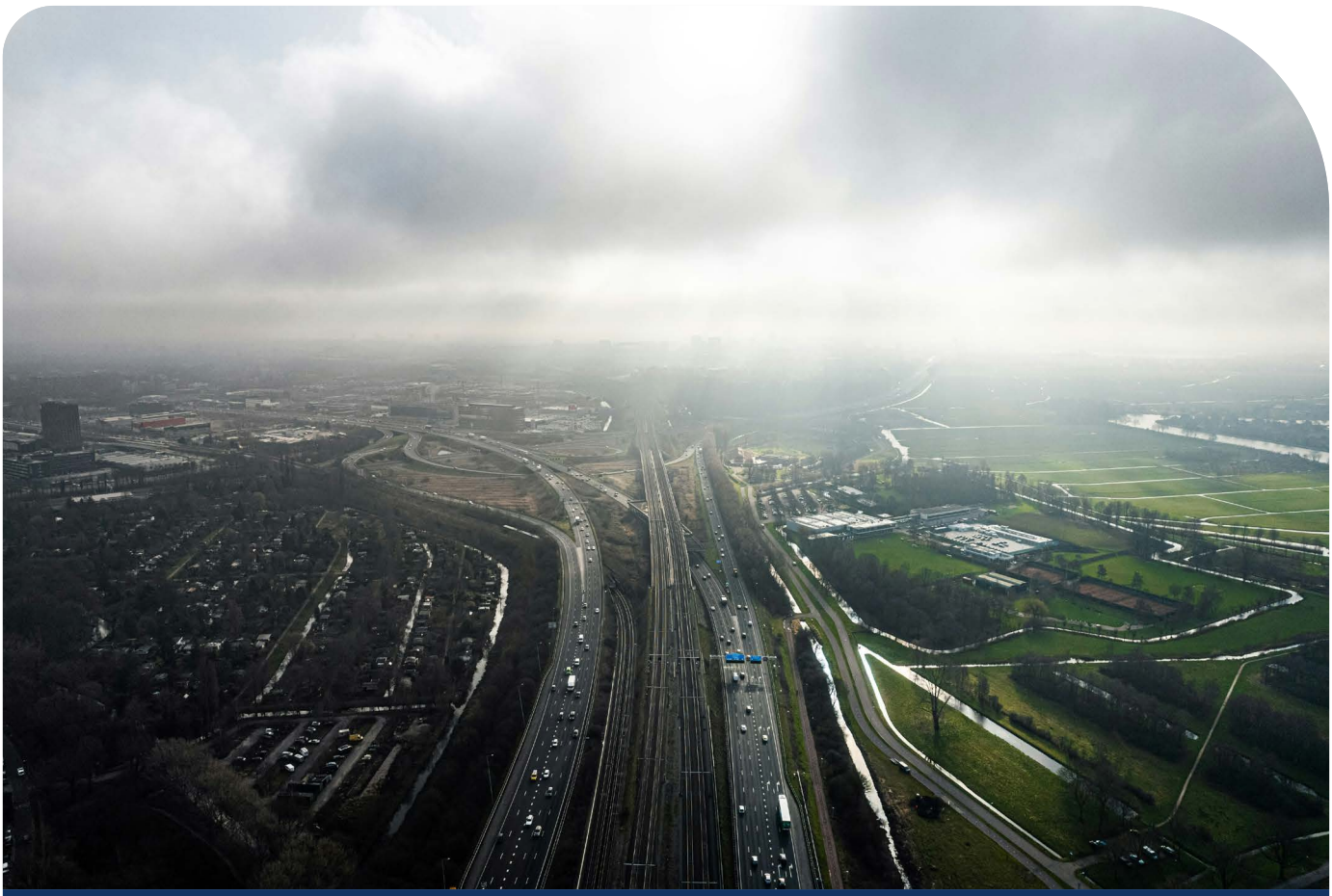

(Voorbereiding op) digitale ontwrichting

Voor adviseurs crisisbeheersing van gemeenten

Handreiking

Auteur
Jelle Kuiper (VNG)

Vragen?
Mocht u vragen hebben naar aanleiding van deze handreiking dan kunt u terecht bij: teamadv@vng.nl

Inhoud

Introductie

In een recent rapport schrijft de WRR bijvoorbeeld dat de internationale verhoudingen "complexer, grimmiger en turbulenter zijn geworden, waarbij we ons ook meer moeten voorbereiden op digitale ontwrichting". De WRR concludeerde eerder al dat we daar nog onvoldoende op voorbereid zijn.[1] Digitale ontwrichting is een vorm van maatschappelijke ontwrichting waar een verstoring van een digitaal (ICT)-systeem aan ten grondslag ligt. In het dreigingsbeeld 2023/2024 stelt de Informatiebeveiligingsdienst (IBD) dat cyberrisico's snel toenemen en de weerbaarheid van gemeenten achterblijft. Bij een fysieke ramp of crisis, zoals een brand of overstroming is duidelijk wie welke rol pakt en op welke wijze de hulpdiensten gecoördineerd op- en afschalen, maar wat te doen bij digitale ontwrichting waarbij het lokale handelingsperspectief nog niet volledig is uitgekristalliseerd? Daarnaast zien we dat ICT en crisisbeheersing in de praktijk veelal twee gescheiden werelden zijn. De hack bij Hof van Twente en bij de gemeente Buren toonde aan dat crisismanagement bij cybercrises nog in de kinderschoenen staat.[2]

Als adviseur crisisbeheersing ben jij betrokken bij (de voorbereiding op) digitale ontwrichting. De gemeente is immers binnen het veiligheidsstelsel primair verantwoordelijk voor de openbare orde en veiligheid, de processen van bevolkingszorg en het herstellen van de maatschappelijke continuïteit. In deze handreiking maken we in onderstaand tabel onderscheid tussen twee categorieën: 1) cyberincident en 2) cybercrisis.

Type	Omschrijving
Cyberincident	Volgens de Wet- beveiliging netwerk- en informatiesystemen (Wbni) is een incident een gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen.
Cybercrisis	Een cybercrisis is een crisis die betrekking heeft op de beveiliging van netwerken en informatiesystemen met aanzienlijke maatschappelijke gevolgen met daaraan gerelateerde cascade- en gevolgeffecten in het fysieke domein / openbare orde en veiligheid.

Cyberincident
Een gemeentelijk cyberincident wordt afgehandeld volgens de procedure beschreven in het incident responsplan. Het gaat hierbij specifiek om een verstoring van een digitaal (ICT) systeem, onbedoeld, moedwillig of door een fout, wat de betrouwbaarheid en/of bereikbaarheid van een gedigitaliseerd proces, (informatie)systeem of informatiedienst, waardoor de dienstverlening niet meer, of nauwelijks, functioneert. De CISO en het gemeentelijk calamiteitenteam zijn dan aan zet en onderhouden nauw contact met de Computer Emergency Response Team (CERT) en Computer Security Incident Response Team (CSIRT) van de Informatiebeveiligingsdienst (IBD). Het gemeentelijk calamiteitenteam heeft als doel om de gevolgen van het incident binnen de organisatie te beperken en de bedrijfscontinuïteit te herstellen wanneer de gemeentelijke organisatie geraakt is. De adviseur crisisbeheersing kan in bepaalde omstandigheden ook betrokken worden bij een gemeentelijk calamiteitenteam. Bijvoorbeeld in een situatie waarin het cyberincident maatschappelijke cascade- en gevolgeffecten heeft en/of er sprake (of een vermoeden) is van opzettelijkheid en/of strafbare feiten, waardoor de lokale driehoek bijeen komt voor extra opsporingsbevoegdheden.

1 Digitale-ontwrichting
2 Lessen uit de hack en datalek gemeente buren

Cybercrisis
Een cybercrisis is een crisis die betrekking heeft op de beveiliging van netwerken en informatiesystemen met aanzienlijke maatschappelijke gevolgen met daaraan gerelateerde cascade- en gevolgeffecten in het fysieke domein. Hierdoor kan opschaling via de GRIP structuur noodzakelijk zijn wanneer digitale ontwrichting (dreigt) door een organisatie of vitale sectoren buiten de gemeentelijke organisatie. Denk bijvoorbeeld aan digitale incidenten met cascade-gevolgeffecten bij (semi)publieke voorzieningen en instellingen, zoals: bruggen, sluizen, scholen, ziekenhuizen, culturele instellingen, verzorgingshuizen, etc.

Als het om vitale infrastructuur gaat (zoals drinkwater, elektriciteit, netwerk en betalingsverkeer etc.) dan valt de digitale oorzaaksbestrijding onder de verantwoordelijkheid van het Nationaal Cyber Security Centrum (NCSC). Meer weten over het landelijke crisisstelsel en de landelijke en regionale aanpak bij digitale incidenten en crisis? Bekijk het Landelijk Crisisplan Digitaal. Bij grootschalige (dreigende) crisis informeert het Nationaal CrisisCentrum (NCC) in de lauwe of warme fase de betrokken veiligheidsregio('s) en lokaal bevoegd gezag over het incident met mogelijke cascade- en gevolgeffecten.

De handreiking *'(voorbereiding op) digitale ontwrichting'* richt zich op digitale ontwrichting met gevolgen voor de openbare orde en veiligheid en/of cascade- gevolgeffecten in het fysieke domein. De handreiking gaat inhoudelijk niet in op intern crisismanagement, wanneer de gemeentelijke informatiesystemen getroffen zijn door een cyberverstoring, zonder maatschappelijke gevolgen buiten de gemeentelijke organisatie. Het onderdeel 'eigen huis op orde' (informatiebeveiliging van de gemeentelijke organisatie) is daarom buiten beschouwing gelaten. Hiervoor kun je informatie vinden op de site van de VNG-Informatiebeveiligingsdienst (IBD).

Voorbereiding, wie en wat is er nodig in de koude en lauwe fase?

Vanwege de steeds verdergaande verbondenheid en digitalisering van de samenleving neemt de kans op digitale ontwrichting toe. Het is daarom van belang dat er in de koude fase voldoende kennis en kunde aanwezig is bij de adviseur crisisbeheersing. Als adviseur crisisbeheersing ben je in de koude fase verantwoordelijk voor het voorbereiden van de multidisciplinaire samenwerking op het gebied van crisisbeheersing zoals beleidsvorming, operationele planvorming en OTO-activiteiten (opleiden, trainen en oefenen).

Gemeentelijke organisatie rondom cybercrisismanagement
Afhankelijk van de ernst van de verstoring, en de impact op de samenleving zijn er verschillende opschalingsniveau's en crisisteam samenstellingen denkbaar. Er is dan ook geen one-size-fits-all aanpak of voorkeur vanuit de VNG. Gemeenten zijn zelf verantwoordelijk voor het inrichten van het incident- en crisismanagementproces. In de koude fase is het van belang om inzicht te krijgen in de verschillende teams op lokaal niveau die geactiveerd kunnen worden bij een cyberincident of -crisis.

Teams	Omschrijving	Aanspreekpunt
Gemeentelijk calamiteitenteam (of soortgelijke benaming)	Effectbestrijding en herstellen van een cyberincident of -crisis in het kader van de gemeentelijke bedrijfscontinuïteit.	Ambtelijk: CISO/ Gemeentesecretaris Bestuurlijk: portefeuillehouder ICT
Lokale driehoek	Bepalen inzet van opsporingsbevoegdheden en bestuurlijke noodbevoegdheden, gezamenlijk met officier van justitie en teamchef van politie.	Ambtelijk: Adviseur OOV/ crisisbeheersing Bestuurlijk: burgemeester
Gemeentelijk Beleidsteam (GBT)	Bestuurlijke advisering over (nood) bevoegdheden, strategische besluiten in het kader van openbare orde en veiligheid, bijstandsaanvragen, afwegen maatschappelijke impact, bestuurlijke afstemming (externe) partijen, scenariodenken en het bepalen van de communicatiestrategie.	Ambtelijk: Adviseur crisisbeheersing Bestuurlijk: burgemeester

Zowel het gemeentelijk calamiteitenteam als de lokale driehoek en het Gemeentelijk Beleidsteam (GBT) kunnen gelijktijdig actief zijn wanneer de gemeente intern getroffen is door een cyberverstoring en dit gevolgen heeft op de openbare orde en veiligheid en/of cascade-gevolgeffecten heeft in het fysieke domein. Indien er sprake is van een cyberincident of -crisis van meer dan plaatselijke betekenis of ernstige vrees van het ontstaan daarvan kan de voorzitter van de veiligheidsregio het besluit nemen om GRIP 4 af te kondigen. Bij (boven)regionale en landelijke crisis wordt automatisch de nationale crisisbeheersingsstructuur geactiveerd door het Nationaal Cyber Security Centrum (NCSC). Voor meer informatie zie het Landelijk Crisisplan Digitaal.

Aandachtspunten voor de koude en lauwe fase

- Borg het thema in het integraal Veiligheidsplan (IVP). Borg het thema '(de voorbereiding op) digitale ontwrichting' structureel in het Integraal Veiligheidsplan. Zie ook: Focusblad Digitale Veiligheid en Digitale veiligheid en de gemeentelijke bestuurder van de VNG.
- Maak duidelijke afspraken over op- en afschalen van het calamiteitenteam naar het Gemeentelijk Beleidsteam. Stem af met de CISO wanneer er opgeschaald moet worden naar het Gemeentelijk Beleidsteam. Leg vast via welke lijnen er opgeschaald moet worden en hoe bestuurder(s) geïnformeerd worden.
- Heeft de gemeente in samenwerking met de veiligheidsregio en andere medeoverheden de risicovolle organisaties en hun (cascade)effecten op het gebied van cyber in beeld? Denk aan Seveso-inrichtingen (voormalige BRZO-bedrijven), datacentra, (zee)havens, logistieke knooppunten binnen de gemeentegrenzen etc. Bespreek dit met ambtelijk en/of bestuurlijk met betrokken partners. Hoe verhoudt de governance zich tegenover deze risicovolle organisaties in relatie tot cyberwaakzaamheid?
- Onderhoud contact met de CISO. Weet elkaar te vinden ook buiten de reguliere kantoortijden door piket of bereikbaarheidsdienst en stem de onderlinge verwachtingen met elkaar af in de koude fase. Neem bijvoorbeeld de CISO mee in de gemeentelijke crisisorganisatie, BOB-structuur en opschalingsstructuur (GRIP) en visa versa. Bespreek met elkaar in hoeverre het gemeentelijk continuïteitsplan aansluit bij de crisisorganisatie.
- Plan periodiek overleggen over digitale veiligheid in met de CISO en betrokken portefeuillehouders.
- Verwachtingen belangrijke stakeholders bepalen. Het cyberdomein vraagt om een flexibele crisisorganisatie met specialistische kennis en expertise die doorgaans niet in de reguliere crisisorganisatie te vinden is. Tijdens een gemeentelijk cyberincident kan de IBD digitaal aanhaken als sparringpartner en gemeenten voorzien van een second opinion bij adviezen en voorstellen van derden. Bij (het vermoeden van) opzettelijkheid of criminele activiteiten is het zaak om de lokale driehoek bijeen te roepen. Het is overigens ook mogelijk om bijvoorbeeld onderling binnen het (regionale) netwerk van gemeenten een beroep te doen op elkaars deskundigheid, capaciteit en ervaring. Voor de rol van de veiligheidsregio zie inzet *'wat kan ik verwachten van de veiligheidsregio?'*.
- Organiseer cyberoefeningen, stel leerdoelen en oefen op structurele basis. Oefen op basis van concrete doelstellingen en/of leerpunten, waar mogelijk in samenwerking met de CISO. Zorg dat dit onderdeel ook structureel geborgd is in het Opleiden, Trainen en Oefenplan op lokaal en/of regionaal niveau. Oefen zowel op ambtelijk als op bestuurlijk niveau, maar ook met externe partijen, zoals: politie, OM en de veiligheidsregio. Dit kan bijvoorbeeld met de VNG cyberoefendriehoek. Wil je als gemeente oefenen met een nationaal cyberscenario? Kijk naar de mogelijkheden om deel te nemen aan de landelijke ISIDOOR oefening of de overheidsbrede cyberoefeningen.

De crisis onder controle krijgen: warme fase

Cybercrises zijn voor gemeenten nog een relatief nieuw crisisdomein. Het aantal cyberaanvallen waarbij sprake is van een crisis met maatschappelijke effecten bij gemeenten is (nog) beperkt. Door ketenafhankelijkheid kan een kleine digitale verstoring grote gevolgen hebben in de fysieke wereld. De cyberaanval op transport- en energiebedrijf Maersk is wat dat betreft een treffend Nederlands voorbeeld. De computersystemen van het Deense bedrijf werden in 2017 platgelegd door gijzelsoftware 'NotPetya' die door hackers was geïnstalleerd. De haven van Rotterdam moest daardoor twee terminals sluiten, waardoor schepen moesten uitwijken. Twee weken lang kon het bedrijf computersystemen niet gebruiken om containers te verschepen. Bij havens over de hele wereld ontstonden verkeersinfarcten. Kilometerslange files van vrachtwagens met containers die Maersk niet kon verwerken vanwege defecte toegangspoorten en camera's.

Een cybercrisis kent niet per definitie een duidelijk afgebakend startpunt. Een cyberaanval kan al enige tijd onder de radar actief zijn in de systemen of pas beginnen wanneer de dreigingsinformatie bekend is. Start indien mogelijk tijdens de lauwe fase (waarin de dreigingsinformatie of cyberaanval bekend is maar nog geen fysieke gevolgen heeft) met de voorbereidingen op de warme fase en het in kaart brengen van de situatie. Besef dat getroffen organisatie(s) buiten de gemeentelijke organisatie vanzelfsprekend primair verantwoordelijk zijn voor de eigen interne processen en cybercrisismanagement.

De burgemeester of voorzitter veiligheidsregio heeft geen extra wettelijke bevoegdheden in cyberspace. Het lokale gezag heeft daarnaast ook geen invloed op het functioneren van de getroffen organisatie of sector zelf (de continuïteit van de verlening van vitale diensten of de aanpak van een cyberincident als zodanig). Echter, wanneer de openbare orde en veiligheid of maatschappelijke continuïteit in het geding is vergt dit ook inspanning van een bestuurder in samenspraak met de adviseur crisisbeheersing.

Aandachtspunten voor de warme fase

- Als adviseur crisisbeheersing adviseer je de burgemeester over openbare orde en openbare veiligheid, de (nood)bevoegdheden van de burgemeester en de uitvoering van de te nemen maatregelen in de eigen gemeente.
- Organiseer overzicht en een gedeeld beeld. Bijvoorbeeld een weergave van getroffen processen en diensten en de volgorde waarin deze weer dienen te worden hersteld.
- Bewaak dat besluiten en de overwegingen tijdens de crisis goed gedocumenteerd zijn.
- Zorg voor de juiste bezetting van het Gemeentelijk beleidsteam (GBT). Overweeg om een liasion van een getroffen organisatie of gemeentelijke leverancier uit te nodigen. Borg ook technische kennis aan de crisistafel, de IBD kan bijvoorbeeld informatie en advies geven of het netwerk inzetten. Kennis van het cyberdomein draagt daarnaast bij aan de vertaling van technische naar bestuurlijke taal. Dit zorgt voor nadere duiding en interpretatie.
- Maak gebruik van de kennis en kunde van de veiligheidsregio. Zie: 'Wat kan ik verwachten van de veiligheidsregio?'
- Escaleer tijdig richting de gemeentesecretaris en bestuurder(s). Een logische keuze is het betrekken van de burgemeester vanwege de OOV-bevoegdheden, maar ook een wethouder met de portefeuille ICT kan (afhankelijk van de situatie) betrokken worden. De burgemeester, of voorzitter veiligheidsregio kan zich bij een (boven)regionale of landelijke crisis ook laten informeren door de voorzitter veiligheidsregio in het Regionaal Beleidsteam (RBT).
- Bepaal de bestuurlijke/strategische dilemma's, sleutelbesluiten en de collectieve impact rondom digitale ontwrichting:
  - Wat communiceer je wel of niet (ook bij dreigende crisis);
  - Hoe om te gaan met het eisen van losgeld (bij ransomware);

  - De classificatie van het type incident of crisis (zie bouwstenen hoofdstuk 4 LCP-D);
  - Welke rol(len) de burgemeester heeft t.a.v. de crisis en richting de samenleving;
  - Prioritering van schaarse middelen voor de bestrijding van digitale ontwrichting;
  - Het (vroegtijdig) in- of uitschakelen van gemeentelijke systemen of dienstverlening;
  - Het inhuren van externe forensische en digitale experts.
- Zorg dat de gemeente transparant communiceert in de warme fase, maar houd rekening met eventuele onzekerheden en wees bewust van het feit dat kwaadwillenden (zoals hackerscollectieven) dit ook tegen de gemeente kunnen gebruiken. Communiceer ook intern naar de directie en medewerkers tijdens de crisis. Dit maakt het makkelijker om in de nafase problemen op te lossen. Voor elke medewerker is het dan duidelijk waar meldingen gemaakt kunnen worden en dit draagt bij aan vertrouwen in de organisatie om problemen op te lossen.
- Maak gebruik van scenariodenken. Een crisis kenmerkt zich door de hectiek van tijdsdruk, onzekerheid en gebrek aan informatie. Maak daarom gebruik van scenariodenken in drie mogelijke uitkomsten: 1) worst case, 2) real case en 3) best case op basis van kans en impact. Hierdoor zijn deelnemers van het GBT beter in staat om vooruit te kijken, prioriteiten te stellen en proactief te handelen.

Wat kan ik verwachten van de veiligheidsregio?
De veiligheidsregio's hebben een uitwerking gemaakt waarin staat dat zij gemeenten kunnen ondersteunen bij digitaal incident of -crisis. Deze ondersteuning is gericht op het proces van crisismanagement en gevolgbestrijding, dus geen technische ondersteuning op ICT-gebied. De regionale crisisorganisatie is als gevolgbestrijder verantwoordelijk voor het bestrijden van de fysieke effecten bij digitale ontwrichting (bijvoorbeeld bij uitval van nutsvoorzieningen, data-en spraakdiensten en regionale zorginstellingen). Gemeenten kunnen gebruik maken van de volgende onderdelen van de regionale crisisorganisatie bij cyberincidenten en -crisis:
- Leiding & coördinatie (crisismanagement):
  De regionale crisisorganisatie kan een *Regionaal Operationeel Leider (ROL)* leveren om zorg te dragen voor het schakelvlak tussen het operationele en bestuurlijke aspect. Een ROL kan coördinerend optreden door de operationele teams aan te sturen en aan te laten sluiten op het bestuurlijk crisisteam. Daarnaast kan er aanspraak worden gemaakt op een technisch voorzitter met een vaste vergaderstructuur het crisisteam kan ondersteunen.
- Informatiemanagement:
  Een *informatiemanager* kan het informatiemanagement van het crisisteam stroomlijnen en zorg dragen voor een gedeeld actueel beeld voor besluitvorming. Dit kan worden uitgebreid met een omgevingsbeeld van ontwikkelingen buiten de gemeentelijke organisatie.
- Crisiscommunicatie:
  Communicatie, zowel intern als extern, kan worden ondersteund door *communicatieadviseurs* uit de piketgroep van de regionale crisisorganisatie. De gemeente kan hiermee ontlast worden als de digitale verstoring langdurig aanhoudt.

De inzet van veiligheidsregio's op het thema cyber verschilt momenteel per regio. Uit onderzoek van het NIPV blijkt dat de veiligheidsregio meerdere mogelijke rollen kan aannemen. Neem contact op met de betreffende veiligheidsregio om de onderlinge verwachtingen scherp te stellen.

Herstel en evaluatie: nafase

De acute crisis zit erop. Na de warme fase volgt de nafase waarin herstel en evaluatie belangrijke facetten zijn. In de nafase draagt de crisisorganisatie de taken over aan de lijnorganisatie. De gemeentesecretaris is vervolgens verantwoordelijk voor de organisatie en coördinatie van de nafase. Bespreek de actiepunten gezamenlijk en zorg voor voldoende ondersteuning bij een langdurige herstelperiode.

Aandachtspunten voor de nafase

- Houd rekening met een lange herstelfase, hoge kosten en grote maatschappelijke impact na digitale ontwrichting. Het kan lastig zijn om te duiden wanneer het weer echt 'veilig' is. Systemen moeten immers weer betrouwbaar en bruikbaar zijn.
- Evalueer de procesmatige aanpak van crisismanagement tijdens de cybercrisis en identificeer leerpunten en implementeer deze in de crisisplannen en/of continuïteitsplan.
- Leg als bestuurder verantwoording af en ondersteun daarbij als adviseur crisisbeheersing, richting de gemeenteraad en/of raadsvragen naar aanleiding van een incident of crisis.
- Houd rekening met specifieke juridische en/of verzekeringsexpertise in de nafase.
- Heb oog voor interne nazorg van betrokken medewerkers.

Relevante documenten

Cyber-introductie voor nieuwe OOV'ers (CCV/VNG)

Cyberwegenkaart 2.0 (CCV/VNG)

VNG Cyber oefenpakket (VNG)

VNG Cyberoefendriehoek (VNG)

Landelijk Crisisplan Digitaal (NCTV)

Gehackt, hoe nu verder? (IBD)

Kennis en kunde voor regionale cybergevolgbestrijding (NIPV)

Bestuurlijke bevoegdheden cyber (NIPV)

Bijlage: One pager

Tip! print de handreiking '(voorbereiding op) digitale ontwrichting' uit en bewaar het als adviseur crisisbeheersing in je crisismap voor noodgevallen. Wanneer digitale systemen uitvallen kan je altijd terugvallen op fysieke documentatie.

Aandachtspunten voor de koude en lauwe fase

- Borg het thema 'voorbereiding op digitale ontwrichting' als onderdeel van het thema digitale veiligheid in het Integraal Veiligheidsplan (IVP).
- Maak duidelijke afspraken over op- en afschalen van het calamiteitenteam naar het Gemeentelijk Beleidsteam.
- Heeft de gemeente in samenwerking met de veiligheidsregio en andere medeoverheden de risicovolle organisaties en hun (cascade) effecten op het gebied van cyber in beeld? Bespreek dit met ambtelijk en/of bestuurlijk met bijvoorbeeld de veiligheidsregio, provincie en andere betrokken partners.
- Onderhoud goed contact met de CISO. Weet elkaar te vinden ook buiten de reguliere kantoortijden door piket of bereikbaarheidsdienst en stem de onderlinge verwachtingen met elkaar af in de koude fase.
- Plan periodiek reguliere overleggen in met de CISO en betrokken portefeuillehouders.
- Onderlinge verwachtingen scherpstellen van belangrijke stakeholders zoals de veiligheidsregio, politie, OM en IBD.
- Organiseer cyberoefeningen, stel leerdoelen en oefen op structurele basis.

Aandachtspunten voor de warme fase

- Als adviseur crisisbeheersing adviseer je de burgemeester over openbare orde en openbare veiligheid, de (nood)bevoegdheden van de burgemeester en de uitvoering van de te nemen maatregelen in de eigen gemeente.
- Organiseer overzicht en een gedeeld beeld. Bijvoorbeeld een weergave van getroffen processen en diensten en de volgorde waarin deze weer dienen te worden hersteld.
- Bewaak dat besluiten en de overwegingen tijdens de crisis goed gedocumenteerd zijn.
- Zorg voor de juiste bezetting van het Gemeentelijk beleidsteam (GBT). Overweeg een liasion van een getroffen organisatie of gemeentelijke leverancier uit te nodigen. Borg technische kennis aan de crisistafel.
- Maak gebruik van de kennis en kunde van de veiligheidsregio.
- Escaleer tijdig richting de gemeentesecretaris en bestuurder(s), niet alleen de burgemeester maar ook een wethouder met de portefeuille ICT kan - afhankelijk van de situatie - uitkomst bieden.
- Bepaal de bestuurlijke/strategische dillema's, sleutelbesluiten en de collectieve impact rondom digitale ontwrichting, zoals:
  - Wat communiceert je wel of niet (ook bij dreigende crisis);
  - Hoe om te gaan met het eisen van losgeld (bij ransomware);
  - De classificatie van het type incident of crisis (zie bouwstenen hoofdstuk 4 LCP-D);
  - Welke rol(len) de burgemeester heeft t.a.v. de crisis en richting de samenleving;
  - Prioritering van schaarse middelen voor de bestrijding van digitale ontwrichting;
  - Het (vroegtijdig) in- of uitschakelen van gemeentelijke systemen of dienstverlening;
  - Het inhuren van externe forensische en digitale experts.
- Zorg dat de gemeente transparant communiceert in de warme fase, maar houd rekening met eventuele onzekerheden en wees bewust van het feit dat kwaadwillende dit ook tegen de gemeente kunnen gebruiken.
- Maak gebruik van scenariodenken en werk dit verder uit: worst case, real case en best case.

Aandachtspunten voor de nafase

- Houd rekening met een lange herstelfase, hoge kosten en grote maatschappelijke impact na digitale ontwrichting. Het kan lastig zijn om te duiden wanneer het weer echt 'veilig' is.
- Evalueer de procesmatige aanpak van het crisismanagement tijdens de cybercrisis en identificeer leerpunten en implementeer deze in de crisisplannen en/of continuïteitsplan.
- Leg als bestuurder verantwoording af en ondersteun daarbij als adviseur crisisbeheersing.
- Houd rekening met specifieke juridische en/of verzekeringsexpertise in de nafase.
- Heb oog voor interne nazorg van betrokken medewerkers.

Vereniging van
Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag
+31 70 373 83 93

info@vng.nl

augustus 2024