veel organisaties de vraag hoe de rollen en mandaten binnen het LDS ingeregeld zijn tijdens de warme fase en wie wanneer welke informatie mag delen. Daarnaast bestonden er veel vragen over de opschaling van de crisisstructuur bij een ICT-crisis bij organisaties. Het NCP-Digitaal was op het moment van de Citrix-crisis nog volop in ontwikkeling. Ook bij Microsoft Exchange werd begin 2021 een viertal kwetsbaarheden ontdekt. Het NCSC verstuurde een high/high-beveiligingsadvies vanwege de urgente update die buiten de reguliere patchcyclus viel.

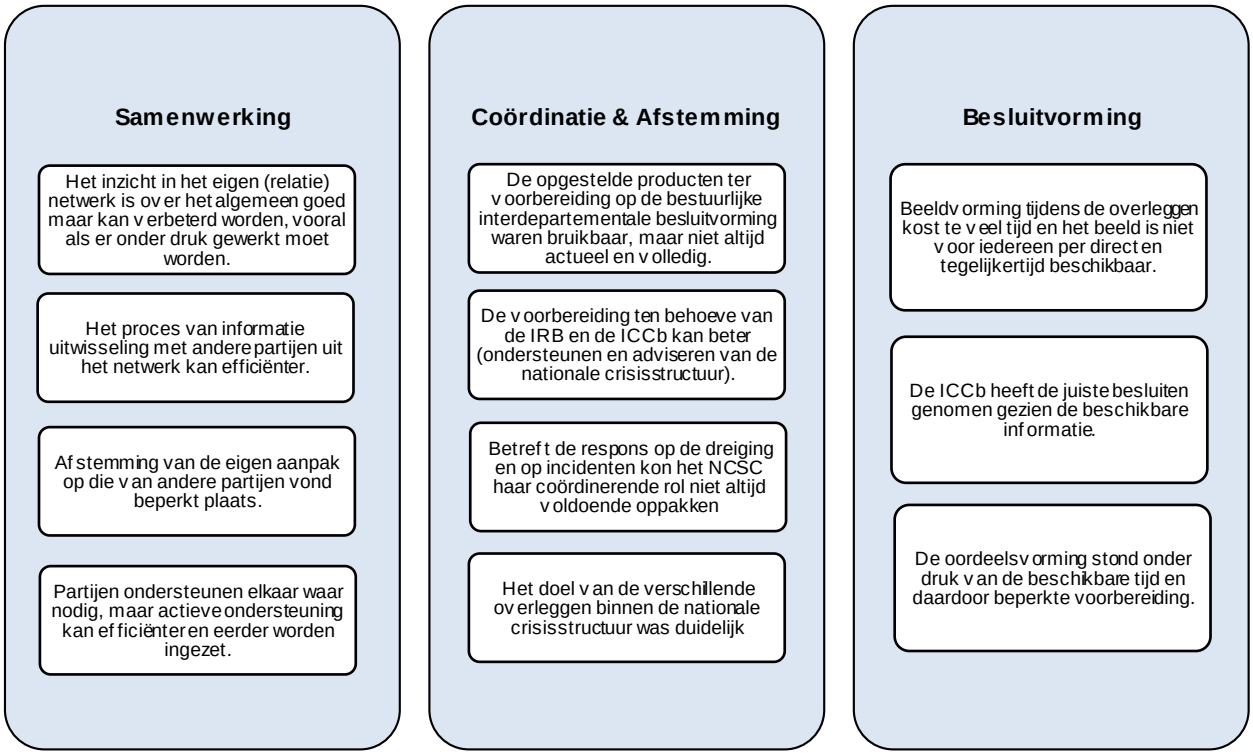
Ransomware incidenten In september 2020 wordt de Veiligheidsregio Noord- en Oost-Gelderland (VNOG) getroffen door een hack met gijzelsoftware. Het was, zover bekend, de eerste keer dat een veiligheidsregio te maken kreeg met een cyberaanval waarvan zij zelf het slachtoffer waren. De VNOG heeft na detectie direct externe hulp ingeschakeld. Bedrijven en semipublieke instellingen worden in toenemende mate doelwit van gijzelsoftware. De opbrengst voor de cybercriminelen is vaak hoog, en de pakkans klein. In Nederland was de onderwijssector een populair doelwit voor dit type aanval.

Data-exfiltratie en 'dubbele' ransom Ransomware-aanvallen gaan steeds vaker gepaard met data-exfiltratie. Wanneer slachtoffers niet willen betalen voor de ontsleuteling van hun bestanden, wordt gedreigd met het openbaar maken van verkregen data. In het eind 2020 verschenen Cyberthreats Report van Acronis, wordt gewaarschuwd dat deze trend in het komende jaar naar verwachting alleen maar gaat toenemen, en wellicht zelfs de primaire aanvalstactiek wordt van cybercriminelen.

Supply-chain aanvallen Ook supply chain aanvallen worden steeds populairder onder cybercriminelen. Bij een supply-chain aanval komen cybercriminelen binnen via een derde partij die toegang heeft tot systemen van de organisatie (bijvoorbeeld een leverancier of dienstverlener). In 2020 kwam een supply-chain incident bij SolarWinds aan het licht. Grote softwareleveranciers werden hierdoor getroffen. Ook in Nederland bleek een aantal organisaties de kwetsbare versie van de software te hebben geïnstalleerd, maar is er zover bekend geen misbruik gemaakt. Het incident toont dat supply-chain aanvallen moeilijk te detecteren zijn en lang onder de radar kunnen blijven. Het is een effectief middel om bij meerdere organisaties binnen te komen.

C. Leerpunten ISIDOOR II

ISIDOOR II vond plaats van maandag 9 oktober tot en met donderdag 12 oktober 2017. Het scenario in de oefening was een simulatie van een cybercrisis in een ICS/SCADA omgeving: procescontrole systemen voor industriële processen zoals de aansturing van bruggen, kerncentrales e.d. In onderstaande tabel een aantal bevindingen per oefendoel uit de evaluatie van de oefening. De leerpunten in een samenvattend overzicht:



Het COT is een gespecialiseerd bureau op het gebied van veiligheids- en crisismanagement. Ons werkterrein strekt zich uit van vraagstukken over security ambities en de vormgeving van lokaal 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: www.cot.nl of cot@cot.nl

Disclaimer

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.