CCV centrum voor criminaliteitspreventie en veiligheid

Lokale cyber-wegenkaart 2.0

De vier wegen naar een cyberweerbare gemeente

Gemeenten hebben een belangrijke rol om te voorkomen dat inwoners, bedrijven, voorzieningen én de gemeente zelf, slachtoffer worden van cybercriminaliteit. Om gemeenten te helpen, worden vier wegen onderscheiden waarop een gemeente actie dient te ondernemen, namelijk:
1. Eigen huis op orde
2. Cyberincidenten en -crises
3. Cybercrime en gedigitaliseerde criminaliteit
4. Online aangejaagde ordeverstoringen

In de beschrijvingen van deze vier wegen wordt duidelijk welke rol de gemeente kan nemen, welke gevaren er op de weg zijn en waar de gemeente hulp (de zogenoemde wegenwacht) kan inroepen. Er is geen volgorde in het nemen van de vier wegen. Elke weg kan nu en naast elkaar genomen worden. Voor elke weg is een aparte factsheet beschikbaar. In deze factsheet gaan we in op 'Cyberincidenten en -crises'.

CYBERINCIDENTEN EN -CRISES

Doel van deze weg

Cyberincidenten en cybercrisis die ontstaan bij bedrijven, instellingen en belangrijke voorzieningen binnen de gemeentegrenzen, kunnen een impact hebben op de samenleving. Vaak kan het bedrijf of instelling het incident zelf oplossen, maar soms kan het ook zijn weerslag hebben op de lokale samenleving waardoor de gemeente betrokken raakt. Met name als het om semipublieke voorzieningen (wegen, bruggen, sluizen, scholen, ziekenhuizen, culturele instellingen, verzorgingshuizen, etc.) gaat, zal de bevolking naar de gemeente en specifiek naar de burgemeester kijken. Goed voorbereide gemeenten weten hoe zij zelf of samen met andere gemeenten en/of de Veiligheidsregio kunnen handelen om de cyberincidenten en -crisis beheersbaar te maken en af te wikkelen.

Risico's op de weg

Bedrijven en instellingen die niet tot de gemeentelijke organisatie behoren kunnen (opzettelijk of niet) getroffen worden door een cyberincident of cybercrisis. Indien het incident veroorzaakt wordt door criminelen, kunnen zij het bijvoorbeeld gemunt hebben op het verkrijgen van geld, het verstoren van de interne bedrijfsprocessen, bedrijfsgeheimen en/of klantgegevens. Dit kan uiteindelijke ook gevolgen hebben voor de openbare orde en veiligheid. De gemeente moet dan in actie komen.

In eerste instantie zijn bedrijven en instellingen zelf verantwoordelijk voor hun interne systemen. Toch blijkt in de praktijk dat gemeenten zelf vaak ook betrokken raken omdat dit het functioneren van de samenleving belemmert of zelfs ontwricht. Denk bijvoorbeeld aan het hacken van een ziekenhuis waardoor er geen patiënten meer behandeld of opgenomen kunnen worden. Of het hacken van een universiteit met ransomware, zodat studenten niet meer kunnen (af)studeren.

Gemeenten moeten bij dit soort cyberincidenten en -crisis blijven investeren in de eigen reguliere crisisorganisatie. De gemeentelijke CISO kan hier vanuit het gemeentelijke perspectief een belangrijke verbindende rol in spelen. Vaak zal de gemeente, in het geval dat een incident of crisis uitgroeit, in nauw contact staan met de Veiligheidsregio. Samen kan er gekeken worden hoe de crisis op te pakken door zowel naar de digitale oorzaak als naar de fysieke gevolgen te kijken. Vanaf GRIP3 (Gecoördineerde Regionale Interventie Procedure) zal de burgemeester het Gemeentelijk Beleidsteam (GBT) bijeenroepen om op bestuurlijk niveau sturing te geven aan de bestrijding van de gevolgen van het incident.

Bij veel incidenten bij bedrijven, instellingen of voorzieningen zal het gaan om incidenten die niet direct de vitale infrastructuur van Nederland raken. Onder vitale infrastructuur worden die producten of diensten verstaan die van essentieel belang zijn voor het dagelijkse leven van de meeste mensen in Nederland, zoals toegang tot drinkwater, elektriciteit, internet en het betalingsverkeer. Als het incident wel de vitale infrastructuur betreft, dan valt de digitale oorzaakbestrijding onder de verantwoordelijkheid van het Nationaal Cyber Security Centrum (NCSC).

Wie zit er aan het stuur

- Bedrijven en instellingen zijn in eerste instantie zelf verantwoordelijk voor een goede beveiliging van hun interne bedrijfssystemen.
- De burgemeester is verantwoordelijk voor de coördinatie van lokale incidenten als deze impact hebben op de samenleving en indien deze niet niveau 3 van de GRIP bereiken.

- De voorzitter van de Veiligheidsregio is verantwoordelijk voor een gecoördineerde aanpak van een crisis/incident indien het een GRIP 4 incident of crisis betreft. De burgemeester blijft wel verantwoordelijk voor de openbare orde en veiligheid in zijn eigen gemeente.
- Het Nationaal Cyber Security Centrum (NCSC) is verantwoordelijk voor het direct ondersteunen en adviseren van vitale sectoren. En voor het delen van dreigingsinformatie en het adviseren en ondersteunen van de overige sectorale CERTs (Computer Emergency Response Teams). Dit gebeurt onder de verantwoordelijkheid van de minister van Justitie en Veiligheid. Ook kan het NCTV - via het NCSC en NCC - worden ingeschakeld voor de niet-vitale structuur als het GRIP 5 betreft.
- De CERTs bieden hulp aan diverse sectoren, regio's en grote organisaties. Zo zijn er CERTs voor bijvoorbeeld de waterschappen, de zorg, verzekeraars en de gemeenten. De CERTs zijn onder andere verantwoordelijk voor het adviseren en ondersteunen van organisaties in hun sector bij het voorkomen, isoleren en mitigeren van computer- en informatiebeveiligingsincidenten.

Welke richting te nemen

Welke weg te nemen hangt af of de digitale crisis of het incident al gaande is (de 'warme fase') of dat men zich voorbereidt op een eventuele digitale calamiteit (de 'koude fase'). In de koude fase wordt er vooral gekeken naar de mogelijke varianten van de crises, de crisisbeheersingsstructuur en de crisisprocessen bij cybergevolgbestrijding. Men oefent de scenario's zodat men in de warme fase weet hoe te handelen. Wanneer er daadwerkelijk een incident of crisis aan de hand is, handelt de burgemeester altijd als het incident of crisis zijn weerslag heeft op de samenleving. Dat betekent dat de burgemeester ook kan optreden wanneer het cyberincident bij bedrijven of instellingen voorkomt. De burgemeester kijkt eerst intern - in afstemming met bijvoorbeeld de CISO en de crisisadviseur Openbare Orde en Veiligheid (OOV) - hoe de processen in goede banen geleid kunnen worden. Als de noodzaak daar is, kan de burgemeester ook de lokale driehoek bijeen roepen en een crisisteam formeren. Ook hier kan de CISO een belangrijke verbindende rol spelen naast de crisisadviseur OOV. Zodra de crisis de gemeentegrenzen (GRIP3 en hoger) overschrijdt, komt de voorzitter van de Veiligheidsregio in actie.

Wegenwacht

- Het Nederlands Instituut Publieke Veiligheid (NIPV) en het Veiligheidsberaad zijn de instanties die zich toeleggen op crisis- en rampenbestrijding. https://nipv.nl
- Meer weten over Gecoördineerde Regionale Incidentbestrijdings Procedure (GRIP)? GRIP is de werkwijze waarmee bepaald wordt hoe de coördinatie tussen hulpverleningsdiensten verloopt in het geval van een crisis. https://www.ifv.nl/kennisplein/Documents/20170523-IFV-KP-GRIP.pdf
- Praktische praktijkvoorbeelden vind je in de CCV-database lokale cyberprojecten zoals over de cybercrisisoefening van gemeente Leeuwarden en van de G4 en van de wijze waarop gemeente Utecht een lokaal cyberweerbaarheidsbeeld organiseert. https://hetccv.nl/onderwerpen/cybercrime/database-lokale-cyberprojecten/
- Meer lezen over digitale ontwrichting: Bekijk het Whitepaper Digitale ontwrichting en cyber https://www.ifv.nl/kennisplein/crises-en-crisisbeheersing/publicaties/whitepaper-digitale-ontwrichting-en-cyber of het WRR-rapport Voorbereiding op digitale ontwrichting https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting
- Het Nationaal Crisisplan Digitaal helpt de vertaalslag te maken van de crisisaanpak op nationaal niveau naar operationeel uitgewerkte plannen en draaiboeken voor overheden, vitale aanbieders en niet-vitale sectoren zoals zorg, onderwijs en watermanagement. https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal
- Meer lezen over de CERTs. Bekijk de handreiking voor CERTs "Effectief opereren in de CERT-gemeenschap". https://www.ncsc.nl/actueel/nieuws/2020/mei/28/ncsc-publiceert-handreiking-effectief-opereren-in-de-cert-gemeenschap
- Voor gemeenten zijn reguliere oefenscenario's gericht op gemeentelijk crisisteam met een digitale component ontwikkeld. https://vng.nl/artikelen/interactieve-cyberoefening
- De Agenda Digitale veiligheid van de VNG biedt handvatten bij het voorkomen en oplossen van cyberincidenten. https://vng.nl/rubrieken/onderwerpen/digitale-veiligheid-en-privacy
- Het ministerie van BZK organiseert jaarlijks een overheidsbrede Cyberoefening. https://www.weerbaredigitaleoverheid.nl/

VOORBEELDEN

- Hack bij gemeente Hof van Twente (2021) https://vng.nl/praktijkvoorbeelden/lessen-uit-de-hack-bij-gemeente-hof-van-twente
- Log4j https://nos.nl/nieuwsuur/artikel/2409121-cyberwaakhond-waarschuwt-voor-gevaarlijk-beveiligingslek

Deze Lokale cyberwegenkaart is in opdracht van het ministerie van Justitie en Veiligheid door het Centrum voor Criminaliteitspreventie en Veiligheid speciaal voor gemeenten ontwikkeld. Ondanks raadplegingen bij diverse netwerkpartners, beseffen wij ons dat wij niet geheel volledig kunnen zijn. En je kunt dan ook geen recht ontlenen aan de genoemde informatie of aan de bronnen waar naar verwezen wordt. Heb je vragen naar aanleiding van deze Lokale cyberwegenkaart, neem dan contact op met het CCV, via info@hetccv.nl.