Auteurs: Marijke Stokkel, Strategisch adviseur cybersecurity en oefenleider OZON 2023, UvA en HvA. Roeland Reijers, Chief Information Security Officer (CISO) en (gedelegeerd) opdrachtgever OZON 2023, UvA en HvA.

Hoe je in 10 stappen een cybercrisis-oefening organiseert

Het is half maart, een week voor de oefening. Marijke, de oefenleider, wordt gebeld door een deelnemer, laten we hem Joris noemen. "Het is me toch nog niet helemaal duidelijk. Kun je vertellen wat er precies van mij wordt verwacht? Waar moet ik me melden op 23 maart? En krijg ik dan een opdracht bij de start van de oefening?"

Joris is bij de briefing geweest, heeft de uitleg en spelregels meegekregen, maar vindt het toch lastig om een voorstelling te maken van de oefening, en vooral van zijn rol hierin.

Eigenlijk niet zo vreemd. Een crisisoefening is een nabootsing van de werkelijkheid, in een min of meer gecontroleerde omgeving met beperkingen en spelregels. Het vergt verbeeldingskracht om daar direct soepel in te opereren. En dit geldt des te meer voor een *cyber*crisisoefening, omdat hier minder concrete elementen zijn waartoe je je kunt verhouden dan bij andere crisisoefeningen - denk aan terreur of brand - zoals een fysieke locatie waar de crisis plaatsvindt, materieel en (nep) slachtoffers. Cybercrisis-oefeningen zijn echter belangrijk voor de digitale weerbaarheid van organisaties (1), het is dus raadzaam om deze te houden. Vooraf zorgvuldig nadenken over de juiste opzet maakt een oefening doeltreffender.

Op 23 en 24 maart jl. werd OZON gehouden, de tweejaarlijkse sectorbrede cybercrisisoefening voor onderwijs en onderzoek. De oefening is een initiatief van SURF (2) en wordt sinds 2016 tweejaarlijks gehouden. De Universiteit van Amsterdam (UvA) en de Hogeschool van Amsterdam (HvA) hebben eerder deelgenomen en waren ook dit jaar van de partij, net als zeventig andere instellingen.

Hoe organiseer je een cybercrisisoefening? Hoe kun je die zo voorbereiden dat de deelnemers optimaal kunnen oefenen? Dit artikel beschrijft hoe de OZON oefening is voorbereid en uitgevoerd bij de UvA en HvA, vanuit het perspectief van de oefenleider en van de opdrachtgever.

Voordat we beginnen: waarom gaat dit artikel over de UvA én de HvA? Waarom samen? Dat komt omdat de instellingen een gemeenschappelijke ICT-dienst (ICT Services genaamd) en één CISO hebben. Dat zijn centrale partijen bij een cybercrisis(-oefening) en daarom was het logisch dat beide instellingen gezamenlijk deelnamen aan de oefening.

Voorbereiding

‘We denken in grote lijnen maar leven in details’ [3]

Omdat we deelnamen aan het initiatief van SURF stond de opzet van de oefening van tevoren al vast. OZON is een zogenaamde simulatie-oefening, waarbij de deelnemers een realistisch scenario naspelen in hun eigen werkomgeving. Een andere bekende variant is een tabletop-oefening. Hier wordt een crisisoverleg nagebootst en hebben de deelnemers meer gelegenheid om tijdens de oefening te reflecteren op hun eigen handelen. Deze variant duurt een stuk korter dan de simulatie-oefening (4).

De UvA en HvA namen deel aan OZON met twee crisisteams en in totaal veertig deelnemers. Dit vergde een gedegen voorbereiding. We wilden een optimale oefenomgeving creëren. We schreven een zo realistisch mogelijk scenario, informeerden de deelnemers via meerdere briefings, bootsten bestaande communicatiemiddelen na en stelden een respons cel samen. We volgden een aanpak die, achteraf gezien, in tien stappen uiteengezet kan worden. Deze aanpak werkte goed voor ons en daarom hebben we hem uitgewerkt in een apart kader.

De oefenleider bereidde zich dus minutieus voor op de oefening. Voor een deelnemer geldt dit idealiter niet. Een crisis komt in de regel onverwacht. Als een deelnemer allerlei voorbereidingen gaat treffen voor een oefening, wordt deze minder waarheidsgetrouw. Het is dus niet de bedoeling dat een deelnemer gaat werken op een andere locatie dan gebruikelijk, of samen met andere deelnemers in één overlegruimte de injects gaat afwachten. Wat een deelnemer wél kan doen, is ervoor zorgen dat er geen belangrijke afspraken in de agenda staan voor de oefendagen. Voor een crisis zeg je belangrijke afspraken af, maar voor een oefening werkt dat net iets anders.

De aanpak van de UvA en HvA in 10 stappen

1. **Zorg voor bestuurlijk commitment.** Een stevig draagvlak bij het bestuur zorgt voor meer animo voor deelname aan de oefening en vergroot de kans dat de aanbevelingen achteraf daadwerkelijk opgepakt gaan worden. Dit draagvlak was bij ons ruim aanwezig. Sterker nog, terwijl het CISO-team en ICT Services overwogen om vanwege meerdere lopende audits en verbetertrajecten dit jaar niet deel te nemen aan OZON, was het bestuur resoluut. Het oefenen gaat door. Dit bestuurlijke draagvlak is heel prettig, want er gaat veel tijd zitten in de voorbereidingen en het is vervelend als er over elk extra uurtje inzet een discussie gevoerd moet worden.

2. **Maak iemand verantwoordelijk.** Stel iemand aan als oefenleider. Bij de UvA en HvA is vanwege de grootte en complexiteit van de oefening gekozen voor twee oefenleiders. Zij hadden elk een eigen aandachtsgebied. De oefenleiders bereidden de oefening voor en leidden de oefendagen.

3. **Denk ook alvast aan de waarnemers.** Waarnemers hebben als taak om de oefening te observeren en achteraf om de evaluatie te leiden. Wij hebben gekozen voor drie waarnemers: één voor het bestuurlijke crisisteam en twee voor ICT Services, waaronder het operationele crisisteam en de incidentresponsteams CERT en SOC. Zorg ervoor dat er qua profiel voldoende aansluiting is met de teams die worden waargenomen.

4. **De oefendoelstellingen zijn het fundament.** Oefendoelstellingen geven gedurende het hele traject focus: bij het opstellen van het scenario en het samenstellen van het deelnemersteam en tijdens de evaluatie. Bedenk in een vroeg stadium wat je wilt bereiken en leg dit voor aan de opdrachtgever of het bestuur. Een cybercrisisoefening is in eerste instantie bedoeld om in de volle breedte een crisis na te bootsen, met alle betrokkenen van de organisatie. De oefendoelen gaan idealiter over de processen en procedures. Werkt men volgens het crisishandboek? Worden de juiste stakeholders betrokken? Hoe verloopt de opschaling naar een crisis? Voor het toetsen van technisch-inhoudelijke vaardigheden is een oefening minder passend, dan volstaat een training of Capture-the-Flag (5) ook.

5. **Stel een team van deelnemers samen.** Op basis van de oefendoelstellingen kun je grotendeels al bepalen wie er deel moeten nemen. Wil je de opschaling naar een crisissituatie oefenen? Zorg er dan voor dat er zowel leden van de operationele uitvoering als van het crisismanagementteam op de deelnemerslijst staan. Wil je de samenwerking oefenen tussen twee afdelingen? Dan doen er afgevaardigden van beide afdelingen mee. Wees flexibel bij het samenstellen van het team. Mensen kunnen afzeggen of uitvallen. Zorg indien mogelijk voor een back-up van sleutelfiguren. Met de uitwerking van het scenario kan ook duidelijk worden dat meer mensen nodig zijn.

6. **Creëer een realistisch scenario van een uitzonderlijke situatie.** Stel een achtergrondverhaal op dat beschrijft hoe de cybercrisis ontstaat. Richt je op een ongewone situatie die veel vergt van de organisatie om aan te pakken en die de organisatie zeer kwetsbaar kan maken. SURF leverde een fraai basisscenario aan. Een van de verhaallijnen was een hackerscollectief dat veel 0-day kwetsbaarheden verzamelde en deze tijdens de oefendag in korte tijd achter elkaar op hun website publiceerde. Voor de UvA en HvA hebben we daarnaast een instellingsspecifiek scenario opgesteld, dat kortgezegd neerkwam op een datalek van zeer vertrouwelijke onderzoeksdata.
   Het was een tijdrovende klus, want we wilden zeker weten dat alle verhaallijnen realistisch waren. We hebben tijdens het opstellen advies ingewonnen van een aantal experts bij de UvA en HvA.

7. **Ontwikkel scenario-injects.** Stel een draaiboek op met berichten (ook wel injects genoemd) die deelnemers ontvangen tijdens de oefening. Een inject is bijvoorbeeld een bericht over inlogproblemen aan de servicedesk van medewerkers. Bedenk hoe de servicedesk hier waarschijnlijk op reageert (ook wel 'expected player action' genoemd). Gaat de medewerker eerst zelf onderzoek doen? Neemt hij of zij contact op met andere afdelingen? Schrijf uit hoe het proces zal lopen. Zorg ervoor dat je voldoende injects achter de hand hebt om de vaart in de oefening te houden. Stel dat er niet geëscaleerd wordt naar het bestuur terwijl dat volgens het scenario wel zou moeten,

dan kun je als responsecel het bestuur op de hoogte brengen. Hiervoor dien je een andere partij te simuleren. Je benadert bijvoorbeeld het bestuur als hoofd van een afdeling - kies iemand die niet deelneemt aan de oefening - met het bericht dat veel van je medewerkers inlogproblemen hebben, dat dat nog niet is opgelost en dat je snel actie van het bestuur vraagt. Beschrijf per inject hoe laat deze ingezet wordt, met welk doel en wat de 'expected player action' is.

8. **Stel een responsecel samen.** Met een responsecel simuleer je de wereld buiten de deelnemers. De deelnemers kunnen niet zomaar met iedereen gaan bellen tijdens de oefening. Als zij contact met iemand willen opnemen die niet in de deelnemerslijst staat, dienen zij dat via de respons cel te doen. Onze responsecel bestond uit zeven mensen: twee security architecten, twee servicemanagers, een communicatieadviseur, een bestuursondersteuner en een functioneel beheerder. In de voorbereiding hielpen deze mensen mee met het realistisch maken van het scenario en tijdens de oefening fungeerden zij als de hele buitenwereld. Voor de communicatie met de spelers gebruikten we een gedeelde mailbox.

9. **Boots communicatiemiddelen na.** Om realistisch te kunnen oefenen, moeten deelnemers gebruik kunnen maken van communicatiemiddelen die normaal ook tot hun beschikking staan. Denk aan een Signal-groepen, maillijsten, intranetpagina's en webpagina's. We wilden niet de echte kanalen gebruiken omdat dat voor verwarring kan zorgen en omdat dat het exporteren van data voor evaluatie-doeleinden in de weg staat. We kozen ervoor om Teams-kanalen en gesimuleerde Signal-groepen in te zetten. Elke bestaande Signal-groep kreeg een OZON-imitatieversie en de andere communicatiemiddelen kregen elk een eigen Teams-kanaal. Dit werkte prima. De kanalen behoefden vooraf weinig uitleg en tijdens de oefening werd er volop gebruik van gemaakt.

10. **Besteed aandacht aan de briefing van deelnemers.** We organiseerden meerdere bijeenkomsten voor de deelnemers. Hierin kwamen de opzet van de oefening, de spelregels en het simuleren van de communicatiemiddelen aan de orde. Uiteraard deelden we niet het inhoudelijke scenario, dat diende geheim te blijven. Voor sommige deelnemers was de materie, zoals het concept van een respons cel, lastig om direct te bevatten. We namen extra tijd om hen goed te informeren.

De uitvoering

Chaos is a friend of mine [6]

Een crisis verloopt niet ordentelijk - als dat wel zo was zou het geen crisis zijn - en dat gold ook voor de crisis in de oefening. Op de oefendag zaten de oefenleiders om negen uur 's ochtends samen met de respons cel als gezamenlijk oefenteam in één ruimte. Draaiboek bij de hand, de visuele weergave van het scenario vergroot uitgeprint aan de muur. Toen de oefening startte, kwam er direct een grote stroom berichten op gang. Vanwege het sectorale karakter van de oefening hadden we hier slechts beperkt invloed op.

Na al het gepuzzel en geverifieer van de voorgaande periode, moest het oefenteam de controle loslaten. De

chaos omarmen. Inspelen op wat er gebeurde. We vonden die omschakeling aanvankelijk best lastig, maar uiteindelijk lukte het aardig.

Over het optreden van de deelnemers kunnen we niet te veel uitweiden, de evaluatie is momenteel in volle gang. Vooral de operationele teams waren druk met het verweer tegen de continue stroom kwetsbaarheden. Er werd redelijk snel opgeschaald, wat te maken had met de talloze alarmerende berichten die binnenkwamen vanuit de sector. De crisisoverleggen verliepen in de regel doelmatig. De crisisteams pasten het BOB-model toe, zoals ook wordt voorgeschreven in de UvA en HvA crisishandboeken. Het BOB-model is het bekendste model voor crisisbeheersing en staat voor *beeldvorming*, *oordeelsvorming* en *besluitvorming*. Het geeft structuur aan crisisoverleggen en draagt bij aan heldere besluitvorming. (7)

In het algemeen kunnen we zeggen dat de crisisteams goed op elkaar ingespeeld waren. De deelnemers overlegden constructief en bewaarden de rust.

De nabeschouwing

Kostbaar is de wijsheid die door ervaring wordt verkregen [8]

De evaluatie is misschien wel de belangrijkste fase. Na het precisiewerk van de voorbereiding en het tumult van de oefendagen, gaat deze fase over lering trekken uit de oefening. Wij hebben in totaal drie evaluatiebijeenkomsten gehouden: twee voor ICT Services en één voor het bestuurlijke crisisteam. Dat deden we direct na de oefening (ook wel 'hotwash' genoemd). Het waren constructieve sessies waarbij de deelnemers stoom konden afblazen, hun enthousiasme deelden en hun grieven konden uiten. De boventoon was positief. We hebben ook een evaluatieformulier gestuurd naar alle deelnemers.

De waarnemers en oefenleider zijn nu bezig om alle observaties en input van deelnemer te verwerken in een evaluatierapport. De UvA en HvA crisishandboeken en de oefendoelstellingen worden hierbij gebruikt als leidraad. Daarna is het zaak om de positieve punten te koesteren en de leerpunten op te pakken ter verbetering.

De OZON 2023 oefening bleek weer een goed leerinstrument. De deelnemers gingen uiterst serieus aan de slag. Het scenario en de oefenomgeving waren een goede benadering van de realiteit. We hebben de doelstellingen uitgebreid kunnen oefenen.
Kortom, we kijken positief terug op de oefening en zijn blij dat we hiermee kunnen bijdragen aan een cyberweerbare organisatie.

Referenties

1. De Nederlandsche Bank ziet het oefenen van een cyberaanval als een van de drie basismaatregelen die aandacht behoeven bij organisaties om zich te beschermen tegen cyberdreigingen: https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/
2. SURF is de ict-coöperatie van de sector onderwijs en onderzoek. Meer informatie: https://www.surf.nl
3. Dit citaat wordt toegeschreven aan de negentiende-eeuwse filosoof en wiskundige Alfred North Whitehead
4. Deze en andere oefenvarianten worden beschreven in de whitepaper van SURF over oefeningen. whitepaper-cybercrisisoefening-ozon-een-gap-bridging-exercise.pdf (surf.nl) p18-20
5. Capture the flag (cybersecurity) - Wikipedia
6. Dit citaat wordt toegeschreven aan Bob Dylan
7. Meer informatie over het BOB-model: Waar komt 'ons' BOB model voor besluitvorming in crisisteams vandaan? - Zaak voor Crisiskunde
8. Dit citaat wordt toegeschreven aan de zestiende eeuwse Britse auteur Robert Ascham