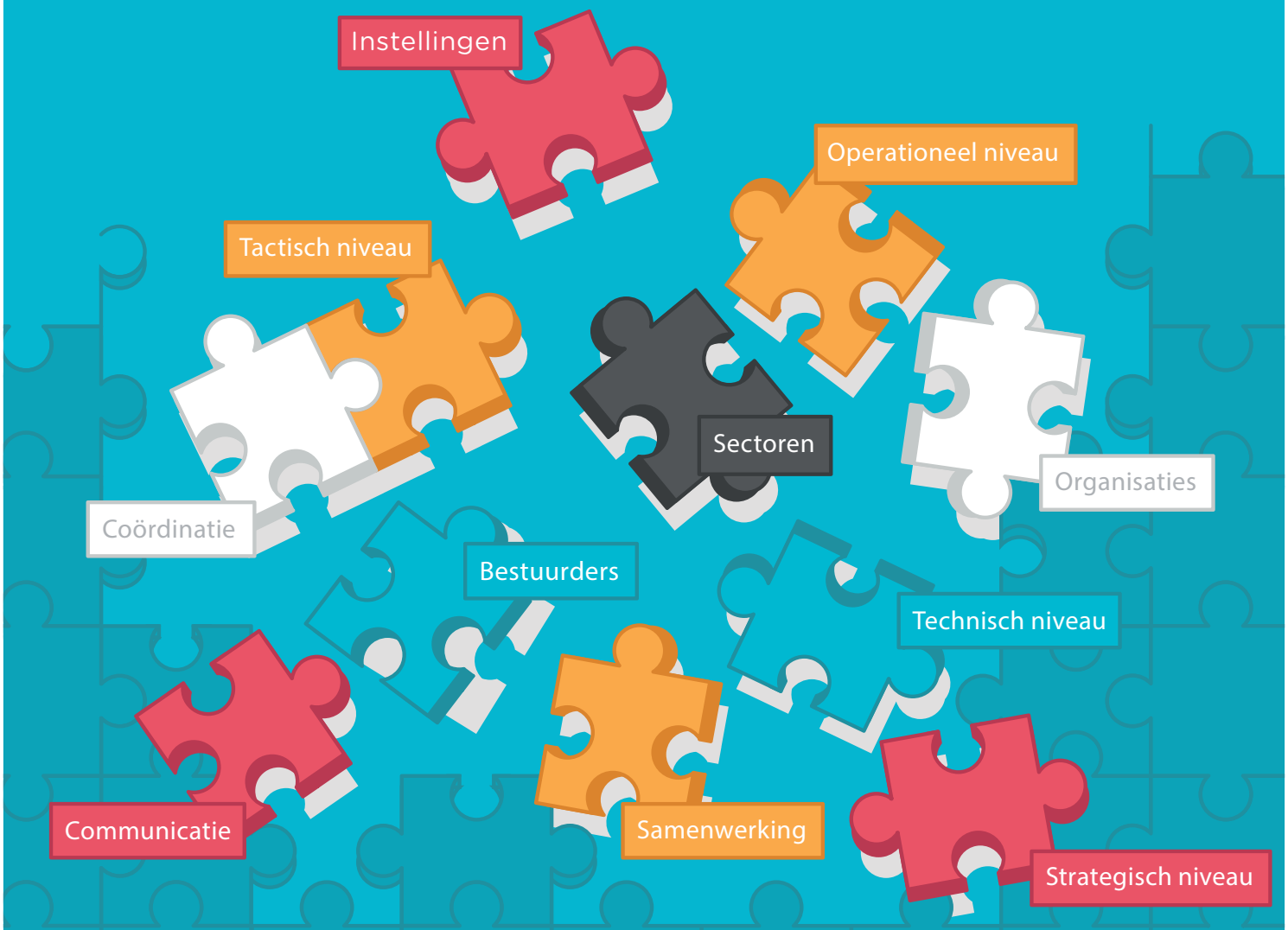
CYBERCRISISOEFENING OZON

EEN GAP BRIDGING EXERCISE



SURF NET


Data Breach
Cyber Attack
System Safety

VOORWOORD

Dat het oefenen van een grote cybercrisis noodzakelijk en nuttig is, is met het enthousiasme waarmee de crisisoefening OZON is voorbereid en uitgevoerd wel bewezen. Cyberdreigingen zijn reëel: iedere instelling kan vandaag of morgen getroffen worden door een incident. Met OZON hebben we kunnen ervaren wat het is om als universiteit zwaar onder vuur te liggen van een gemotiveerde hackersgroep. De deelnemende instellingen werden in de oefening flink op de proef gesteld met technische aanvallen en morele dilemma's. Hierdoor hebben wij op alle fronten onze procedures, interne samenwerking en escalatie kunnen testen.

De opzet van deze oefening was om zowel de technici te interesseren als de bestuurders te betrekken en hier is de oefening volledig in geslaagd. Ik heb met veel plezier de voorbereiding meegemaakt en de oefening zien ontstaan. Het is dan voor de organisatie enorm spannend of zo'n oefening ook aanslaat, zeker als het de eerste keer is en als het zo grootschalig is. Als stuurgroep waren we niet op de hoogte van de inhoud van de oefening. Hierdoor was ik in staat in mijn eigen rol in de oefening mee te spelen: een enorm boeiende en leerzame ervaring.

OZON heeft bruggen geslagen, binnen instellingen en tussen instellingen. Crisisoefeningen, in verschillende vormen en intensiteiten, zijn een noodzakelijk onderdeel geworden van de beveiligingsaanpak om de weerbaarheid van de instellingen te vergroten. Als sector zijn we er nog niet, maar we zijn op goede weg. Met OZON hebben we weer een flinke stap gezet in het in conditie houden van de bescherming van onze informatiehuishouding.

Maarten Brouwer
Directeur IT Wageningen University & Research
Voorzitter stuurgroep OZON

INHOUDSOPGAVE

1. INLEIDING

ICT en internet zijn steeds vaker onmisbaar en analoge alternatieven verdwijnen. Informatie wordt in toenemende mate via internet gedeeld, ook in het onderwijs en onderzoek. Als gevolg hiervan stijgt de mogelijke impact van cyberdreigingen op de ICT-infrastructuur, die voor de instellingen essentieel is. In de onderwijs- en onderzoekssector is al veel aandacht voor bedreigingen van de bedrijfscontinuïteit, zoals een ongeval of een terroristische aanslag. Daar komen cyberdreigingen[1] bij.

De huidige crisisstructuren zijn vaak nog onvoldoende ingericht om aan een grote cyberdreiging het hoofd te bieden. Om de organisatie beter weerbaar te maken tegen een cyberdreiging, heeft SURFnet in oktober 2016 een grootschalige cybercrisisoefening georganiseerd. Cybercrisisoefening OZON was een initiatief van SURFcert in samenwerking met SURFnet en 31 onderzoeks- en onderwijsinstellingen.

In deze whitepaper lees je hoe je een cybercrisisoefening kunt opzetten en wat het belang is van cybercrisisoefeningen voor de crisisorganisatie. Daarna wordt ingegaan op hoe cybercrisisoefening OZON is georganiseerd. Vervolgens worden de uitkomsten en aanbevelingen van de cybercrisisoefening OZON beschreven. Deze whitepaper is bedoeld voor (ICT) beleidsmakers en beveiligingsspecialisten en kan gebruikt worden als handreiking om een oefening op te zetten.

Leeswijzer
Hoofdstuk 2 biedt inzicht in de achtergrond van crisisbeheersing. Eerst wordt een definitie gegeven van (cyber)incidenten en (cyber)crisis. Aan bod komt de crisisaanpak, met onder meer aandacht voor het crisisplan. Verder komen diverse fysieke, sociale en cyberrisico's aan de orde, met voorbeelden uit de praktijk. De nadruk ligt op cyberrisico's voor onderzoeks- en onderwijsinstellingen die relevant zijn voor cybercrisisoefening OZON. Ook worden de belangrijkste actoren, dreigingen en kwetsbaarheden beschreven.

Hoofdstuk 3 laat zien welke oefeningsvormen mogelijk zijn voor specifieke doelen en geeft inzicht in het belang en in de doelen van crisisoefeningen. Het hoofdstuk beschrijft enkele voorbeelden van reeds georganiseerde cybercrisisoefeningen.

Hoofdstuk 4 beschrijft de opzet van een simulatieoefening (zoals cybercrisisoefening OZON), aan de hand van de drie stadia van een crisisoefening: de voorbereiding, de uitvoering en de evaluatie.

Tenslotte staat in hoofdstuk 5 cybercrisisoefening OZON centraal. Dit hoofdstuk start met de opzet van de oefening. Alle aspecten van de oefening komen aan bod, waaronder het scenario en de overwegingen bij het scenario, de verschillende rollen en taken in de voorbereiding en het verloop van de oefening. Vervolgens worden de uitkomsten van de oefening gepresenteerd.

Hoofdstuk 6 sluit af met aanbevelingen voor de crisisorganisatie en voor het opzetten van cybercrisisoefeningen.

[1] *Cyber wordt breed gedefinieerd en omvat zowel verstoring, uitval als misbruik van ICT. Zie ook https://www.nctv.nl/organisatie/cs/index.aspx (geraadpleegd op 20-10-2016)*

2. CRISISBEHEERSING

2.1 Van incident naar crisis

De onderwijs- en onderzoekssector is voorbereid op verschillende incidenten. De meeste incidenten hebben een operationeel karakter en worden opgepakt door de lijnorganisatie, bijvoorbeeld bedrijfshulpverlening, beveiliging of IT.

> *"Een incident is een ongewenste gebeurtenis, al dan niet opzettelijk veroorzaakt, die negatieve impact heeft op de kwaliteit van welzijn, gebouw en/of bedrijfsprocessen en die met dagelijkse procedures kunnen worden opgelost."*[2]

Een incident kan uitgroeien tot een crisis:

> *"Een crisis is een gebeurtenis die diep ingrijpt in het functioneren van een organisatie of een sociaal systeem en waarbij in onzekerheid en onder tijdsdruk ingrijpende beslissingen moeten worden genomen".*[3]

De kans op een crisis groeit door factoren als media-aandacht, onrust onder leerlingen, ouders, patiënten, werknemers of de maatschappij als geheel.

2.2 Crisisaanpak

Een gedegen voorbereiding[4] draagt eraan bij dat we de impact van een crisis kunnen beheersen. Bij een crisis is een gecoördineerde aanpak nodig om besluitvorming te regisseren en te stroomlijnen. Taken en rollen moeten helder zijn en iedereen moet snel kunnen schakelen. Bij een crisis is de dreiging, urgentie en onzekerheid over de situatie veel groter dan bij een incident, waarbij men meestal voldoende tijd heeft om te reageren.

Een crisisplan draagt bij aan het nemen van beslissingen, om onnodige escalatie te voorkomen. De meeste bestaande plannen en procedures zijn gericht op operationele processen. Er is nog weinig aandacht voor het strategisch deel.[5] Om meer aandacht aan het strategisch deel te geven, is het van belang dat professionele omgang met een crisis op directieniveau op de agenda staat en dat er concrete afspraken worden gemaakt.[6] Een crisisplan gaat onder meer in op hoe je je voorbereidt op een crisis en hoe je die beheerst. Het ministerie van OCW stimuleert dat instellingen een crisisplan opzetten en ermee oefenen. Dat doet het ministerie onder meer via het programma Integraal Veilig Hoger Onderwijs[7].

Om het crisisplan zowel beleidsmatig als organisatorisch vorm te geven, kan een coördinator worden aangewezen. De crisis coördinator kan in de voorbereidende fase het crisisplan opstellen en de samenstelling van de crisisteams vormgeven. Hij/zij kan ook de crisisoefeningen organiseren. Om een goed beeld te hebben van mogelijke risico's die tot een crisis kunnen leiden kunnen met een risicoanalyse de mogelijke risico's in kaart gebracht worden. In paragraaf 2.3 wordt ingegaan op het inventariseren van risico's.

2 *Geformuleerd op basis van http://www.bcmacademy.nl/nl/bcm-academy/informatie-over-het-vak/begrippenlijst en COT (2011) (geraadpleegd op 10-10-2016)*
3 *COT "Leren van incidenten" (2011), p. 37*
4 *http://www.integraalveilig-ho.nl/continuiteitmanagement/ (geraadpleegd op 15-09-2016)*
5 *COT "Elf Bouwstenen voor een Crisisplan" (2014) p. 2*
6 *http://crisismanagement.schoolenveiligheid.nl/algemeen/ (geraadpleegd op 12-09-2016)*
7 *www.integraalveilig-ho.nl (geraadpleegd op 10-10-2016)*

Besluitvorming en coördinatie

Tijdens een crisis is er behoefte aan heldere besluitvorming en communicatie. Bij een crisis van grote omvang is een crisisteam nodig dat coördineert en besluit. Meestal wordt eerst een operationeel crisisteam ingesteld die over operationele vraagstukken gaat. Bij een crisis van grote omvang kan het noodzakelijk zijn om op te schalen naar een bestuurlijk crisisteam. Het bestuurlijke crisisteam gaat meer over de strategische vraagstukken. De taken en verantwoordelijkheden van de crisisteams worden in het crisisplan vastgelegd. Veel beslissingen op operationeel niveau kunnen een strategische impact hebben. Een tijdige en goede informatie-uitwisseling is daarbij belangrijk. Hoe die informatie-uitwisseling vorm krijgt, kan worden vastgelegd in een alarmerings- en opschalingsstructuur. Als teams samenwerken, voorkomt dat dat er tegenstrijdige berichten naar buiten worden gebracht en dat teams langs elkaar heen werken. Nadien is het van belang ook de crisis weer af te schalen. Uit de informatie moet blijken of de crisis voldoende onder controle is. Achteraf kan geëvalueerd worden en de geleerde lessen in de organisatie worden toegepast. [8]

Externe communicatie

Steeds vaker krijgen onderwijs- en onderzoeksinstellingen tijdens een crisis te maken met persaandacht. Dit kan grote druk leggen op instellingen. Ook kunnen interne en externe stakeholders, zoals studenten en patiënten grote druk leggen op de instellingen. Het opstellen van een persprotocol en een communicatiestrategie draagt bij aan het behouden van de regie en goed kunnen communiceren naar pers en betrokkenen.

Om ervoor te zorgen dat leden van de crisisteams over de juiste kennis en kunde beschikken, kunnen opleidings-en trainingstrajecten ingezet worden. Ook bevordert regelmatig oefenen met crisisscenario's de vaardigheden van de crisisteams. [9]

In april 2016 was er media-aandacht van NRC Handelsblad voor het werkklimaat bij de Hogeschool van Utrecht. Dit bericht werd snel opgepikt door onder meer RTV Utrecht. Het College van Bestuur zag zich genoodzaakt een reactie te geven.[10]

2.3 Risico's

Een risicoanalyse geeft inzicht in de mogelijke veiligheidsrisico's en de impact ervan. Zowel fysieke, sociale als cyberrisico's kunnen uitmonden in een grote crisis.[11] Hoe groter het risico, hoe groter de kans dat de crisis een bedreiging voor de continuïteit vormt. Hoeveel impact een risico heeft, hangt af van specifieke kenmerken van de instelling zoals de gebruikers van het gebouw, de locatie, de omvang en de bedrijfsprocessen. De dreiging kan zowel van buitenaf als van binnenuit komen. Risico's ontwikkelen zich. Daarom is het goed om een risicoanalyse een jaarlijks onderdeel te maken van de 'Plan Do Check Act'-cyclus.[12] Daarin wordt beoordeeld hoe risico's zich hebben ontwikkeld en wat dit betekent voor het beleid en de maatregelen.[13]

[8] *COT "Elf Bouwstenen voor een Crisisplan" (2011), p. 12*
[9] *COT "Leren van Incidenten" (2011), p. 12*
[10] *http://www.rtvutrecht.nl/nieuws/1461998 (geraadpleegd op 20-10-2016)*
[11] *Zie ook http://www.integraalveilig-ho.nl/ voor een integraal beeld van de mogelijke risico's voor het hoger onderwijs.*
[12] *Onder andere opgenomen in ISO 27001 voor informatiebeveiliging en in ISO 22301 voor bedrijfscontinuïteit*
[13] *COT "Leren van Incidenten" (2011), p. 15*

Voorbeelden van fysieke veiligheidsrisico's zijn:
- brand
- arbeidsongeval
- ziekte
- terrorisme
- uitval van ondersteunende diensten en processen (klimaatbeheersing)

Voorbeelden van sociale veiligheidsrisico's zijn:
- fraude (tentamenfraude, plagiaat)
- discriminatie
- vandalisme
- pesterijen,
- agressie
- radicalisatie [14]

In 2008 heeft een felle brand het Bouwkundegebouw van de TU Delft verwoest. Een deel van het complex is ingestort. De brand werd veroorzaakt door kortsluiting. Op het moment dat de brand uitbrak, waren er twee-tot driehonderd man in het pand aanwezig. Gelukkig raakte er niemand gewond.[15]

Cyberrisico's

Bedrijfscontinuïteitsmanagement richt zich op het voorkomen van toekomstige incidenten en crises en het paraat hebben van alternatieven in de vorm van plannen en instrumenten. [16] Vaak zijn crisisplannen gericht op maatregelen voor directe, zichtbare en meestal fysieke schade. Hierbij is alleen nog weinig aandacht voor de risico's van cyberincidenten en cybercrises.

SURF Cyberdreigingsbeeld 2015 noemt de volgende cyberrisico's: [17]
- spionage
- verkrijging en openbaarmaking van data
- identiteitsfraude
- verstoring ICT
- manipulatie van digitale opslag van data
- overname en misbruik van ICT
- bewust beschadigen imago

2.4 Van cyberincidenten naar een cybercrisis

Een cyberincident is een 'IT-verstoring die de verwachte beschikbaarheid van diensten en/of de ongeoorloofde openbaarmaking, aankoop en/of de wijziging van informatie' verstoord.[18]

Een cyberincident, al dan niet moedwillig veroorzaakt, heeft met name operationele impact en er wordt volstaan met een technische IT-respons. Meestal heeft een incident geen blijvende gevolgen. Bestuurlijke aandacht is dan niet nodig en het

14 Zannoni, Kuipers en Wensveen "Realisme in veiligheid en crisismanagement" (2012), p. 2
15 http://www.nu.nl/algemeen/1565130/brand-verwoest-faculteitsgebouw-bouwkunde-in-delft-video.html (geraadpleegd op 20-10-2016)
16 Zannoni, Kuipers en Wensveen "Realisme in veiligheid en crisismanagement" (2012), p. 4
17 SURF Cyberdreigingsbeeld, (2015), p. 27
18 ENISA, "Strategies for Incident Response and Cyber Crisis Cooperation" (2016), p. 105

mandaat ligt bij de ICT-beheerders.[19] Een cyberincident onderscheidt zich van veel andere incidenten doordat het lang onzichtbaar kan blijven. De urgentie en de impact van het incident is dan niet meteen duidelijk.[20] Daardoor kan een cyberincident zich ontwikkelen tot cybercrisis.

> *Een cybercrisis is 'een abnormale en onstabiele situatie waarbij strategische doelen, reputatie en betrouwbaarheid in het geding komen doordat een verstoring van de IT, bewust of onbewust, het hart van de organisatie raakt.'*[21]

Een cybercrisis heeft een veel grotere impact op de organisatie dan een cyberincident. Gevolgen van een cybercrisis zijn vaak:
– verlies van vertrouwen (integriteit);
– veel (politieke en media) aandacht (reputatieschade);
– verlies van inkomsten (financiële schade).[22]

Bij een cybercrisis is niet altijd duidelijk wat nodig is om grip te krijgen op de situatie en de gevolgen voor de bedrijfscontinuïteit te overzien. Als een cybercrisis onderschat wordt, kan deze zich als een olievlek uitbreiden en ook andere partijen treffen.[23]

2.5 Cyberdreigingen voor onderwijs en onderzoeksinstellingen

Actoren

Uit het SURF Cyberdreigingsbeeld 2015 blijkt dat met name de dreiging van studenten, medewerkers, cybercriminelen en cybervandalen relevant zijn voor de onderwijs- en onderzoekssector.[24] Landelijk komt de grootste dreiging van beroepscriminelen en statelijke actoren. Ook zorgen hacktivisten (hackers met activistische doeleinden) voor dreiging.[25] Uit het Cybersecuritybeeld 2016 van het NCSC[26] blijkt dat er een groeiende dreiging van cybervandalen en scriptkiddies komt. Vaak zorgen ook interne actoren als individuen die (tijdelijk) in een organisatie aanwezig zijn of zijn geweest voor een dreiging. Voorbeelden zijn (ex)medewerkers, inhuurkrachten, leveranciers en studenten.[27]

Cyberdreigingen

In het SURF Cyberdreigingsbeeld[28] worden cyberdreigingen voor de onderwijs- en onderzoeksinstellingen geïdentificeerd.

- Instellingen zijn steeds vaker doelwit van **cyberspionageaanvallen** die als doel hebben **informatie te verkrijgen** en/of deze **openbaar te maken**.[29] Binnen wetenschappelijk onderzoek is **manipulatie van onderzoeksdata** een grote bedreiging voor de integriteit van de data.[30] Dit brengt allerlei dilemma's met zich mee op het gebied van privacy en beveiliging.[31] Wanneer de integriteit, betrouwbaarheid of vertrouwelijkheid van deze informatie in het geding komt, kan dat grote schade aanrichten.[32]

[19] *Zannoni "Van incident tot crisis: voorbereid zijn op cyber crisismanagement loont" (2016)*
[20] *http://www.cot.nl/pdf/COT-Leren-van-Dorifel-15-januari-2013.pdf (geraadpleegd op 12-09-2016)*
[21] *COT "concept scenariokaart Cyberaanval" (2016) zie ook ENISA "Report on cyber crisis cooperation and management" (2014)*
[22] *Zannoni "Van incident tot crisis: voorbereid zijn op cyber crisismanagement loont" (2016)*
[23] *http://www.cot.nl/pdf/COT-Leren-van-Dorifel-15-januari-2013.pdf (geraadpleegd op 12-09-2016)*
[24] *SURF Cyberdreigingsbeeld (2015), p. 18*
[25] *SURF Cyberdreigingsbeeld (2015), p. 19*
[26] *NCSC Cybersecuritybeeld Nederland (2016)*
[27] *NCSC Cybersecuritybeeld Nederland (2015), p. 30*
[28] *SURF Cyberdreigingsbeeld (2015)*
[29] *NCSC Cybersecuritybeeld Nederland (2015), p. 23*
[30] *Denk onder meer aan gevoelige informatie over chemische, biologische, radiologische en nucleaire informatie uit onderzoek. Zie verder NCSC Cybersecuritybeeld Nederland (2015), p. 19*
[31] *SURF Cyberdreigingsbeeld (2015), p. 15*
[32] *SURF Cyberdreigingsbeeld (2015), p. 18 is een overzicht opgenomen van de verschillende securityaspecten.*

- Onderwijs- en onderzoeksinstellingen krijgen in toenemende mate te maken met **identiteitsfraude.** Daarbij misbruiken kwaadwillenden gestolen identiteiten voor malafide doeleinden zoals spam of phishing. Een groeiende bron van zorgen zijn studenten die hun tentamen of examen door een ander proberen te laten maken om zo betere studieresultaten te halen. [33]
- Ook kan het **netwerk** van instellingen **misbruikt** worden voor malafide doeleinden.[34] De open, stabiele en snelle ICT-infrastructuur van de Nederlandse universiteiten en hogescholen is een goede uitvalsbasis voor digitale aanvallen elders. Dat kan reputatieschade opleveren voor de onderwijsinstellingen.[35]
- **Verstoring ICT:** binnen de onderwijs- en onderzoekssector komen veel DDoS-aanvallen voor. Opvallend is dat direct na schoolvakanties, tijdens tentamenperiodes en aan het begin van het schooljaar pieken in activiteit te zien zijn. [36] Het actief verstoren van de ICT-faciliteiten heeft impact op de lopende processen en is een van de manieren om schade te berokkenen. Het is van belang dat de beschikbaarheid van systemen en verbindingen hoog is en interrupties tot een minimum beperkt blijven.[37] Met name als dit grote essentiële systemen treft kan dat grote gevolgen hebben, denk bijvoorbeeld aan ziekenhuisapparatuur.
- **Bewust beschadigen imago:** waarbij bijvoorbeeld websites worden beklad of social-media- accounts worden gehackt.[38]

Kwetsbaarheden

Deze bedreigingen kunnen doel treffen als ze gebruik weten te maken van kwetsbaarheden in de technologie, het proces of van de menselijke factor.[39]

- **Technologie** - De toegankelijkheid binnen onderwijs- en onderzoeksinstellingen neemt toe.[40] Instellingen bieden steeds vaker lessen, tentaminering en opdrachten via het internet aan. Steeds meer apparaten zijn met elkaar en met het internet verbonden. Dat maakt het netwerk kwetsbaar voor potentiele aanvallen.[41] Ook zijn studenten, onderzoekers en docenten steeds meer buiten het netwerk van de instelling online, waardoor gegevens binnen de onderwijsinstelling ook buiten het campusnetwerk te vinden zijn. De traditionele beveiliging aan de rand van het netwerk is niet meer voldoende om de data veilig te stellen. Het wordt dan ook steeds belangrijker om de data zelf te beveiligen en om toegang tot de data anders te organiseren.[42] Doordat steeds meer apparaten met elkaar verbonden zijn, groeit ook het aantal apparaten dat moet worden geüpdatet. Het is niet altijd eenvoudig om systemen en apparatuur te updaten. Systemen zitten complex in elkaar of zijn afhankelijk van hardware en andere systemen.[43]

- **Proces** - Onderwijs- en onderzoeksinstellingen hebben te maken met stijgende aantallen gebruikers die vaak wisselen en met sterk groeiende hoeveelheid data. De toegang tot de data en het gebruik van die data moet goed georganiseerd zijn. Processen als identiteits- en toegangsbeheer zijn daarvoor essentieel. Hiervoor gebruiken onderwijs- en onderzoeksinstellingen steeds vaker clouddiensten.[44] Niet alleen het bedrijfsnetwerk moet goed worden beveiligd, maar ook de toegang tot clouddiensten en de opslag van data.[45] Vaak is een wachtwoord niet sterk genoeg

[33] *SURF Cyberdreigingsbeeld (2015), p. 30*
[34] *SURF Cyberdreigingsbeeld (2015), p. 32*
[35] *SURF Cyberdreigingsbeeld (2015), p. 19*
[36] *SURF Cyberdreigingsbeeld (2015), p. 39*
[37] *SURF Cyberdreigingsbeeld (2015), p. 3*
[38] *SURF Cyberdreigingsbeeld (2015), p. 27*
[39] *SANS "People, Process, and Technologies Impact on Information Data Loss"(2012) en SURF Cyberdreigingsbeeld (2015), p. 19*
[40] *ENISA Threat Landscape (2014), voorbeelden hiervan zijn beamers, printers, laptops, vaste telefonie, mobiele telefoons, tablets, maar ook ziekenhuisapparatuur, gebouwbeheerapparatuur en keukenapparatuur.*
[41] *SURF Cyberdreigingsbeeld (2015), p. 16*
[42] *SURF Cyberdreigingsbeeld (2015), p. 14*
[43] *Idem*
[44] *SURF Cyberdreigingsbeeld (2015), p. 6*
[45] *Idem*

of zijn herstelmogelijkheden zwak. Wachtwoorden kunnen hierdoor makkelijk achterhaald of veranderd worden. Er is bij de gebruiker meer bewustzijn nodig bij de keuze van wachtwoorden. Dienstaanbieders zouden betere controles moeten uitvoeren bij het veranderen van wachtwoorden. Het gebruik van veiligere inlogmethoden zoals tweefactorauthenticatie helpt het wachtwoorddilemma te doorbreken. Het risico op spionage of overtreding van privacywetgeving wordt vergroot doordat veel van de cloudopslagdiensten niet in Nederland staan.[46] In het Juridisch Normenkader voor Hoger Onderwijs[47] zijn afspraken over voorwaarden voor toegang, beveiliging en internationale aspecten van clouddiensten geregeld. Deze kunnen de basis vormen voor afspraken met cloudleveranciers.

- **Gebruiker** - De gebruiker speelt een belangrijke rol in het gebruik van de technologie en processen. Steeds vaker gebruiken studenten en medewerkers onvoldoende sterke wachtwoorden, onveilige apparaten zoals USB-sticks, of onvoldoende beveiligde clouddiensten. Gebruikers updaten hun computers en mobiele apparatuur vaak niet voldoende doordat ze soms lastig te updaten zijn. Ook stellen veel gebruikers een update uit. Ook treft spearphishing[48] steeds vaker doel doordat de nepmails bijna niet meer van echte e-mail te onderscheiden zijn. Daarnaast is social engineering nog altijd populair en vooral succesvol wanneer het gaat om gerichte activiteiten. Ook neemt de vermenging van zakelijk en privégebruik toe waardoor het voor organisaties lastig is om bijvoorbeeld phishing door middel e-mailfiltering tegen te houden.[49] Het blijkt in de praktijk lastig om algemene vaardigheden over te brengen op de gebruiker. Wat voor de gebruiker vooral werkt is het oefenen en aan de slag gaan met een duidelijk en realistisch probleem. [50]

Gerichte aanvallen op de onderwijs- en onderzoeksinstellingen

Kwaadwillenden maken gebruik van de kwetsbaarheden van de onderwijs- en onderzoekssector. De meeste aanvallen om gevoelige data te verkrijgen worden gedaan met spearphishing. Deze tactiek is een geavanceerde digitale aanval waarbij phishing-e-mails verspreid worden die bijna niet meer van echt zijn te onderscheiden.[51] De e-mails zijn gericht op een enkele of een beperkte groep personen binnen een bedrijf. Ze zijn bedoeld om specifieke informatie te achterhalen en om toegang te krijgen tot de interne netwerken van organisaties. Een voorbeeld van spearphising is een e-mail waarin de aanvaller zich voordoet als de CEO of CFO van het bedrijf (CEO/CFO fraude). Hoewel er methoden bestaan om e-mails als authentiek te kunnen identificeren[52], worden die nog weinig gebruikt. Als er malware via websites of besmette e-mails wordt verspreid, spreken we van wateringhole-aanvallen.[53]

Cybercriminelen maken steeds vaker gebruik van verschillende methoden gedurende een lange tijd, ook wel Advanced Persistent Threats (APT's) genoemd. Doordat ze vaak de bestaande beveiligingsmaatregelen omzeilen, zijn ze moeilijk te detecteren. Via Remote Acces Tools (RAT's) is het mogelijk veel functies van de gewone gebruiker over te nemen.[54] Ze richten hun aanvallen vaak op systeembeheerders, onderzoekers of bestuurders van onderwijs- en onderzoeksinstellingen.[55] Actoren richten zich zelden op één organisatie, maar meestal op tientallen publieke en/of private organisaties tegelijkertijd.

[46] *NCSC Cybersecuritybeeld Nederland (2015), p. 5*
[47] *SURF Juridisch Normenkader (Cloud)services 2016 - geraadpleegd via https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html op 16 november 2016*
[48] *Spearphishing is een geavanceerde digitale aanval waarbij phishing-e-mails gericht op een of meerdere specifieke personen worden verspreid.*
[49] *NCSC Cybersecuritybeeld Nederland (2015), p. 43*
[50] *NCSC Cybersecuritybeeld Nederland (2015), p. 10*
[51] *Het 'vissen' naar inlog- en andere gegevens van gebruikers*
[52] *Denk aan; digitale handtekeningen, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), en Domain-Based Message Authentication, Reporting and Conformance (DMARC)*
[53] *Dit worden wateringhole-aanvallen genoemd. Zie ook NCSC Cybersecuritybeeld Nederland (2015), p. 43*
[54] *NCSC Cybersecuritybeeld Nederland (2015), p. 41*
[55] *SURF Cyberdreigingsbeeld (2015), p. 16*

In 2015 werden 7000 phishingmails zogenaamd vanuit INholland verstuurd naar studenten met als doel om studentgegevens te achterhalen.[56] Ook zorginstellingen zijn steeds vaker het doelwit van spearphishing omdat medische gegevens steeds interessanter worden voor cybercriminelen.[57]

Impact

Een crisis kan grote impact hebben op de organisatie (organisatie, onderzoek en bedrijfsvoering[58]) en gepaard gaan met verlies van inkomsten (financiële schade), verlies van vertrouwen (integriteit) en veel aandacht van stakeholders, politiek en media (imagoschade). Soms kan een crisis zelfs verlies van levens veroorzaken.[59] Vaak is er bij een crisis sprake van meerdere vormen van schade.

- **Dienstverlening** - Uitval van ICT-systemen en primaire processen zorgen voor grote verstoring van de dienstverlening. Als bijvoorbeeld essentiële ICT-systemen en medische apparaten van ziekenhuizen geraakt worden kan dat fatale gevolgen hebben voor de patiënten. Uitval van systemen voor onderwijs en onderzoek kan gevolgen hebben voor de uitvoering; lessen en tentamens vinden geen doorgang, onderzoek moet worden uitgesteld of overnieuw gedaan worden.

Dat uitval van het netwerk vervelende gevolgen heeft voor de dienstverlening, ondervond het ROC West Brabant Breda-Noord in 2013. Wekenlang kon deze instelling niet of nauwelijks gebruik maken van het netwerk, doordat een student het computernetwerk met DDoS-aanvallen had platgelegd.[60]

- **Financiële impact** - De economische impact van een cybercrisis is meestal groot. Onderzoeksinstellingen beschikken vaak over uiterst gevoelige data, waarbij verlies en openbaarmaking kunnen leiden tot ingrijpende aansprakelijkheidsclaims. Dit kan als gevolg hebben dat studenten besluiten elders te gaan studeren, dat subsidies van bijvoorbeeld het NWO wegvallen en dat derdegeldstroomopdrachten aan anderen worden gegund.[61] Als bedrijfsgevoelige informatie op straat komt te liggen, kan dat direct invloed hebben op de concurrentiepositie van dat bedrijf en tot schadeclaims leiden. Wanneer nog niet gepubliceerde onderzoeksgegevens openbaar gemaakt worden kan dit leiden tot een verslechterde concurrentiepositie. Een slechte reputatie in het onderwijsproces kan leiden tot minder aanmeldingen, wat ook de nodige financiële gevolgen met zich meebrengt. Ook kost crypto- en ransomware vaak veel geld. Naast het betalen van de hoge bedragen aan de criminelen zijn ook hoge kosten gemoeid met herstelwerkzaamheden en met het niet beschikbaar zijn van het netwerk.

[56] *http://www.at5.nl/artikelen/148428/waarschuwing_voor_phishingmail_inholland (geraadpleegd op 20-10-2016)*
[57] *NCSC Cybersecuritybeeld Nederland (2015), p. 76*
[58] *SURF Cyberdreigingsbeeld (2015), p. 19*
[59] *Zannoni "Van incident tot crisis: voorbereid zijn op cyber crisismanagement loont" (2016)*
[60] *http://www.nu.nl/tech/3627406/16-jarige-jongen-opgepakt-cyberaanval-school.html (geraadpleegd op 16-10-2016)*
[61] *SURF Cyberdreigingsbeeld (2015), p. 28*

In 2015 was de VU het slachtoffer van ransomware.[62] Ongeveer 200 computers waren besmet. De malware heeft zich verspreid via e-mailbijlagen. De impact kon worden beperkt doordat er goede backups waren, hierdoor hoefde het geëiste bedrag niet te worden betaald. De geschatte schade voor deze crisis was 154.000 euro.[63] In juni 2016 heeft een universiteit in Canada wel het gevraagde bedrag van 20.000 dollar betaald om weer toegang te krijgen tot e-mails en andere ge-encrypte files.[64]

- **Verlies van vertrouwen en imagoschade** - Bij een (dreigende) cybercrisis worden vaak individuele, organisatorische en maatschappelijke belangen geschaad. Wanneer gevoelige informatie over de instelling of over anderen op straat komen te liggen, tast dat het vertrouwen en het imago van de instelling aan. Mensen kunnen het vertrouwen in de instelling verliezen als ze zich zorgen maken over datalekken, privacywaarborgen en onvoldoende beschikbaarheid van ICT-services. Ze zullen dan wellicht minder gebruikmaken van de ICT-services of voor alternatieven kiezen.[65] Dit kan ervoor zorgen dat de economische groei of innovatieve ontwikkelingen worden geremd.

Een dergelijke crisis bleek in juni 2016 een reëel risico, toen in het informatiesysteem van de Universiteit van Amsterdam (UvA) en de Hogeschool van Amsterdam (HvA) een lek werd gevonden waardoor de gegevens van 385.000 studenten van de HvA en van 237.000 van de UvA op straat kwamen te liggen. Een student had toegang tot deze gegevens via een deel van het systeem dat niet meer gebruikt werd, maar nog wel toegankelijk was.[66]

In 2011 werden hackende scholieren van het Thorbecke Lyceum in Rotterdam betrapt op het stelselmatig aanpassen van cijfers. Tegen betaling zouden ze dit ook voor andere studenten hebben gedaan. Ze konden dit doen doordat ze wachtwoorden van docenten in bezit hadden. In 2014 gebeurde iets soortgelijks bij het Barlaeus Lyceum in Amsterdam, waar studenten een jaar lang toegang hadden tot het registratiesysteem van de school. Ze verhoogden cijfers en verwijderden meldingen van absenties.[67]

In 2012 stonden tientallen medische dossiers en de gegevens van 493.000 patiënten van het Groene Hart Ziekenhuis in Gouda op een server die nauwelijks beveiligd was. Daardoor waren de gegevens via internet toegankelijk.[68]

Vergroten van weerbaarheid

Om de weerbaarheid te vergroten moet allereerst duidelijk zijn waar de zwakke plekken zitten en tegen welke dreigingen de organisatie weerbaar moet zijn. Hiervoor kan een risicoanalyse gebruikt worden. Omdat alle omstandigheden voortdurend aan verandering onderhevig zijn is een gestructureerde aanpak nodig bijvoorbeeld door een securitymanagement proces in te richten. Het is verstandig hierbij aansluiting te zoeken met ander veiligheidsgebieden en een integraal veiligheidsbeleid op te stellen.

[62] *http://infosecuritymagazine.nl/2015/03/11/vrije-universiteit-amsterdam-besmet-met-ransomware/ (geraadpleegd op 16-10-2016)*
[63] *SURF Cyberdreigingsbeeld (2015) p. 28*
[64] *http://www.bbc.com/news/technology-36478650 (geraadpleegd op 16-10-2016)*
[65] *NCSC Cybersecuritybeeld Nederland (2015), p. 52*
[66] *http://www.nu.nl/internet/4280591/studentgegevens-uva-en-hva-waren-makkelijk-vindbaar-systeemlek.html (geraadpleegd op 16-10-2016)*
[67] *http://www.nu.nl/internet/2427939/hackende-scholieren-betrapt-cijferfraude.html en http://www.nu.nl/binnenland/3931116/cijferfraude-leerlingen-amsterdams-gymnasium.html (geraadpleegd op 16-10-2016)*
[68] *http://www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medische-dossiers.html (geraadpleegd op 16-10-2016)*

- **Securitymanagement** - Het managementsysteem voor informatiebeveiliging beschermt de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie door een risicobeheerproces toe te passen. Daarnaast geeft het systeem belanghebbenden het vertrouwen dat risico's adequaat worden beheerd.[69]
  Een onderdeel van securitymanagement is het in kaart brengen van de waardevolle 'bezittingen'[70] van een organisatie. Daarnaast laat het zien welke dreigingen er zijn tegen die bezittingen en hoe die het beste daartegen beschermd kunnen worden. De organisatie legt daarvoor de taken en verantwoordelijkheden vast. De beschermingsmaatregelen zijn een mix van beleidsmaatregelen en operationele maatregelen die onderhouden worden en periodiek geëvalueerd worden. Een crisisoefening is een voorbeeld van een ultieme test om de effectiviteit van de genomen maatregelen voor het beschermen van de bezittingen van een organisatie te toetsen.

- **Risicomanagement** – Om in kaart te brengen welke dreigingen er zijn, voeren instellingen risico-inventarisaties uit. Met een risico-inventarisatie en -analyse brengen ze de risico's in kaart. Risicomanagement leidt ertoe dat instellingen doelbewust securitymaatregelen inzetten als integraal onderdeel van de bedrijfsvoering van het bedrijf.[71] Het is goed om inzicht te hebben in de cyberrisico's die crisispotentie hebben.[72] Cyberrisico's veranderen voortdurend. Daarom stelt SURFnet elk jaar een Cyberdreigingsbeeld[73] op voor de onderwijs- en onderzoeksector. Dat beeld kunnen instellingen gebruiken om de risico's elk jaar opnieuw in te schatten en het crisisplan daarop in te richten. Het inzichtelijk hebben van de mogelijke risico's maakt dat dreigingen snel gedetecteerd kunnen worden en dat er gehandeld kan worden.

- **Cyber onderdeel van crisisplan -** Omdat een cybercrisis zowel operationele als strategische maatregelen nodig heeft is het van groot belang dat de informatie gedeeld wordt en dat er tijdig besluiten genomen kunnen worden. In het crisisplan kunnen goede afspraken gemaakt worden, zodat de IT-afdeling op tijd kan handelen en de cybercrisis naar het strategisch niveau kan brengen. Ook is het handig als de IT-afdeling onderdeel is van het crisisteam. Het onderwerp cyber moet een vast onderdeel zijn van het crisismanagementplan.

- **Awareness** – Als je het bewustzijn van mensen vergroot, kun je menselijke fouten voorkomen. Als gebruikers zich realiseren wat de gevolgen van hun eigen handelen kunnen zijn, gedragen ze zich veiliger. Daarom proberen verschillende campagnes, waaronder 'Cybersafe Yourself',[74] meer bewustzijn te creëren.

- **Operationele maatregelen** – Bewustwording is niet altijd voldoende. Daarom moeten ook andere maatregelen genomen worden om weerbaar te zijn tegen een crisis.[75] Zo is een extra methode als tweefactorauthenticatie nodig om het risico te verkleinen dat kwaadwillenden en andere onbevoegden[76] aan wachtwoorden en usernames komen. Daarnaast versleutelen organisaties steeds vaker informatie bij het opslaan en verzenden van data.

[69] *ISO 27001:2013 Information Security Management, okt. 2013*
[70] *Zowel fysiek als logisch: kennis en informatie*
[71] *NCSC Cybersecuritybeeld Nederland (2015), p. 12*
[72] *Zie paragraaf over cyberrisico's.*
[73] *https://www.surf.nl/persberichten/2015/12/surf-publiceert-cyberdreigingsbeeld-2015.html (geraadpleegd op 15-10-2016)*
[74] *https://www.cybersaveyourself.nl/ zie ook: https://www.surf.nl/diensten-en-producten/cybersave-yourself/index.html (geraadpleegd op 10-10-2016)*
[75] *Denk aan DKIM, SPF en DMARC*
[76] *Zoals de eerder beschreven methoden (spearphishing en APT's)*

Samenwerking binnen instellingen en tussen instellingen

In de digitale samenleving zijn de ICT-structuren sterk met elkaar verweven. Omdat binnen de onderwijs- en onderzoekssector de connectiviteit groot is en omdat instellingen veel data uitwisselen, hebben cybercrises vaak impact op meerdere instellingen. Soms is de cybercrisis zelfs sectorbreed of sectoroverstijgend. Cyberrisico's kunnen daarom niet meer door één organisatie worden aangepakt; samenwerken is noodzakelijk.
Ook is kennis nodig om een crisis goed aan te pakken. Als organisaties kennis met elkaar delen, is minder inspanning nodig om een completer beeld te krijgen van de situatie. Door samen te werken kunnen ze sneller reageren en in onderling overleg tot een adequate respons komen. Daarnaast zorgt samenwerken er ook voor dat organisaties beter weten hoe ze moeten reageren op een cybercrisis. Zowel nationaal als internationaal zoeken organisaties steeds meer de samenwerking op.[77]

Oefenen met cybercrisisscenario's

Oefenen met cybercrisisscenario's leert instellingen hoe ze in de praktijk op een crisissituatie moeten reageren. Er worden steeds vaker cybercrisisoefeningen georganiseerd voor verschillende sectoren.[78] Door mee te draaien in dergelijke oefeningen leren medewerkers en organisaties wat zij moeten en kunnen doen bij een dreigende cybercrisis.[79] Daarnaast is leren van elkaar minstens zo waardevol.

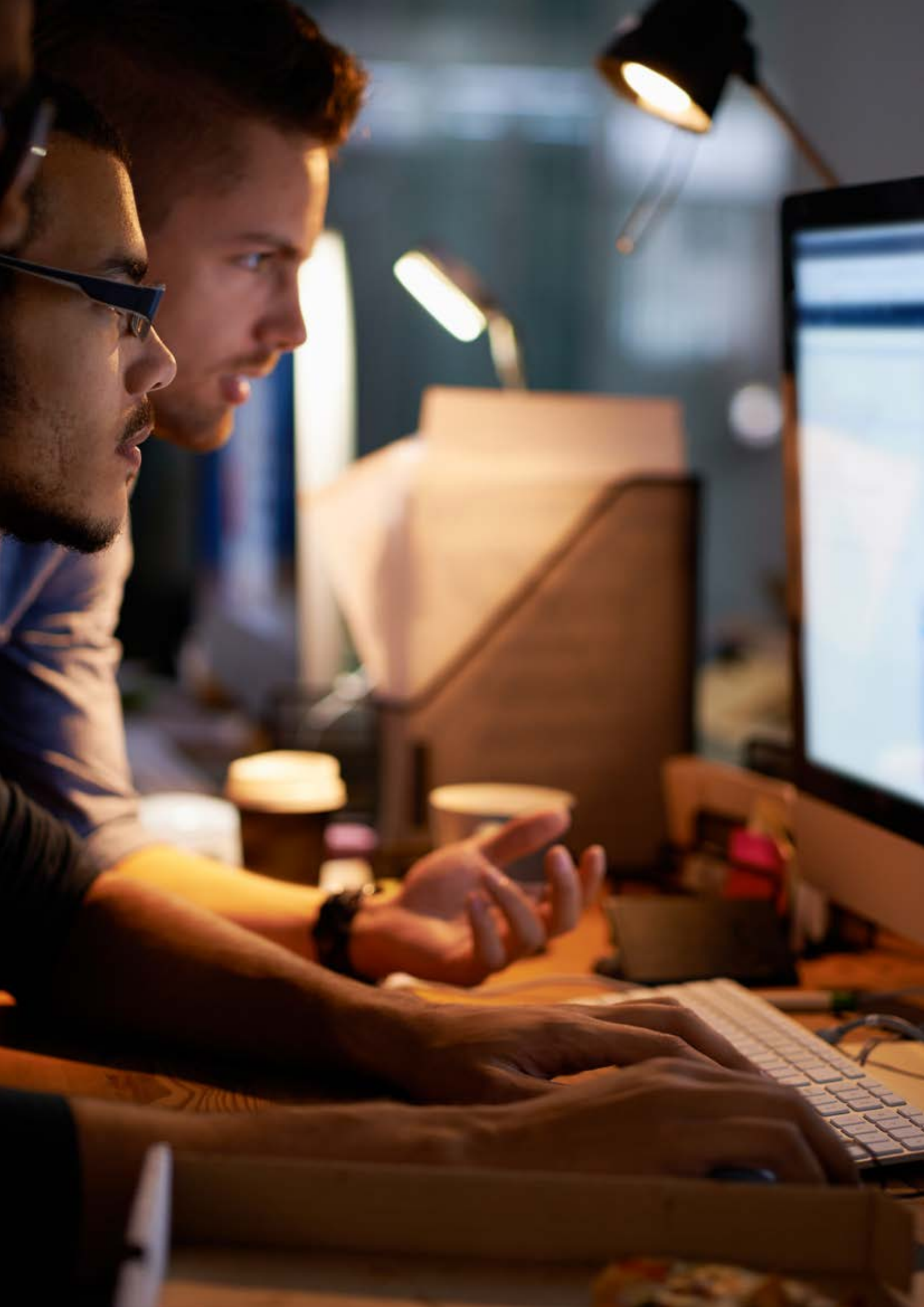
2.6 Conclusie

Wanneer een instelling onvoldoende weerbaar is kan een kwaadwillende actor actief gebruik maken van kwetsbaarheden en is een instelling ook kwetsbaar voor ander onheil. Belangen van de instellingen en andere partijen kunnen worden geschaad. Om het hoofd te bieden aan dreigingen zal de instelling ervoor moeten zorgen dat ze weerbaar is en blijft. Het is daarbij essentieel dat de betrokkenen zich bewust zijn van de risico's en de vaardigheden hebben om zich te verdedigen tegen een aanval. Ook operationele en strategische maatregelen zijn hierbij essentieel. Een van die strategische maatregelen is dat een instelling de weerbaarheid verhoogt door cybersecurity onderdeel te maken van de algemene crisisaanpak.

SURFnet speelt een actieve rol in het verbeteren van de weerbaarheid tegen cyberdreigingen en draagt bij aan de samenwerking tussen de onderwijs- en onderzoeksinstellingen, onder andere door het jaarlijks opstellen van een sectorspecifieke Cyberdreigingsbeeld. Een nieuw hulpmiddel daarbij is dat we oefenen met een cybercrisis. Zo'n oefening zorgt voor meer draagvlak voor cybersecurity op bestuurlijk niveau. Dat geldt met name voor die cyberrisico's die een veelomvattende cybercrisis kunnen worden, met imagoschade als gevolg. Een dergelijke crisis is niet alleen met een technische maatregel op te lossen. In het verleden is al gebleken dat dergelijke scenario's realistisch zijn.

Om de weerbaarheid tegen cyberdreigingen te vergroten, heeft SURFnet in oktober 2016 de eerste Cybercrisisoefening OZON voor aangesloten instellingen georganiseerd. Alvorens in te gaan op de aspecten van cybercrisisoefening OZON zal eerst ingegaan worden op de vormen en achtergronden van crisisoefeningen in het algemeen.

[77] *Voorbeelden hiervan zijn de samenwerkingen binnen de banken op nationaal en internationaal niveau en binnen de (internationale) telecomsector. Zie ook ENISA "On national and International Cyber Exercises" (2012), p. 2*
[78] *Voorbeelden hiervan zijn; Op 13 en 14 oktober 2016 heeft ENISA's Cyber Europe (Europees) oefening plaatsgevonden, in juni 2015 ISIDOOR, georganiseerd door het NCTV (nationaal), en in oktober 2014 CyberDawn voor de telecomsector (nationaal)*
[79] *NCSC Cybersecuritybeeld Nederland (2015), p. 52*



3. CRISISOEFENINGEN

3.1 Inleiding

De weerbaarheid van een organisatie tegen een crisis wordt groter door te oefenen met een crisisscenario. Bij sociale en fysieke veiligheidsrisico's is het al gebruikelijk om te oefenen. Bij cyberdreigingen is dit in opkomst. De algemene werkwijze van crisisoefeningen kan toegepast worden op cybercrisisoefeningen. In dit hoofdstuk wordt daarom eerst de algemene achtergrond van crisisoefeningen uiteengezet om vervolgens in te gaan op cybercrisisoefeningen.

3.2 Het belang van oefenen

Medewerkers worden zich bewust van de mogelijke risico's door te oefenen met een crisisscenario. Omdat werknemers beslissingen vaak onder druk moeten nemen, is het goed om deze vaardigheden te trainen. Daarnaast kunnen de crisisstructuren aan de (fictieve) werkelijkheid getoetst worden. Hieruit kan afgeleid worden of de crisisstructuur goed is ingericht en of mensen elkaar weten te vinden. Een ander effect van het oefenen met crisisscenario is dat leden van het crisismanagementteam elkaar onderling beter leren kennen in crisisomstandigheden.[80] De oefeningen verbeteren zowel de interne als de externe samenwerking. Hierdoor kunnen werknemers snel en effectief handelen bij een echte crisis. Bovendien kunnen de geleerde lessen van de oefening gebruikt worden om de crisisorganisatie te verbeteren. [81]

3.3 Doel van oefening

Een van de eerste stappen bij het opzetten van een oefening is om het doel van de oefening vast te stellen; dit bepaalt het verloop en de evaluatie van de oefening. In de ISO richtlijn voor crisisoefeningen worden 5 hoofddoelen onderscheiden: verkennen, testen, trainen, samenwerken en experimenteren.[82]

1. Bij **verkennen** gaat het om een eerste verkenning van een crisissituatie of samenwerking met een relevante partijen. De focus ligt op de inhoud (crisisspecifiek) of meer algemeen (samenwerking, communicatie). [83]

2. Bij **testen** en evalueren van de vaardigheden van deelnemers, organisaties en systemen ligt de nadruk op de kritische processen zoals: melden en alarmeren, opschalen, informatie managen en leidinggeven en coördineren. Getest wordt of de crisisorganisatie in staat is om met een crisis om te gaan. [84]

3. Bij **trainen** gaat het om het trainen, leren en ontwikkelen van competenties van individuen. Dit kan bijdragen aan het verdiepen van individuele kennis en inzicht.[85] [86] [87] De deelnemers kunnen het geleerde in de organisatie toepassen.

[80] http://www.cot.nl/w/Artikel-COT-in-Magazine-Nationale-Veiligheid.pdf (geraadpleegd op 12-09-2016)
[81] ENISA "On national and International Cyber Exercises" (2012), p. 7
[82] ISO 22398:2013 Social Security - Guidelines for exercises, sept. 2013, p. v
[83] Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie", (2013), p. 7
[84] Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie", (2013), p. 7
[85] Idem
[86] ISO 22398:2013 Social Security - Guidelines for exercises, sept. 2013
[87] ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 17

4. Bij **samenwerken,** krijgen mensen en organisaties de kans om te leren samenwerken aan een gemeenschappelijk doel en gezamenlijk een resultaat te bereiken.[88]

5. Bij **experimenteren** proberen de deelnemers nieuwe methoden en/of procedures uit met de bedoeling om bestaande methoden en procedures te verfijnen. [89]

Oefendoelen op organisatieniveau

Op basis van bovenstaande hoofddoelen kunnen specifieke, organisatiegerichte oefendoelen worden geformuleerd. Bij crisisoefeningen zijn de meest voorkomende subdoelen: het testen van de procedures, de besluitvorming, de kritische processen, en de interne en externe communicatie en het trainen van deelnemers en het opdoen van ervaring. Bij cybersecurityoefeningen ligt de focus veelal op het testen en het ontwikkelen van vaardigheden, het trainen van deelnemers en het verdiepen van kennis.[90]

Op basis van hoofddoelen kunnen organisaties subdoelen formuleren. Veel voorkomende subdoelen zijn: [91]

Procedures en oordelen
- kennen en toepassen van plannen, procedures, processen en structuren
- beeld-, oordeel- en besluitvorming

Interne en externe communicatie
- afstemmen en communiceren
- crisiscommuniceren
- samenwerken
- functioneren van een team

Kritische processen
- alarmeren en opschalen
- informatie managen
- leidinggeven en coördineren

Ervaring
- Ervaring opdoen en bedreven raken

3.4 Vormen van crisisoefeningen

Er bestaan verschillende vormen van crisisoefeningen. Het doel van de oefening bepaalt welke crisisoefening geschikt is. Elke vorm heeft zijn eigen formats, methoden, kosten en opbrengsten.

Crisisoefeningen kunnen in twee typen worden ingedeeld:
1. **Discussie-oefeningen**[92] waarbij deelnemers vertrouwd raken met de plannen, het beleid en de procedures. Bij discussie-oefeningen wordt een specifiek dilemma voorgelegd waar deelnemers in een vooraf gedefinieerde vorm over discussiëren.

2. **Praktijkoefeningen** worden gebruikt om plannen, beleid en procedures te testen en medewerkers te trainen. Meestal kiest men voor een vorm van simulatie die aansluit op een realistische omgeving. [93]

[88] *ISO 22398:2013 Social Security - Guidelines for exercises, sept. 2013, p. v*
[89] *ISO 22398:2013 Social Security - Guidelines for exercises, sept. 2013, p. v*
[90] *ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 17*
[91] *Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, (2013), p. 19*
[92] *ISO 22398:2013 benoemt ze ook wel als "dilemma exercises"; art. 5.2.13, p. 16*
[93] *ISO 22398:2013, art. 5.2.13, p. 16*

Voorbeelden van discussie-oefeningen[94]

- **Desk Check** - Een desk check is een methode om (wijzigingen van) plannen en procedures te valideren. Meestal gebeurt dit in een gesprek met de auteur van de plannen en procedures. In dit gesprek worden de plannen en procedures aan de hand van een scenario stap voor stap doorlopen. Dit maakt duidelijk welke stappen nodig zijn en hoe deze uitgevoerd moeten worden.[95]

- **Walkthrough** - Een walkthrough geeft de mogelijkheid om een specifiek scenario, bijvoorbeeld een cybercrisis, uit te diepen. Een walkthrough laat zien wie wat wanneer doet en wat voor maatregelen je kunt nemen. Met een walkthrough kan heel specifiek de verschillende stappen in een crisis doorlopen worden, van detectie tot opschaling, respons, nabehandeling en afsluiting van de situatie. Een walkthrough duurt gemiddeld een dagdeel.[96] Een walkthrough kan zowel intern geoefend worden als met andere partners die een rol tijdens een crisis spelen.

- **Workshop** – In een workshop kan naast het stap voor stap doorlopen van een scenario ook de reacties en acties van deelnemers besproken worden. Het is mogelijk om de reacties en acties van teams en individuele deelnemers te repeteren zonder tijdsdruk. Dit helpt om goed met crisissituaties en scenario's om te gaan.

- **Tabletop-oefening** - Bij een tabletop-oefening worden aspecten van het crisis-management doorlopen. Spelers krijgen van tevoren dezelfde informatie over de gesimuleerde crisissituatie en over hun rol. Tijdens de oefening kunnen spelers gebruik maken van gesimuleerde (media)berichten. Het crisisteam kan met de tabletop relevante informatie delen, overzicht krijgen en (adequate) besluiten en (communicatie)maatregelen nemen.[97] Een tabletop is een goede optie als men in relatieve rust de crisisstructuur en de onderlinge samenwerking wilt oefenen en/of specifieke vaardigheden wilt trainen. Ook wanneer een organisatie (nog) niet toe is aan een interactieve simulatieoefening is een tabletop-oefening een goede optie.

Voorbeelden van praktijkoefeningen

- **Comms check** - Een Comms check (oproepoefening) voer je uit om communica-tiemethoden en kennisgevingssystemen te checken en valideren. Deze oefenvorm wordt gebruikt om de systemen en infrastructuur te checken en te testen of alles werkt.[98]

- **Distributed tabletop-oefening** – Bij de distributed tabletop-oefening worden plannen en procedures doorlopen op basis van een scenario waarbij spelers hun rol volgens routine spelen.[99] Deze oefening is qua opzet gelijk aan een tabletop-oefening, maar er is geen mogelijkheid tot discussie. Deelnemers moeten handelen alsof er daadwerkelijk een crisis plaatsvindt. De mogelijke reacties kunnen even-tueel later in een evaluatie worden besproken. Dit heeft als voordeel dat deel-nemers de handelingen routinematig kunnen oefenen.

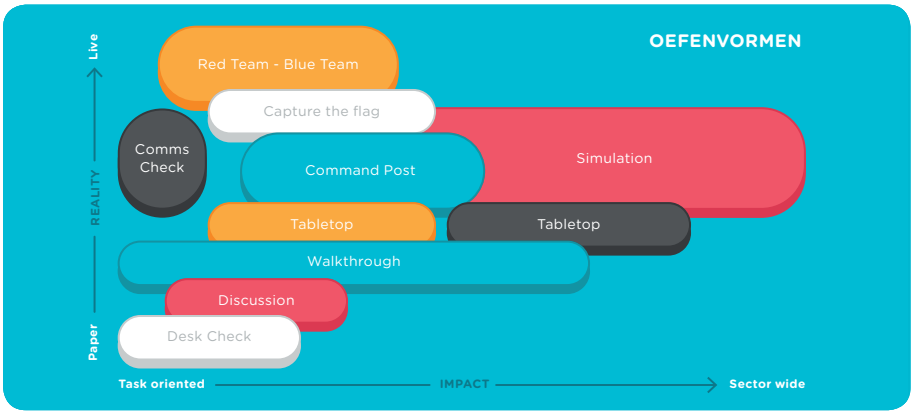
- **Een Command Post Exercise (CPX)**[100] - Bij een CPX (zandbakoefening) wordt een crisis gesimuleerd zonder inzet van hulpdiensten, externe omgevingsfactoren en spelers. De crisisteams krijgen in een realistisch en evoluerend scenario vragen en opdrachten. Zo kunnen de teams in hun eigen omgeving met hun eigen faciliteiten, acties en reacties op een veranderend scenario oefenen.[101]

[94] *dit kan ook computerbased learning zijn.*
[95] *ENISA "On national and International Cyber Exercises" (2012), p. 15*
[96] *http://www.cot.nl/crisismanagement/crisisoefeningen/walkthrough/ (geraadpleegd op 05 september 2016)*
[97] *http://www.cot.nl/crisismanagement/crisisoefeningen/tabletop/ (geraadpleegd op 05 september 2016)*
[98] *ENISA "On national and International Cyber Exercises" (2012), p. 15*
[99] *Idem*
[100] *http://www.pm.be/oefeningen_op_maat/command_post_exercise.html (geraadpleegd op 12-09-2016)*
[101] *ENISA "On national and International Cyber Exercises" (2012), p. 15*

- **Simulatieoefening** - Bij een simulatie speelt men in de eigen omgeving een realistisch scenario na. Deelnemers oefenen zoveel mogelijk onder normale omstandigheden met eigen middelen in de eigen omgeving. Het scenario van de oefening ontwikkelt zich aan de hand van de eigen besluiten en acties. Een simulatieoefening is geschikt als men wil oefenen onder druk en de reacties van deelnemers in de eigen omgeving wil testen en trainen.[102] De intensiteit en de ontwikkeling in het scenario hangen af van het aantal deelnemers en hun ervaringsniveau. Ook is het van belang of alleen interne of ook externe partijen deelnemen. Een simulatieoefening duurt een dagdeel tot meerdere dagen.

- **Capture the Flag** - Bij een operationele capture the flag is het de bedoeling om een 'vlag' of ander element te vinden en veroveren. Dit kan in teams of individueel en wel of niet in competitieverband. Bij een cybergerelateerde capture the flag is vaak het doel om hackers in (gesimuleerde) ICT-systemen op te sporen en te pakken te krijgen.

- **Red Team/Blue Team -** Bij een Red Team/Blue teamoefening valt het rode team het netwerk of een ander belangrijk bedrijfsonderdeel aan en moet het blauwe team de aanval proberen te verijdelen. Deze oefening vergroot het bewustzijn van mogelijke risico's. Ook geeft de oefening inzicht in de mogelijke kwetsbaarheden en de methoden om hiermee om te gaan. Bovendien geeft de oefening inzicht in strategieën om een aanval te detecteren en erop te reageren.[103]



Gap bridging exercise

Met crisisoefeningen kunnen bruggen geslagen worden tussen het tactisch/operationeel niveau en het strategisch niveau, en/of tussen technische en niet-technische actoren. Bij een oefening met dit karakter wordt de opschaling van het operationele crisisteam naar het strategisch crisisteam getest en getraind en wordt de onderlinge samenwerking gestimuleerd. Het oefenscenario kan voor dit doel specifiek toegespitst worden op een crisissituatie die zowel op operationeel niveau als op strategisch niveau dilemma's kent waarbij men alleen tot een oplossing komt door samen te werken. Naast de interne samenwerking kan een oefening ook organisatie-overstijgend of zelfs sectoroverstijgend worden gemaakt.

3.5 Cybercrisisoefening

De afgelopen jaren groeit de aandacht voor het oefenen van cybersecurityscenario's. De Europese Commissie heeft in haar mededeling van 2009, Kritieke informatie-infrastructuur Protectie COM (2009) - 149, de lidstaten verzocht om "*regelmatig cybercrisisoefeningen te organiseren voor grootschalige netwerksecurity incident response*

[102] http://www.cot.nl/crisismanagement/crisisoefeningen/tabletop/ *(geraadpleegd op 05 september 2016)*
[103] https://www.encs.eu/wp-content/uploads/2015/08/2015_ENCS_Factsheet_RedBlue_Training_v1.pdf *(geraadpleegd op 20-10-2016) Deze oefenvorm wordt binnen verschillende sectoren gebruikt waaronder ICT, defensie en de energiesector.*

en herstel bij grote incidenten".[104] In COM (2011) – 163 onderstreepte de Europese Commissie opnieuw het belang van cybercrisisoefeningen.

> *"Er bestaat een brede consensus dat cybercrisisoefeningen helpen om de paraatheid, reactievermogen en de kennis van stakeholders te verbeteren bij het reageren op cyberincidenten."*[105]

Het oefenen van een cyberscenario is een belangrijk hulpmiddel om crisis- en communicatiestructuren te testen. Daarnaast draagt oefenen bij aan het bepalen en vergroten van de weerbaarheid van een organisatie tegen cybercrises, ICT-technische mankementen, en incidenten met kritieke informatiestructuren. Cybercrisisoefeningen helpen om bruggen te slaan tussen het tactisch/operationeel niveau en het strategisch niveau. Belanghebbenden die bij een crisis betrokken zijn, werken vaak nog niet samen of communiceren zelfs niet met elkaar. De oorzaak is dat ze elkaar in de dagelijkse processen niet tegenkomen en vooral op de eigen organisatie gericht zijn[106]. Oefeningen helpen om de samenwerking zowel binnen als tussen organisaties te verbeteren.

Voorbeelden van cybercrisisoefeningen

- In dezelfde maand als de cybercrisisoefening OZON van SURFnet organiseerde ENISA zijn tweejaarlijkse cybersecurity-oefening: **Cyber Europe 2016**[107]**.** Vele duizenden experts van 28 EU-lidstaten, Zwitserland en Noorwegen oefenden mee. Vanaf april 2016 ontwikkelde het scenario zich op operationeel en technisch niveau en op 13 en 14 oktober kwam het tot een climax. Het scenario dreigde grote impact te hebben op de eenheid van de digitale markt. Het motto van de oefening was 'Stronger together.' Samenwerking op alle niveaus was nodig om succesvol te anticiperen op een groot en grensoverschrijdende cybercrisis. Het was de eerste keer dat er gebruik werd gemaakt van een simulatie.

- In 2012, tijdens **Cyber Europe 2012**, oefenden 300 cybersecurityprofessionals uit 25 landen mee met een tabletop-oefening georganiseerd door ENISA. Dit was een oefening op landelijk niveau en het NCSC was het primaire contactpunt voor Nederland.[108]

- In 2014 organiseerden het NCSC en CERT-Bund een tabletop-oefening om de samenwerking tussen Duitsland en Nederland in een cybercrisis te verkennen.[109]

- In oktober 2014 hield de Telecomsector in Nederland voor het eerst de grootschalige cybersecurity-oefening **CyberDawn**[110]. Het doel was om te testen hoe de samenwerking binnen de nationale sector en met de overheid en private partners in andere vitale sectoren verloopt bij een groot cyberincident.

- In Juni 2015 organiseerde het NCTV samen met dertig publieke en private partners een nationale operationele cybersimulatieoefening **ISIDOOR**. Tijdens de oefening simuleerden ze cyberincidenten en was er sprake van datalekken en kwetsbaar heden in systemen. De overheid moest in samenwerking met publieke en privatepartijen beslissingen nemen over de operationele respons op dit incident.[111] SURFcert nam deel aan deze oefening.

[104] *ENISA "On national and International Cyber Exercises" (2012), p. 7*
[105] *ENISA "On national and International Cyber Exercises" (2012), p. 2*
[106] *ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 25*
[107] *https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016 (geraadpleegd op 21-10-2016)*
[108] *https://www.ncsc.nl/actueel/nieuwsberichten/internationale-oefening-cyber-europe-2012.html (geraadpleegd op 15-09-2016); De eerste oefening, Cyber Europe 2010, werd door ENISA op 4 november 2010 georganiseerd.*
[109] *https://www.ncsc.nl/actueel/nieuwsberichten/duits---nederlandse-oefening.html (geraadpleegd op 20-10-2016)*
[110] *https://www.nederlandict.nl/news/telecomsector-bouwt-met-grootschalige-oefening-cyberdawn-aan-sterke-samenwerking-op-cyber-security/ (geraadpleegd op 20-10-2016)*
[111] *Zie www.ncsc.nl; het NCSC (Nationaal Cyber Security Centrum) draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief.*

- Jaarlijks wordt de internationale 'capture-the-flag' wedstrijd **Cyberlympics** gehouden waar vooral 'incident respons teams' van grote dienstverleners aan deelnemen. In 2013 won Nederland zowel goud, zilver als brons op dit WK met teams van Deloitte en KPN.[112]

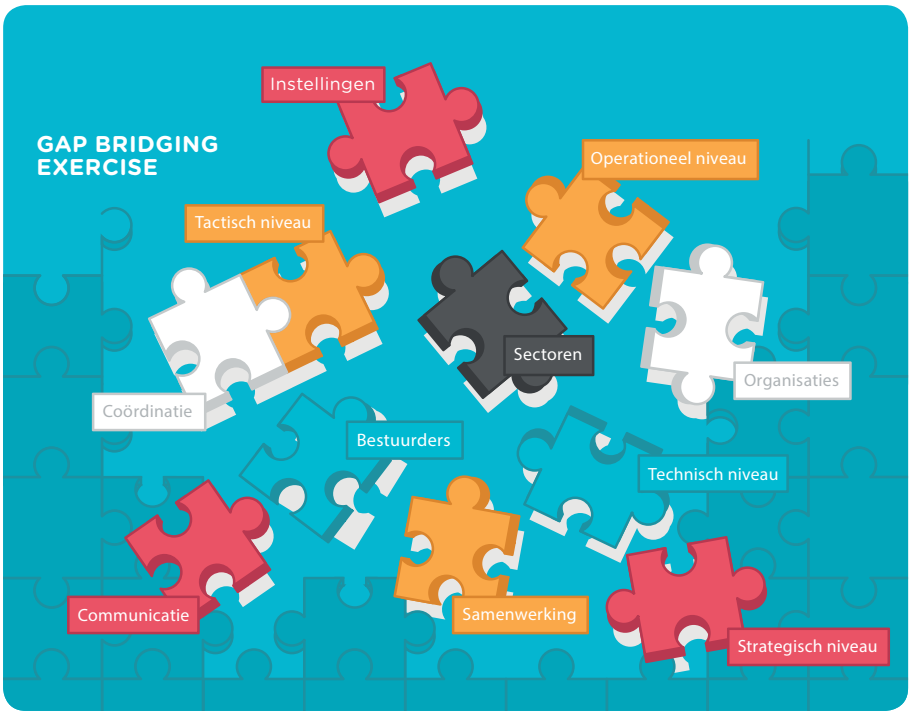
3.6 Conclusie

Het toepassen van cybersecurityoefeningen is nog in een verkennende fase.[113] Er zijn weliswaar enkele grote voorbeelden van cybercrisisoefeningen, maar in de praktijk wordt nog weinig geoefend. Bij veel organisaties zijn er nog geen vastomlijnde crisisstructuren gericht op cybercrises. Oefenen kan helpen om deze structuren vorm te geven. Bij oefeningen als Cyber Europe (internationaal) en Cyber Dawn (nationaal) was de verkenning van de samenwerking tussen betrokken partijen een belangrijk doel.

Ook als je de gestelde doelen niet (volledig) bereikt, kan een oefening toch geslaagd zijn omdat er zwakke punten aan het licht komen.[114] Het proces en de uitkomsten kunnen kennishiaten blootleggen en de deelnemers bewust maken van hun eigen handelen tijdens een crisis.

Een oefening mislukt als de opzet van de oefening niet goed is ingericht. Maar een crisisoefening hoeft geen ingewikkelde opzet te hebben om van toegevoegde waarde te zijn. Elke oefening draagt bij aan de ontwikkeling van de crisisstructuur, het leren omgaan met een crisis en het vergroten van het bewustzijn.[115]

Een crisisoefening kan ingezet worden om bruggen te slaan tussen de verschillende niveaus (technisch/operationeel en strategisch niveau), en tussen verschillende organisaties of zelfs sectoroverstijgend. Een cybercrisisoefening wordt dan een gap bridging exercise.



[112] http://webwereld.nl/security/79360-nederland-wint-goud--zilver-en-brons-op-wk-ethisch-hacken (geraadpleegd op 21-10-2016)
[113] ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 25
[114] ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 28
[115] ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 29

4. OPZET VAN EEN SIMULATIEOEFENING

Voor cybersecurityoefeningen zijn de meest gekozen vormen tabletop- en simulatie-oefeningen.[116] In dit hoofdstuk wordt toegelicht hoe een simulatieoefening (zoals cybercrisisoefening OZON) opgezet kan worden. De organisatie van een crisis-oefening is in drie stadia onder te verdelen; voorbereiding, uitvoering en evaluatie.[117]

4.1 Voorbereiding

In de voorbereiding van een oefening worden de oefendoelen vastgesteld. Op basis hiervan wordt de oefenvorm bepaald. De oefenvorm bepaalt in grote mate hoe de inhoud en de planning van de voorbereiding eruitziet.

Projectteam

Eén of meerdere projectteams bereiden de oefening voor. Binnen het projectteam vervullen projectleden verschillende rollen. Voor de centrale organisatie en coördinatie van de oefening is het raadzaam een projectteam te vormen met projectleider, projectsecretaris, communicatiemedewerker, projectleden en een observator.[118] De projectleider is verantwoordelijk voor de planning en de uitvoering van de oefening. Het projectteam is verantwoordelijk voor het scenario, de documentatie, de logistiek van de oefening en de evaluatie.[119]

Wanneer meerdere organisaties deelnemen aan de oefening is het gewenst om naast het projectteam een programmagroep aan te stellen waarbij uit elke organisatie één lid deelneemt. Voor een complexe oefening waarbij meerdere partijen deelnemen, is het bovendien raadzaam om een overkoepelende stuurgroep aan te stellen voor strategische beslissingen.

Planning

De planning is afhankelijk van de complexiteit (operationeel/tactisch/strategisch), de omvang en de beschikbare middelen. Bij veel deelnemende instellingen met volle agenda's is het nuttig om vergadermomenten van tevoren in te plannen. De meeste tijd wordt besteed aan het bedenken en uitwerken van het scenario. Het is aan te raden om de hele planning van tevoren in een draaiboek vast te leggen.

In de planning staat onder meer:
- datum en tijd van de oefening
- duur van de oefening
- vakantieperiodes
- voorbereiding van het scenario
- voorbereiding van het technische en strategische bewijsmateriaal voor het scenario.
- uitnodigen, informeren en brieven van deelnemers
- evaluatie

Voorwaarden voor de oefening

- **De duur van de oefening** is afhankelijk van de oefendoelen, beschikbaarheid deelnemers en impact op de organisatie (vakanties e.d.). De duur kan variëren van een paar uur tot een paar dagen.

[116] *ENISA "The 2015 Report on National and International Cyber Security Exercises", (2015), p. 17*
[117] *Vastgelegd in ISO 22398:2013(E)*
[118] *ISO 22398:2013(E), art. 5.2.4.1, p. 10*
[119] *ISO 22398:2013(E), art. 5.2.1, p. 8*

- Als ervoor gekozen wordt om de dagelijkse bedrijfsvoering niet te veel te verstoren dient de **impact op de lopende processen** binnen de organisatie zo minimaal mogelijk te zijn, net als de **impact op de bestaande infrastructuur.**
- Om het scenario te ontwerpen is specifieke kennis van de organisatie nodig. Daarom is het goed om te bepalen wie deze kennis in huis heeft en wie in het **voorbereidingsteam** plaats neemt. De oefenvoorbereiders kunnen niet deelnemen aan de oefening zelf, hier moet men van tevoren rekening mee houden.
- Om te voorkomen dat een oefenscenario als een echte crisis wordt opgevat, moet men maatregelen nemen die een **gesloten karakter** waarborgen. Hiervoor worden onder meer spelregels opgesteld. Een vastgelegde 'gesloten' adreslijst met deelnemers en een gesloten omgeving voor het verspreiden van berichten zorgen ervoor dat de oefening en realiteit zich niet gaan vermengen. Alleen de deelnemers op deze lijst mogen worden benaderd. Als iemand niet op de adreslijst staat, dan is het de bedoeling om contact met de responscel (dit begrip zal in paragraaf 4.2 worden toegelicht) op te nemen.

Spelregels

Spelregels dragen bij aan een goed verloop van de oefening. Enkele belangrijke spelregels zijn:

- Alle communicatie binnen het spel wordt voorzien van een codewoord dat aangeeft dat het om een oefening gaat. Dit om te voorkomen dat er verwarring tussen de realiteit en de simulatie ontstaat.
- De projectleider kan een 'NO PLAY' situatie uitroepen om de oefening (tijdelijk) stil te leggen als de omstandigheden hierom vragen. Bijvoorbeeld bij een echte calamiteit die alle aandacht vraagt.[120]
- Om zo dicht mogelijk bij de algemene dagelijkse praktijk te blijven, gebruiken deelnemers de communicatiemiddelen die ze normaal gesproken ook gebruiken.
- Om het gesloten karakter van de oefening te behouden, wordt een 'gesloten' adreslijst gebruikt.

Ontwerpen scenario

Het scenario is de basis van de oefening en heeft de gewenste effecten als het aansluit bij de realiteit waarin de deelnemers zich herkennen. De spelers raken dan sneller betrokken bij de crisissituatie en zullen daardoor realistisch reageren op de crisissituatie. Het is raadzaam om binnen de organisaties een inventarisatie te maken van realistische crises die de basis kunnen vormen voor het oefenscenario. Ook moet het scenario niet te complex zijn om te voorkomen dat je de deelnemers overlaadt met details. Om te bepalen wat er noodzakelijk is voor het scenario kan de programmagroep (en stuurgroep) een need/nice to have list opstellen.[121] Een 'need' geeft aan welke onderdelen moeten terugkomen in het scenario, een 'nice' geeft aan wat wenselijk is om op te nemen in het scenario.

De structuur en inhoud van het scenario wordt vastgelegd in een 'master event list' die bestaat uit events, acties en injects.[122] In het scenario kunnen zowel technische/operationele als strategische dilemma's opgenomen worden. Hiervoor kan op beide niveaus injects voorbereid worden, net zoals dat in praktijksituaties ook gebeurd.

[120] *ISO 22398:2013(E), art. 5.3.4.2, p. 20*
[121] *ISO 22398:2013(E), annex B, p. 27*
[122] *ISO 22398:2013(E), art. 5.2.14, p. 17*

Begrippen

Master event list – Een tijdlijn waarin de injects en acties zijn opgenomen. Deze dient als leidraad voor de oefening.
Event – Een gebeurtenis met algemene inhoud. Het aantal events hangt af van de oefendoelen. Verschillende events zijn nodig om een realistisch scenario te bereiken.[123]
Actie – De consequenties die volgen uit een event. Een actie is bedoeld om een reactie te veroorzaken bij de deelnemers. Deelnemers moeten handelen en beslissingen nemen op basis van de events. De reacties van de deelnemers brengen het scenario verder.
Inject – Hiermee kun je acties bij de deelnemers onder de aandacht te brengen. De injects bestaan uit sociale mediaberichten (zoals twitter), kranten en media-berichten, telefoontjes van stakeholders, telefoontjes van journalisten en e-mailberichten van gesimuleerde contacten.

Technische voorbereiding
Om het scenario realistisch te maken, kun je gebruik maken van allerlei hulpmiddelen en bewijsmateriaal zoals websites en gelekte (nep)documenten. Om de technische kant te oefenen kun je allerlei technische spelelementen inbrengen. Voorbeelden zijn malware, raspberry pi's in het netwerk en simulatieomgevingen van bestaande productieomgevingen. Deze (technische) hulpmiddelen moeten van tevoren voorbereid en gebouwd worden.

Briefing deelnemers
Het is raadzaam om voorafgaand aan de oefening alle deelnemers in te lichten over de spelregels en de wederzijdse verwachtingen. Dit kan door een informatiepakket en een persoonlijke briefing met uitleg over de oefening, spelregels, adreslijst en achtergrondinformatie te verstrekken. Deelnemers weten hierdoor wat er van hen verwacht wordt en wat ze kunnen verwachten, waardoor ze betrokken raken. Dit zorgt voor een goed verloop van de simulatie. Ook kun je als inleiding op het scenario een lead in of teasers verspreiden. Hierdoor starten alle deelnemers met dezelfde informatie en worden ze opgewarmd voor de oefening.

4.2 Uitvoering

Rollen tijdens de oefening

- De **oefenleider** houdt het centrale scenario in de gaten, overlegt met de responscellen om te inventariseren hoe de oefening bij de organisaties loopt en stuurt zo nodig bij. Dit kan door injects toe te voegen of te verminderen of door alternatieven te bieden om het spel zo realistisch mogelijk te maken.
- De **centrale responscel** simuleert alle rollen van de buitenwereld zoals gemeentes of andere overheden, hulpdiensten zoals politie en brandweer, belangenverenigingen, journalisten e.d.
- De **interne responscel** verspreidt de injects voor de eigen organisatie en simuleert alle rollen van de interne betrokkenen die niet met de oefening meespelen.
- Tijdens de oefening kan een **waarnemer** aangewezen worden. De waarnemer kan op de werkvloer observeren of en hoe de gestelde doelen worden behaald. Deze waarnemingen kunnen een bijdrage leveren aan het evaluatieproces.[124] De waarnemer kan ook met de interne responscel schakelen om tijdens de oefening met injects het scenario bij te sturen.
- De **deelnemers** zijn de spelers die op de werkvloer geconfronteerd worden met de acties en injects. Zij moeten op basis van het crisisscenario acties en beslissingen nemen om de crisis te managen, alsof zij daadwerkelijk met een crisis te maken hebben.

[123] *ISO 22398:2013(E), art. 5.2.14, p. 18*
[124] *ISO 22398:2013(E), art. 5.4.2, p. 20*

Rol van de deelnemers

Tijdens de simulatieoefening moeten de deelnemers reageren zoals ze dat tijdens een gewone werkdag ook zouden doen. Dit houdt in dat ze net zo laat beginnen met werken of thuiswerken als anders en contact opnemen met diegene met wie ze dat normaal gesproken ook zouden doen. Hiermee boots je een zo realistisch mogelijke situatie na. Als ze contact op willen nemen met deelnemers die niet aan de oefening meedoen, dan kan dat via de responscel.

Start-up briefing

Voorafgaand aan de oefening is het goed om met de responscellen een korte start-up briefing te hebben. Hierin spreek je de doelen door en stem je onderling het gebruik van de ruimten, telefoons en adresboek af. Daarnaast bespreek je de regels voor het rollenspel en doorloop je kort het scenario en de regels voor het eventueel afbreken van de oefening.[125]

Verloop van de oefening

Door de eerste injects te verspreiden wordt het scenario in gang gezet en de eerste acties uitgezet. De responscellen doen daarna injects om het spel op gang te houden. Deelnemers reageren hierop. Zo ontstaat een samenspel tussen de deelnemers en het scenario. De druk op de deelnemers wordt steeds groter. Dit zal leiden tot veel acties, beslissingen en communicatie.

Injects kunnen zowel technische als strategische acties en beslissingen vereisen. Een inject waaruit bijvoorbeeld blijkt dat er iets mis gaat bij het inloggen kan leiden tot onderzoek van de (gesimuleerde) productieomgeving. Een krantenbericht waarin gevoelige informatie openbaar is gemaakt, zal leiden tot een reactie van het College van Bestuur. Met name de scenario's waarbij de deelnemers zonder strategische beslissing geen technische handeling kunnen uitvoeren, zijn interessant. In zo'n geval zullen beide niveaus actief met elkaar in gesprek moeten.

Aan het einde van de oefening zal de oefening ook weer afgeschaald en beëindigd worden. Tijdens de oefening kunnen zich onverwachte situaties voordoen, bijvoorbeeld wanneer iemand denkt met een echte crisis te maken te hebben of wanneer zich een echte calamiteit voordoet. Dit vergt flexibiliteit en improvisatievermogen van de oefenleider en responscellen. De oefenleider kan de oefening (tijdelijk) stilleggen.

4.3 Evaluatie

Een evaluatie is *"het (systematische) proces dat de resultaten vergelijkt van de meting ten opzichte van erkende criteria om de verschillen tussen de bedoeling en de werkelijke prestaties te bepalen."*[126] Veelal zal men de oefening aan de hand van de oefendoelen evalueren. De oefendoelen zijn daarom bepalend voor de evaluatiecriteria.[127] Gestructureerde monitoring en evaluatie helpen om de feedback en de geleerde lessen in de organisatie te kunnen toepassen.[128] [129] Voor het evalueren wordt gebruik gemaakt van de ervaringen van deelnemers, van het voorbereidingsteam en van de waarnemers.[130] Daarnaast kun je een survey inzetten om de mening van de projectgroep, de programmagroep en de deelnemers te inventariseren.

[125] *ISO 22398:2013(E), art. 5.3.2, p. 19*
[126] *ISO 22398:2013(E)*
[127] *Evaluatiecriteria zijn (beslissende) kenmerken aan de hand waarvan de crisisoefening wordt gewaardeerd.*
[128] *ENISA "On national and International Cyber Exercises" (2012), p. 18*
[129] *ISO 22398:2013(E), p. 21*
[130] *ISO 22398:2013(E), p. 22*

Evaluatie van de oefening

Er zijn verschillende niveaus waarop de uitkomsten van de oefening geëvalueerd kan worden. Allereerst kan gekeken worden of het proces van de oefening goed is verlopen. De focus ligt hierbij dan op de organisatie van de oefening en hoe de oefening door het voorbereidende team en door de deelnemers ervaren is.

Vragen die hierbij aan de orde kunnen komen zijn:
- Hoe is de voorbereiding ervaren?
- Hoe is de intensiteit van de oefening ervaren?
- Is het scenario succesvol uitgevoerd en waren er voldoende injects of juist te weinig?
- Heeft het scenario de gewenste impact gehad?
- Hebben de deelnemers het scenario als realistisch ervaren?
- Zijn er situaties geweest die impact hebben gehad op de uitvoering van de oefening?
- Zijn er aanbevelingen voor een volgende oefening?

Evaluatie van interne crisisprocessen

Naast de evaluatie van hoe de oefening verlopen is, kan ook geëvalueerd worden hoe en of de crisisstructuur binnen de organisatie gefunctioneerd heeft tijdens de oefening.

Hierbij kan naar het proces gekeken worden waarbij de kritische processen het uitgangspunt zijn. Beoordeeld wordt of de crisisstructuur werkt zoals beoogd. De focus ligt dan vooral op de juiste handelswijze. Ook kan gekeken worden naar de uitkomsten. De nadruk ligt dan met name op de resultaten die het oefenproces heeft opgeleverd. Hierbij gaat het vooral over de doelmatig- en doeltreffendheid van de genomen maatregelen.[131]

Om leer- en verbeterpunten voor de crisisorganisatie vast te leggen, kan tijdens de evaluatie vragen gesteld worden als wat gebeurde er? (beschrijven), waarom gebeurde dat? (verklaren), wat zegt dat? (analyseren en reflecteren).[132] Uit de oefening kunnen lessen getrokken worden over het verloop van de oefening en de effectiviteit van de crisisbeheersing, die de basis vormen voor het verbeteren van de interne crisisstructuur.

4.4 Slotwoord

Als de gestelde oefendoelen niet (volledig) worden bereikt kan een oefening toch geslaagd zijn omdat ze leerpunten aan het licht brengt. Een oefening slaagt niet als de opzet niet deugt. Bijvoorbeeld wanneer de oefening niet goed is voorbereid, het scenario niet aansluit bij de beleving van de spelers of de oefening vanwege calamiteiten vroegtijdig moet worden afgebroken. Een oefening slaagt al snel in zijn opzet als deelnemers acties en beslissingen hebben moeten nemen op basis van het oefenscenario en als de deelnemers de oefening als realistisch en leerzaam ervaren.

[131] *Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie", (2013) p. 29*
[132] *Wein, Willems, "Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie", (2013) p. 24*

5. CYBERCRISIS-OEFENING OZON

5.1 Inleiding

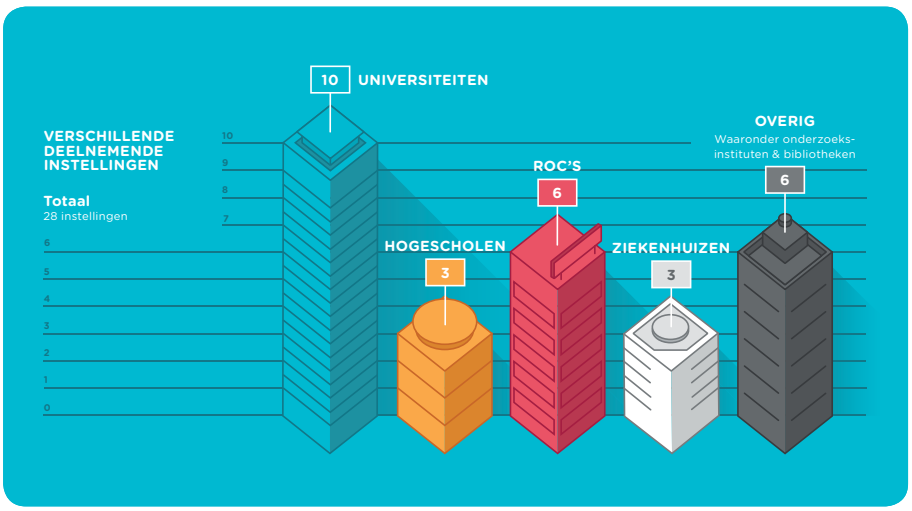
Cybercrisisoefeningen zijn in opkomst als nieuw hulpmiddel om de weerbaarheid tegen cybercrises te vergroten. In 2015 heeft SURFcert meegedaan aan de landelijke oefening ISIDOOR van het NCSC. Hierdoor geïnspireerd heeft SURFcert samen met SURFnet het initiatief genomen om voor de onderwijs- en onderzoeksinstellingen een cybercrisisoefening te organiseren.
Het organiseren van een crisisoefening is een omvangrijke inspanning. SURFnet heeft hiervoor een deel van de innovatiegelden van het onderzoeksprogramma security en privacy ingezet.

Oefening

De oefening is uitgevoerd op 4 en 5 oktober 2016. Op de eerste dag is van 8.15 uur tot 17.00 uur geoefend en op de tweede dag van 09.00 uur tot 12.00 uur. Op de middag van de tweede dag is met oefenvoorbereiders en een deel van de spelers centraal geëvalueerd. Om rekening te houden met de intensiteit, reistijd en eventuele mogelijkheid voor evaluatie is besloten om onder kantoortijden te spelen.

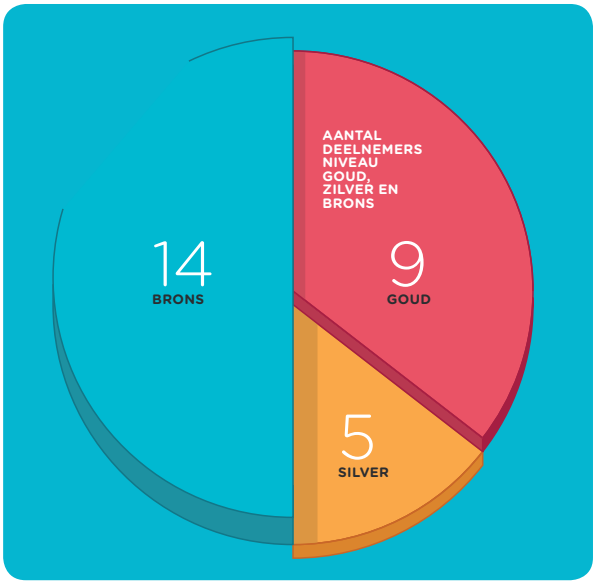
Deelnemers

Aan Cybercrisisoefening OZON hebben 28 onderzoeks- en onderwijsinstellingen meegedaan, waaronder universiteiten, hogescholen, ROC's, ziekenhuizen en onderzoeksinstellingen. Ruim 200 deelnemers waren betrokken op tactisch, operationeel, technisch en strategisch niveau. Onder de deelnemers waren security- en privacy-officers, ICTmanagers, leden van Colleges van Bestuur, stafdiensten, incident response teams en communicatie- en persvoorlichters. Instellingen konden op goud-, zilver- of bronsniveau meespelen. De belangstelling overtrof alle verwachtingen, daarom is de inschrijving vervroegd gesloten.



Niveau	Inhoud
Goud	Op goudniveau is een simulatiescenario ontwikkeld en geoefend om bruggen te slaan tussen het tactisch/operationeel, en technisch en het strategisch niveau. Leden van het College van Bestuur/directieraad oefenen mee.
Zilver	Op zilverniveau is een simulatiescenario ontwikkeld en geoefend om het tactisch/operationeel en technisch niveau te testen en trainen.
Brons	Op bronsniveau hebben de instellingen de ontwikkelingen van de simulatieoefening geobserveerd. Dit geeft kennis en inzicht in de ontwikkeling en aanpak van een crisis. Brons-spelers kregen ook een 'capture the flag' opdracht.

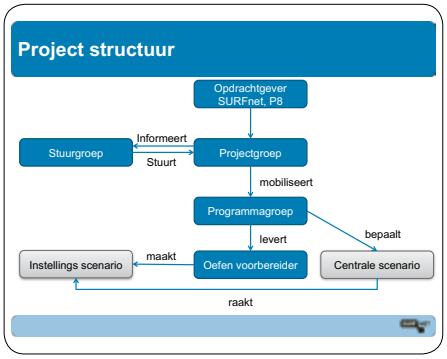
De oefening is van start gegaan met 31 instellingen. De voorbereiding van een crisisoefening is intensief en moet niet worden onderschat; in deze fase vielen drie instellingen af. (Waarvan 1 goud en 2 zilverspelers). Eén instelling heeft gekozen om in plaats van goud als brons mee te spelen.



5.2 Voorafgaand aan cybercrisisoefening OZON

Rollen

De opdrachtgever van cybercrisisoefening OZON was SURFnet. **De stuurgroep** bestond uit acht goudspelers en nam beslissingen op strategisch niveau.



De programmagroep bestond uit de oefenvoorbereiders van de instellingen die op goud- en zilverniveau meespeelden. De leden beoordeelden het centrale scenario en bedachten de instellingsscenario's en werkten die uit. Verder brieften ze de eigen interne spelers van de instelling om ze voor te bereiden op de oefening. Tijdens het spel voerden ze als interne responscel de nodige interventies uit om het spel op gang te houden.

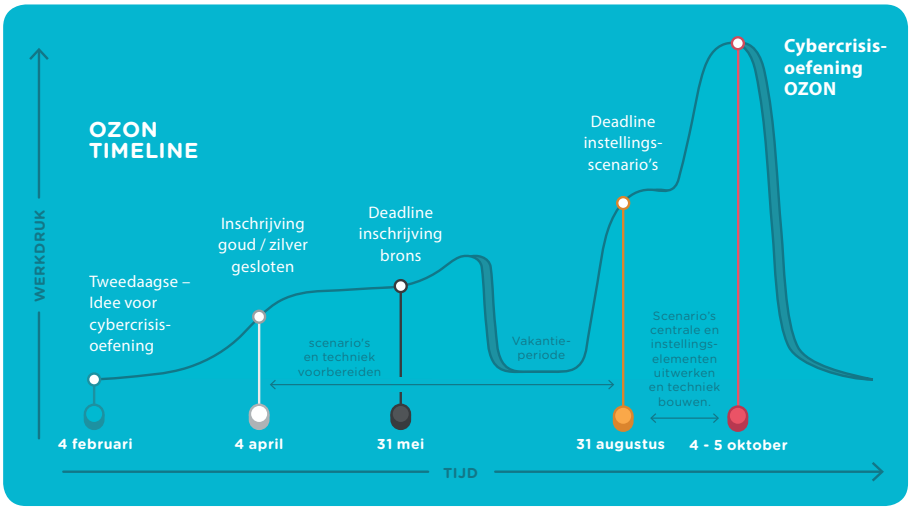
De projectgroep nam de taken van de overkoepelende organisatie op zich. De projectgroep bestond uit de projectleider, projectsecretaris, communicatiemedewerker, begeleider instellingsscenario's, leden van SURFcert en een aantal projectleden. De projectgroep heeft het centrale scenario voorbereid, de instellingen geholpen bij het ontwerpen en maken van het instellingsscenario en bij het aanleveren en voorbereiden van de stukken. Daarnaast deed de projectgroep de centrale communicatie over de oefening.

De projectgroep heeft samen met de programmagroep de oefening zowel strategisch als technisch voorbereid. De websites zijn gebouwd, de simulatiemalware geschreven en de raspberry pi's geconfigureerd en in het veld gezet. Ook maakte de projectgroep deel uit van de centrale responscel.

Externe partij – Omdat er nog geen ervaring was met het opzetten van zo'n grootschalige cybercrisisoefening is de hulp ingeschakeld van een extern expertisebureau. Zij hielpen bij de strategische invulling, leverden oefenmiddelen zoals de 'master event list' en de mediasimulator en ondersteunden de oefenleider.

Planning

De totale voorbereiding van idee tot uitvoering heeft acht maanden geduurd. In deze acht maanden is gestart met het uitwerken van het idee en de budgetten, met draagvlak verwerven binnen SURFnet en het vormen van een projectgroep. Daarna zijn uitnodigen verstuurd. Vanwege grote belangstelling is de inschrijving voor de deadline gesloten. De projectgroep, stuurgroep en programmagroep hebben de outline van het scenario geschreven, en de 'needs en nice to have list' opgesteld. In de maanden daarna is samen met de programmagroep de instellingsscenario's op technisch en strategisch vlak voorbereid. Dit heeft het leeuwendeel van de doorlooptijd in beslag genomen. Nadat de instellingsscenario's klaar waren, zijn de scenario's in detail uitgewerkt, de krantenberichten geschreven, de twitterberichten gemaakt en opgenomen in de mediasimulator. De stuurgroep heeft in totaal drie keer vergaderd en de programmagroep vijf keer.



Interne communicatie

Voor de interne communicatie tijdens het voorbereidingsproces zijn werkmateriaal, technische details, master event lists en communicatie over de oefening gedeeld via de e-mail en via een wiki.

Briefing deelnemers

Voorafgaand aan de oefening zijn de deelnemers gebrieft. Hierbij is het informatiepakket, de spelregels en het adresboek gebruikt. Om de deelnemers op te warmen

voor de oefening is een lead-in met de context van het scenario gebruikt. Een van de deelnemende instellingen had als teaser een filmpje over mogelijke aanvallen door het hackerscollectief verstrekt, deze is met de andere deelnemende instellingen gedeeld.[133]

5.3 De oefening

Voorafgaand aan de oefening zijn door de projectgroep, stuurgroep en programmagroep hoofd- en subdoelen opgesteld. Hierop gebaseerd hebben de instellingen interne doelen opgesteld.

Hoofd- en subdoelen

Het centrale doel van de cybercrisisoefening was de weerbaarheid en awareness van instellingen in een cybercrisissituatie vergroten. De subdoelen waren:

- Het functioneren van de keten testen.
- De effectiviteit van de crisiscommunicatie toetsen.
- Samenwerking tussen en binnen de instellingen vergroten.

Interne doelen

Op basis van de hoofd- en subdoelen van de oefening hebben instellingen interne doelstellingen geformuleerd. De meest voorkomende interne doelen waren:

- Het stimuleren van security awareness.
- Bewustwording van de cyberrisico's.
- Het testen van de interne en externe communicatie.
- Het verbeteren van de communicatie tussen operationeel- en managementniveau.
- Het testen of de interne processen goed ingericht zijn bij een cybercrisis.
- Het testen van de securityprotocollen.

Het scenario

Op basis van de vooraf opgestelde oefendoelen is een scenario ontworpen waarin de deelnemers zowel de interne communicatie als de escalatie naar strategisch niveau konden oefenen. Daarom is gekozen voor een simulatieoefening waarbij spelers in hun eigen werkomgeving met een oefenscenario geconfronteerd werden. De oefening moest zowel voor crisismanagement als voor IT-afdelingen voldoende uitdaging bieden. Ook was het belangrijk dat de oefening voor alle verschillende instellingen die meespeelden voldoende herkenbare en realistische elementen bevatten. Het scenario moest genoeg lastige dilemma's bevatten om te zien of deelnemers op tijd knopen doorhakten.

Om te zorgen dat de crisis niet op te lossen was zonder te schakelen met het strategisch niveau is een scenario geschreven waarbij zowel technische als strategische dilemma's aan de orde kwamen die de deelnemers niet zonder een strategische beslissing konden oplossen. Bovendien is het centrale scenario voorzien van een ethisch element om te bewerkstelligen dat instellingen met elkaar afstemden over hoe ze hiermee moeten omgaan.

Met dit vertrekpunt in gedachten is een lijst gemaakt van dilemma's die de aandacht van het College van Bestuur vereisten:

- Imagoschade
- Claims
- Persoonlijke reputatie
- Reputatie organisatie
- Bestuurlijke aansprakelijkheid
- Ethische kwesties

[133] *Voor uitleg over het briefen van deelnemers en inhoud van informatiepakket, adresboek en spelregels zie hoofdstuk 4.*

Deze dilemma's zouden de volgende risico's met zich mee kunnen brengen:
- Openbaarmaking
  - Medische dossiers
  - Persoonsgegevens
  - Onderzoeksdata
  - Bedrijfsgegevens
  - Organisatiegegevens
- Afpersing
- Geëncrypte databestanden
- Spionage
- Aangepaste/gemanipuleerde gegevens

Centraal Scenario
Het centrale scenario bestaat uit twee simultane dreigingen: een aanval van een idealistisch hackerscollectief en een criminele component.

Op basis van bovenstaande uitgangspunten is gekozen om een deel van de oefening vanuit een fictief idealistisch hackerscollectief te laten komen, dat door een groot deel van Nederland (en binnen de instellingen) als sympathiek wordt gezien. Dit collectief heeft zowel een ethische als een criminele component. Hierdoor zijn de dilemma's niet zomaar van tafel te vegen. De dreiging van deze hackers raakt de gehele onderwijs- en onderzoekssector. Dit stimuleert de samenwerking tussen de instellingen.

Het hackerscollectief vindt dat er te veel informatie in bezit is van bedrijven en instanties die om economische redenen niet publiek gemaakt wordt. Hun visie is dat de ontwikkeling van de menselijke beschaving versneld wordt als alle data beschikbaar is voor iedereen. Het niet delen van informatie hindert vooruitgang en daarom zijn ze fel tegen alle vormen van intellectueel eigendom. Hun doel is om zoveel mogelijk gegevens integraal openbaar te maken. Hierbij houden ze geen rekening met privacygevoelige data.

Het hackerscollectief heeft in de publieke opinie veel credits verdiend met hun onthullingen en heeft nu aangekondigd de activiteiten uit te breiden naar Nederland. Hierbij hebben zij de pijlen ook op de onderwijs- en onderzoekssector gericht. Het scenario heeft een sterk technische component om hun doel te bereiken. Ze hebben op grote schaal malware verspreid. Het is multifunctionele malware die bestanden kan verzamelen en doorsturen, maar ook in staat is om op commando alle bestanden op de computer of aangesloten netwerk te versleutelen. Hiermee heeft het hackerscollectief veel gevoelige data verzameld. In een media-offensief zal het hackerscollectief deze data openbaar maken.

Aan medewerkers van Nederlandse onderwijs- en onderzoeksinstellingen wordt door het collectief gevraagd de malware executable te downloaden en installeren op instellingscomputers. De executable verspreidt zichzelf via een Windows zero-day en maakt zo nieuwe datacollectie mogelijk. Bovendien wordt gevraagd om een mirror te maken van de website met onthulde data. Er is onder andere van raspberry pi's gebruik gemaakt om deze mirrors in de lucht te brengen.

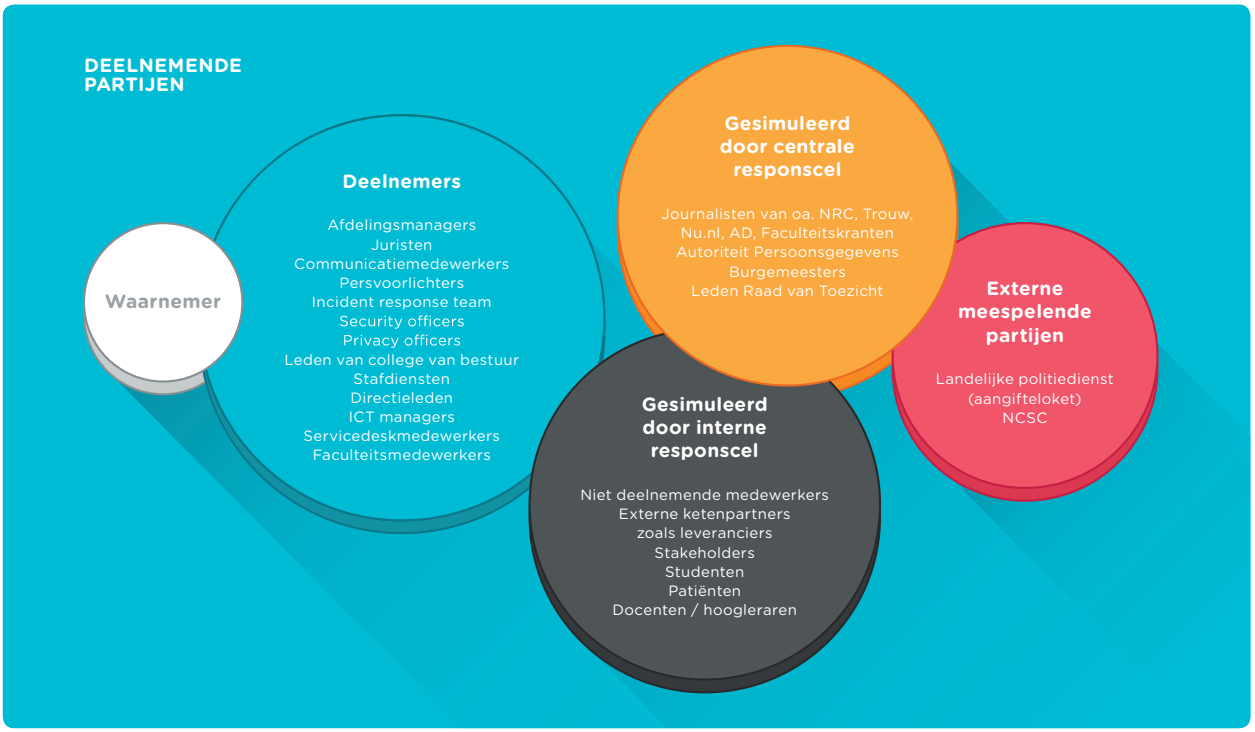
Een aantal hoogleraren heeft aanvankelijk steun uitgesproken aan het onthullen van de data. Ze veroordelen weliswaar het hacken, maar steunen de onthullingen omdat deze ethisch onverantwoord onderzoek aankaarten. Ook wordt een webpetitie gestart, die onderzoekers kunnen ondertekenen.

Daarnaast kent het scenario een criminele component. Een journalist ontdekt een webportal waar het mogelijk is om cijfers tegen betaling aan te passen, cijferadministraties

openbaar te maken, medische dossiers van bekende Nederlanders openbaar te maken, compromitterende foto's van medestudenten en docenten te openbaren en tentamengegevens in te zien. Een mogelijke link met het hackerscollectief wordt gesuggereerd, maar het is niet duidelijk of deze er ook echt is.

Instellingsspecifiek scenario
Het centrale scenario heeft impact op de gehele onderwijs- en onderzoekssector. Op basis van het centrale scenario hebben de instellingen hun eigen instellingsscenario afgestemd op hun eigen oefendoelen, deelnemers en oefensituatie. In de voorbereiding is met een need/nice to have list geïnventariseerd waaraan de instellingsscenario's moesten voldoen. Vanwege onbekendheid met de materie heeft de projectgroep de instellingen actief ondersteund bij het maken van de instellingsscenario's. Dit om er zeker van te zijn dat deze goed aansloten bij het hoofdscenario en voldoende uitdaging boden om zowel de technische, de tactische als de bestuurlijke spelers aan de oefening te binden. Hierbij is nagegaan welke informatie binnen de instellingen gevoelig is bij openbaarmaking en welke systemen dit soort informatie bevatten.

Nadat de gevoelige informatie in kaart was gebracht, hebben de oefenvoorbereiders met ondersteuning vanuit de projectgroep de spelelementen[134] van het scenario zo realistisch mogelijk gemaakt. De oefenvoorbereiders hebben het instellingsscenario uiteindelijk vastgelegd in een 'master event list', een combinatie van events voor het generieke scenario en instellingsspecifieke events.



Rol van media en maatschappij

Een bijzondere rol was weggelegd voor de media en de maatschappij. De centrale responscel simuleerde de rol van de buitenwereld zoals diverse journalisten, Raden van Toezicht en de Autoriteit Persoonsgegevens. Kranten en social-mediaberichten zijn van tevoren voorbereid en werden tijdens de oefening verspreid via een simulatieomgeving. De responscellen simuleerden tijdens de oefening verschillende telefoontjes van pers, toezichthouders en andere betrokkenen. De nationale politie

[134] *Als inject diende twitterberichten, facebookberichten, krantenberichten, e-mails van stakeholders, telefoontjes van stakeholders en journalisten. Ook werd gebruik gemaakt van communicatiemiddelen als jabber, whatsapp en skype.*

speelde via een digitaal aangifteloket mee. Het NCSC stuurde waarschuwingen naar de spelers. De interne responscel simuleerde medewerkers die niet meespeelden, externe partners zoals leveranciers en stakeholders zoals studenten, patiënten en docenten of hoogleraren. De centrale en de interne responscel regisseerden de oefening vanaf een centrale locatie in Utrecht.

Gesloten karakter

Om het gesloten karakter van de oefening te bewaken is gebruik gemaakt van een adresboek en aparte SCIRT- en SCIPR-mailinglijsten[135]. Verder was de centrale oefenleiding bereikbaar via een centraal e-mailadres.

Randvoorwaarden voor het slagen van de oefening

- **Impact op lopende processen:** Om niet te veel de dagelijkse operatie te storen, mocht de oefening zo weinig mogelijk impact hebben op de lopende processen.

- **Impact op infrastructuur:** Om geen impact te hebben op de bestaande infrastructuur hebben enkele instellingen een simulatieomgeving gebouwd. De instelling mochten zelf beslissen of ze gebruik wilden maken van de simulatiemalware en raspberry pi's.

- **Rol van security officers:** Omdat veel security officers deel uitmaakten van het voorbereidingsteam, waren zij bij de uitvoering niet aanwezig op de eigen locatie. Instellingen hebben hiervoor zelf een passende oplossing gevonden. Dit bood bovendien de kans om te oefenen hoe de organisatie functioneert bij afwezigheid van de security officer.

- **No Play-situatie**[136]**:** De bevoegdheid om de oefening stil te kunnen leggen (No Play-situatie) lag bij de projectleider. Ten tijde van cybercrisisoefening OZON heeft er zich geen No Play-situatie voorgedaan.

Oefenleiding

Voor een oefening van deze omvang is een centrale oefenleiding noodzakelijk. Deze werd voor OZON ingevuld door de projectleider en de oefenleider (bij OZON ondersteund door een extern bureau). De oefenleiding hield het verloop van het scenario in de gaten en stuurde zo nodig bij door met de responscellen de voortgang van het scenario te bespreken. Om die reden werd elk uur een korte briefing gehouden waarbij elke responscel kort vertelde hoe binnen de eigen instelling geacteerd werd op het scenario. Bijsturing vond plaats door injects toe te voegen of te verminderen.

Waarnemer

De meeste instellingen hadden een waarnemer aangesteld om de interne crisisprocessen en crisisoverleggen te observeren. Deze waarnemingen zijn van toegevoegde waarde om de oefendoelen intern te evalueren. De waarnemer schakelde tevens met de responscel over de voortgang van het scenario. Hierdoor konden ze ook bijsturen op basis van interne waarnemingen.

[135] SCIRT en SCIPR zijn de security en privacy communities van de bij SURF aangesloten instellingen.
[136] Voor uitleg over No Play situatie en andere spelregels zie hoofdstuk 4

Oefenverloop gezien vanuit de responscel

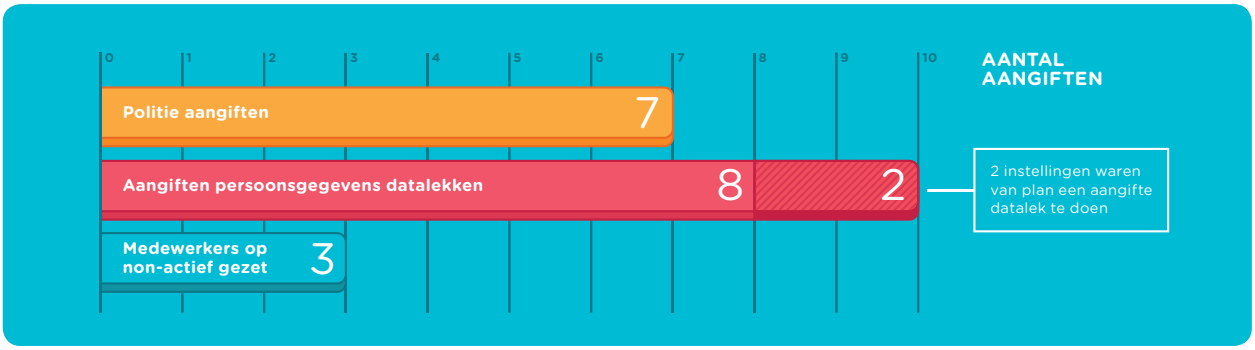
Aanvankelijk werd aarzelend gestart. Het was vooral spannend hoe de deelnemers de oefening zouden ontvangen. Al snel werd duidelijk dat binnen de instellingen het scenario en de acties goed opgepakt werden. De deelnemers van de instellingen speelden actief mee, de media-simulator werd gevolgd en de instellingen twitterden actief mee op de mediasimulator. De responscel kon zien dat deelnemers actief meededen en hun rol serieus namen. De oefening onderscheidde zich nauwelijks van een realistische crisis. De opzet was geslaagd.

Vooraf werd gedachten dat er wellicht elementen aan de oefening moesten worden toegevoegd om deze op gang te houden. Om elf uur bleek dat er wellicht eerder moest worden afgeremd dan bijgeschakeld. Uiteindelijk is er marginaal bijgestuurd. De injects vonden hun weg naar de deelnemers en zij reageerden hier actief op. De druk was gedurende de dagen goed en verspreid. De algemene sfeer bleef goed. Omdat voor velen aan het einde van de eerste dag de doelstellingen bereikt waren en er spelmoeheid optrad, hebben we de simulatie iets eerder gestopt dan gepland. De freeze (het beëindigen van het spel door een eindsignaal) kwam voor sommigen wat onverwacht. Het bleek dat sommige instellingen zo in het spel verdiept waren dat ze een paar uur later nog altijd in overleg waren over de mogelijke consequenties en te volgen strategie.

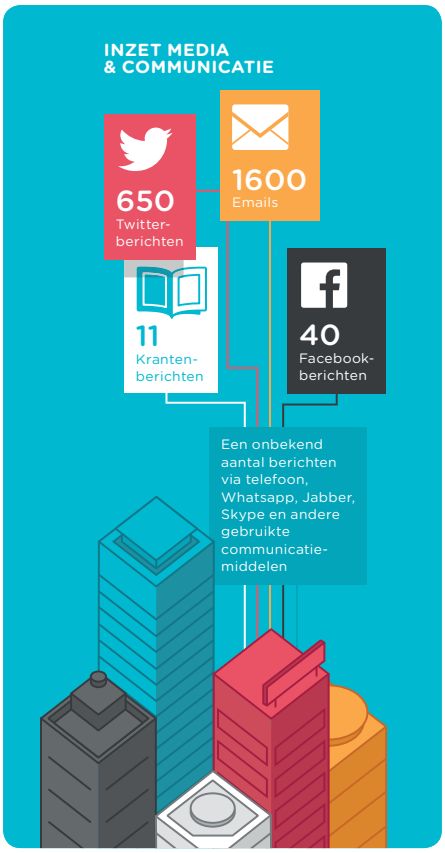
De spelers die meespeelden, speelden enthousiast door. Zelfs bestuursleden die alleen op de eerste dag een paar uur zouden deelnemen, vroegen of ze weer mee mochten spelen. Tijdens de tweede dag is met name ingezet op het uitspelen van de spellijn van de eerste dag. Bij sommigen zijn nog enkele extra injects toegevoegd. Het spel bleek ook de tweede dag gemakkelijk op gang te houden. Om deelnemers op tijd te laten stoppen en de oefening te beëindigen is het goed om tijdig te beginnen met het afschalen van de oefening met daarop gerichte injects.

Er zijn geen situaties geweest die tot stilleggen van de oefening hebben geleid. Wel is bij een instelling een afdeling afgehaakt omdat de normale werkzaamheden te veel onder druk kwamen te staan.[137] De oefening heeft geen impact gehad op de bestaande infrastructuur. Wel is gebleken dat de oefening veel intensiever was dan van tevoren ingeschat. Dit punt wordt bij de uitkomsten nog nader besproken.

In totaal zijn er door de goud- en zilverspelers zeven aangiften bij de politie gedaan en acht aangiften bij de Autoriteit Persoonsgegevens. Twee bronsspelers wilden aangifte doen bij de Autoriteit Persoonsgegevens. Ook zijn er tijdens het spel drie medewerkers (fictief) op non-actief gezet.



[137] *Dit werd bij die instellingen opgevangen door de spelbegeleider van die instelling in de interne responscel en had maar beperkte gevolgen voor de voortgang.*



Mediaberichten en communicatie tijdens de oefening

In de anderhalve dag van de oefening zijn uiteindelijk 650 tweets verstuurd (waarvan er al 500 waren voorbereid), 40 facebookberichten gemaakt en 11 krantenartikelen gepubliceerd. Ook hebben de instellingen samen meer dan 1600 e-mails uitgewisseld.[138] Deze e-mailconversaties zijn gelogd in een centraal cc-adres.

Deelnemers Brons

Bronsdeelnemers observeerden de simulatieoefening. Zij hadden toegang tot de mediaberichten, waarmee ze de ontwikkeling van de crisis volgden. Daarnaast kregen zij een 'capture the flag'-opdracht. Een student voorzien van software op een laptop die in het netwerk gedetecteerd kon worden, bevond zich in of nabij het gebouw van de bronsdeelnemer. Om het verrassingseffect zo groot mogelijk te houden waren de bronsdeelnemers hiervan niet op de hoogste gesteld. In de praktijk bleek echter dat de meeste bronsdeelnemers slechts een simulatie verwachtten. Ook toen meerdere e-mails vanuit SURFcert verstuurd werden, bleken veel instellingen hier wel intern mee aan de slag te gaan, maar niet actief naar de student op zoek te gaan. De conclusie is dat bij een volgende 'capture the flag' oefening in ieder geval één of meerdere medewerkers intern op de hoogte stellen zodat ze intern kunnen sturen. Zo zal ook dit spelelement meer tot zijn recht komen.

5.4 Evaluatie

Evalueren draagt bij aan het formuleren van leer- en verbeterpunten. Ook het benoemen van positieve punten helpt de ontwikkeling van zowel de oefening als de interne crisisprocessen. Aan het einde van de tweede dag is met 45 deelnemers en oefenvoorbereiders geëvalueerd. Mede door ruimtegebrek is niet de volledige deelnemersgroep uitgenodigd om te evalueren. Voorafgaand aan de centrale evaluatie is een eerste interne evaluatie door de instellingen uitgevoerd; de uitkomsten hiervan zijn meegenomen in de centrale evaluatie.

Tijdens de evaluatie zijn met name generieke punten ter sprake gekomen, zoals de centrale oefendoelen en de mate waarin de oefening heeft bijgedragen aan deze oefendoelen. Tijdens de evaluatie is niet ingegaan op het functioneren van de instellingen tijdens de oefening. Het is aan de instellingen zelf om interne conclusies te trekken. Ook is een survey onder alle deelnemers verspreid. De uitkomsten hiervan zijn in de volgende paragraaf opgenomen.

[138] *De e-mails werden gemonitord door alle gebruikers de verstuurde e-mails te laten forwarden naar een cc-adres.*

5.5 Uitkomsten

De uitkomsten worden besproken aan de hand van de observaties tijdens de oefening en de resultaten van de evaluatie. Hierbij wordt ingegaan op:
- aspecten van de oefening zelf;
- de voorbereiding op de oefening;
- de impact van de oefening;
- interne communicatie en coördinatie;
- de informatiedeling tussen de instellingen;
- het duiden van informatie;
- awareness en
- capture the flag (bronsoefening)

5.5.1 De oefening

- **Realistisch scenario**
  Uit de evaluatie bleek dat de deelnemers tevreden waren over het scenario. Veel spelers gaven aan dat ze de oefening als erg realistisch en leerzaam hadden ervaren. Vanuit de stuurgroep was de opdracht gegeven om de oefening zo realistisch mogelijk te maken en bij de werkelijkheid aan te sluiten. De opzet hiervan is geslaagd.
  Het scenario bevatte voldoende strategische en technische uitdagingen en het niveau van het scenario sloot goed aan bij de oefendoelen. Ook ervoeren de deelnemers het scenario als aansprekend. Vanuit de oefening waren er geen grote omissies. Er hebben zich geen situaties voorgedaan waarbij het scenario de verkeerde kant opging en er waren geen verrassingen tijdens de uitvoering. De improvisatie bestond vooral uit het naspelen van partijen zoals in het scenario was voorzien.
  Door de grootschalige opzet van de oefening konden veel partijen aanhaken, zowel instellingen als externe partijen zoals politie, Autoriteit Persoonsgegevens en het NCSC. Dat draagt bij aan het realistisch effect van de oefening.
  Om de leden in staat te stellen in hun eigen rol te spelen, was de stuurgroep voorafgaand aan de oefening niet op de hoogte van het scenario. Dat werd niet als probleem ervaren. Juist bij dergelijke oefeningen is het goed om geen weet te hebben van de inhoud van de oefening. Hierdoor konden ze in hun eigen rol meespelen.
  De social-media- en krantenberichten zorgden voor een realistische toevoeging. Bij veel instellingen werden de berichten gelezen en er werd actief op gereageerd.

Lessons learned
- Om de mediaberichten te verspreiden is het raadzaam om gebruik te maken van een goed doorzoekbare en intuïtieve simulatieomgeving.
- Cybercrisisoefening OZON is erin geslaagd om een realistische oefening te creëren.
- Een realistisch scenario draagt bij aan de beleving van de deelnemers en creëert een fictie die als zeer realistisch en leerzaam wordt ervaren.
- Een grootschalige oefening biedt de mogelijkheid om externe partijen makkelijker te laten deelnemen aan de oefening. Denk aan politie, Autoriteit Persoonsgegevens, NCSC en andere partijen.

- **Verhouding centraal scenario en instellingsscenario's**
  Het centrale scenario creëerde een instellingsoverstijgende cybercrisis. De instellingen konden hun eigen instellingsscenario hierop baseren. Dit ervoeren ze als erg waardevol. Iedere instelling kon het scenario hierdoor aan de eigen wensen en oefendoelen aanpassen. De modulaire opzet is hiermee geslaagd.
  Tijdens de voorbereiding kwam de nadruk te liggen op een cybercrisis binnen de eigen instelling. In het begin zijn een aantal samenwerkingsverbanden opgezet

tussen verschillende instellingen zoals bij de ROC's en de ziekenhuizen. Dit maakte het mogelijk een gezamenlijk scenario te maken en de last van de voorbereiding te verlichten. Deze gezamenlijke scenario's zijn niet helemaal uit de verf gekomen. De oorzaak hiervan is mede de onbekendheid met een cybercrisisoefening en de nadruk die op de interne processen werd gelegd. Dit leidde tot veel verschillende 'op de eigen instelling gerichte' scenario's. Bij de huidige opzet was het aantal deelnemende instellingen precies goed.

Lessons learned
- Doordat we naast het centrale scenario voor elke instelling een apart scenario hebben gemaakt werd het totale scenario gecompliceerd.
- Bij de huidige opzet van de oefening was het aantal deelnemers precies goed. Bij meer deelnemers bestaat het risico dat de oefening onoverzichtelijk wordt.
- De mogelijkheid om het centraal scenario aan de wensen van de instelling aan te passen werd als zeer waardevol ervaren.
- De modulaire opzet is goed geslaagd.

- **Betrokkenheid van bestuurlijk niveau**
  Bij veel instellingen was de betrokkenheid van het bestuurlijke niveau groot. Bij één instelling was het bijvoorbeeld de bedoeling dat het bestuurlijk niveau slechts twee uur mee zou spelen. Omdat ze de oefening zeer realistisch en leerzaam vonden, hebben ze ruimte in hun agenda gemaakt om langer mee te kunnen oefenen. Ook het animo voor deelname was groot, wat resulteerde in het vroegtijdig sluiten van de inschrijving voor gouddeelnemers (bestuurlijk niveau).

Lesson learned
- De cybercrisisoefening OZON heeft bijdragen aan het op de kaart zetten van cyberdreigingen bij het bestuurlijk niveau.

- **Deelname van de spelers**
  Opvallend was dat de spelers vol enthousiasme mee-oefenden. De meeste spelers gingen er serieus in mee. Een van de voorbeelden hiervan is dat men aan het einde van de eerste dag, ver na het signaal dat het spel beëindigd was nog doorspeelde, overleggen plande en het spel aan het spelen was. De deelnemers werkten hard en geconcentreerd.

Lesson learned
- Bij een realistisch, instellingsspecifiek scenario lukt het goed om deelnemers te enthousiasmeren en werkelijk te laten oefenen alsof het een realistische dreiging is.

5.5.2 Voorbereiding van de oefening

De voorbereiding van de oefening heeft meer tijd gevergd dan gedacht, zowel van de projectgroep als de instellingen. Uit de evaluatie bleek dat deze voorbereiding het waard is geweest. Veel tijd is geïnvesteerd in het uitwerken van het centrale en het instellingsscenario. In de planning bleek met name de vakantieperiode een obstakel te zijn. Binnen kleine instellingen kostte het moeite om voldoende resources vrij te maken om een dergelijke grote oefening voor te bereiden.

Ook bleek dat er zowel technische als strategische expertise nodig is om een realistisch scenario te ontwerpen. Dit was voor verschillende instellingen een uitdaging. Op het moment dat de juiste personen met de juiste kennis van het team deel uitmaakten, kwam de voorbereiding goed op gang. Uit de evaluatie bleek dat er een groot vertrouwen was in het voorbereidingsteam doordat ze getuigden van een groot enthousiasme en enorme inzet.

Lessons learned
- Het uitwerken van het scenario op zowel technisch als op strategisch niveau vergde veel tijd en expertise.
- Het opzetten en ontwerpen van de cybercrisisoefening was voor iedereen nieuw. Daarom werd het voorbereiden en het ontwerpen en uitwerken van het scenario als complex ervaren.

- **Hulp bij voorbereiding scenario**
  De ondersteuning vanuit de projectgroep bij het opzetten van het instellingsscenario was van toegevoegde waarde. Tegelijk gaf het een steuntje in de rug om tot productie over te gaan. Verder droegen concrete voorbeelden van dilemma's, een opzet van een master event list en verschillende spelelementen bij tot een realistisch scenario. Meerdere oefenvoorbereiders benadrukten dit punt.

Lesson learned
- Begeleiding bij het bedenken en opstellen van het instellingsscenario is van toegevoegde waarde. Concrete voorbeelden van dilemma's, een opzet van een master event list en verschillende spelelementen dragen bij aan het opzetten van een instellingsscenario.

- **Draagvlak**
  Sommige oefenvoorbereiders vonden het lastig om deelnemers binnen de instelling enthousiast te maken om mee te oefenen. Na de oefening hebben deelnemers aangegeven dat ze hadden willen doornemen als het belang ervan duidelijker was geweest. Ook hadden instellingen lang de tijd nodig om te besluiten of ze wel of niet mee wilden doen en op welk niveau (goud, zilver of brons). In de organisatie van een crisisoefening moet je hier rekening mee houden. Bovendien heeft de opzet van een grootschalige oefening een aanzuigende werking.

Lessons learned
- Het delen van de uitkomsten van oefeningen, communiceren over oefeningen en het oefenen op kleine schaal zorgt voor draagvlak op operationeel en strategisch niveau.
- In de voorbereiding dient rekening gehouden te worden met de benodigde tijd voor besluitvorming van instellingen.
- Gezamenlijk oefenen creëert draagvlak binnen de sector.

5.5.3 Impact tijdens de oefening

- **Rol van de interne responscel en waarnemer**
  Toen het spel eenmaal liep, vielen de puzzelstukjes voor de interne responscellen op hun plek. De interne responscellen hielden het spel goed in de gaten en stuurden waar nodig het spel bij. Dit ging op eigen initiatief dan wel in samenspraak met de centrale responscel en oefenleiding. De rol van de interne responscel was goed uit te

voeren. Wel gaven de leden aan dat het noodzakelijk was om een goed overzicht te houden van wat er binnen de instelling speelde. Hiervoor was het zeer waardevol om met een waarnemer ter plaatse te kunnen schakelen. Ook kreeg de responscel geen volledig beeld van alle communicatie binnen de instellingen. Slechts een deel was op afstand te volgen. De rol van waarnemer was ook erg waardevol om de interne processen te kunnen evalueren.

Lessons learned

- Het is voor de interne responscel relevant om een goed overzicht te houden van wat gaande is binnen de instelling, om eventueel in overleg met de oefenleiding bij te kunnen sturen.
- De waarnemer kan informatie delen met de interne responscel en heeft daarnaast een toegevoegde waarde voor de interne evaluatie.

- **Gesloten karakter**

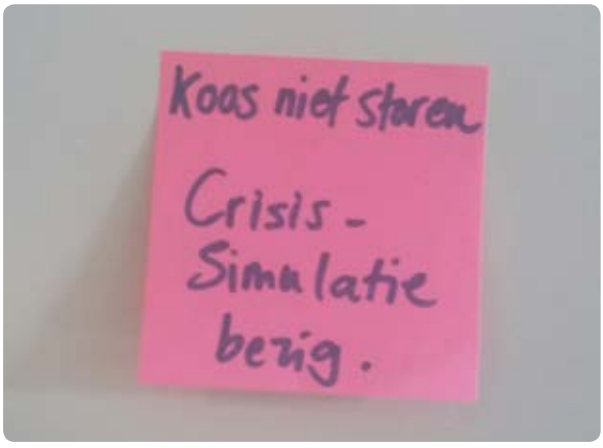
  Het gesloten karakter van de oefening is goed gehandhaafd. Slechts in een enkel geval raakten niet-deelnemers betrokken bij de oefening. Slechts In één geval kon een deelnemer niet goed het onderscheid maken tussen een oefensituatie en de realiteit. De spelelementen zijn hierop aangepast zodat er niet nogmaals verwarring kon ontstaan. In verschillende communicatie-uitingen (e-mails) moesten deelnemers eraan herinnerd worden de oefenmarkering te gebruiken.

Lessons learned

- De spelregels, gesloten simulatieomgeving voor mediaberichten, gesloten deelnemerslijst en de gesloten e-mailomgevingen zoals OZON-SCIRT en OZON-SCIPR hebben het gesloten karakter van de oefening weten te waarborgen.

- **Intensiteit van de oefening**

  De deelnemers ervoeren de werklast van de oefening als veel intensiever dan van tevoren door de oefenvoorbereiders was ingeschat. Omdat de oefening voor het eerst werd voorbereid en georganiseerd, hadden de oefenvoorbereiders nog niet voldoende ervaring om de werklast in te schatten. Tijdens de voorbereiding dachten de oefen-voorbereiders dat er wellicht te weinig spelelementen zouden zijn. Daarom zijn extra interventies voorbereid om de oefening van meer inhoud te voorzien. Omdat de oefening voldoende uitdaging bood, is hier geen gebruik meer van gemaakt.
  Tijdens de oefening werden vooral de communicatieafdelingen zwaarder belast dan verwacht. Hieruit werd duidelijk dat de communicatie tijdens een grote crisis een aan-zienlijke rol heeft.



Bij een tweetal instellingen zijn enkele afdelingen voortijdig met de oefening gestopt omdat voorrang werd gegeven aan interne zaken. De interne responscel heeft de rol van de uitgevallen afdelingen overgenomen. Ook hebben enkele instellingen besloten om de tweede dag geen nieuwe interventies meer te doen omdat de oefendoelen al ruimschoots behaald waren en om de spelers niet onnodig te belasten. De spelregels zorgden voor extra druk, omdat de deelnemers volgens bepaalde regels moesten communiceren en daarbij het adresboek moesten hanteren. Dit wijkt af van de normale procedure bij een crisis.

Lessons learned
- Een realistische simulatieoefening is zeer intensief, zeker als het scenario zo pakkend is als bij cybercrisisoefening OZON.
- Een complexe crisissituatie vergt veel meer tijd en aandacht van de betrokkenen en kan niet zomaar 'naast het werk gedaan worden.'
- De communicatieafdelingen hebben een aanzienlijke rol bij een grote crisis.
- Een oefening van deze aard is effectief door de grote intensiteit. Dit zal bij een volgende oefening van meet af aan duidelijk moeten zijn.
- De oefening bood veel spel en uitdagingen waardoor de belasting voor de instellingen hoger was dan verwacht.

- **Verlies van focus en belasting deelnemers**
  Aan het einde van de dag werd bij de deelnemers verlies van focus waargenomen. Dit kwam ook uit de evaluatie naar voren. De oorzaak was enerzijds de grote druk en intensiteit van de oefening, anderzijds soms juist ook te weinig uitdaging. Door regelmatig te inventariseren en waar nodig bij te sturen konden de instellingen de scherpte bij de deelnemers vasthouden.
  Bij sommige instellingen bleek dat de druk slechts bij enkele deelnemers kwam te liggen. Dit kan te maken hebben met de verdeling van taken binnen het crisisteam. Ook de persoonlijke inzet en/of de belasting tijdens de oefening kan een rol spelen.

Lessons learned
- Bij een langdurig en intensieve oefening treedt verlies van focus op bij deelnemers.
- Interveniëren (door het vermeerderen of verminderen van acties) kan bijdragen aan het behoud van scherpte bij de deelnemers.
- Een goede taakverdeling binnen het crisisteam zorgt voor een evenredige verdeling van druk over de deelnemers.
- Oefenen draagt bij aan het verhelderen van rollen, taken en de invulling hiervan binnen de crisisteams.
- Tijdens de oefening bleek dat soms taken teveel bij enkele personen zijn belegd. Het is belangrijk een goede balans te vinden tussen teveel en te weinig inzet van deelnemers, zowel tijdens de oefening als tijdens een echte crisis.

- **Duur van de oefening**
  Sommige instellingen hadden genoeg aan één oefendag. Andere instellingen waren juist na de eerste dag nog fanatiek in het spel verwikkeld en hadden de uitloop van de tweede dag nodig om de crisis onder controle te krijgen. Sommige deelnemers hadden ook verwacht dat er in de nacht zich nieuwe ontwikkelingen zouden voordoen; dat was in dit scenario niet het geval. Hieruit blijkt dat een heldere communicatie over de kaders van de oefening van toegevoegde waarde is. Ook werd gesteld dat meer tijd tussen de oefening en de evaluatie meer mogelijkheden zou bieden om intern goede conclusies te trekken.

Lessons learned
- Eén oefendag biedt de mogelijkheid om het gehele crisisproces te testen, zolang iedereen het spel kan uitspelen.
- Heldere communicatie over start, einde en de kaders van de oefening draagt bij aan een helder verwachtingspatroon bij de deelnemers.
- Meer tijd tussen de oefening en de centrale evaluatie maakt het mogelijk om een eerste interne evaluatie te doen en de bevindingen in te brengen bij de centrale evaluatie.

5.5.4 Interne communicatie en coördinatie

- **Rolverdeling en escalatie een communicatie tussen verschillende lagen**
  Bij veel instellingen konden het technisch en bestuurlijk niveau en de communicatie elkaar goed vinden. De meeste instellingen waren tevreden over de mate van escalatie binnen de instellingen. Ze ervoeren de brede betrokkenheid van alle lagen als zeer waardevol. Bij sommige instellingen was het voor de eerste keer dat een volledig crisisteam op cybersecurityniveau werd samengesteld. Dit werd als zeer leerzaam en waardevol ervaren. Een goede rolverdeling draagt hierin bij aan een snelle opschaling en maakt het mogelijk de juiste personen aan te haken. Ook de bekendheid met interne procedures zorgt ervoor dat betrokkenen snel kunnen handelen.
  Bij sommige instellingen stonden de strategische crisisteams al in de starthouding. Dit is niet altijd even realistisch. Het is ook belangrijk om het formeren van het crisisteam en reageren op de eerste signalen van een crisis te testen. Ook bleek tijdens het spel dat sommige spelers er behoefte aan hebben andere mensen (buiten de deelnemerslijst) in het spel te betrekken.

Lessons learned
- In de dagelijkse werkzaamheden komen bestuur, communicatie en techniek vaak niet met elkaar in aanraking. Tijdens de oefening bleek dat ze elkaar bij een crisis kunnen versterken.
- Een brede betrokkenheid van alle lagen werd als zeer waardevol ervaren.
- Een simulatieoefening is geen afspiegeling van de werkelijkheid, maar geeft wel inzicht in hoe medewerkers in een echte situaties zouden reageren. Oefenen draagt bij aan het inzichtelijk krijgen van de rollen en taken van de spelers.
- Er is behoefte aan meer en intensievere communicatie binnen de instellingen.
- Soms zijn andere partijen nodig dan van tevoren bedacht.
- Een ‘gap bridging exercise’ is in staat om bruggen te slaan tussen bestuur, communicatie en techniek. Oefenen draagt bij aan het voorbereid zijn op echte crisissituaties.

5.5.5 Delen van informatie tussen instellingen

- **Gebruik van bestaande communicatiemiddelen**
  In het algemeen werkt binnen de IT-community kennisdeling via de bestaande communicatiemiddelen zoals SCIRT en SCIPR goed. Tijdens de oefening zijn deze communicatiemiddelen niet optimaal gebruikt. Niet iedereen binnen de doelgroep is bekend met de bestaande communicatiemiddelen en communicatielijnen. Ook nam een aanzienlijk deel van de sleutelfiguren in het voorbereidingsteam deel (en dus niet aan de oefening zelf). Hierdoor werd de communicatie niet zoals gebruikelijk op gang gebracht.

Lessons learned
- Wanneer een significant deel van sleutelfiguren uit de crisisorganisatie wordt gehaald doordat ze in de oefenvoorbereiding meedoen, heeft dit zijn weerslag op het delen van informatie tijdens de oefening.
- SCIRT, SCIPR en andere communicatiemiddelen en -methoden dragen bij aan de onderlinge samenwerking.
- Niet iedere instelling maakt deel uit van de SCIRT- en SCIPR-communities en -lijsten. Bij een crisis is het nodig om een middel te hebben om iedereen, ook niet leden, te bereiken.

- **Key-players maakten deel uit van de organisatie van de oefening**
  Doordat veel sleutelfiguren in de organisatie deelnamen in de oefenvoorbereiding konden niet meedoen met de oefening. Bij een normale crisis zouden zij deel uitmaken van het crisisteam. Sommige deelnemers ervoeren dit als problematisch, omdat ze normaal gesproken een zeer actieve rol tijdens een dergelijke crisis zouden hebben. Een van de oefenvoorbereiders heeft tijdens de oefening twee rollen vervuld, zowel bij de voorbereiding als tijdens de oefening zelf. Dit bleek in de praktijk erg lastig. De conclusie was dat het goed is om voor de volgende keer voor één rol te kiezen en die te vervullen.

Lessons learned
- Het zou goed zijn als de security officers die nu deel uitmaakten van het voorbereidingsteam ook de mogelijkheid krijgen mee te oefenen.
- Het vervullen van een rol in zowel de oefenvoorbereiding als de crisisorganisatie is niet aan te bevelen. Het is beter een van de twee te kiezen en te vervullen.
- Het ontbreken van sleutelfiguren in de crisisorganisaties heeft impact op de mate van kennis- en informatiedeling tussen de instellingen.

- **Informatiedeling tussen instellingen**
  Zowel tijdens de oefening als uit de evaluatie kwam naar voren dat de focus meer op het intern oplossen van symptomen lag dan op het delen van de informatie tussen de instellingen. Vooral in het begin van de oefening was dit zichtbaar. Op technisch niveau kwam later in het spel de samenwerking op gang, maar op organisatorisch niveau was deze niet zichtbaar. Er was wel enig één-op-één-contact, maar niet sectorbreed. Andere communities zoals de persvoorlichters, zochten wel onderling contact. Ook sloegen enkele onderwijs- en zorginstellingen de handen ineen om informatie uit te wisselen en de dreiging het hoofd te bieden.
  Uit de evaluatie bleek dat het contact tussen de instellingen (waar dit op gang kwam) bijzonder gewaardeerd werd. Ook omdat medewerkers van verschillende instellingen die elkaar anders nooit tegenkomen elkaar nu hebben leren kennen. De wens werd uitgesproken om meer te oefenen, zowel in onderling verband als op sectorniveau.

Lessons learned
- De oefening bracht nieuwe contacten tussen instellingen tot stand.
- Er is behoefte aan een intensievere communicatie, zowel tussen instellingen als sectorbreed.
- Een grootschalige oefening met meerdere instellingen biedt de mogelijkheid om onderlinge samenwerking en kennisuitwisseling te versterken en van elkaars expertise gebruik te maken.

- **Coördinatie tussen de instellingen**

Tijdens de oefening bleek dat de instellingen zich eerst op de eigen crisis richtten en pas later de samenwerking met anderen opzochten. Dit gold zowel voor de technische als de strategische dilemma's. Tijdens de evaluatie werd gesteld dat de reflex is om tijdens een crisis eerst de eigen problemen op lossen, terwijl soms juist een gezamenlijke actie nodig is. Zo probeerden de instellingen allemaal zelf de technische dilemma's op te lossen, en deelden ze niet met elkaar waarmee ze bezig waren. Hierdoor was men voornamelijk bezig met symptoombestrijding.[139] Het is niet efficiënt om allemaal dezelfde raspberry pi te onderzoeken of de malware te analyseren. Dergelijke acties zouden veel meer gecoördineerd kunnen worden. Verder kwam tijdens de oefening de rol ter sprake van partijen als de VSNU, VH en de MBO-raad.

[139] *(Zoals Mirrors uit de lucht halen, wachtwoorden resetten, raspberry pi's analyseren)*

Ook rees de vraag in hoeverre er sprake kan of moet zijn van centrale coördinatie bij een landelijke crisis. Hierbij dient helder te zijn waar het mandaat ligt en of er op centraal niveau acties gecoördineerd kunnen worden. Dit is een onderwerp dat met de betrokken partijen geagendeerd gaat worden om nader te verkennen en afspraken over te maken.

Lessons learned
- Veel aandacht werd besteed aan symptoombestrijding.
- Er is meer behoefte aan coördinatie en onderlinge afstemming tussen de instellingen.
- Het leggen van contacten wordt als erg waardevol gezien.

5.5.6 Duiden van informatie

- **Beeld en duiding van informatie**
  Het duiden van de situatie blijkt een van de lastigste opgaven. Tijdens de oefening bleek dat deelnemers het lastig vonden om een volledig beeld te krijgen van de totale omvang van de crisis. Een goede informatiedeling is daarom cruciaal. Een gedegen samenkomst van informatie op technisch tactisch/operationeel en strategisch niveau is noodzakelijk. Ook moet de juiste informatie op de juiste plek landen. Eventuele ruis en irrelevante informatie moet gefilterd worden. Bovendien heeft elke partij en elk niveau verschillende informatie nodig.

  Naast het duiden van de informatie vonden de deelnemers ook de veelheid aan bronnen van informatie en communicatie lastig. De deelnemers vonden het moeilijk om alle media, zoals mediaberichten, journalisten die bellen, interne communicatie, verschillende chatomgevingen en e-mail, bij te houden. In de toekomst zal de hoeveelheid informatiebronnen alleen maar groter worden. Er is behoefte aan een methode om al deze informatie goed te verwerken.

Lessons learned
- Om een volledig en juist beeld te kunnen krijgen van de crisissituatie is een goede informatiedeling en een gedegen samenkomst van informatie op alle drie de niveaus noodzakelijk.
- Een goede structuur om de relevante informatie te filteren en de juiste personen van de juiste informatie te voorzien draagt bij aan het duiden van de informatie en aan een efficiëntere en een snellere verwerking van de relevante informatie.
- Het is een uitdaging om de volledige situatie te duiden en slagvaardige keuzes op zowel operationeel als strategisch niveau te maken.

5.5.7 Awareness

Er worden regelmatig crisisoefeningen gehouden om te oefenen met fysieke en sociale risico's. Bij cyberrisico's is dat veel minder het geval. Cybercrisisoefening OZON heeft de dreiging van een cyberaanval voelbaar gemaakt en de aandacht voor cyberrisico's op de kaart gezet.

Uit de evaluatie blijkt dat men erg tevreden was over het toegenomen bewustzijn onder alle deelnemers. Binnen instellingen zijn vervolgacties uitgezet om cybersecurity meer op de kaart te zetten. Tegelijk werd ook geconcludeerd dat het bewustzijn bij veel andere partijen die niet hebben mee geoefend, vergroot moet worden.

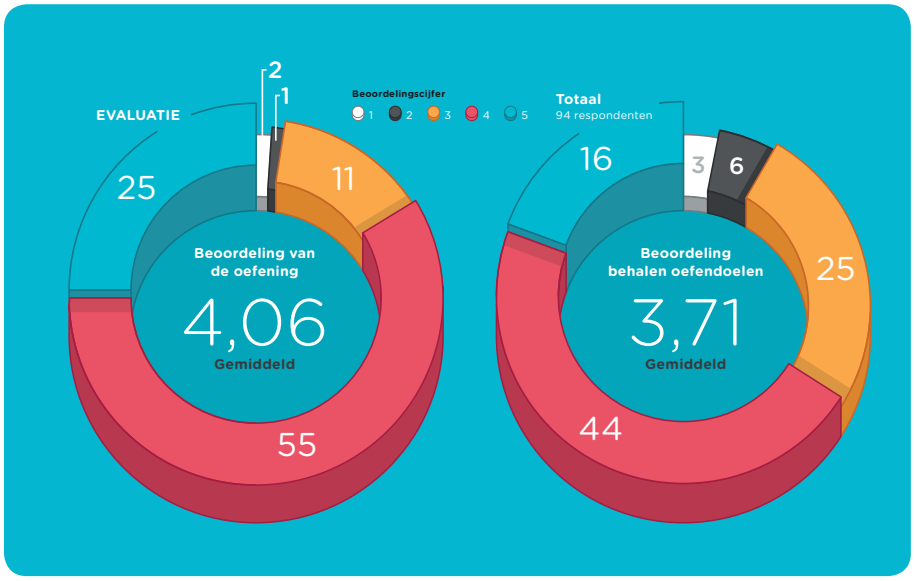
Lessons learned
- Cybercrisisoefening OZON heeft de aandacht voor cyberrisico's op de kaart gezet.
- Cybercrisisoefeningen dragen bij aan het vergroten van het bewustzijn en het ontwikkelen van vaardigheden, zowel op individueel niveau als op organisatie- en collectief niveau.

5.5.8 Capture the Flag (Bronsoefening)

De bronsdeelnemers observeerden de oefening. Hierdoor kregen de meeste instellingen een goed beeld hoe een crisis zich kan ontwikkelen. Ook waren ze op de hoogte van een mogelijke dreiging die de instelling kon raken. Ze waren van tevoren echter niet op de hoogte gesteld van de aanwezigheid van een student met simulatiemalware in hun netwerk. Dit was een bewuste keuze om te testen of de instellingen de studenten zouden detecteren en opsporen. Doordat veel bronsdeelnemers zich ingesteld hadden op een simulatieoefening, waren ze hier niet op bedacht. Voor diverse instellingen kwam de aanwezigheid van de student als een verrassing. Uit de evaluatie is gebleken dat dit vooral door de verwachtingen kwam. Een enkele instelling heeft wel gereageerd en de activiteit ontdekt. Hierop is verschillend geacteerd.

Achteraf zijn veel instellingen positief verrast door de aanwezigheid van de student en zijn de instellingen de gegevens gaan analyseren. De oefening heeft veel gespreksstof opgeleverd. Veel instellingen ervoeren de informatie als nuttig. De 'capture the flag'-oefening heeft daardoor bijgedragen aan het bewustzijn en de weerbaarheid van de instellingen. Hiermee is het doel van de oefening bereikt. Het bleek tijdens de oefening lastig om meerdere oefensystemen tegelijk te besturen. De focus richtte zich er vooral op dat alle studenten op locatie waren en de aanvalssoftware in de lucht kregen.

Lessons learned
- Het observeren van de oefening heeft bijgedragen aan het bewustzijn en de beeldvorming over hoe een crisis zich kan ontwikkelen.
- De student is niet in het netwerk opgemerkt doordat er voorafgaand aan de oefening verschillende verwachtingen bestonden. Dit heeft achteraf tot veel gespreksstof en onderzoek geleid met een positief effect.



5.6 Conclusie

Cybercrisisoefening OZON is een succesvolle eerste simulatieoefening geweest. De instellingen en spelers hebben actief en enthousiast geoefend. Het algemene oordeel over de oefening is een 4,06 op de score van 1 tot 5 (gemiddelde van 94 respondenten, oefenvoorbereiders en spelers). Bij het behalen van de oefendoelen is de score 3,71. Al aan het einde van de eerste speldag concludeerden veel instellingen dat de oefendoelstellingen behaald waren.

Het was goed om te zien dat er veel gecommuniceerd werd tussen de verschillende lagen, bestuur, communicatie en ICT-afdelingen. Verschillende bestuurders vroegen of ze langer mochten meedoen. De spelers hebben het scenario als zeer realistisch, leuk en erg leerzaam ervaren. Sommige instellingen speelden ook na het sluitsignaal nog fanatiek door en de tweede dag werd opnieuw enthousiast gestart. De oefening is als uitermate nuttig, zeer realistisch en leerzaam ervaren.

Het functioneren van de keten is getest en de effectiviteit van de crisiscommunicatie getoetst. Tijdens de oefening blijkt taakverdeling, onderlinge communicatie (zowel intern als extern) en het duiden van de informatie een uitdaging. Meer coördinatie en regie, binnen de instelling en tussen de instellingen, kunnen bijdragen aan een snellere en efficiëntere informatiedeling. Ze kunnen er ook toe bijdragen dat instellingen gezamenlijk zoeken naar oplossingen, zowel op tactisch/operationeel als strategisch niveau. Het vastleggen van draaiboeken meer gericht op cybersecurityrisico's kan hierbij helpen.

De voorbereiding is intensief geweest en heeft de oefenvoorbereiders veel tijd gekost. Ook voor de spelers bleek de oefening veel zwaarder dan verwacht. Het moeilijkste was in te schatten hoe de escalatie en communicatie tussen operationeel, ICT- en strategisch niveau zou verlopen. In dit scenario is veel moeite gedaan om dit onderdeel goed vorm te geven. Ook waren een aantal sleutelpersonen onderdeel van het voorbereidingsteam, waardoor ze in de operatie gemist werden. Dat was tijdens de oefening merkbaar.

Cybersecurity-oefening OZON is een 'gap bridging exercise' geweest waarbij bruggen zijn geslagen tussen bestuurders, communicatie en de ICT-afdelingen, zowel intern als tussen de instellingen. De samenwerking tussen en binnen de instellingen is hiermee vergroot. Het belang van oefenen voor het vergroten van het bewustzijn is gevoeld. Voor instellingen is dit een directe aanleiding om meer aandacht aan cybersecurity te besteden. De deelnemers en oefenvoorbereiders hebben bijzonder veel geleerd en kennis opgebouwd. Veel betrokkenen hebben de wens uitgesproken om deze kennis te behouden en te delen, en de vraag voor herhaling is reeds meerdere malen geuit.

6. AANBEVELINGEN

Op basis van de uitkomsten van de oefening zijn de belangrijkste 5 aanbevelingen:

- Maak cybersecurity een integraal onderdeel van het crisismanagement en leg heldere afspraken over proces, rollen en taken vast in een crisisplan. Een goede en evenwichtige taakverdeling en coördinatie binnen het crisisteam geven allen betrokkenen duidelijkheid en houvast.
- Deel meer informatie tussen instellingen, en doe dat al eerder in het crisisproces. Maak meer gebruik van de bestaande netwerkmogelijkheden. Dit maakt het voor betrokkenen eenvoudiger om informatie te duiden, het proces te coördineren en gezamenlijk problemen aan te pakken.
- Doe onderzoek naar welke vorm van landelijke coördinatie bij een sector-overstijgende cyberdreiging het meest geschikt is. Daarbij moet de autonomie van de instellingen en het mandaat om dergelijke acties uit te voeren, goed afgebakend zijn.
- Houd vaker groot- en kleinschalige oefeningen gericht op de sector of op een bepaald onderwerp[140] om bewustzijn, draagvlak en weerbaarheid te vergroten. Pak de voorbereiding en uitvoering van oefeningen gezamenlijk op omdat het veel tijd en inspanning kost.
- Draag de uitkomsten, conclusies en aanbevelingen van oefeningen uit om bewustzijn en draagvlak voor cyberdreigingen (en oefeningen) te krijgen.

6.1 Aanbevelingen voor crisissituatie

We maken onderscheid tussen aanbevelingen voor de crisissituatie en voor de oefening. Voor de effectiviteit van de interne crisisprocessen en voor de samenwerking tussen de instellingen geven we de volgende adviezen:

Interne crisisprocessen

- Maak cybersecurity integraal onderdeel van het crisismanagement en maak gebruik van de bestaande escalatielijnen.
- Leg heldere afspraken over het proces, rollen, taken van het crisisteam vast in het crisisplan. Een goede en evenwichtige taakverdeling en coördinatie binnen het crisisteam kan bijdragen aan een snellere informatiedeling en betere samenwerking en houvast voor alle betrokkenen. Zo'n taakverdeling draagt tevens bij aan een betere spreiding van werkdruk. Leg niet alles vast en maak maximaal gebruik van kennis, creativiteit en improvisatievermogen.
- Zodra je het vermoeden hebt dat een crisis langer gaat duren, zet dan meerdere crisisteams op die elkaar kunnen aflossen. Zorg voor een tijdige escalatie en overdracht om te zorgen voor continuïteit en borging.
- Oefen regelmatig en met verschillende samenstellingen van teams; oefen zowel met als zonder sleutelfiguren.

Samenwerking tussen instellingen

- Maak meer gebruik van de onderlinge netwerkmogelijkheden, zoals SCIRT en SCIPR om het onderlinge contact te versterken. Hierdoor zal men elkaar eerder en sneller vinden tijdens een echte crisis.
- Bevorder informatiedeling tussen instellingen in het crisisproces; dit maakt het voor betrokkenen eenvoudiger om informatie te duiden, het proces te coördineren en gezamenlijk problemen aan te pakken.
- Onderzoek de mogelijkheden van landelijke coördinatie bij een sectoroverstijgende cyberdreiging. Een centrale coördinatie voor analyse en duiding kan van toegevoeg-

[140] *Bijvoorbeeld een ziekenhuisvariant, datalekvariant, cijfermanipulatievariant*

de waarde zijn, zolang de autonomie van instellingen is gewaarborgd. Afhandeling van incidenten moet lokaal aangestuurd worden. Het mandaat hiervoor dient goed afgebakend te zijn.

6.2 Aanbevelingen voor oefening

Voor de voorbereiding van de oefening, het proces tijdens de oefening en de keuze van de soort oefening adviseren we het volgende:

Voorbereiding van de oefening

- Stem de duur van de oefening goed af op de doelen ervan. Ga na of het mogelijk is de oefening tot een dag te beperken.
- Houd bij de aanmeldprocedure rekening met de tijd die nodig is voor besluitvorming bij de instellingen.
- Ruim voldoende tijd in en stel voldoende resources beschikbaar voor de voorbereiding van het scenario en de oefening.
- Zorg voor zowel technische als strategische expertise in het voorbereidingsteam door teamuitbreiding of door interne hulp in te schakelen.
- Een mogelijkheid om de expertise van het voorbereidingsteam te ontwikkelen is gezamenlijke werksessies en workshops organiseren. Daarin kunnen de deelnemers gezamenlijk aan de scenario's werken, ervaringen uitwisselen en hun kennis verbreden. Dat maakt meer samenwerking tijdens de oefening mogelijk.
- Het kost veel tijd om de spelelementen, zoals de berichten, uit te werken. Stel de deadline voor de instellingsscenario's daarom ruim voor de oefening om hier voldoende tijd voor te hebben.
- Ondersteun vanuit de projectgroep de oefenvoorbereiders bij het maken van de instellingsscenario's.
- Overweeg of je onderling werkmateriaal kunt delen; denk aan 'master event lists' en mediaberichten. Voorbeelden helpen bij de totstandkoming van een goed en realistisch scenario en bevorderen de samenwerking.
- Manage de verwachtingen van de deelnemers in de aanloop naar de oefening zodat zij weten wat er van hen verwacht wordt, wat ze kunnen verwachten en wat de randvoorwaarden zijn. Een briefing, spelregels, informatiepakket en adresboek dragen hieraan bij. Geef ook aandacht aan de werkdruk die de oefening kan genereren bij de deelnemers.
- Houdt bij het opzetten van een oefening rekening met de rol die sleutelfiguren in de organisatie innemen en overweeg wie in de oefenvoorbereiding plaatsneemt en wie mee-oefent.
- Ruim meer tijd in tussen de oefening en de centrale evaluatie voor interne evaluatie. Deze interne evaluatiepunten kunnen als input dienen voor de centrale evaluatie.

Tijdens de oefening

- Overweeg om een waarnemer aan te stellen die de interne processen kan observeren. Dit helpt om de gestelde oefendoelen intern te evalueren en om feedback te geven aan de oefenleiding om het verloop van de oefening op de werkvloer te monitoren.
- De centrale en interne responscel staan in nauw contact met elkaar. Het is daarom aan te bevelen om vanuit één ruimte te werken. Wel moet er voldoende ruimte zijn om uit te wijken om bijvoorbeeld te telefoneren.
- Maak gebruik van een simulatiesysteem voor de mediaberichten, zoals krantenberichten en social media. Dit draagt bij aan de overzichtelijkheid en aan het behouden van het gesloten karakter van de oefening. Ook het werken met een gesloten adresboek draagt hieraan bij.
- Communiceer tijdens de oefening helder over de start, einde en de kaders van de oefening en kondig veranderingen in het scenario op tijd aan. Dit draagt bij aan een helder verwachtingspatroon bij de deelnemers.

- Geadviseerd wordt om de taken van oefenvoorbereider en uitvoerende taak op de eigen werkvloer niet te combineren.
- Stel ook bij de brons-deelnemers een oefenvoorbereider aan. Dit draagt bij aan betere voorbereiding voorafgaand en de oefening, het beter managen van de verwachtingen en biedt de mogelijkheid om tijdens de oefening beter bij te sturen.

Specifieke oefeningen en scenario's

- Oefen realistische cyberscenario's met behulp van de verschillende[141] vormen van oefeningen (zie hoofdstuk 3). Oefenen vergroot het bewustzijn en geeft medewerkers de mogelijkheid om bekend te raken met procedures, rollen en de taakverdeling binnen het crisisteam.[142]
- Ontwikkel scenario's gericht op bijvoorbeeld universiteiten, hogescholen, ROC's, UMC's of onderzoeksinstellingen. Ook kunnen sectorgerichte scenario's bijdragen aan het stimuleren van meer onderlinge samenwerking. Dat maakt het mogelijk om de schaal van de oefening te vergroten.
- Een grootschalige oefening zoals OZON heeft grote impact op de organisatie en de voorbereiding. Organiseer naast grootschalige simulatieoefeningen ook kleinere oefeningen gericht op een sector, onderwerp[143] of soort oefening.[144]
- Organiseer 'gap bridging exercises' op groot- en kleinschalig niveau om de communicatie en coördinatie tussen de verschillende lagen van bestuur, communicatie- en ICT-afdelingen te bevorderen.

[141] *Zoals een 'table top oefening', 'capture the flag' of red/team blue/team oefening; zie hoofdstuk 3*
[142] *Zie voor een uitgebreide beschrijving hiervan hoofdstuk 2*
[143] *Bijvoorbeeld een ziekenhuisvariant, datalekvariant, cijfermanipulatievariant*
[144] *Bijvoorbeeld 'tabletop' oefening voor strategisch niveau of 'capture the flag' voor operationeel niveau; zie voor een compleet overzicht hoofdstuk 3*

REFERENTIES

Normen en standaarden

- **SURF Juridisch Normenkader (Cloud)services 2016 -** geraadpleegd via https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html op 16 november 2016
- **Normenkader Informatiebeveiliging HO (2015)** (Moens, 2015) - geraadpleegd via https://www.surf.nl/diensten-en-producten/surfaudit/normenkader-surfaudit/index.html op 20 oktober 2016
- **Normenkader Informatiebeveiliging MBO (2015**) (Kennisnet/saMBO-ICT, 2015) geraadpleegd https://www.sambo-ict.nl/wp-content/uploads/2015/02/IBBDOC2-Normenkader-Informatiebeveiliging-MBO-versie-1.0-Creative-Commons.pdf op 20 oktober 2016
- **ISO 27001:2013** ISO 27001:2013 Information security management, oktober 2013 geraadpleegd via http://www.iso.org/iso/home/standards/management-standards/iso27001.htm op 20 september 2016
- **ISO 22398:2013(E)** ISO 22398:2013(E) Social Security - Guidelines for exercises, september 2013 geraadpleegd via http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50294 op 20 september 2016
- **ISO 22301:2012** Business Continuïteits management, mei 2012, geraadpleegd via http://www.iso.org/iso/catalogue_detail?csnumber=50038 op 19 september 2016

Bronnen

- **COT (2011)** Schaap, S.D, van der Veen, M.J., Hendriks van der Weem, C.J *"Leren van incidenten",* In vijf stappen beter voorbereid, COT, mei 2011 geraadpleegd via http://www.cot.nl/pdf/Leren_van_incidenten.pdf Op 12 september 2016
- **COT (2014)** COT, *"Elf bouwstenen voor een crisisplan",* van incidentbestrijding naar crisismanagement, COT, maart 2014 Geraadpleegd via http://www.cot.nl/pdf/COT_Elf_bouwstenen_voor_een_crisisplan.pdf op 12 september 2016
- **COT (2016)** COT, *"Instituut voor veiligheids- en crisismanagement, bijlage bij het verslag van het vierde Regionaal kennisplatform Integraal Crisisplan Zorg: concept scenariokaart Cyberaanval",* mei 2016 Geraadpleegd via http://www.otoportaal.nl/sites/default/files/redactie/icp_concept_scenariokaart_cybercrisis_regio_amsterdam.pdf op 15 september 2016
- **ENISA (2012)** Trimintzios, P., Razvan, G. *"On national and International Cyber Exercises",* Survey, Analysis and Recommendations "Cyber crisis Exercises Analysis Report", ENISA, 2012 geraadpleegd via https://www.enisa.europa.eu/publications/exercise-survey2012 op 12 september 2016
- **ENISA (2014) 01** Panagiotis Trimintzios, Roger Holfeldt, Mats Koraeus ea. *"Report on cyber crisis cooperation and management",* ENISA, November 2014 Geraadpleegd via https://www.enisa.europa.eu/publications/ccc-study op 05 september 2016
- **ENISA (2014) 02** ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats (27-01-2015 ed.). ENISA. Geraadpleegd via https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014 op 05 september 2016
- **ENISA (2015)** ENISA *"The 2015 Report on National and International Cyber Security Exercises"*, final, 0.99, ENISA, dec. 2015 geraadpleegd via https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises op 12 september 2016

- **ENISA (2016)** De Muynck, Jo, Portesi, Silvia *"Strategies for Incident Response and Cyber Crisis Cooperation",* version 1.1, ENISA, august 2016 geraadpleegd via https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation op 12 september 2016
- **NCSC (2013)** NCSC, "*De aanhouder wint"* de wereld van Advanced Persistent Threat Factsheet FS-2013-02C, NCSC, Versie 1.3, 03 oktober 2013 geraadpleegd via https://www.ncsc.nl/actueel/factsheets/factsheet-de-aanhouder-wint-advanced-persistent-threats.html op 10 september 2016
- **NCSC (2014)** NCSC, *Cyber security Assessment*, 2014 geraadpleegd via https://www.ncsc.nl/english/current-topics/news/cyber-securty-assessment-netherlands-4-cybercrime-and-digital-espionage-remain-the-biggest-threat.html op 11 oktober 2016
- **NCSC (2015)** Cybersecuritybeeld Nederland 2015 CSBN, NCSC geraadpleegd via https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-5.html op 05 september 2016
- **NCSC (2016)** Cybersecuritybeeld Nederland 2016 CSBN, NCSC geraadpleegd via https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html op 20 september 2016
- **SANS (2012)** Janes, P. "*People, Process, and Technologies Impact on Information Data Loss*" SANS, november 2012 geraadpleegd via https://www.sans.org/reading-room/whitepapers/dlp/people-process-technologies-impact-information-data-loss-34032 op 5 september 2016
- **SURF (2015)** SURFnet Cyberdreigingsbeeld Sector Hoger onderwijs en wetenschappelijk onderzoek, 2015 geraadpleegd via https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2015/cyberdreigingsbeeld-2015.pdf op 15 september 2016
- **Wein, Willems (2013) 01** Wein, B, Willems, R, *"Een raamwerk voor het effectief evalueren van crisisoefeningen, verkorte versie"*, Nijmegen, April 2013 geraadpleegd via https://www.wodc.nl/images/2062-verkorte-versie_tcm44-502151.pdf op 10 september 2016
- **Wein, Willems (2013) 02** Wein, B, Willems, R, "*Een raamwerk voor het effectief evalueren van crisisoefeningen,* Nijmegen, April 2013, geraadpleegd via https://www.wodc.nl/images/2062-volledige-tekst_tcm44-498999.pdf op 10 september 2016
- **Zannoni, Kuipers en Wensveen (2012**) Zannoni, Marco, Kuipers Frank & Wensveen, Maike, *'Realisme in veiligheid en crisismanagement'*, COT, Mei 2012, http://www.cot.nl/pdf/Realisme_in_veiligheids-encrisismgtMBOHO.pdf geraadpleegd op 15 september 2016
- **Zannoni (2016)** Zannoni, Marco, *'Van incident tot crisis: voorbereid zijn op cyber crisismanagement loont',* april 2016 geraadpleegd via https://www.linkedin.com/pulse/voorbereid-zijn-op-een-cybercrisis-marco-zannoni?published=u op 05 september 2016

Websites

- http://www.bcmacademy.nl/nl/bcm-academy/informatie-over-het-vak/begrippen-lijst Geraadpleegd op 10 oktober 2016
- http://www.cot.nl/pdf/COT-Leren-van-Dorifel-15-januari-2013.pdf geraadpleegd op 12 september 2016
- http://www.cot.nl/pdf/Artikel-COT-in-Magazine-Nationale-Veiligheid.pdf geraadpleegd op 12 september 2016
- http://www.cot.nl/crisismanagement/crisisoefeningen/walkthrough/ geraadpleegd op 05 september 2016
- http://www.cot.nl/crisismanagement/crisisoefeningen/tabletop/ geraadpleegd op 05 september 2016
- http://crisismanagement.schoolenveiligheid.nl/algemeen/ geraadpleegd op 12 september 2016
- www.crisisplan.nl geraadpleegd op 12 september 2016

- https://www.cybersaveyourself.nl/ geraadpleegd op 10 oktober 2016
- https://www.encs.eu/wp-content/uploads/2015/08/2015_ENCS_Factsheet_Red-Blue_Training_v1.pdf geraadpleegd op 20 oktober 2016
- https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016 geraadpleegd op 21-10-2016
- http://www.integraalveilig-ho.nl geraadpleegd op 10 oktober 2016
- http://www.integraalveilig-ho.nl/continuiteitmanagement/ geraadpleegd op 15 september 2016
- http://www.pm.be/oefeningen_op_maat/command_post_exercise.html geraadpleegd op 12 september 2016
- www.ncsc.nl geraadpleegd op 15 september 2016
- https://www.ncsc.nl/actueel/nieuwsberichten/internationale-oefening-cyber-europe-2012.html geraadpleegd op 15 september 2016
- https://www.ncsc.nl/actueel/nieuwsberichten/duits---nederlandse-oefening.html geraadpleegd op 20 oktober 2016
- https://www.nctv.nl/organisatie/cs/index.aspx geraadpleegd op 20 oktober 2016
- https://www.surf.nl/persberichten/2015/12/surf-publiceert-cyberdreigingsbeeld-2015.html geraadpleegd op 15 oktober 2016
- https://www.surf.nl/diensten-en-producten/cybersave-yourself/index.html geraadpleegd op 10 oktober 2016

Nieuwsbronnen

- http://www.nu.nl/algemeen/1565130/brand-verwoest-faculteitsgebouw-bouwkunde-in-delft-video.html geraadpleegd op 20 oktober 2016
- http://www.nu.nl/tech/3627406/16-jarige-jongen-opgepakt-cyberaanval-school.html geraadpleegd op 16 oktober 2016
- http://www.at5.nl/artikelen/148428/waarschuwing_voor_phishingmail_inholland geraadpleegd op 20 oktober 2016
- http://www.rtvutrecht.nl/nieuws/1461998 geraadpleegd op 20 oktober 2016
- http://www.bbc.com/news/technology-36478650 geraadpleegd op 16 oktober 2016
- http://infosecuritymagazine.nl/2015/03/11/vrije-universiteit-amsterdam-besmet-met-ransomware/ geraadpleegd op 16 oktober 2016
- http://www.nu.nl/internet/4280591/studentgegevens-uva-en-hva-waren-makkelijk-vindbaar-systeemlek.html geraadpleegd op 16 oktober 2016
- http://www.nu.nl/internet/2427939/hackende-scholieren-betrapt-cijferfraude.html geraadpleegd op 16 oktober 2016
- http://www.nu.nl/binnenland/3931116/cijferfraude-leerlingen-amsterdams-gymnasium.html geraadpleegd op 16 oktober 2016
- http://www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medische-dossiers.html geraadpleegd op 16 oktober 2016
- https://www.nederlandict.nl/news/telecomsector-bouwt-met-grootschalige-oefening-cyberdawn-aan-sterke-samenwerking-op-cyber-security/ geraadpleegd op 20 oktober 2016
- http://webwereld.nl/security/79360-nederland-wint-goud--zilver-en-brons-op-wk-ethisch-hacken geraadpleegd op 21 oktober 2016

OZON TIMELINE

start · vergadering · actie · deadline · evaluatie

WERKDRUK

TIJD

- 4 februari — Tweedaagse – Idee voor cybercrisisoefening
- 24 februari — Startbijeenkomst
- 15 maart — Uitnodiging verstuurd
- 4 april — **Inschrijving goud/zilver gesloten**
- 15 april — Aanvankelijke inschrijving deadline goud
- 20 april — Eerste stuurgroep-vergadering
- 27 april — Aanvankelijke deadline inschrijving zilver/brons
- 28 april — Eerste programma-groepvergadering
- 12 mei — Vaststelling centraal scenario
- 18 mei — Tweede programma-groepvergadering
- 31 mei — **Inschrijving brons gesloten**
- 8 juni — Derde programma-groepvergadering
- 29 juni — Tweede stuurgroep-vergadering
- 6 juli — Vierde programma-groep-vergadering
- 8 juli
- 20 augustus — **Deadline instellings-scenario's**
- 31 augustus — Laatste programma groepvergadering
- 7 september — Laatste stuurgroep-vergadering
- 15 september — Uitloop deadline instellings-scenario's
- 30 september — Technische elementen klaar (malware / logfiles / websites)
- 1 oktober — Briefing van deel-nemers
- 3 oktober — Briefing responscel
- 4 / 5 oktober — **Cybercrisis-oefening OZON**
- 25 oktober — Evaluatie Cybercrisis-oefening OZON
- 1 november — Evalueren en uitwerken uitkomsten Cybercrisis-oefening OZON

Budget en draagvlak creëren

Project-groep formeren

Aanmel-dingen

Stuurgroep formeren

Scope en oefendoelen bepalen

Schrijven centraal scenario

Dilemma's instellingsscenario's uitwerken en opzet master event list en spelelementen

Vakantieperiode

Uitwerken instellingsscenario's master event list en spelelementen

Centrale en instellings-elementen uitwerken, totale master event list maken en mediasimulator vullen

Evalueren en uitwerken uitkomsten Cybercrisisoefening OZON

Raspberry Pi's verspreid

COLOFON

Tekst
SURFnet

Auteurs
Sandy Janssen, Alf Moens

Ontwerp
Vrije Stijl, Utrecht

Fotografie en illustraties
Alf Moens, Charlotte Verhees, iStock, Jaap van Ginkel,
Thomas Rohlfs, Studio Taeks, Amsterdam

November 2016

SURFnet

+31 (0)88 787 30 00
www.surf.nl