CCV centrum voor criminaliteitspreventie en veiligheid

Cyberoefening gemeente Leeuwarden en partners

Speel in op cybercrisis

Response cel gemeente Leeuwarden

Hoe speel je in op een cybercrisis? In Leeuwarden vond een oefening plaats waarin goed gekeken werd naar de rolverdeling en de impact op de gemeente en haar omgeving. Het scenario betrof een hack op systemen van de gemeente waarbij gevoelige informatie was buitgemaakt. In deze factsheet delen we de observaties en belangrijkste aanbevelingen met je. Want een cybercrisis kan overal voorkomen, dus zorg dat je voorbereid bent.

Het Gemeentelijk Beleidsteam (GBT) Leeuwarden, het Regionaal Operationeel Team (ROT) van de Veiligheidsregio Fryslân, het gemeentelijk cyberteam en diverse (vitale) partners van de gemeente Leeuwarden deden mee aan de oefening. Het Instituut voor Veiligheids- en Crisismanagement (COT) was betrokken bij het ontwikkelen, observeren en evalueren van de oefening. Juist de opzet met zowel vitale partners (telecom) alsook met een gemeentelijk team gaf een interessante dynamiek en resulteerde in belangrijke inzichten.

De leerdoelen voor de oefening waren:

A. kennismaken met de bijzonderheden van het crisistype cyber;
B. de samenwerking tussen het ROT en het GBT;
C. de samenwerking met externe partners;
D. de rolverdeling bij een cyberincident dat impact heeft op de gemeente en haar omgeving.

Het betrof een GRIP 3 oefening waarbij door een hack bij de gemeente Leeuwarden gevoelige informatie was buitgemaakt. Hierbij werd ook gedreigd met uitval van vitale systemen voor de inwoners van Leeuwarden. Vanwege storingen (DDoS aanvallen) bij Vodafone Ziggo werd al snel de relatie gelegd met uitval van telefonie en bereikbaarheid van hulpdiensten.

Gemeentelijk Beleidsteam (GBT)

Overkoepelend beeld

- De oefening heeft waardevolle leerpunten opgeleverd. Het kunnen omgaan met onzekerheden en het maken van keuzes vormden de grootste uitdagingen. De uitdagingen die bij dit crisistype horen, kwamen zichtbaar terug tijdens de oefening. Wat is er precies aan de hand? Wie kan de situatie voor ons duiden? Is er nog sprake van vervolgdreiging en welke rol en taak hebben de teams?

- Dankzij het gemeentelijk cyberteam had de gemeente snel zicht op wat er zich in het eigen huis afspeelde. Het was lastig om dit inzicht en de duiding van wat er aan de hand was op het grensvlak tussen gemeente en ROT scherp te krijgen. Hierdoor ontstonden twee werelden: Die van de gemeente Leeuwarden (data-lek) en die van de veiligheidsregio (dreiging uitval telefonie). Een overkoepelend aandachtspunt was de rolverdeling: wie richt zich op wat?

- Door de teams zijn snel goede maatregelen genomen om de impact te bepreken. Het gemeentlijke cyberteam heeft onder andere het account van de hacker geblokkeerd en binnen de veiligheidsregio zijn door de hulpdiensten preventieve maatregelen genomen om de eigen continuïteit veilig te stellen. In een latere fase daarentegen ontbraken kaders en focus omdat de mogelijke impact ongewis was. Scenario denken in relatie tot de dreiging en het handelen op basis van de feitelijke situatie liepen toen door elkaar.

- Het was complex om met behulp van LCMS en in het telefonische contact tussen de voorzitters ROT en GBT een helder en duidelijk beeld van de situatie aan elkaar over te dragen. Dit maakte dat er veel onduidelijkheid was over hoe reëel de dreiging (nog) was en in hoeverre er drastische maatregelen genomen moesten worden, zoals bijvoorbeeld het communiceren aan de bevolking over bereikbaarheid van 112. Het beeld of er nu sprake was van uitval of alleen nog van dreiging verschilde tussen de teams.

OVERZICHT MET BELANGRIJKSTE AANBEVELINGEN

1. Zorg dat de rol en taak van de betrokken teams wordt afgebakend en alle teams in verbinding staan met elkaar op het gebied van kennis en expertise.
2. Zorg dat er duidelijkheid is bij de teams over de status van de informatie: is het een feit of een risico (dreiging) en hoe waarschijnlijk/groot is het risico (dreiging) dan.
3. Zorg dat de eerste duiding in de briefing tussen en in de teams uitgebreid wordt besproken. Noem mogelijke worst case/best case/realistische case. Maak inzichtelijk waar mogelijke sleutelmomenten en – besluiten liggen. Zorg dat het team de scenario's kan uitwerken in de vorm van een advies.
4. Zorg dat een ROT is voorzien van uitgangspunten en of een kader tot waar er geprepareerd moet worden bij een dreiging.
5. Zorg dat het gemeentelijk beleidsteam en het ROT afspraken maken over de scope: wie pakt welk aspect op? Hoe zorgen we samen voor een integraal beeld?
6. Zorg dat het mandaat in het gemeentelijk cyberteam helder is en dit is gecommuniceerd met de burgemeester.
7. Zorg dat de politie wordt betrokken, ook in de vorm van cyberexpertise voor de duiding.
8. Zorg dat het ROT duidelijk thema's accentueert (visualiseert) die belangrijk (kunnen) zijn.
9. Zorg dat de impact van mogelijke maatregelen bij een dreiging wordt besproken in het ROT en GBT.
10. Zorg dat er een werkwijze/modus wordt bedacht voor een goede en effectieve informatieoverdracht tussen de voorzitter van het ROT en de voorzitter van het GBT. Zorg ook dat de leden van de teams hierin kunnen worden meegenomen indien noodzakelijk.
11. Laat het gemeentelijk cyberteam ook scenario's ontwikkelen voor verschillende cybercrises: hiermee kan de ICT afdeling getraind worden in het leren omgaan met onzekerheid.

INTERESSE

Wil je meer weten over de cyberoefening in Leeuwarden? Neem dan contact op met Grethe Faber of Freddy Dijkstra, gemeente Leeuwarden, tel 14058.

Gemeente Leeuwarden

MKB Cyber Campus

VEILIGHEIDSREGIO FRYSLÂN

vodafone ziggo

COT | Instituut voor Veiligheids- en Crisismanagement
an Aon company

POLITIE Fryslân

Deze factsheet is tot stand gekomen dankzij gemeente Leeuwarden