VERSLAG

Webinar Onbewust Onbekwaam: de rol van de OOV'er bij een cybercrisis.
Datum: 3 juli 2024, online
Spreker: Remco Groet (IBD)

Enkele voorbeelden van incidenten
Remco begint zijn presentatie met een aantal voorbeelden van (recente) incidenten:
- Incident (ransomeware) bij VCS, een leverancier van een camera toepassing: informatie over opstellingen van camera's / plaatsingen van camera's waren gelekt. Zij hadden bijv veel camera's staan voor gemeente Amsterdam. Dit is gevoelige informatie. In samenwerking met de politie is er voorkomen dat deze informatie op straat kwam te liggen.
- Een cyber incident bij Addcom: heel veel gevoelige post loopt via dit bedrijf. Zij hebben de criminelen betaald om te voorkomen dat de data openbaar werd gemaakt.
- Gemeente Buren: ransomware aanval, alle gegevens op slot en gestolen. Groot deel van deze gegevens zijn gepubliceerd op het Darkweb. Ook van de afdeling OOV.
- Incidenten bij Werkbedrijven (Senzer): hier was er een risico dat uitkeringen en toeslagen in 6 gemeentes niet uitbetaald konden worden.

Dit soort incidenten hebben veel impact op de bedrijfsvoering en de dienstverlening van de gemeentelijke organisaties. Let op: ook incidenten die alleen indirect jouw gemeente treffen, kunnen enorm veel gevolgen hebben voor jouw (interne) organisatie.

Gemeenten zijn onvoldoende voorbereid
Iedere gemeente moet zich op een dergelijk incident voorbereiden, want cijfers tonen aan dat dit veel voorkomende criminaliteit is! Helaas zijn gemeenten op dit moment beperkt voorbereid op dergelijke (grote en impactvolle) incidenten. Remco constateert o.b.v. observaties bij diverse oefeningen van gemeenten:

1. Interne crisisteams zijn onbewust onbekwaam.
   Gemeenten weten niet goed wat ze moeten doen als ze zowel het bevoegd gezag én zelf slachtoffer zijn. Managementteams zijn niet gewend om in crisissituatie te werken.

2. Het reguliere crisisteam is juist onbewust bekwaam.
   Iedereen kent z'n rol en is heel rolvast met één gedeeld situationeel beeld. Maar wel alleen in de klassieke crisissituatie waarin politie, brandweer etc. ingezet moet worden.

3. Echte plannen ontbreken.
   Alle plannen die gemaakt worden gaan alleen maar over de techniek. Er is een blinde vlek voor alle andere -niet technische- zaken die ook opgelost moeten worden bij een interne (cyber)crisis. Bijvoorbeeld: hoe gaan we mensen ontvangen, als we alle balies moeten sluiten? Hoe gaan we er (evt met de bank) toch voor zorgen dat we uitkeringen kunnen uitkeren?

4. Hybride oefeningen (extern en intern gelijktijdig) maskeren knelpunten.
   Er wordt weinig geoefend met het scenario dat alleen de bedrijfsvoering van de gemeenten helemaal plat ligt. In een hybride oefening komen echte (nieuwe) dilemma's komen te weinig aan bod. Daarnaast hebben veel bestuurders tijdens dergelijke oefeningen sterk de neiging om vooral in te gaan op wat er speelt bij inwoners, waardoor de aandacht vaak weggetrokken wordt bij het thema 'bedrijfscontinuïteit'. Terwijl juist op dit laatste veel geoefend moet worden.

5. Een interne crisis is complexer dan een externe crisis.

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl

Je bent crisismanager en slachtoffer tegelijkertijd… Hoe ga je om met deze dubbelrol? Welke dilemma's komen daarbij kijken?

Wat kan de OOV'er doen?
OOV'ers kunnen een belangrijke rol vervullen om de gemeente hierop voor te bereiden. Dit kan op verschillende manieren. Bovenaan staat: organiseer oefeningen (samen met je CISO)! Een manier om te oefenen is met de Table Top oefening van het IBD. In deze Table Top oefening worden meerdere incidenten, met bijkomende dilemma's, besproken. Neem als OOV'er het initiatief om dit te agenderen bij de bestuurder / burgemeester. Vanwege jouw rol sta je veel dichterbij de burgemeester (dan de CISO) en daardoor zal het ook meer impact hebben als jij het agendeert.

En verder kan jij als OOV'er aan de slag met het volgende:

- Procesbegeleiding bij een interne crisis:
  OOV'ers hebben als geen ander het oog en oor van de bestuurder. Wendt dit dus aan. En loop ook eens bij de CISO binnen om te vragen wat extra aandacht behoeft. Deze aandachtspunten kun je vervolgens aandragen bij de burgemeester.

- Advies over bedrijfscontinuïteit:
  Trek hierin op met je CISO en vraag rond bij verschillende afdelingen: wat doen jullie als we niet meer op de servers kunnen? Hoe zijn jullie daarop voorbereid?
  Doe in ieder geval minimaal 1x per jaar een oefening.

- Privacy / Gevolgen datalekken:
  Vooral voor de kwetsbare groepen kunnen de gevolgen van datalekken van enorme impact zijn. Ga bijv. een keer met het sociaal domein praten, om bepaalde procedures door te spreken (bijv. plannen maken hoe je de mensen met een uitkering alsnog kunt uitbetalen). Maar ook: geboorte aangiftes moeten nog gemeld kunnen worden. Dit soort scenario's kunnen al samen uitgedacht worden, voordat een gemeente getroffen wordt. Voer het gesprek hierover in de koude fase!

- Crisiscommunicatie:
  Als OOV'ers kan je, samen met je collega van de communicatieafdeling, van te voren al lijntjes leggen met de veiligheidsregio, etc.

Table Top oefening
De IBD kan zo'n interne Table Top organiseren bij jouw gemeente!
Wat? Tijdens de oefening zijn er 4 momenten waarin een ransomware aanval wordt ingezet. Hierbij bespreken we ook dilemma's, bijvoorbeeld die van het wel/niet betalen van losgeld.
Voor wie? Voor directiemanagement van de gemeente.
Tijdsinvestering: 3 uur
Wat te organiseren? een ruimte, de uitnodiging, en een lokale lekkernij. Daarnaast heeft de IBD nog een voorgesprek met met de mensen van de ICT, zodat het lijkt op wat er in gemeente speelt, én met de gemeentesecretaris om ook daar draagvlak te bewerkstelligen.

Meer informatie over en aanmelden voor een Table Top oefening, kan hier.

De PowerPoint bij de presentatie is te downloaden op onze website. Inlog is vereist.