Project Crisisoefening

Gemeente Leeuwarden, Vodafone Ziggo, KPN, Stichting Cybersafety Noord Nederland, NHL, DDFR, Veiligheidsregio Fr., Politie Noord Nederland, OM

Aanleiding:

Dit projectplan is ontstaan doordat diverse partijen de behoefte zien om ook cybercrisisoefeningen te gaan uitvoeren om ook dit soort crises te kunnen managen. Directe aanleiding is een voorstel dat de gemeente Leeuwarden heeft gedaan in het kader van een subsidieaanvraag bij het CCV.

Doel:

Het voorbereiden van een cybercrisisoefening in Q3 2019, oktober waarin een scenario wordt geoefend. Dit gebeurt in 2 stappen. Een kleine table-top oefening om te kijken waar we met de echte oefening rekening mee moeten houden en in Q3 een grotere oefening. Deze oefening moet resulteren in een factsheet met lessons learned en het realiseren van de vooraf vastgestelde leerdoelen. Scope is opschaling vanaf GRIP 1 (lokaal) tot en met GRIP 4.

Randvoorwaarden:

- samenwerking met in ieder geval de gemeente Amsterdam (en G4) ism CCV en ministerie van JenV
- vertrouwelijkheid key tussen de deelnemende partijen
- externe toetsing en begeleiding op het proces en terugkoppeling
- de leerdoelen van elke deelnemende partij moeten aan bod komen in het scenario en oefening

Benodigde middelen:

- Uit de financieringsaanvraag bij het CCV (ook de enige financieringsbron)
- Deels uit interne capaciteit van de deelnemende partijen: inzet door uren door de partners
- Geen financiering uit andere ministeries
- Indien benodigd zal gemeente Leeuwarden aanvullende financiering beschikbaar stellen (bv. COT)
- Waar mogelijk samenwerken met initiatief Amsterdam om inzet capaciteit te delen en daarmee de kosten

Scope:

Is mede afhankelijk van het beschikbare budget maar in ieder geval opschaling tot en met GRIP 4

Opdrachtgeverschap:

Gemeente Leeuwarden: dit project is op initiatief van de gemeente Leeuwarden tot stand gekomen en heeft partners en private partijen uitgenodigd mee te doen. Ook het COT (Instituut voor Veiligheids- en Crisismanagement) is door de gemeente Leeuwarden benaderd en participeert in het project.

Uitgangspunten:

- Inzet NHL studenten in de vorm van stages (mogelijk ook de RUG-campus Leeuwarden)
- Zoveel mogelijk gebruik maken van “interne” capaciteit
- Kennis delen met andere regio’s, ook veiligheidsregio’s waar al kennis/ervaring is opgedaan
- Interne bewustwordingsprogramma’s zitten niet in het project zelf
- Data in oktober staan 7, 9, 10 en 11 oktober en sluiten aan bij al geplande data vanuit de VRF

Organisatie:

- Werkgroep scenario
- Projectgroep incl. projectleider, regievoerder
- Projectleider afkomstig uit Stichting Cybersafety Noord Nederland (linking pin met onderwijs en de partijen betrokken bij deze stichting)
- Externe organisatie om de grote cybercrisisoefening te faciliteren/begeleiden:
  - Hier in gesprek met COT die specifieke kennis/expertise heeft t.a.v. cybercrisisoefeningen
  - Is aanwezig bij de kick off om lessons learned uit hun praktijk toe te lichten
- Deelnemers crisisoefening (incl. waarnemers)
- Onderwijsinstellingen (MBO juridisch, HBO)

Kennis/capaciteit nodig van:

- Traditionele crisisbeheersing en GRIP-structuur
- Crisisoefeningen uitvoeren en voorbereiden
- Communicatie/informatievoorziening
- Technische kennis cyberscenario's: er moet een realistisch scenario komen

Op te leveren resultaten:

- Lessons Learned in de vorm van een factsheet:
  aanbevelingen, adviezen, valkuilen voor andere gemeentes, veiligheidsregio's
- Doelen gerealiseerd van de deelnemende partijen

Samenwerking Amsterdam

- Het CCV zal samen met het ministerie van J en V de totstandkoming van het contact tot stand brengen
- Amsterdam maakt op de stap naar GRIP5

Mogelijke relatie met andere projecten/initiatieven:

- NHL onderzoek burgemeesters in cybercrime
- Andere oefeningen die mogelijk plaatsvinden zoals de VRF-KPN oefening oktober 2019
- Master Cybersafety NHL
- Project in Amsterdam waar ook een cybercrisisoefening wordt voorbereid

Doelen:

Een eerste inventarisatie van mogelijke doelen:

- Oefenen eigen crisisorganisatie/crisisplan
- Stel dat communicatie (Data/spraak) uitvalt, bepalen impact op:
  - Externe communicatie richting stakeholders, burgers, andere partijen in de keten;
  - Communicatie hulpdiensten;
  - Interne communicatie in de organisatie;
  - Opbouwen nieuwe/tijdelijke communicatievoorzieningen.
- Toetsen regie op uitbestedingsdiensten onderzoeken
- Hoe loopt de dreigingsinformatie cyber vanuit NCSC naar bv. VRF
- Welke bestuurlijke dilemma's kunnen optreden als gevolg van cyber
- Hoe liggen de bestuurlijke verantwoordelijkheden als er bovengemeentelijke zelfs landelijke impact is, zeker in geval bron en effect niet in dezelfde gemeente liggen
- Hoe en waar moet cyber in de GRIP-structuur een plek krijgen?
- Afgeleide doelen kunnen liggen op het gebied van kennisdeling

Aanpak

Voorbereiden PvA
Afstemmen deelnemers
Subsidiecriteria helder

Programma binnen de deelnemende organisaties

Gemeente Leeuwarden
Ziggo/Vodafone
DDFR (datadiensten Fryslân)
VeiligheidsRegio Fryslân)
..

- Wat is de impact van deze doelen op de eigen organisatie
- Awareness sessies
- Bewustwordingsprogramma op deze doelen met oefening als kapstok
- Mogelijk processen aanpassen
- Mensen opleiden

In de crisisoefening meten effecten bewustwordingsprogramma

Maken Webinar/kenniselementen vanuit de oefening

Doelen deelnemers

Kleine cybercrisisoefening 1

Cybercrisisoefening 2

Factsheet
Lessons Learned

Plan van Aanpak
Projectorganisatie en begroting
Deelnemende partijen helder
Meten volwassenheid
Capaciteit intern/extern
Voorbereiden 1e kleine oefening

Voorbereiden definitieve oefening
Scenario werkgroep samengesteld
Voorbereiden oefening

vv

Uitvoeren en evalueren

Evalueren
Voorbereiden 2020

Q4 2018 | Q1 2019 | Q2 2019 | Q3 2019 | Q4 2019

Project Cybercrisisoefening

Bijlage: eerste inventarisatie Beschikbare kennis/namen deelnemende partijen in project/scenariowerkgroep:

- Veiligheidsregio Fryslân:
  - Pim Wanders: vakbekwaamheid
  - Johan Haasjes
  - Christiaan Bruggen
  - Martin Kool
- Politie Noord Nederland:
  - Dennis van Gelderen/Ed Oosterveld
- KPN: verloopt in eerste instantie via Piet Voesten, vanaf juni ook Jos Oostdam vanuit KPN
- Gemeente Leeuwarden:
  - Esther Holman
  - Petra Waringa
  - Grethe Faber
  - Claire de Jong
  - Freddy Dijkstra
- Openbaar Ministerie:
  - Frank Smilda
- Ziggo/Vodafone:
  - Piet Voesten (contactpersoon namens de telecomsector voor Veiligheidsregio's)
  - Rene Blankenstein
- Datadiensten Fryslân:
  - Else Maria van de Meulen (directeur)
- Stichting Cybersafety Noord Nederland:
  - Erik Miedema (voorzitter stichting Cybersafety Noord Nederland)
  - Henk van Ee (kwartiermaker/projectleider)
  - Menno Pot (stagiair integrale veiligheid)