Samen aanjagen van vernieuwing

OZON 2018

Evaluatie van een 'digitale brandoefening voor onderwijs en onderzoek'

Auteur(s): Charlie van Genuchten

Versie: 1.0

Datum: maart 2019

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
info@surf.nl
www.surf.nl

Inhoudsopgave

1 Inleiding

Waarom een cybercrisisoefening?

Cybercrisisoefeningen worden georganiseerd om een organisatie de gelegenheid te bieden op een veilige manier (aspecten van) het afhandelen van een cybercrisis te testen. De meeste instellingen hebben intern wel een crisishandboek of -plan liggen dat aangeeft hoe er gehandeld moet worden bij grote verstoringen en wie er allemaal op de hoogte gesteld of betrokken moeten worden. In 'het heetst van de strijd' wordt dit echter nog weleens over het hoofd gezien. Ook kan het gebeuren dat niet tijdig wordt opgemerkt dat een incident feitelijk een crisis is geworden (opschaling). Al dit soort aspecten zijn te testen en te oefenen met een cybercrisisoefening, vergelijkbaar met een brand- of ontruimingsoefening.

OZON 2016: eerste grote cybercrisisoefening

In 2016 werd op initiatief van SURFcert – geïnspireerd door hun deelname aan de landelijke ISIDOOR-oefening door het NCSC - voor het eerst een grote cybercrisisoefening opgezet door SURF. Mede omdat het de eerste keer was, werd er veel aandacht besteed aan het 1-op-1 begeleiden van instellingen. Aan deze OZON-oefening deden 28 instellingen mee, 14 op Brons-niveau en 14 op Goud- of Zilver-niveau. Bij deelname op Brons-niveau bleef de oefening beperkt tot operationeel niveau, op Zilver-niveau werd ook het management betrokken en bij Goud werd er potentieel opgeschaald tot het bestuur van een instelling.

OZON 2018: meer deelnemers

OZON 2018 was de tweede grote cybercrisisoefening georganiseerd door SURF. Gezien het succes van OZON 2016 was de ambitie om een veel groter aantal instellingen mee te kunnen laten doen, tegen vergelijkbare kosten. Dat betekende onder andere dat er van 1-op-1 begeleiding overgestapt werd op centraal georganiseerde voorbereidingsdagen voor instellingen. Aan OZON 2018 deden uiteindelijk 50 organisaties mee op Goud-, Zilver- of Brons-niveau, 10 hiervan op Brons-niveau de rest op Zilver of Goud.

Wat lees je wel en niet in dit rapport?

Dit rapport is bedoeld om een beeld te geven van de opzet en het verloop van de OZON 2018 oefening. Ook worden er gezamenlijke leerpunten en aanbevelingen in benoemd, eerst op inhoudelijk crisismanagement niveau en daarna op organisatorisch vlak.

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. Veelvoorkomende feedback vanuit de instellingen op de (organisatie van de) oefening wordt echter wel opgenomen.

2 Doelen, opzet en verloop oefening

2.1 Doelen

De doelen van OZON 2018 waren:

- de weerbaarheid van (hoger)onderwijs-, onderzoeks- en zorginstellingen en SURF zelf te vergroten
- te testen hoe tussen de instellingen zou worden samenwerkt in het geval van een landelijke cybercrisis

Naast deze overkoepelende doelen, stelden alle deelnemende instellingen ook specifieke oefendoelen voor de eigen organisatie. Voorbeelden van deze doelstellingen zijn:

- een nulmeting om te zien hoe samenwerking tussen verschillende niveaus tijdens een cybercrisis gaat
- interne communicatie testen
- externe communicatie testen
- weerbaarheid van specifieke delen van de instelling testen

2.2 Opzet

In de opzet van OZON 2018 voor Goud- en Zilver-niveau organiseerde SURF de volgende zaken centraal:

- een centraal scenario (zie **bijlage 1**) en per instelling een template om een eigen scenario uit te werken
- 4 voorbereidende dagen om met alle oefenvoorbereiders om de voorbereiding van de oefening door te nemen en onderling te sparren
- een mediasimulator om de 'buitenwereld' (Twitter, Facebook en nieuws) te simuleren.
- technische spelelementen, zoals gesimuleerde malware, om op operationeel niveau echt mee te kunnen oefenen
- een wiki, buddysysteem en mailinglijst om samenwerking en uitwisseling van materiaal te bevorderen
- een centrale responscel tijdens de oefening met extra simulanten die als journalisten, raad van toezicht-leden of boze burgers konden worden ingezet
- betrokkenheid van externe partijen als de VSNU, VH, MBOraad, SaMBO-ICT, Autoriteit Persoonsgegevens en de politie

Alle instellingen moesten daarnaast een eigen oefenvoorbereider leveren, die verantwoordelijk was voor onder andere:

- het uitwerken van het scenario voor de eigen instelling. Zo moest er bijvoorbeeld worden besloten wat er door de vanuit het centrale oefenscenario gesimuleerde ransomware werd geraakt en hoe dat voor tactische en strategische uitdagingen zou zorgen

- het benaderen en voorbereiden van de mensen binnen de instelling die mee zouden doen aan de oefening

- het betrekken van waarnemers, mollen en andere hulp bij de uitvoering van de oefening

- het uitwerken van (nep)twitterberichten, nieuwsberichten en mails om de crisis levensecht te laten lijken

- het leiden en (laten) evalueren van de oefening

Door deze opzet konden er meer instellingen meedoen dan aan OZON 2016 (toen er 12 instellingen op Goud- en Zilver-niveau meededen). Er was hierdoor minder persoonlijke aandacht per instelling vanuit de centrale projectgroep, maar deze aanpak bevorderde wel meer samenwerking tussen de oefenvoorbereiders.

2.3 Verloop van de oefening

Hieronder volgt een korte weergave van hoe de oefening verliep op 4 en 5 oktober 2018. Het scenario dat hieraan ten grondslag lag vind je in **bijlage 1**.

Begin

Op 4 oktober kregen alle deelnemers om 9.30 uur het startsein van de oefening. De eerste Twitterberichten begonnen te lopen, de nep-malware van NLNetNeutrality was stiekem al gestart door de mollen binnen de instellingen en de oefenvoorbereiders in Utrecht maakten zich klaar voor de eerste fase van de oefening.

Fase 1: Defacement websites (rookgordijn)

Rond 9.55 uur werd een nep-phishingmail verstuurd door NLNetNeutrality naar alle spelers en om 10.00 uur begonnen op Twitter en in het nieuws meldingen te komen dat de websites van een hele hoop instellingen een raar statement over netneutraliteit weergaven.

Deze defacement van de websites was bedoeld als rookgordijn om alle spelers wakker te schudden, maar het was niet de insteek dat iedereen hiermee al de crisisorganisatie op zou starten. Doordat iedereen echter vanaf minuut één klaar zat voor de crisisoefening, begonnen sommige organisaties in deze fase al te escaleren naar het centrale crisisteam. Daarnaast werd in sommige gevallen de impact van de defacement overschat, waardoor men soms ‘s middags nog bezig was met deze fase.

Defacement websites

Fase 2: Ransomware en publiek maken eisen

Vanaf 11.00 uur begonnen studenten, medewerkers, patiënten en onderzoekers te klagen over het niet beschikbaar zijn van data. Om 12.00 uur werd duidelijk hoe dit kwam: NLNetNeutrality maakte de lijst met

instellingen openbaar die waren gehackt en gaf weer hoeveel zij moesten betalen om hun data weer terug te krijgen.

Deze fase was voor veel instellingen de piek van de crisis: er ging heel veel informatie door elkaar lopen en de mediasimulator werd zo druk bezocht dat deze af en toe niet te bezoeken was. Mollen die geraakt waren door de ransomware, werden op het matje geroepen. Sommige instellingen begonnen contact met elkaar en met de onderwijskoepels te krijgen om een gezamenlijk statement op te stellen en uit te dragen. Sommige instellingen besloten tijdelijk het netwerk dicht te gooien. Door alle informatie die in de mediasimulator langskwam, ging men in sommige instellingen op zoek naar problemen die niet relevant waren voor hun instelling.

Fase 3: Data openbaar maken

Om de crisis nog wat aan te zetten op strategisch gebied, mailde de hacker achter NLNetNeutrality tussen 13.00 en 14.00 uur een groot aantal instellingen om aan te geven dat hij ook data geëxfiltreerd had en deze zou gaan lekken als er niet werd betaald.

In veel gevallen hadden instellingen echter ondertussen het besluit genomen om niet te betalen, waardoor deze extra bedreiging minder extra twijfel betekende dan van tevoren gedacht. De verschillende sectoren begonnen ondertussen gezamenlijke statements op te stellen en in veel gevallen, hoewel zeker niet alle, begon men een orde in de chaos van informatie te scheppen.

Tweet van NLNetNeutrality

Fase 4: De-escalatie

De deelnemende instellingen kwamen op heel verschillende momenten in de de-escalatiefase terecht. In sommige gevallen begonnen instellingen al met de de-escalatie in de middag van 4 oktober. In andere gevallen werd er door instellingen gede-escaleerd op de ochtend van 5 oktober. Dit verschil had vaak te maken met de beslissing van instellingen om überhaupt één dag mee te spelen, waardoor de oefenvoorbereider een scenario had uitgewerkt dat in één dag uit te spelen was. Logischerwijs hadden de oefenvoorbereiders voor de instellingen die anderhalve dag meespeelden een scenario uitgewerkt dat op het eind van de eerste dag net over zijn hoogtepunt was. Een andere factor die meewoog was dat ransomware een casus is waar ondertussen veel instellingen een vast proces voor hebben, dat in veel gevallen snel en effectief werd gevolgd.

3 Inhoudelijke evaluatie

Elke instelling die meedeed aan de oefening heeft een eigen evaluatie gehouden om de eigen crisisorganisatie te verbeteren. Om veelvoorkomende leerpunten op te halen, heeft de projectgroep op 5 oktober ook een survey onder de spelers en oefenvoorbereiders uitgezet, die op 9 oktober bij de centrale evaluatie nog verder is besproken.

Doelen gehaald

De overkoepelende doelen van OZON 2018 zijn gehaald. Door de oefening hebben instellingen hun crisisprocedures en organisatie kunnen testen, waardoor zij weerbaarder zijn geworden. Daarnaast werd samenwerking tussen de deelnemende organisaties bevorderd door het scenario en door het deelnemen van de onderwijskoepels. Bestaande community's zoals SCIPR en SCIRT werkten meer samen dan in 2016 en op woordvoerdersniveau werd ook veel contact gezocht.

Naast de overkoepelende doelen zijn de oefendoelen die de instellingen voor zichzelf hadden gesteld ook grotendeels gehaald, bleek uit de survey en evaluatie.

Goede beoordeling

Uit de survey en evaluatie kwam naar voren dat het overgrote deel van de spelers zeer tevreden was over de oefening. Deze werd dan ook beoordeeld met gemiddeld een 8,2. De oefening werd uitdagend, realistisch en gewoonweg als heel leuk ervaren. Bijna alle mensen die de survey in hebben gevuld zouden hun collega's aanraden om een volgende keer mee te doen aan de OZON oefening.

Centrale locatie tijdens OZON 2018

3.1 Conclusies

Uit de evaluatie kwamen verschillende en vaak ook tegenstrijdige dingen naar voren over wat de successen en leerpunten in crisismanagement waren geweest. Er waren echter een paar punten die vaak terugkwamen in de antwoorden op de survey, waar we de volgende conclusies uit kunnen trekken:

- Er was veel moeizame communicatie door het verschil in taalgebruik tussen de technische teams en de rest van de organisatie.

- Communicatie terug naar operationeel vanaf strategisch/tactisch niveau liep vaak niet goed.

- Scenariokaarten voor cybercrisis ontbreken bij veel instellingen of moeten verder worden uitgewerkt bij de instellingen die ze al hebben.

- Er was soms een gebrek aan de vereiste technische kennis om het probleem goed te analyseren. In veel andere gevallen was er één persoon binnen de instelling die deze kennis had, maar als die persoon niet aanwezig was, liep het crisisproces vertraging op.

- De rolverdeling binnen de crisisprocedure was vaak niet duidelijk. Er waren ook vaak problemen met dubbelrollen die mensen binnen de organisatie hebben.

- Samenwerking tussen instellingen kwam in 2018 beter op gang dan in 2016, mede door de betrokkenheid van de onderwijskoepels. Ondanks de betere samenwerking bleef de vraag bestaan of er op strategisch niveau niet een coördinerende partij nodig was geweest.

3.2 Aanbevelingen

Naar aanleiding van de conclusies zijn er een aantal stappen die de deelnemende instellingen in samenwerking met SURF kunnen nemen.

Aanbevelingen

- *Verbeter de kennisoverdracht van technische teams naar het tactische en strategische niveau.*

Communicatie tussen operationeel en de rest van de organisatie tijdens een crisis liep in sommige gevallen moeilijk door verschil in taalgebruik. Dit terwijl het juist in een crisissituatie belangrijk is dat de laag die de beslissingen neemt (crisisteam of management) een goed beeld heeft van de situatie en de afwegingen. Ook voor interne en externe communicatie is het belangrijk dat de mensen die hiervoor verantwoordelijk zijn, goed begrijpen wat er speelt en waarom zodat zij bijvoorbeeld de gebruikers goed kunnen inlichten. Deze kennisoverdracht kan worden verbeterd door mensen op operationeel niveau te trainen in kennisoverdracht naar tactisch en strategisch niveau.

- *Zorg voor basis-cybersecuritykennis op tactisch en strategisch niveau om de communicatie en begrip van tactisch en strategisch niveau richting operationeel niveau te verbeteren.*

Communicatie hoort uiteraard tweerichtingsverkeer te zijn. Tijdens de oefening bleek ook dat de communicatie ‘terug’ lastig liep of simpelweg werd vergeten. Juist voor tactisch en operationele teams is het belangrijk om erug te horen wat er met de door hen aangeleverd informatie wordt gedaan en uiteraard ook welke beslissingen op basis hiervan zijn genomen. Ook de afwegingen en redenen voor specifieke beslissingen zijn belangrijk om terug te koppelen, zodat op alle niveaus binnen een organisatie duidelijk is waarom deze zijn genomen en (dus) ook waarom bepaalde acties moeten worden uitgevoerd. Om dit begrip mogelijk te maken is een basiskennis van cybersecurity nodig op tactisch en strategisch niveau.

- *Verzamel best practices voor crisismanagement in het geval van cybercrises.*

Tijdens de oefening kwam ook naar voren dat scenariokaarten voor cybercrisis ontbreken bij veel instellingen of nog verder moeten worden uitgewerkt bij de instellingen die ze al wel hebben. Hoewel de specifieke uitwerking van een scenariokaart uiteraard afhangt van de interne organisatie van een instelling, is het principe van een scenariokaart algemeen genoeg om ervaringen bij het uitwerken hiervan te delen en gezamenlijk op te pakken.

- *Zorg voor genoeg technische kennis en vaardigheden op operationeel niveau om een cybercrisis het hoofd te kunnen bieden en vermijd een single point of failure, door deze kennis bij meerdere mensen te beleggen.*

Bij veel instellingen zat de meest ervaren persoon op securityvlak in de organisatie van de oefening, waardoor diegene niet meespeelde. Het analyseren en oplossen van de technische elementen van de oefening gingen daardoor vaak langzamer dan het in de realiteit tijdens een crisis zou gaan. Om te zorgen dat het goed afhandelen van een crisis niet afhankelijk is van één persoon, is het van belang om meerdere mensen met genoeg technische kennis en vaardigheden te hebben. Dit kan bijvoorbeeld bereikt worden met de trainingen die nu al worden geregeld binnen SCIRT.

- *Maak afspraken over rolverdeling en kennisdeling binnen de sector tijdens een crisis.*

Bij incidenten en crises die meerdere instellingen raken, speelt SURFcert al een duidelijke rol in coördinatie en kennisdeling. Op strategisch niveau ontbreekt die centrale rol echter, of is niet helemaal duidelijk wie die zou moeten oppakken. Uit de oefening bleek al wel dat instellingen elkaar op dat niveau sneller weten te vinden dan bij de eerste OZON-oefening in 2016, mede doordat de koepelorganisaties deelnamen (VSNU, VH en MBO-raad). Het lijkt echter verstandig de verschillende verantwoordelijkheden die SURF, de koepelorganisaties en mogelijk anderen hebben bij een crisis, explicieter te maken. Zo kan worden voorkomen dat bijvoorbeeld kennisdeling niet wordt opgepikt op het moment dat het nodig is, of dat dit juist dubbel wordt gedaan.

De ‘hacker’ is opgepakt

4 Uitgangspunten organisatie

Met de eerste OZON-oefening in het achterhoofd werden de volgende uitgangspunten opgesteld voor OZON 2018:

- Alle instellingen die mee willen doen, moeten mee kunnen doen.
- De oefenvoorbereiders op Goud- en Zilver-niveau moeten eerder aan de slag kunnen met het organiseren van de oefening dan in 2016.
- De Brons oefening moet zo makkelijk mogelijk te organiseren zijn voor de Brons deelnemers en zo weinig mogelijk tijd kosten voor de projectgroep tijdens de oefening.
- De oefening moet niet meer kosten dan in 2016.

Omdat we ditmaal geen limiet voor het aantal inschrijvingen wilden instellen, verwachtten we een groot aantal inschrijvingen. In overleg werd daarom besloten dat:

- Veel meer nadruk op zelfstandigheid van de instellingen zou worden gelegd. Actief bijwonen van de voorbereidende dagen was verplicht, niet bijwonen kon leiden tot uitsluiting van de oefening.
- De stuurgroep bestaat uit één vertegenwoordiger per sector (WO, HBO, MBO en Zorg), in plaats van een vertegenwoordiger van elke deelnemende instelling op Goud-niveau.

Ook kon OZON 2018 ditmaal nog uit innovatiebudget worden bekostigd voor de centrale organisatie, kosten van deelnemende instellingen waren ook de vorige keer al voor eigen rekening.

Door de grote hoeveelheid inschrijvingen betekende dit dat de oefening twee keer zo groot werd als in 2016 met hetzelfde budget. Daar stond tegenover de grotere nadruk op eigen verantwoordelijkheid van de instellingen, ook was er in tegenstelling tot 2016 niemand fulltime bezig met OZON en was er ook geen medewerker van SURFnet om alle deelnemende instellingen (op Goud- en Zilver-niveau) 1-op-1 te begeleiden in het uitwerken van hun scenario's.

4.1 Aanpak organisatie

Voorbereiding

Om te zorgen dat de deelnemende instellingen op een goede manier hun instellingsscenario's uit konden werken, koos de projectgroep voor de volgende aanpak in de voorbereiding met de deelnemende instellingen:

- Het centrale scenario werd met een kleine groep mensen opgesteld en bij de eerste bijeenkomst met alle oefenvoorbereiders doorgesproken. Hierdoor konden de oefenvoorbereiders in maart beginnen met het uitwerken van hun scenario's. In 2016 duurde het tot eind mei voordat de oefenvoorbereiders aan de slag konden met hun eigen scenario's.
- Alle oefenvoorbereiders kwamen in totaal vier keer bijeen in Utrecht om daar met elkaar en met de projectgroep te sparren.
- Om te bevorderen dat oefenvoorbereiders ook met elkaar zouden sparren tussen de centrale bijeenkomsten, werden alle instellingen in buddygroepjes ingedeeld.

- Deze indeling werd ook vastgehouden bij de bijeenkomsten zelf, zodat iedere keer hetzelfde groepje mensen met elkaar kon overleggen.

- De instellingsscenario's werden op de wiki opgebouwd, zodat de projectgroep kon bijhouden of instellingen achter kwamen te lopen met de voorbereidingen, of scenario's bedachten die het centrale scenario in de weg zouden zitten. Daarnaast konden oefenvoorbereiders hierdoor makkelijk naar andermans scenario kijken om inspiratie op te doen.

- Door de projectgroep werden een aantal deadlines gesteld om alle instellingen op tijd hun oefendoelen te laten opstellen, hun instellingscasus uit te laten werken, hun event lists af te laten maken en al zoveel mogelijk social-mediaberichten voor te bereiden.

Tot slot konden alle deelnemende instellingen zelf beslissen of zij één of anderhalve dag wilden oefenen. De meeste instellingen kozen voor één dag.

Brons

Deelnemers op Brons-niveau konden meekijken met de oefening op Goud- en Zilver-niveau en kregen een element om zelf mee te oefenen. Voor elke instelling op Brons-niveau werd ook een oefenvoorbereider aangewezen, die in september een korte briefing kreeg over wat er moest worden georganiseerd voor hun eigen oefening. De oefening was zo laagdrempelig mogelijk gemaakt, zodat de oefenvoorbereider niet meer dan een dagdeel aan de voorbereiding kwijt zou zijn en de centrale oefenleiding er tijdens de oefening weinig omkijken naar zou hebben.

Techniekgroep

Het doel van de techniekgroep was om het scenario realistischer te maken door enkele onderdelen van het centrale scenario echt te bouwen. De techniekgroep is gestart nadat het algemene scenario was uitgewerkt.

De eerste taak van de techniekgroep was bepalen welke infrastructuur nodig was om het centrale scenario te ondersteunen. Deze werd opgedeeld in componenten en voor elk onderdeel werd een trekker aangewezen. Een architectuurplaat maakte de koppelvlakken van de componenten en de methode van onderlinge communicatie inzichtelijk. De werkzaamheden werden individueel uitgevoerd, met eens in de drie weken een overleg waarbij de voortgang werd besproken en de details werden verfijnd. Richting de afronding moest er een afweging gemaakt worden tussen enerzijds het testen van de infrastructuur in productie en anderzijds het vertrouwelijk houden van de componenten. Uiteindelijk is gekozen om alles door te testen, ook de onderdelen die binnen de instellingen moesten worden uitgezet. Veel problemen konden daardoor in de aanloop worden opgelost, al was het wel zo dat sommige van die problemen werden veroorzaakt doordat virusscanners gedurende een langere periode de tijd hadden om de fictieve malware te herkennen en te bestrijden.

Uitvoering oefening

De coördinatie van de oefening vond plaats in Utrecht, waar de projectgroep samen met bijna alle oefenvoorbereiders op het SURFnet kantoor de oefening aanstuurde. Om de oefening zo realistisch mogelijk te laten verlopen, speelden ook de onderwijskoepels VSNU, VH en MBOraad (samen met SaMBO ICT) mee in Utrecht. Daarnaast speelden vier SURFnet-medewerkers mee als simulanten, die konden worden ingezet als journalisten, boze medewerkers of andere gesimuleerde externen. Om de druk op de simulanten niet te groot te maken, werd de oefenvoorbereiders van tevoren gevraagd om zoveel mogelijk onderling injects door gesimuleerde externen onder te verdelen (bij voorkeur in de eigen buddygroepjes).

De projectgroep, techniekgroep en simulanten waren allemaal duidelijk herkenbaar zodat de oefenvoorbereiders snel de juiste persoon te konden vinden als zij even moesten sparren of een vraag hadden. De projectgroep was opgedeeld in twee coördinatoren voor Goud- en Zilver- en één coördinator voor Brons-niveau, één persoon die de mediasimulator beheerde, iemand die alle mails en berichten vanuit de hacker stuurde en een perschef. Elke twee uur werd er een ronde gemaakt door de coördinatoren bij alle oefenvoorbereiders om te polsen hoe de oefening verliep. Hierdoor was de centrale coördinatie goed te behappen.

Alle spelers die meededen aan de oefening konden elkaar bereiken door de spelerslijst van de oefening te raadplegen en door maillijsten zoals ozon-scipr te gebruiken. Doordat er meer dan 1200 spelers meededen, werd de adressenlijst zo afgeschermd mogelijk gedeeld door de oefenvoorbereiders. Dit zorgde ervoor dat in sommige gevallen het moeilijk was voor spelers om erachter te komen wie meespeelden van andere instellingen.

Pers

Deze keer werd de pers van tevoren actief benaderd en konden de geïnteresseerde kranten bij de hele oefening aanwezig zijn. Vooraf is de afweging gemaakt of we de pers bij zo'n kwetsbaar moment voor de deelnemers moesten laten zijn. Juist om het belang van een oefening op grote schaal breed te delen, hebben we ervoor gekozen hen toch toe te laten. Meerdere instellingen waren positief over deze mogelijkheid en hebben journalisten toegelaten.

Tijdens de dag waren er drie journalisten aanwezig die over de oefening verslag deden. Een journalist van Tweakers.net was de gehele dag aanwezig in het coördinatiecentrum in Utrecht, een journalist van de Volkskrant was in Utrecht en in Zwolle bij Hogeschool Windesheim. Trouw tenslotte was op bezoek bij de Technische Universiteit Eindhoven.

deVolkskrant

Voorpagina | Nieuws & Achtergrond | Columns & Opinie | Video | Wetenschap | Mensen | De Gids | Cultuur & Media | Foto | Economie | Sport

REPORTAGE CYBERCRISIS OEFENING

'Digitale brandoefening' moet hogescholen voorbereiden op eventuele cyberaanval

De verijdelde Russische hack bevestigt hoe reëel het gevaar van de cyberaanval is. Maar wat doe je als je organisatie daadwerkelijk wordt getroffen? Dat oefenden vijftig onderwijsinstellingen vorige week donderdag en vrijdag door een levensechte cybercrisis na te bootsen.

Niels Waarlo 10 oktober 2018, 19:37

Artikel website de Volkskrant

Deze drie journalisten hebben elk een groot artikel geschreven en geplaatst in hun medium. Hiernaast heeft het persbureau Hoger Onderwijs (HOP) een bericht geschreven dat door veel universiteitsbladen is opgenomen.

Publicatie	**Kosten advertentie zelfde grootte (euro)**	**Bereik (lezers)**
de Volkskrant volledige pagina, maandag	38.553	680.000 ma/vr
Trouw driekwart pagina, zaterdag	15.000 (schatting)	430.000
Tweakers	8.000	130.000
Subtotaal (excl andere plaatsingen)	61.553	1.240.000

Een overzicht van rapportages over OZON is te vinden in bijlage 2.

4.2 Conclusies

- De doelstelling van een twee keer zo grote oefening voor hetzelfde geld is gehaald.
- Alle instellingen die mee wilden spelen, hebben mee kunnen doen.
- De aanpak in de voorbereiding zorgde voor (in bijna alle gevallen) goed uitgewerkte scenario's met veel uitwisseling van ideeën, vooral tijdens de voorbereidende dagen en op de wiki.
- Het buddysysteem werkte niet voor alle groepen even goed. Zo was de indeling voor sommige instellingen niet ideaal, vooral als een ervaren oefenleider ontbrak in de groep.
- De inzet van simulanten zorgde voor goed tegenspel vanuit journalisten. Doordat oefenleiders bepaalde injects ook voor elkaar uitvoerden, kostte het in de voorbereiding veel tijd om duidelijk te krijgen wie wat zou doen.
- De coördinatie van de oefening verliep goed door een duidelijke taakverdeling binnen de projectgroep en het feit dat bijna alle oefenvoorbereiders en meespelende organisaties aanwezig waren in Utrecht. De meespelende organisaties die niet aanwezig waren in Utrecht (zoals de politie en Autoriteit Persoonsgegevens) kregen te weinig mee van de oefening om goed mee te spelen.
- Onderling contact tussen spelers van verschillende instellingen kwam niet of moeizaam op gang, waarschijnlijk doordat de spelerslijst moeilijk te bereiken was. Het is echter onduidelijk of dit echt invloed heeft gehad op het verloop van de oefening of dat in 'echte crises' mensen dit onderlinge contact ook niet snel opzoeken.
- De voorgekookte social-mediaberichten waren niet goed te timen, wat ervoor zorgde dat berichten vaak niet goed aansloten bij waar de instelling was in de oefening.
- Voor de Brons oefening is dit jaar een goed werkend concept bedacht, wat makkelijk hergebruikt kan worden.

4.3 Aanbevelingen

- Houd voor de voorbereiding en uitvoering in 2020 grotendeels dezelfde aanpak aan.
- Zorg dat in elke buddygroep in ieder geval één ervaren oefenleider aanwezig is.
- Wees nog duidelijker in welke injects centraal worden uitgevoerd door bijvoorbeeld simulanten en welke injects door de instellingen zelf moeten worden geregeld.
- Overleg met iedere externe (mogelijk) betrokken instantie (onderwijskoepels, NCSC, OCW, Politie, etc.) van tevoren wat hun rol is in de oefening en zorg dat in ieder geval één afgevaardigde per organisatie aanwezig is in Utrecht tijdens de oefening, zodat alle spelers goed aangehaakt zijn.
- Zorg vanaf inschrijving voor duidelijkheid over de spelerslijst en waar die voor wordt gebruikt, inclusief een bijbehorende privacyverklaring, zodat het verspreiden van de spelerslijst voorafgaand aan de oefening beter verloopt.
- Geef eerder toegang tot de mediasimulator om inzicht te geven wat daarmee mogelijk is, maar laat de oefenvoorbereiders tweets offline voorbereiden en tijdens de oefening posten. Alle berichten die vooraf al in de mediasimulator moeten worden gezet zijn puur achtergrondruis.
- Gebruik volgende keer dezelfde oefening voor het Brons-niveau. Als een instelling al een keer deze oefening heeft gedaan, wordt Brons-niveau in dat geval de mogelijkheid om waar te nemen bij een Goud of Zilver deelnemer tijdens de oefening.

Bijlage 1: Scenario

Achtergrond profiel Koen D.

Koen heeft een hostingbedrijf. Hij verhuurt zijn infrastructuur aan verschillende partijen. Veel van zijn klanten hebben een dubieus verdienmodel en gebruiken de infrastructuur voor het verzenden van spam of webpagina's voor phishing. Koen krijgt regelmatig verzoeken van CERT's over de hele wereld om spullen offline te halen. Koen kiest ervoor om dit te negeren. Het is niet dat Koen illegaal bezig is, als hij een gerechtelijk bevel krijgt dan doet hij wat hem opgedragen wordt. Alle andere verzoeken voor hulp gaan bij hem echter rechtstreeks de prullenbak in. Zijn klanten weten dit, zijn hier heel tevreden over en vinden het geen probleem dat de prijs van Koen wat hoger ligt. Zijn afnemers tippen de hostingdienst aan anderen en zo groeit zijn klantenkring verder met dubieuze klanten.

In september 2018 komt Koen in het vizier van Mailhaus. Zijn infrastructuur komt op een reeks aan zwarte lijsten te staan waardoor de websites van zijn klanten nauwelijks nog bereikbaar zijn en mail zo goed als niet meer verstuurd kan worden. Zijn klanten zijn hierop voorbereid en schakelen massaal over naar andere dienstverleners. Voor Koen was dit totaal onverwacht, hij deed immers niets illegaals?
Ineens keldert het inkomen van Koen. Dit komt op een slecht moment, hij had bijna lang genoeg een stabiel inkomen om een hypotheek te kunnen opnemen. Een gevoel van groot onrecht groeit.

Hij is zich aan het beraden hoe hij dit zijn vriendin moet gaan vertellen, ze kennen elkaar nog niet lang maar ze hebben al grote plannen. Eerder had hij haar verzekerd dat het goed ging komen. Voordat hij daarvoor de kans krijgt belt ze hem huilend op. Ze zegt dat ze zijn naam in Google heeft opgezocht en daar zijn duistere praktijken had gevonden. Ze verwijt hem hier nooit iets van gezegd te hebben en verbreekt ieder contact. Verbijsterd zoekt Koen zichzelf op en komt uit bij een lijst van Mailhaus waar hij met naam en foto genoemd wordt. Hij voelt zich enorm geslachtofferd. Hoe kan een partij dit zomaar doen? Hij zoekt op het Internet naar Mailhaus en komt erachter dat het onder andere in zijn eigen land draait. Bij SURF, medegefinancierd met zijn belastinggeld dat hij altijd keurig heeft betaald... Koen is woest over wat hem is aangedaan en neemt zich voor degenen die Mailhaus steunen hard terug te pakken. Koen doet dit onder het alias NLNetNeutrality.

Dinsdag 25 september 2018

NLNetNeutrality voert een phishingaanval uit op de SURFnet aangesloten instellingen. De phishing is in de huisstijl van SURFnet heeft een SURFnet-afzender als displaynaam en bevat een link naar een portal waar na het invullen van inloggevens een geïnfecteerde bijlage gedownload kan worden. De bijlage wordt geopend door (minimaal) een beheerder van een website en een gebruiker met schrijftoegang tot bedrijfskritische data (denk aan back-upbeheerder om ook het back-upsysteem te raken). Bij het openen van de bijlage wordt een sessie geopend naar de aanvaller.

Donderdag 4 oktober 2018

NLNetNeutrality voert in het begin van de ochtend opnieuw een phishingaanval uit op de SURFnet aangesloten instellingen. Deze keer naar heel veel mensen (alle spelers). De phishing is in de huisstijl van SURFnet en bevat een link naar een portal waar na het invullen van inloggevens een geïnfecteerde bijlage gedownload kan worden.

Met de op 25 september geoogste logingegevens van de webbeheerder wordt van elke getroffen instelling een publieke website overgenomen en voorzien van (fake)nieuws (mediasimulator): Mailhaus blokkeert onder de vlag van 'een veiliger netwerk' veel legitieme bedrijven.

Terwijl de websites alle aandacht krijgen begint gelijktijdig ‘s ochtends een proces bestanden op de machine van de gecompromitteerde gebruiker te versleutelen.

Gebruikers beginnen zich (langzaam toenemend) te melden bij de servicedesk. Ze hebben problemen om hun documenten te openen. De aandacht verschuift hiernaar en het blijkt dat in hoog tempo bestanden versleuteld worden. De besmetting komt uit minimaal één computer. De interface van de applicatie die aan het versleutelen is laat een waarschuwing zien dat bij het afsluiten van de applicatie de data niet hersteld kan worden. Er staat ook een link op naar een website met instructies over hoe de data terug te krijgen (kopen).

De hacker treedt naar voren en laat op een 'live' dashboard zien welke instellingen zijn getroffen, hoeveel data versleuteld is (dat loopt nog op, maar grootste leed is al geschied), of dat er betaald is.

De getroffen organisaties krijgen de mogelijkheid om te betalen voor het ontsleutelen van de data. De eerste die betaalt kan zijn data voor (de bitcoin-variant van) 1 euro terugkrijgen. De tweede voor 5.000, de derde voor 10.000 en vanaf daar wordt het bedrag steeds verdubbeld.

De media heeft het opgepakt en er wordt op diverse platformen flink gediscussieerd over de ethiek van chantabel zijn vs. 'hoe stom kun je zijn dat je niet direct 1 euro overmaakt'. Ook medewerkers en studenten mengen zich in de discussie.

Bedrijven die betalen worden uitgebreid op social media besproken en gerangschikt.

De cryptoware-applicatie gebruikt veel internetverkeer, ca. 5% van de data die versleuteld wordt. Rond 14.00 uur wordt bij enkele instellingen duidelijk waarom: NLNetNeutrallity neemt contact met hun op en geeft aan in het bezit te zijn van interessante stukken. De instelling krijgt de kans om via een betaling aan hun wallet zich te verzekeren van de confidentialiteit.

Vrijdag 5 oktober 2018

Mogelijk hebben de spelers een manier gevonden om de sleutel uit het geheugen te halen en de data te decrypten. Voor zover dat niet het geval is:

De politie heeft ondertussen een aantal aangiftes gekregen. Hier had de politie voldoende aan om de dader te traceren en over te gaan tot aanhouding. Bij de aanhouding worden de decryptiesleutels en de gestolen data aangetroffen. De aangiftes die ‘opsporingswaardig’ zijn worden gekoppeld aan de sleutels en daarmee krijgen de betreffende instellingen van de politie hun decryptiesleutels om de data terug te halen.

Bijlage 2: Overzicht media-aandacht

Medium	Link naar artikel
ANP	https://www.perssupport.nl/persbericht/1d1e6ad3-0080-42f0-a7fb-f6bad51aeb1c/nederlands-hoger-onderwijs-en-onderzoek-oefent-met-landelijke-hack
Avans	https://punt.avans.nl/2018/10/oefening-boze-hacker-valt-hoger-onderwijs-aan/
Beveilingswereld	http://www.beveiligingswereld.nl/Nieuws/1/6725-nederlands_hoger_onderwijs_en_onderzoek_oefent_met_landelijke_hack
Business & IT	https://businessenit.nl/2018/10/08/nederlands-hoger-onderwijs-en-onderzoek-oefent-met-landelijke-hack/
Computable	https://www.computable.nl/artikel/nieuws/security/6472804/250449/50-instellingen-doorstaan-nepaanval-ransomware.html
de Volkskrant	https://www.volkskrant.nl/nieuws-achtergrond/-digitale-brandoefening-moet-hogescholen-voorbereiden-op-eventuele-cyberaanval~bf658521/
Delta	https://www.delta.tudelft.nl/article/oefening-boze-hacker-valt-hoger-onderwijs-aan
DUB	https://www.dub.uu.nl/nl/nieuws/oefening-boze-hacker-valt-hoger-onderwijs-aan
Erasmus	https://www.erasmusmagazine.nl/2018/10/05/oefening-boze-hacker-valt-hoger-onderwijs-aan/ https://www.eur.nl/nieuws/eur-oefent-met-landelijke-hack
Executive People	https://executive-people.nl/609505/simulatie-bereidt-onderwijs-en-onderzoekssector-voor-op-cybercrisis.html "Vijf instellingen en ruim twaalfhonderd mensen" ??
ICT Magazine	https://www.ictmagazine.nl/50-instellingen-in-oefening-cybercrisis-surf/
Info security magazine	https://www.infosecuritymagazine.nl/2018/10/08/nederlands-hoger-onderwijs-en-onderzoek-oefent-met-landelijke-hack/

(Belgie)	https://www.infosecuritymagazine.be/nederlands-hoger-onderwijs-en-onderzoek-oefent-met-landelijke-hack/
Nationale Onderwijs Gids	https://www.nationaleonderwijsgids.nl/hbo/nieuws/45690-nederlands-hoger-onderwijs-en-onderzoek-oefent-met-landelijke-hack.html
Trouw	Cybercrisis op school nagespeeld https://www.trouw.nl/samenleving/help-een-cyberaanval-gooi-je-alle-systemen-plat-of-wacht-je-tot-er-meer-bekend-is-~ad9c76e8/ (scan van artikel in de krant van zaterdag 6 oktober)
Tweakers	https://tweakers.net/reviews/6605/ozon-2018-een-kijkje-achter-de-schermen-bij-een-grote-cyberincidentoefening.html
U-today	https://www.utoday.nl/news/66022/oefening-boze-hacker-valt-hoger-onderwijs-aan
Univers	https://universonline.nl/2018/10/17/oefenen-met-een-grote-cyberaanval
Universiteit Leiden	https://www.medewerkers.universiteitleiden.nl/mededelingen/2018/09/landelijke-cybercrisisoefening
Universiteit Twente	https://www.utwente.nl/nl/cyber-safety/nieuws/!/2018/9/153148/cybercrisisoefening-ozon