Datum
28 maart 2023

Onderwerp
VNG inbreng CD Cybercrime 30 maart

Geachte woordvoerders (digitale) veiligheid,

Op donderdag 30 maart debatteert u over cybercrime. Gedigitaliseerde criminaliteit is een veelkoppig monster waar de samenleving haar handen vol aan heeft. Gemeenten zien ook de verschillende vormen van cybercrime en hebben bovendien direct te maken met de handhaving ervan door o.a. de politie. Wij delen graag enkele aandachtspunten met u voorafgaand aan het debat.

Meer capaciteit voor digitale kant van criminaliteit
Diverse lokale initiatieven op gedigitaliseerde criminaliteit komen onvoldoende van de grond door een gebrek aan capaciteit bij politie en OM. Dit heeft invloed op de lokale aanpak van cybercrime en gedigitaliseerde criminaliteit. De aanpak van cybercrime verdient een verbreding en intensivering vanwege een toenemende digitalisering van criminaliteit. Het gaat hierbij om het gehele proces van intake naar opsporing en vervolging. Het ministerie van J&V moet zo snel mogelijk kijken naar meer urgentie, capaciteit of her-prioritering, zodat er ruimte vrijgespeeld wordt voor digitale vraagstukken. Gemeenten zijn vanwege hun kennis van de lokale problematiek en netwerken in staat om op lokaal niveau burgers en bedrijven te faciliteren in het nemen van preventieve maatregelen. De VNG werkt daarom graag mee aan een integrale lokale aanpak.

Breid informatiepositie uit
Het is van belang de kennis- en informatiepositie van gemeenten, politie en OM te vergroten. Door digitalisering kennen klassieke vormen van criminaliteit steeds vaker een digitaal component, waardoor meer vraag is naar kennis en expertise in het digitale domein. Om voldoende zicht te krijgen op slachtoffer- en daderkenmerken, modus operandi en trends en ontwikkelingen dient er snel ingezet te worden op een zogenaamd multi-beeld. Momenteel loopt een project om vanuit de politie te komen tot een uniform landelijk cyberbeeld. Dit geeft gemeenten beter inzicht waar zij lokaal beleid op moeten inzetten. De VNG vindt dat dit beeld verrijkt moet worden met gegevens van andere publieke/private bronnen om een zo compleet mogelijk beeld te krijgen. Dit beeld geeft richting op welke fenomenen moet worden ingezet en kan helpen bij beleidsvorming en prioriteitsstelling.

Ransomware: gemeenten dragen steentje bij
De ontwikkeling van ransomware vormt een bedreiging voor inwoners, bedrijven en overheid. De werking hiervan en de impact is bij u bekend. Cybercriminelen zoeken actief naar beveiligingslekken in software om binnen te komen voor een ransomware-aanval, soms zijn de

slachtoffers willekeurig. Een ransomware-aanval op een gemeente kan directe en gigantische gevolgen hebben voor inwoners, bijvoorbeeld bij de dienstverlening.
Het Digital Trust Center is verantwoordelijk voor het verhogen van de cyberweerbaarheid van ondernemers. Gemeenten zien het belang om ook een steentje bij te dragen door middel van de City Deal Lokale Weerbaarheid Cybercrime, waarbij ook aandacht wordt gevraagd voor ransomware. Het is van belang om niet alleen de basis op orde te hebben, maar ook voorbereidingen te treffen op digitale ontwrichting, incidenten en crisis. Vanuit de VNG bieden we daarom een cyberoefenpakket aan, zodat gemeenten, lokale driehoeken en veiligheidsregio's kunnen oefenen.

Grote vragen rond impact Europese regelgeving

Tot slot wijzen wij (opnieuw) naar de grote gevolgen van de implementatie van Europese wet- en regelgeving en certificering.
Sinds 16 januari 2023 is de NIS2-richtlijn van kracht. Dit betekent dat EU-lidstaten de richtlijn per oktober 2024 in nationale wetgeving omgezet moeten hebben. De BIO wordt wettelijk verankerd. Lokale overheden zullen als belangrijke entiteit onder de NIS2 vallen en worden geacht te voldoen aan de cyberbeveiligingsmaatregelen uit de BIO om te voorkomen dat zij slachtoffer worden van de toenemende ransomwareaanvallen. De NIS2 verplicht essentiële en belangrijke entiteiten om een breed scala aan basis cyberhygiënepraktijken toe te passen, zoals zero-trust-principes, software-updates, configuratie, netwerksegmentatie, identiteits- en toegangsbeheer of gebruikersbewustzijn, hun personeel trainen en het bewustzijn vergroten met betrekking tot cyberdreigingen, phishing of social engineering-technieken.

Momenteel beschikken lokale overheden over onvoldoende middelen, kennis en expertise om aan de BIO te voldoen, en het is onzeker of dit vóór oktober 2024 zal veranderen.

In het kader van de NIS2 en de Cyber Resilience Act, zijn lokale overheden op zoek naar duidelijkheid over de afbakening van verantwoordelijkheden met betrekking tot informatiebeveiliging binnen ketenprocessen, zoals bij medebewind, uitbestedingen en gemeenschappelijke regelingen. Lokale overheden zijn op zoek naar helderheid over welke afspraken en normen zij dienen vast te leggen in samenwerking met leveranciers. Daarnaast is er budget nodig om voldoende kennis en expertise bij gemeenten om uitvoering te geven aan de NIS2 en CRA-wetgeving.

Trusted flaggers

Vanaf januari 2024 zal de Digital Services Act (DSA) de aansprakelijkheid van tussenpersonen moderniseren en extra verplichtingen toevoegen op het gebied van Notice and Takedown (NTD) procedures, transparantie-eisen en rapportageverplichtingen. Hierbij wordt het concept van 'trusted flaggers' geïntroduceerd, die door alle online platformaanbieders erkend moeten worden. Het ministerie van J&V is bezig om een publiek-private samenwerking op lokaal niveau op te zetten met relevante stakeholders om de praktische uitvoerbaarheid en haalbaarheid te waarborgen en te bespreken waar de verantwoordelijkheden van de overheid en de sector liggen. Lokale overheden zijn benieuwd naar welke rol zij in dit verband kunnen vervullen.