Overkoepelende evaluatie OZON 2023

Basis op orde, tijd voor sectorale samenwerking

17 mei 2023

Inhoudsopgave

1 Inleiding ... 3
1.1 Aanleiding ... 3
1.2 Over de oefening ... 3
1.3 Aanpak evaluatie ... 4
1.4 Opbouw rapportage ... 4

2 Overkoepelend beeld en aanbevelingen ... 5
2.1 Overkoepelend beeld ... 5
2.2 Aanbevelingen ... 5

3 Observaties per oefendoel ... 7
3.1 Crisisanalyse en incidentrespons ... 7
3.2 Samenwerking en informatiedeling ... 8
3.3 Awareness ... 9

1 Inleiding

1.1 Aanleiding

ICT-coöperatie SURF organiseert sinds 2016 een tweejaarlijkse cyberoefening voor de onderwijs- en onderzoek sector. Onder de naam OZON oefent de sector met technische uitdagingen, afstemming en samenwerking en bestuurlijke en politieke vraagstukken.

Op 23 en 24 maart 2023 vond de cybercrisisoefening OZON 2023 plaats. Het was de vierde keer dat SURF de cyberoefening organiseerde. Er deden 72 organisaties en ruim 2.000 mensen in de onderwijs- en onderzoeksector mee.

1.2 Over de oefening

De oefening bestreek anderhalve dag. Daarnaast vond op donderdag 13 april een evaluatiedag plaats, waar oefenleiders en waarnemers van de betrokken instellingen met elkaar reflecteerden op de oefening.

Oefendoelen

De overkoepelende oefendoelen waren als volgt:

1. Crisisanalyse en incident response– het omgaan met de analyse van de casus en het komen tot een beeld van wat er daadwerkelijk aan de hand is
2. Samenwerking en informatiedeling – de samenwerking en informatiedeling tussen de instellingen en op sectorniveau
3. Awareness – het creëren van awareness voor cybersecurity-dreigingen, -incidenten en -crises op operationeel, tactisch en strategisch niveau

Naast de overkoepelende oefendoelen, stelde elke organisatie haar eigen organisatie-specifieke oefendoelen op. Deze worden in dit rapport niet behandeld: de focus ligt op de overkoepelende oefendoelen.

Het scenario

De oefening begint op 23 maart met de publicatie van een grote verzameling van kwetsbaarheden door een hackergroep die zichzelf de Vulnerability Liberators noemt. Zij openbaren - onder de noemer 'exploit piñata' - elke 20 minuten een nieuwe kwetsbaarheid op hun website. De kwetsbaarheden hebben geen directe impact op de rest van het scenario, en zijn vooral bedoeld om instellingen te laten oefenen met het prioriteren van informatie en ze aan te zetten om samen te werken en informatie uit te wisselen. Daarnaast worden de kwetsbaarheden door sommige instellingen gebruikt om extra injects te genereren voor hun eigen scenario.

Naast de piñatas van de Vulnerability Liberators, draait het scenario vooral om cryptomiljonair Elaine Geurtjes. Zij is van mening dat de bestuurders van de onderwijs en onderzoeksinstellingen (en SURF) hebben gefaald in het bieden van onderwijs voor iedereen. Ze start daarom ‘Operatie: Schoon Schip’ en wil de bestuurders dwingen af te treden en het hoger onderwijs forceren toegankelijker te worden. Om dit te bereiken koopt Elaine Geurtjes een aantal medewerkers van SURF en de aangesloten instellingen om die werken aan diensten die veel gebruikt worden in de sector en creëert ze zo een ‘insider threat’ voor veel van de bij SURF aangesloten instellingen. Door middel van de insiders zorgt ze voor diverse aanvallen op de sector. Er is sprake van vier verschillende insiders. De eerste twee insiders zitten bij SURF en zorgen voor problemen in de netwerkverbinding en de inlogsystemen van instellingen. Daarnaast zitten er twee insiders bij Studielink en CAMBO die sleutelen aan de integriteit van de berichtenstroom naar instellingen en studenten. Studenten ontvangen berichten die niet kloppen over de hoogte van het collegegeld, bevestiging tot uitschrijving of foutieve resultaten van examens en toetsen.

Elke instelling wordt door minstens één van de insiders geraakt. Naarmate de oefening vordert, zet ook de politiek en de media druk op de instellingen.

Oefenbeperkingen

Een oefening is altijd een simulatie van de werkelijkheid; de evaluatie moet gelezen worden met dit in gedachten. Niet alles gaat zoals het in de werkelijkheid ook zou gaan: de oefening is voorbereid en de

opschaling kan daarom ook snel verlopen en beoefend worden. Tegelijkertijd kunnen ervaringen uit de oefening voorspellen hoe de respons in werkelijkheid zou kunnen gaan. We hebben de bevindingen getoetst bij betrokken deelnemers en gevraagd of dit in werkelijkheid ook zo zou kunnen gaan.

1.3 Aanpak evaluatie

Leren van oefeningen gebeurt op verschillende niveaus en momenten. Niet alleen de ervaringen tijdens de oefening en de evaluatiedag zelf zijn leermoment, maar ook de voorbereiding draagt bij aan het leervermogen.

Elke deelnemende organisatie stelde voorafgaand aan de oefening een of meerdere waarnemers aan. Op basis van de vooraf opgestelde overkoepelende oefendoelen stelde het COT een online vragenlijst op. Deze werd door de waarnemers na het einde van de oefening ingevuld. De antwoorden dienden als input voor de evaluatiedag. Daarnaast vonden er een tweetal sessies plaats waarin waarnemers van het COT reflecteerden op de observaties en de rode draden analyseerden.

De evaluatiedag op 13 april stond in het teken van gezamenlijke reflectie. Oefenleiders en waarnemers van de deelnemende organisaties gingen met elkaar in gesprek over de overkoepelende ervaringen en leerpunten. De opbrengsten dienden als input voor deze rapportage, evenals de ingevulde vragenlijsten en de observaties tijdens de oefendagen. De focus van deze evaluatie ligt op de ketensamenwerking en niet op het handelen van elke individuele organisatie. Het COT doet op basis van de waarnemingen en de analyses daarvan een aantal aanbevelingen. Het is aan de sector zelf om te bepalen hoe ze hiermee om willen gaan.

1.4 Opbouw rapportage

In hoofdstuk 2 geven we ons overkoepelend beeld van de oefening en doen we een aantal aanbevelingen die hieruit volgen. Het overkoepelend beeld en de aanbevelingen worden verder toegelicht in hoofdstuk 3 ‘observaties per oefendoel’. Deze observaties liggen ten grondslag aan het overkoepelend beeld en de aanbevelingen.

2 Overkoepelend beeld en aanbevelingen

2.1 Overkoepelend beeld

OZON 2023 was een geslaagde oefening: meer dan 80% van de instellingen geeft aan dat de oefening heeft bijgedragen aan het bewustzijn over cybersecurity en cybercrises binnen de organisatie. Zowel tijdens de voorbereiding als tijdens de oefening zijn er nieuwe ervaringen en inzichten opgedaan rondom de crisisanalyse en incidentrespons, en informatiedeling en samenwerking. Op verschillende niveaus is sprake van informatiedeling en collegiale samenwerking binnen de organisaties. Deelnemende organisaties beschikken over een crisisprotocol, en deze wordt door een meerderheid ook tijdens de oefening gebruikt. Escalatie- en opschalingsprocedures werden gevolgd en de teams op de verschillende niveaus werkten goed met elkaar samen.

We zien dat er behoefte is aan centrale coördinatie op informatiedeling en samenwerking, zowel op technisch, als op tactisch/strategisch niveau. Op technisch niveau wordt van SURFcert verwacht dat zij een rol pakken in de coördinatie van het technische totaalbeeld. Dat doen zij op dit moment ook door middel van het delen van factsheets. Niet elke instelling is hier voldoende op aangesloten. Op bestuurlijk niveau is het nog niet duidelijk bij wie deze coördinatie zou moeten liggen. Een optie zou kunnen zijn om dat te beleggen bij de koepels of het ministerie van OCW. Het gaat daarbij om procesondersteuning en coördinatie op beeldvorming. Besluitvorming over de continuïteit ligt bij de instellingen zelf. Tegelijkertijd is het prettig om op de hoogte te zijn van de situatie en maatregelen bij andere instellingen en zorgt eenduidige communicatie voor rust bij studenten en medewerkers.

In de afgelopen jaren is er bij de individuele instellingen veel geïnvesteerd in de ontwikkeling van cyberbewustzijn en respons. Dit zien we terug tijdens OZON 2023. De conclusie is dat het nu tijd is voor sectorale samenwerking. Om dat te bereiken is het van belang om met elkaar te bespreken hoe de coördinatie op bestuurlijke samenwerking kan worden vormgegeven. Daarbij is het nodig om ook elkaars rollen en verantwoordelijkheden te bespreken: wie staat er in deze sector waarvoor aan de lat bij een cybercrisis?

2.2 Aanbevelingen

1. **Behoud wat goed gaat.** De oefening laat zien dat er al veel goed gaat. De samenwerking tussen ICT en onderwijsprocessen is beter geworden en er is op veel meer niveaus samengewerkt dan in eerdere edities van OZON. Deelnemende organisaties hebben vaak gericht getraind en geoefend op cybercrisis en dat maakt hen beter voorbereid. Het is van belang om vast te blijven houden wat goed gaat. Dit is een aanbeveling voor alle betrokken partijen.

2. **Neem het proces van technisch informatiemanagement onder de loep en zorg dat dit proces de samenwerking ondersteunt.** In de operatie zijn er een aantal dingen goed geregeld; SURFcert vult een platform met technische informatie om een overzicht te bieden. Het is wel goed om daar nog eens naar te kijken: is dat begrijpelijk genoeg, heeft iedereen voldoende tijd om de informatie te interpreteren en weet iedereen ervan? Zorg daarbij ook dat de informatie gedeeld wordt op een manier dat het de samenwerking bevordert. Oplossingen in de ene organisatie kunnen bijvoorbeeld (sneller) gedeeld worden zodat andere instellingen die kunnen overnemen. Neem hierin ook mee waar dit proces belegd kan worden. De basis hiervoor ligt al bij SURF en voor deze aanbeveling kan SURF ook het initiatief nemen.

3. **Bespreek gezamenlijk of en hoe de coördinatie op bestuurlijke informatiedeling en samenwerking kan worden vormgegeven.** Het is daarbij van belang om gezamenlijk te kijken wie de coördinatie op zou kunnen pakken, wanneer het nodig is om op bestuurlijk niveau te gaan samenwerken en op welke manier de coördinatie wordt vormgegeven. Het initiatief hiervoor zou bij de koepels moeten liggen.

4. **Bespreek met elkaar welke rol en verantwoordelijkheden de overkoepelende partijen binnen de sector hebben.** Wat kunnen instellingen verwachten van SURF, van de koepels en

van het ministerie van OCW? Is dat realistisch? Dit geldt ook andersom: wat hebben de overkoepelende partijen nodig van de instellingen om hun rol goed te kunnen vervullen? Maak de verantwoordelijkheden specifiek. Ook het initiatief voor deze ontwikkeling zou vanuit de koepels moeten komen.

5. **Beschrijf sectorale samenwerking in een sectoraal responsplan.** Voor bovenstaande gaan we steeds uit van crises die (grote) delen van de sector raken. Voor die situaties zijn er geen overkoepelende crisisplannen. Individuele instellingen zijn steeds beter voorbereid, maar sectorale voorbereiding ontbreekt. Met de toegenomen afhankelijkheid van ICT en de kwetsbaarheid van data is ook de kans op sectorale crises toegenomen. In een sectoraal of landelijk crisisplan onderwijs zou de sectorale voorbereiding vastgelegd kunnen worden. Ook dit initiatief kan vanuit de koepels gestart worden omdat het wellicht eenvoudiger is om eerst per onderwijskoepel afspraken te maken voordat er een landelijk crisisplan kan komen. Voorbeelden kunnen ontleend worden aan bijvoorbeeld de zorgsector. Het zal hier vooral gaan over afstemming, informatiedeling en mogelijke gezamenlijk woordvoering.

3 Observaties per oefendoel

3.1 Crisisanalyse en incidentrespons

Onder crisisanalyse en incidentrespons verstaan we het omgaan met de analyse van de casus en het komen tot een beeld van wat er daadwerkelijk aan de hand is en de manier waarop de crisis is afgehandeld

Het komen tot een correct beeld van de situatie was voor veel instellingen een uitdaging.
De deelnemende instellingen kregen tijdens de oefening te maken met veel input: er gebeurde, zeker aan het begin van de eerste dag, een heleboel. Elke twintig minuten werd er een nieuwe piñata gelanceerd. De technische teams van de instellingen moesten hiermee aan de slag: wat is er aan de hand en wat is de impact hiervan op onze instelling? Daarbij gold dat niet elke instelling te maken had met elke kwetsbaarheid: de impact van de piñatas was dus verschillend per instelling.

Het was een uitdaging voor instellingen om een juist en actueel beeld van de eigen situatie te maken, zowel op technisch vlak als op de impact op de continuïteit van het onderwijs of onderzoek. Een aantal instellingen geeft aan dat er heel veel informatie was, waardoor het lastig was om een goed beeld van de impact te kunnen vormen. Informatie van andere instellingen zorgde daarbij soms voor verwarring. Daarnaast was een aantal instellingen zo druk bezig met het onderzoeken van de piñatas, dat zij amper toekwamen aan het hoofdscenario (de insiders en de eisen van Elaine Geurtjes). Iets meer dan de helft van de instellingen (56%) geeft in de ingevulde survey aan dat zij een goed beeld hebben kunnen vormen van de crisissituatie en de impact op de eigen organisatie. Meer dan een derde van de organisaties (38%) geeft aan dat dit voor hen ‘een beetje’ is gelukt. Een klein deel (3%) geeft aan dat het vormen van een beeld van de crisissituatie voor hen niet is gelukt[1].

Samenwerking tussen de instellingen had hierbij kunnen helpen: het verdelen van taken met betrekking tot het onderzoeken van de kwetsbaarheden had kunnen helpen in de efficiëntie en een *overload* aan informatie kunnen voorkomen. Tegelijkertijd zagen we dat instellingen in eerste instantie zelf te druk bezig waren met het uitzoeken of de kwetsbaarheden ook voor de eigen organisatie golden en wat de (technische) impact was, waardoor er nog geen aandacht was voor de samenwerking (zie ook paragraaf 3.2).

De wisselwerking tussen technisch niveau en andere niveaus verloopt beter dan in eerdere oefeningen.
Op verschillende niveaus waren teams actief. Op technisch niveau waren veelal CERTs/beheerders bezig om het technische beeld van de situatie helder te krijgen. 70% van de instellingen geeft aan dat er binnen de organisatie voldoende technische kennis en kunde aanwezig om de crisis aan te pakken. 15% geeft aan dat dit een beetje geldt, voor 5% van de instellingen was er niet voldoende technische kennis en kunde aanwezig. Dit was in eerdere oefeningen een aandachtspunt. Ondanks de aanwezigheid van kennis en kunde, wordt opgemerkt dat niet altijd alle relevante functionarissen voldoende werden betrokken bij de respons. Zo werden bij meerdere instellingen de functionarissen gegevensbescherming onvoldoende aangehaakt, waardoor het perspectief van privacy-experts in communicatie en maatregelen gemist werd.

Naast het in huis hebben van technische kennis, is de wisselwerking tussen het technisch niveau en het tactisch/strategisch niveau van belang. Die wisselwerking is nodig om de vertaalslag van het technische niveau naar de impact op de organisatie te maken: wat betekent de uitval van systeem X voor de continuïteit van ons onderwijs en onderzoek? Het maken van de vertaalslag van technisch naar tactisch/strategisch niveau is een uitdaging die in meerdere sectoren speelt wanneer het gaat om een cybercrisis; vaak verloopt dit lastig door een verschil in taalgebruik. Dit is tijdens OZON 2023 beter gegaan dan voorheen. Het is belangrijk om hierin te blijven investeren; de crisisrespons is mede afhankelijk van die vertalers.

[1] De overige instellingen geven aan hier geen zicht op te hebben gehad

3.2 Samenwerking en informatiedeling

Onder samenwerking en informatiedeling verstaan we de manier waarop instellingen en koepelorganisaties onderling en op sectorniveau informatie hebben uitgedeeld en hebben samen gewerkt

Er is behoefte aan een totaalbeeld van de situatie. Het ontbrak tijdens de oefening aan een partij die dit totaalbeeld verzorgde.
Gedurende de oefening was er behoefte aan meer centrale informatiedeling. Iets meer dan een kwart van de instellingen (26%) geeft aan een totaalbeeld te hebben verkregen van de crisis. Een meerderheid (56%) geeft aan dat dit voor hen 'een beetje' geldt, en 10% gaf aan dat zij helemaal geen totaalbeeld hadden verkregen. Met name het centraal verzamelen en delen van essentiële informatie voor de gehele sector werd gemist. Dit had bijgedragen aan een completer beeld van de situatie. Instellingen geven aan nu zelf te moeten bedenken waar en hoe ze overkoepelende informatie verkregen, waardoor ze soms relevante informatie mistten die andere onderwijsinstellingen al wel hadden.

Tegelijkertijd wordt vaak benoemd dat te veel informatie verwarrend is. Het risico is dat men te veel uitgaat van wat er bij een ander speelt ("dan zal dat ook bij ons spelen"), terwijl dat niet altijd geldt. Hierdoor werden sommige problemen die uiteindelijk niet bij de instelling bleken te spelen wel meegenomen in de beeldvorming. Het is dus van belang om niet alleen informatie te verzamelen, maar ook te verifiëren.

Op technisch vlak speelt SURFcert een coördinerende rol als het gaat om informatiedeling. Deze rol kwam tijdens de oefening niet volledig tot zijn recht, omdat SURFcert vanuit de responscel meedeed met de oefening. Op tactisch/strategisch niveau ontbrak het tijdens de oefening aan een of meerdere partijen die het totaalbeeld verzorgen en een rol kunnen spelen in centrale informatiedeling. Een veelgehoorde suggestie is dat de koepels daar een rol in kunnen spelen, evenals het ministerie van OCW.

CERTs hebben informatie met elkaar gedeeld, maar er was weinig sprake van technische samenwerking.
Technische informatie werd door de technische teams onderling gedeeld via de SCIRT- en SCIPR-mailinglijsten. CERTs brachten elkaar daar op de hoogte van wat er bij hun eigen instelling plaatsvond. SURFcert heeft hierin een rol gespeeld: zij brachten informatie bij elkaar en stelde overzichten op van de gebeurtenissen op technisch niveau voor de instellingen. Een aantal van de instellingen zijn niet aangesloten bij SCIRT of SCIPR, en misten daarom informatie.

Toch was er naast het delen van informatie weinig sprake van technische samenwerking. Meerdere instellingen geven aan dat zij gedurende de oefening nog te veel bezig waren met het uitzoeken van de eigen situatie, waardoor zij nog geen tijd en ruimte hadden voor sectorale afstemming. Men keerde zich dus vooral naar binnen om de eigen crisis op te lossen, in plaats van om zich heen te kijken en de samenwerking op te zoeken. Tegelijkertijd hebben sommige besluiten wel impact op andere instellingen. Denk aan het afsluiten van systemen, maar ook het stilzetten van onderwijsprocessen of het sluiten van locaties zonder dat alle betrokken partijen hierover geïnformeerd zijn.

Er wordt op verschillende niveaus overlegd, maar er is weinig zicht op welke gremia actief zijn.
Op meerdere niveaus wordt instelling overstijgend overlegd. Zo stemmen de CISOs met elkaar af, net als de Functionarissen Gegevensbescherming, crisismanagers/integrale veiligheidsmanagers, bestuurders en woordvoerders. Dit werkt prettig: hier werd informatie uitgewisseld en afgestemd. Er is echter geen overzicht wie op welk niveau met elkaar afstemt en op welke manier. Daarnaast zijn niet alle instellingen op deze overleggen aangesloten.

De koepels (MBO Raad, Vereniging Hogescholen en Universiteiten van Nederland) zouden een rol kunnen spelen in het coördineren van de samenwerking op bestuurlijk niveau.
Naast het uitwisselen van informatie, was er behoefte om op bestuurlijk niveau samen te werken. Instellingen geven aan dat er nu geen sprake was van gezamenlijke duiding van de situatie (gaat het om een aanval op het onderwijs? Is er sprake van een grootschalige storing?) of het eventueel afstemmen en elkaar informeren over eigen maatregelen.

Bestuurders hebben tijdens de oefening met elkaar contact gehad op informeel niveau. Ook in appgroepen en mailinglijsten van de koepels is er onderling contact geweest. Tijdens de oefening bleek dat er niet één partij is die de coördinatie van de samenwerking op bestuurlijk niveau naar zich toe trok.

Een deel van de instellingen geeft aan dat coördinatie wenselijk is. Een ander deel zegt juist dat dit niet zou helpen; niet alle instellingen hadden met dezelfde problemen te maken en elke organisatie heeft een eigen inrichting waardoor ook in de respons ander keuzes en maatregelen worden genomen. Het is van belang om gezamenlijk te kijken waar de behoefte ligt met betrekking tot bestuurlijke samenwerking en wie daarin het voortouw neemt. Hier zou een rol voor de koepels kunnen liggen. Het gaat er daarbij niet om dat er op centraal niveau beslissingen voor de gehele sector worden gemaakt. De instellingen behouden zelf regie over hun maatregelen. Wel zouden de koepels een rol kunnen spelen in geven van een overzicht van maatregelen en besluiten en bij een gezamenlijk duiding. Deze hebben namelijk ook invloed op andere instellingen. Weten wat er bij andere instellingen speelt helpt om een afweging te maken tussen verschillende mogelijke maatregelen. Daarbij kunnen de koepels een deel van de communicatie op zich nemen.

Hierbij is ook van belang dat het voor deelnemende partijen duidelijk is welke rol de koepels en het ministerie van OCW vervullen en hoe deze rollen zich tot elkaar verhouden. Wie doet wat tijdens een cybercrisis? Tijdens de oefening bleek dat de verwachtingen hierover niet voor iedereen gelijk waren.

Coördinatie op informatiedeling en samenwerking	
INFORMATIEDELING	
Voordelen	***Uitdagingen***
Draagt voor instellingen bij aan een completer beeld van de situatie	Te veel informatie werkt verwarrend; risico is dat men zich laat leiden door informatie van een ander
Elke organisatie beschikt over dezelfde informatie	Niet alle informatie is voor elke organisatie relevant
Organisaties weten waar overkoepelende informatie gehaald kan worden	Informatie moet wel opgehaald/aangeleverd worden door instellingen en de coördinerende partij
SAMENWERKING	
Samenwerking draagt bij aan een eenduidig beeld en voorkomt mogelijk onnodige onrust	Niet elke organisatie heeft te maken met dezelfde problemen
Samenwerking kan helpen bij gezamenlijke duiding	Iedere organisatie heeft een eigen inrichtingen waardoor zij ook verschillende keuzes maken
Samenwerking zorgt voor een eenduidige communicatielijn	Samenwerking moet beperkt worden tot die thema's die ook echt om samenwerking vragen

3.3 Awareness

Onder awareness verstaan we het creëren van bewustzijn voor cybersecurity-dreigingen, -incidenten en crises op operationeel, tactisch en strategisch niveau

De oefening heeft bijgedragen aan het vergroten van awareness over cybersecurity en cybercrises. Een meerderheid van de instellingen (83%) geeft aan dat de oefening heeft bijgedragen aan het vergroten van de awareness over cybersecurity en cybercrises. Dit geldt niet alleen voor de oefening zelf, maar ook het voortraject heeft hierin geholpen. Bij sommige instellingen zijn er naar aanleiding van de oefening onderzoeken gedaan of er daadwerkelijk kwetsbaarheden zijn. Tegelijkertijd geven meerdere instellingen een kanttekening aan: bewustwording is goed, maar dat alleen is niet voldoende. Er moet ook doorgepakt worden: de ervaringen delen met de rest van de organisatie, het aanpassen van protocollen etc. Daarbij wordt ook opgemerkt dat het personeelsverloop binnen instellingen vaak hoog is. Het regelmatig blijven trainen en oefenen is daarom extra belangrijk.

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.