

Strategische punten cybercrime

Tijdens de netwerkdagen grote steden op 16 en 17 november 2017 hebben ambtenaren openbare orde en veiligheid uit verschillende steden strategische punten op het gebied van cybercrime benoemd. Het CCV heeft deze punten voor u op een rijtje gezet. Doe er uw voordeel mee en gebruik de punten bij de voorbereidingen van het nieuwe collegeprogramma en het opstellen van een nieuw integraal veiligheidsplan.

Eenheid begrip cybercrime/cybersecurity/gedigitaliseerde criminaliteit

Er bestaat veel onduidelijkheid over de verschillende begrippen die onder de noemer cybercrime gebruikt worden. De politie gebruikt de termen cybercrime en gedigitaliseerde criminaliteit. De VNG en het CCV hebben daar nog een derde term aan toegevoegd: veiligheid met een digitale component.

Cybercrime: criminaliteit met ICT als middel én doelwit. Zo bevatten de meeste telefoons en bankpassen computerchips die gemanipuleerd kunnen worden door cybercriminelen. Maar ook bedrijfssystemen, moderne auto's en chipkaarten zijn vatbaar voor cybercrime. Voor het plegen van cybercrime gebruiken criminelen speciale apparatuur en software.

Gedigitaliseerde criminaliteit: 'ouderwetse' criminaliteit die een nieuwe impuls heeft gekregen door de opkomst van computer-technologie. Denk hierbij onder meer aan internetoplichting (fraude op online handelsplaatsen), online bedreiging of het witwassen van geld via digitale betaalmethoden.

Veiligheid met een digitale component: de verbinding tussen de digitale en fysieke wereld waarin de digitale wereld zich op een dergelijke manier organiseert of manifesteert wat impact kan hebben op de openbare orde en veiligheid in de fysieke wereld.

Actie: De VNG en het CCV hebben aan de hand van Kernbeleid Veiligheid een overzicht gemaakt van alle vormen van cybercrime. Dit overzicht vindt u op vng.nl/onderwerpenindex/veiligheid/cyberveiligheid.

Expertise/concrete casuïstiek delen

Het is van belang om meer expertise te krijgen op het gebied van cybercrime. Aangezien het nog relatief nieuw is, is het onderwerp nog relatief onbekend. Voorbeelden van hoe andere gemeenten cybercrime oppakken zijn gewenst.

Actie: De VNG en het CCV verzamelen voorbeelden van gemeenten die cybercrime aanpakken. Deze voorbeelden worden in de loop van 2018 op de CCV-website gepubliceerd.

Lokaal dreigingsbeeld op cybercrime

Het is noodzakelijk om per gemeente een duidelijk beeld te hebben van de grootste risico's ten aanzien van cybercrime. Zo heeft de ene gemeente een vliegveld en de andere een haven. Door de risico's per gemeente in kaart te brengen, kunnen er gerichte preventieve acties ingezet worden. Gemeenten kunnen dit bijvoorbeeld samen met de veiligheidsregio oppakken.

Samenwerking in de regio, inclusief politie en OM

Vooralsnog loopt de politie voorop in de strijd tegen cybercrime en gedigitaliseerde criminaliteit. We staan echter pas aan het begin en er valt nog veel te leren. Het is daarom noodzakelijk om samen op te trekken. De nieuwe regionale (politie-) beleidsplannen, die op 1 januari 2019 ingaan, bieden een kans om gezamenlijke afspraken te maken. Maak hiervan melding in uw collegeprogramma.

Bevoegdheden burgemeester in cyberspace

Alle steden kennen gevallen waarbij de openbare orde in de fysieke wereld in gevaar kwam. We weten vaak heel goed hoe we hiermee om moeten gaan. Tegenwoordig zijn er ook steeds meer openbare ordeverstoringen die op het snijvlak van de fysieke en digitale wereld plaatsvinden, zoals project-X in Haren en de treitervlogger uit Zaandam.

Dient de burgemeester zich nu ook in cyberspace te gaan bewegen? Ja, een burgemeester kan zich niet alleen meer alleen met offline maatregelen bezighouden. Een burgemeester moet ook kunnen optreden bij online openbare ordeverstoringen die zijn weerslag hebben in de gemeente.

Actie: Wouter Stol, lector Cybersafety aan de NHL Hogeschool en de Politieacademie, doet onderzoek naar dit fenomeen en komt in het voorjaar van 2018 met zijn bevindingen.

Rampenoefening over cybercrime

Bij rampenoefeningen moet rekening gehouden worden met cybercrime. Wat nu als bijvoorbeeld het computersysteem van de sluizen gehackt wordt?

Portefeuilleverdeling: cybercrime bij één bestuurder?

Tijdens de netwerkdagen werd de vraag gesteld of het verstandig is om cybercrime onder te brengen bij één bestuurder. Gelet op het feit dat cybercrime/gedigitaliseerde criminaliteit overal mogelijk is, werd geconcludeerd dat dit geen goed idee is. Elke bestuurder dient er rekening mee te houden dat cybercrime op zijn of haar beleidsterreinen plaats kan vinden. Daarnaast is het ook goed als het hele college verantwoordelijkheid draagt.

Positionering van de Ciso

Informatiebeveiliging is een groot goed, zeker nu er ook Europese regelgeving is die per 25 mei 2018 ingaat. De gemeentesecretaris dient ervoor te zorgen dat de Ciso (Chief information security officer) een goede positie binnen de gemeente krijgt, waarbij hij/zij voldoende daadkracht op dit onderwerp kan laten zien. Samenwerking tussen de afdeling OOV en de Ciso zorgt er daarnaast voor dat de gevaren die de gemeente loopt, uitgewisseld kunnen worden. Een goede voorbereiding op de gevaren kan veel leed schelen.

Cybercrime bovenop alle andere veiligheidsproblematiek

Cybercrime en gedigitaliseerde criminaliteit zijn voor veel gemeenten nieuwe uitdagingen. Ze komen niet in plaats van andere criminaliteitsvormen, maar er helaas juist extra bovenop. Uit het eerder genoemde overzicht van de VNG en het CCV blijkt immers dat bijna elke vorm van criminaliteit een digitale variant kent. Er moet dus op beide fronten geïnvesteerd blijven worden.

Preventieve rol gemeente

Een belangrijke taak van gemeenten is inwoners en ondernemers bewust te maken van de gevaren van digitale criminaliteit. Het moet duidelijk zijn wat de impact van de digitale wereld op de fysieke wereld van inwoners binnen maar ook buiten de gemeente kan zijn. Gemeenten zouden in samenwerking met andere partijen, zoals de politie, een grotere rol in de preventie van digitale criminaliteit moeten gaan spelen.

Bescherming rechtsstaat

Cybercrime kan de rechtstaat behoorlijk ontwrichten. Het is dus niet de vraag of gemeenten in samenwerking met partners iets moeten gaan doen. Het is tijd dat elke gemeente in afstemming met de regio en het Rijk actie onderneemt om de rechtsstaat te beschermen. Wie welke rol moet oppakken, zal in de loop van de tijd duidelijker worden.

MEER INFORMATIE

- vng.nl/onderwerpenindex/veiligheid/cyberveiligheid
- cbs.nl/nl-nl/nieuws/2017/39/drie-kwart-cybercrimedelicten-niet-gemeld
- politieacademie.nl/kennisenonderzoek/Onderzoek/onderzoekers/Paginas/Wouter-Stol.aspx