Samen aanjagen van vernieuwing

OZON 2021

Evaluatie sectorbrede cybercrisisoefening voor onderwijs en onderzoek

Auteur(s):	Charlie van Genuchten
Versie:	1.0
Datum:	juni 2021

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
info@surf.nl

www.surf.nl

Inhoudsopgave

1 Inleiding

Belang van oefenen
Het aantal en de complexiteit van securityincidenten binnen onderwijs en onderzoek is de afgelopen jaren alleen maar toegenomen. Het onderwerp staat daarom steeds hoger op de (bestuurlijke) agenda. Tegelijk is bij daadwerkelijke crises en incidenten steeds meer aandacht voor dit onderwerp vanuit de media en de politiek. Om als sector te groeien in het omgaan met de complexiteit van technische uitdagingen, groeiende externe aandacht en bestuurlijke en politieke vraagstukken, oefent de sector elke twee jaar een cybercrisis onder de naam OZON.

Derde grote cybercrisisoefening
Op 18 maart 2021 vond OZON plaats. Dit was de derde keer dat SURF deze grote simulatieoefening organiseerde. In 2016 initieerde SURFcert de eerste OZON-oefening naar voorbeeld van ISIDOOR, de landelijke oefening van het Nationaal Cyber Security Centrum (NCSC). Wat in 2016 begon als een oefening met 12 instellingen op Goud- en Zilver-niveau, is ondertussen uitgegroeid tot een oefening waaraan meer dan 1.000 mensen meedoen.

In deze 2021-editie deden 40 organisaties mee op Goud- of Zilver-niveau en 22 op Brons-niveau. De instellingen die op Goud- en Zilver-niveau meededen, oefenden de hele dag met een groot deel van hun organisatie. Op Brons-niveau deden de deelnemers een kleine kant-en-klare operationele oefening en konden ze meekijken met Goud en Zilver via de mediasimulator.

Oefenen tijdens corona
Een groot verschil met de vorige edities van OZON was dat veel mensen deze keer vanuit huis meespeelden vanwege de coronarestricties. In een simulatieoefening is het belangrijk om zo realistisch mogelijk te oefenen en wordt deelnemers gevraagd om de werkdag te beginnen alsof er niets aan de hand is. Hier hoort ook bij dat iedereen vanaf zijn eigen werkplek mee wordt genomen in de toenemende crisis. Doordat deze werkplek voor bijna iedereen thuis was, konden we deze keer (noodgedwongen) goed oefenen hoe een cybercrisis te managen was met veel mensen thuis aan het werk, en een paar mensen op locatie.

Wat lees je wel en niet in dit rapport?
Dit rapport geeft een beeld van de opzet en het verloop van de OZON-oefening en de leerpunten die hieruit naar voren zijn gekomen. Leerpunten van individuele organisaties worden niet in dit rapport benoemd; deelnemende instellingen zijn zelf verantwoordelijk voor het evalueren van hun eigen oefendoelen en het opstellen en uitvoeren van leerpunten uit deze oefening.

De Brons-oefening is organisatorisch geëvalueerd, maar is in opzet zo klein dat daar geen leerpunten over inhoudelijk crisismanagement uit zijn gekomen. Dit rapport gaat daarom alleen over de Goud- en Zilver-niveaus van de OZON-oefening.

2 Doelen, opzet en verloop oefening

Doelen

De overkoepelende doelen van OZON 2021 waren:

- de weerbaarheid van (hoger)onderwijs-, onderzoeks- en zorginstellingen en SURF zelf te vergroten
- te testen hoe de instellingen samenwerken tijdens een landelijke cybercrisis

Daarnaast stelden alle deelnemende instellingen ook specifieke oefendoelen voor de eigen organisatie. Voorbeelden daarvan zijn:

- een nulmeting doen van de samenwerking tussen verschillende niveaus tijdens een cybercrisis
- testen of de verbeterpunten van eerdere oefeningen goed zijn geïmplementeerd
- interne communicatie testen

Uitgangspunten scenario

Voor het OZON-scenario hebben we input gebruikt van mensen uit verschillende sectoren (deze keer wo, hbo en onderzoek+) en vanuit verschillende invalshoeken (operationeel, tactisch en strategisch). We hebben daarnaast de feedback en de inzichten van de vorige oefeningen meegenomen.

Het scenario moest voldoen aan de volgende eisen:

- Het is toepasbaar en realistisch voor alle instellingen die meespelen.
- Het is zo uitdagend dat een volledige escalatie van het crisisproces binnen de instelling realistisch is. Het moet dus zowel operationele, tactische als strategische vraagstukken bevatten.
- Het start op strategisch niveau om de escalatie vanuit die hoek te testen. De vorige twee oefeningen startten namelijk vanuit de operationele laag.
- Het daagt instellingen uit om zoveel mogelijk samen te werken over de grenzen van de instellingen heen en de ketenpartners realistisch te betrekken.
- Het moet raken aan actuele thema's en dreigingen.

Met deze uitgangspunten in het achterhoofd hebben we gekozen voor een aanval van een (fictieve) statelijke actor. Deze maakt gebruik van ingebouwde achterdeuren in cloudsoftware en netwerkhardware van twee grote leveranciers die gevestigd zijn in dat fictieve land. In het scenario maken onderwijs en onderzoek veelvuldig gebruik van deze diensten (zie Verloop van de oefening voor meer details).

Deze casus snijdt belangrijke thema's aan zoals afhankelijkheid van (cloud)leveranciers, kennisveiligheid en de afweging tussen het zelf oplossen van de crisis en het samenwerken met andere partijen, zoals instellingen, SURF en koepels.

Opzet

Net als de vorige editie van OZON moest elke deelnemende instelling (op Goud- en Zilver-niveau) een oefenvoorbereider en een waarnemer aanleveren. De oefenvoorbereider werkte de doelen voor de eigen instelling uit en stelde samen met de waarnemer(s) een evaluatieplan op. Waarnemers observeerden tijdens de oefening of de verwachte acties werden genomen en of de procedures werden gevolgd. Op centraal niveau regelde SURF een gezamenlijk scenario, technische oefenonderdelen, een mediasimulator en begeleiding. Elke oefenvoorbereider werkte aan de hand daarvan de impact en verloop van het scenario voor de eigen instelling uit.

Twee elementen die deze keer anders waren ten opzichte van de vorige editie van OZON:

- *Meer nadruk op worldbuilding*
  Er waren knipselkranten en vier websites ontwikkeld om de fictieve delen van het scenario tot leven te brengen. Dit materiaal zorgde ervoor dat deelnemers meer werden meegenomen in de wereld van de

oefening.

- *De uitdagingen vanwege coronarestricties*
  Alle voorbereidende bijeenkomsten, en de oefening zelf, vonden online plaats vanwege corona. Het was dus uitdagend om de voorbereidingen van de deelnemers goed te volgen, en om goed contact met hen te houden. Daarom hebben we, naast de online centrale voorbereidende bijeenkomsten, ook extra online spreekuren ingesteld en buddygroepen gemaakt. Het voordeel hiervan was dat de deelnemers niet steeds naar SURF hoefden te reizen.
  Bij de eerdere edities van OZON zaten de organisatie en de oefenvoorbereiders van de deelnemende instellingen samen in de *war room* op het SURF-kantoor. Vanwege corona was ook dat niet mogelijk. Via diverse back channels kon de organisatie die dag contact houden met de oefenvoorbereiders. Ook de oefenvoorbereiders onderhielden op deze manier contact met hun waarnemers binnen de eigen instelling. Over het algemeen lukte het goed om de oefening op deze manier te leiden en te observeren. Op deze manier hebben we goede ervaring opgedaan in hybride samenwerking tijdens een crisis, wat in het huidige veranderende werklandschap zeker vaker voor zal komen.

Verloop van de oefening

Niveaus Goud en Zilver: aanval van Guilder, een statelijke actor
Guilder is een klein land aan de rand van Europa. Het wordt met strakke hand geleid door een dictatoriaal regime, maar vist wel naar een EU-lidmaatschap. Het land herbergt twee grote IT-spelers: een grote clouddienstverlener en een van ’s werelds grootste netwerkhardware-producenten. Nederlandse onderwijs- en onderzoeksinstellingen gebruiken en masse deze diensten en producten uit Guilder.

Al een aantal jaar zijn de verhoudingen tussen Nederland en Guilder gespannen, om politieke redenen.

9.00 uur – Alle colleges van bestuur ontvangen een memo van het ministerie van Binnenlandse Zaken over de toenemende dreiging vanuit Guilder. Advies is om Guilder hardware te ontkoppelen en het exit-scenario te starten voor de software uit dat land.

9.30 uur - De eerste tweets en nieuwsberichten verschijnen in de mediasimulator. Studenten en medewerkers van verschillende instellingen twitteren dat de mail het niet doet, of dat ze niet kunnen inloggen op de elektronische leeromgeving. Wat is er aan de hand?

10.00 uur – De Universiteit van Harderwijk is gehackt. Op de mailinglijst van SCIRT, de community van securityspecialisten bij onderwijsinstellingen, vragen mensen hulp aan elkaar en aan SURF: hebben anderen dezelfde issues? Weet SURF al meer over de oorzaak van de problemen?

11.00 uur – Journalisten, in werkelijkheid medewerkers van SURF, bellen naar woordvoerders bij instellingen om opheldering te vragen over de situatie. Hebben jullie ook software uit Guilder? Hoe groot is de impact? Kunnen studenten wel tentamen doen?

14.00 uur - Er heerst nog steeds grote onrust onder studenten en medewerkers van onderwijs- en onderzoeksinstellingen. Die kunnen niet meer inloggen in online werkomgevingen.

15.00 uur - De vertrouwelijke memo van het ministerie van Buitenlandse Zaken aan de bestuurders is gelekt naar de pers, er worden kamervragen aan de minister van OCW gesteld: waarom maken instellingen nog steeds gebruik van producten uit Guilder, terwijl die afhankelijkheid al jaren als zorgwekkend wordt gezien? De deelnemers op strategisch niveau worden dus ook flink aan het werk gezet.

15.30 - De deelnemers krijgen gedurende de dag de crisis technisch gezien wat meer controle. Een aantal deelnemers heeft de malware ontdekt en is die aan het onderzoeken. Ook hun routers zijn ze aan het onderzoeken, die komen immers ook uit Guilder. En ze zijn aan het werk met de Indicators of Compromise (IoC’s) die gedeeld zijn door SURFcert, het computer emergency response team (CERT) van SURF.

17.00 uur - De oefening wordt afgesloten.

Niveau Brons: verdachte USB-stick gevonden
De instellingen die op Brons-niveau meespelen krijgen te maken met een verdachte USB-stick die afkomstig

blijkt van een hacker. Op de stick staan allerlei vertrouwelijke studentgegevens, maar ook een logbestand waaruit blijkt dat een collega-instelling is gehackt, namelijk de Universiteit van Harderwijk. Aan de deelnemers de opdracht om uit te zoeken wat ze met die informatie moeten doen. Melden ze een datalek? Informeren ze de Universiteit van Harderwijk? Met andere woorden: doen ze de juiste dingen om erger te voorkomen, voor hun eigen instelling en voor collega-instellingen? Naast deze oefening kijken de Brons-deelnemers mee met de mediasimulator van het Guilder-scenario.

3 Evaluatie

Beoordeling oefening
De oefening werd met een 8 door de spelers zeer goed beoordeeld en 95% van de deelnemers zou nogmaals meedoen aan de oefening en deze aanbevelen aan collega's. De deelnemers gaven vooral aan enthousiast te zijn over de uitgebreide worldbuilding.

Tijdens de centrale evaluatie van de oefening gaven de oefenvoorbereiders van de deelnemende instellingen aan dat ze met de oefening bijna al hun oefendoelen hadden gehaald. Ook zagen de meeste instellingen die eerder hadden meegedaan aan OZON, veel verbeteringen in hun interne crisismanagement ten opzichte van die eerdere oefeningen.

Conclusies
Uit de evaluatie kwamen per instelling verschillende successen en leerpunten in crisismanagement naar voren. Overkoepelend kwamen de volgende punten naar voren.

Samenwerking tussen organisaties liep goed via bestaande kanalen, maar landelijke coördinatie is een aandachtspunt.
De deelnemers deelden in vergelijking met eerdere OZON-oefeningen sneller en meer informatie binnen de vooraf opgezette kanalen, zoals de mailinglijsten van de community's voor operationele en beleidsmatige security (SCIRT en SCIPR). De onderwijskoepels activeerden ook sneller en meer dan in de vorige oefeningen bepaalde gremia om informatie uit te wisselen en een gezamenlijk beeld te krijgen van de crisis. Denk aan gremia als integrale veiligheid, Functionaris Gegevensbeheer-overleggen, Coördinerend SURF Contactpersonen (CSC), bestuurlijk overleg, app-groepen van woordvoerders. Net als bij de vorige oefening, kwamen hier een aantal gezamenlijke persberichten uit voort.

Naast het delen van informatie, probeerden de instellingen samen met de onderwijskoepels binnen de deel-sectoren (wo, hbo en mbo) ook gezamenlijke coördinatie van de crisis op te pakken. Hierbij werd echter duidelijk dat mensen die normaal een verbindende rol hadden vanuit de instellingen, nu – begrijpelijkerwijs – te veel in beslag werden genomen door de crisis bij hun eigen organisatie om ook een grotere coördinerende rol op te pakken. De onderwijskoepels, het ministerie van OC&W en SURF probeerden deze coördinatie op landelijk niveau op te pakken. Daarbij bleek dat de rollen en taken van deze partijen in dit soort crises nog niet helder is.

Zo hadden de onderwijskoepels vrij snel contact met hun achterban om informatie te vergaren, maar misten zij de inhoudelijke kennis om de informatie te duiden. De verwachting vanuit de onderwijskoepels was dat SURF deze inhoudelijke kennis en meer coördinatie op zou pakken. Omdat SURF in het scenario zelf ook werd aangevallen, was het lastig te laveren tussen de eigen crisis en hun landelijke rol. Tegelijk probeerde het ministerie van OC&W veel informatie op te vragen bij de onderwijskoepels om een beeld te krijgen van de crisis. Dit kwam echter op een moment dat de koepels en instellingen zelf nog bezig waren met beeldvorming van de crisis, waardoor deze vraag vooral extra stress opleverde.

Analyse van de crisis was de grootste uitdaging.
Er was een enorme hoeveelheid informatie beschikbaar, en de crisis had op elke instelling een andere impact. Door deze factoren vonden deelnemers het moeilijk om een goed beeld te krijgen van wat er precies aan de hand was, zowel binnen de eigen instelling, als op sectorniveau. De oefening was zo opgezet dat de impact van de aanval niet bij alle instellingen tegelijk duidelijk werd, zoals dit bij echte crises ook het geval is. Daardoor vroegen deelnemers veel informatie op over casussen van eerder getroffen instellingen, die ze in de mediasimulator zagen. Als de beeldvorming en oordeelsvorming daarna niet gedegen werd gedaan, kon dit leiden tot verkeerde beslissingen en gebrekkige interne coördinatie van de crisis.

Officiële crisisprocedures waren vaak niet bekend bij de deelnemers en werden daardoor niet gevolgd.
Ten opzichte van de eerste OZON-editie hebben al veel meer instellingen procedures voor een cybercrisis opgesteld. Deze zijn echter niet altijd bekend bij de relevante medewerkers, waardoor zij tijdens de oefening vaak improviseerden in plaats van de procedures te checken.

Er was gebrek aan mankracht en/of technische kennis bij instellingen die meespeelden.
De technische kant van de oefening werd door veel instellingen niet opgelost. Gedeeltelijk kwam dit doordat spelers niet doorhadden dat zij daadwerkelijk malware konden opsporen en acties konden ondernemen. Dat is een standaard euvel bij simulatieoefeningen, omdat er soms onduidelijkheid is over welke elementen gesimuleerd worden en welke elementen de spelers voor waar aan moet nemen.
Bij verschillende instellingen was echter ook de benodigde mankracht en/of technische kennis niet in huis om deze kant van de oefening goed aan te pakken. Reden hiervoor kan zijn dat oefenvoorbereiders, die over veel technische kennis beschikken, niet meespeelden en er daardoor weinig kennis en kunde binnen de instelling was om de crisis op te lossen.

Aanbevelingen

Naar aanleiding van de conclusies zijn er een aantal stappen die SURF samen met haar leden en ketenpartners kan nemen.

Maak binnen de onderwijs en onderzoek sector afspraken over rolverdeling en kennisdeling tijdens een crisis.
Gezien de uitdagingen tijdens deze oefening om tot landelijke coördinatie van de crisis te komen, is het aan te bevelen om de verschillende verantwoordelijkheden explicieter te maken die SURF, de koepelorganisaties en het ministerie van OC&W hebben bij een crisis. Dit voorkomt bijvoorbeeld dat kennisdeling niet wordt opgepikt op het moment dat het nodig is, of dat er teveel van aangevallen instellingen wordt gevraagd terwijl zij nog bezig zijn met het vormen van een eigen beeld van de crisis.

Vergroot kennis van cybercrises en manieren om tot een goede crisisanalyse te komen.
In elke crisis is het een uitdaging om een goede beeldvorming, oordeelsvorming en besluitvorming te krijgen (de BOB-procedure). In een cybercrisis is dit een extra grote uitdaging, omdat het lange tijd onzichtbaar en ongrijpbaar kan zijn wat er gaande is. Het is hiervoor van groot belang dat het centrale crisismanagementteam en de operationeel medewerkers genoeg kennis hebben om de situatie te duiden. Daarnaast is het belangrijk om de BOB-structuur te blijven oefenen en toepassen. SURF kan, net als na de OZON-oefening in 2018, algemene gezamenlijke sessies en trainingen voor deze onderwerpen organiseren. Specifieke trainingen voor de eigen crisisstructuur zullen de instellingen zelf moeten organiseren.

Organiseer uitwisseling van (best) practices voor cybercrisismanagementmateriaal.
Veel instellingen hebben inmiddels cybercrises meegenomen in hun centrale crisismanagementprocedures. Er is echter nog veel behoefte aan het uitwisselen van materiaal om deze procedures en hulpmiddelen te verbeteren. Er ligt hiervoor een taak bij SURF samen met de community's SCIRT en SCIPR om meer kennisdeling op dit gebied te faciliteren.

Blijf oefenen.
Het blijkt dat de bestaande procedures vaak niet bekend zijn of gevolgd worden, en dat het moeilijk is om een goede crisisanalyse te maken. Dit laat zien dat het belangrijk is om te blijven oefenen. Oefeningen op grote schaal, zoals OZON, helpen om het bewustzijn te vergroten en het hele crisisproces te doorleven. Maar het is ook belangrijk om kleinere oefeningen tussendoor te blijven doen, zoals de tabletop-oefening NOZON en operationele oefeningen als Capture the Flag van SURFcert. SURF en SURFcert zullen deze oefeningen blijven organiseren.

Zorg voor meer securityexpertise op operationeel niveau.
Uit de oefening bleek dat er of te weinig mankracht beschikbaar was voor de oefening en/of dat technische expertise ontbrak. Dit kan komen doordat de oefenvoorbereider van de instelling de meeste expertise bezit. Een precaire situatie, omdat alles dan van één persoon afhangt. Het advies is om de zowel in mankracht op te schalen, als expertise binnen een instelling te spreiden en op voldoende niveau te hebben. Dit is een gezamenlijke uitdaging voor de instellingen en SURF, maar is tegelijk ook een breder nationaal vraagstuk, gezien het algehele tekort aan cybersecurityprofessionals.