Gemeente Amstelveen

Draaiboek
Cybergevolgbestrijding
Gemeente Aalsmeer-Amstelveen

Zaaknummer: Z22-051497/D22-210895
Vastgesteld door directie: 07-07-2022

Inhoud

Beheer document

Beheerder: CISO, Nasim Ahmadi & OOV-adviseur, Niels Westerveld

Elke twee jaar wordt dit document herijkt, of eerder indien noodzakelijk.

Het bijbehorende meterkastdocument wordt elke drie maanden herijkt, of eerder indien noodzakelijk. Dit wordt na herijking niet opnieuw vastgesteld, maar de laatste versie wordt wel gepubliceerd op een vooraf vastgestelde locatie (zie hiervoor bijlage X)

DEEL 1: De organisatiestructuur van cybergevolgbestrijding

I. Algemeen

Inleiding

Onze afhankelijkheid van gedigitaliseerde processen en systemen is zo groot geworden dat verstoring, uitval of misbruik kan leiden tot maatschappij-ontwrichtende effecten. Deze maatschappij-ontwrichtende effecten leiden dan tot een crisis waarbij de (lokale) overheid een centrale rol heeft in de crisisbeheersing. Het Cybersecuritybeeld Nederland (CSBN) stelt onder meer dat door de omvang van de dreiging en het achterblijven van de weerbaarheid, risico's ontstaan voor de nationale veiligheid. Om de weerbaarheid te vergroten is het essentieel dat de overheid snel en effectief kan reageren op een cybercrisis.

In dit draaiboek is beschreven op welke wijze de gemeenten Aalsmeer en Amstelveen zich hebben voorbereid om snel en effectief te kunnen reageren op een cybercrisis. Het draaiboek bevat een beschrijving van de taken en verantwoordelijkheden, de organisatiestructuur alsmede een invulling op hoofdlijnen van een aantal thema's dat tijdens de cybergevolgbestrijding aan de orde kan komen.

In het continuïteitsplan van de AA-organisatie (zie ook bijlage VIII) staat beschreven wat er gebeurt en in welke volgorde als er sprake is van een uitwijk/herstel van de gemeente Amstelveen/Aalsmeer. Dat hoort dus niet tot de scope van dit document.

1.1 Definitie van een cybercrisis

De term 'cyber' is een containerbegrip voor alles wat met informatie- en communicatietechnologie (ICT) samenhangt. De Nederlandse taal telt meer dan 700 woorden die beginnen met cyber, zoals (cyber)verstoring, (cyber)politie, (cyber)criminaliteit en (cyber)spionage. Dit laat zien hoezeer deze technologie is verweven met onze fysieke wereld. Voor dit draaiboek wordt een cybercrisis gedefinieerd zoals onderstaand staat beschreven. Voor deze definitie sluiten we aan bij de cybersecurity definitie van de Nederlandse Cybersecurity Agenda. Cybergevolgbestrijding is het zoveel mogelijk beperken van de impact van een cybercrisis.

Definitie Cybercrisis:
Een cybercrisis is iedere (opzettelijke) verstoring, uitval of misbruik van een gedigitaliseerd proces, (informatie)systeem of informatiedienst die de maatschappelijke continuïteit, openbare orde en veiligheid bedreigt of verstoort.

1.2 Het cyberlandschap

Cyber is dus een breed begrip. Een cybercrisis is niet eenvoudig af te bakenen als één specifiek soort crisis. Het betreft echter altijd een digitale verstoring. Digitale verstoringen kunnen niet-opzettelijk zijn waarbij de oorzaak van het incident niet met opzet is ontstaan. Niet-opzettelijke verstoringen kunnen bijvoorbeeld veroorzaakt worden door menselijk falen, technisch falen en natuurgeweld (zoals hitte, droogte, vocht). Bij een cybercrisis kunnen verschillende actoren betrokken zijn, verschillende doelwitten worden geraakt en daarnaast worden verschillende methodieken gebruikt om weer verschillende doelen te bereiken. Ook heb je verschillende partners nodig bij de afhandeling.

• **Actoren:** Indien er sprake is van opzettelijk handelen, spreken we van actoren die een cyberincident veroorzaken, bijvoorbeeld criminelen (netwerken), hacktivisten, cybervandalen, insiders, terroristen of staten. De term 'actoren' kan ook worden gebruikt om partijen te benoemen die zich met de crisisbeheersing bezighouden zoals in het NCP-digitaal wordt aangegeven. Om verwarring te voorkomen wordt in dit document alleen naar actoren verwezen bij personen, groepen of organisaties die opzettelijk een cyberincindent (dreigen) te veroorzaken.
We spreken over partners wanneer het gaat over organisaties die zich met de crisisbeheersing bezighouden.

• **Doelwit:** cyberaanvallen kunnen gericht zijn op ieder individu en iedere organisatie in de maatschappij, van burger, private partijen tot publieke organisaties zoals gemeenten. De impact van een cyberaanval hangt onder andere af van de partij waarop de verstoring is gericht.

• **Doelen:** een cybercrisis kan worden veroorzaakt door storing en uitval van ICT, cyberspionage, cybersabotage, cybercriminaliteit, cyberterrorisme, cyberactivisme (en vandalisme).

• **Methodieken:** de methoden en technieken die gebruikt worden om een cybercrisis te veroorzaken, zijn onder andere een DDoS-aanval, malware-aanval, ransomware-aanval of phishing.

• **Partners:** specifieke partijen die kunnen worden ingeschakeld ten behoeve van monitoring van het cyberlandschap, bronbestrijding, duiding in de effectbestrijding.

Ieder jaar wordt op landelijk niveau in het CSBN een update gegeven van de grootste cyberdreigingen op dat moment. Het CSBN 2019 van de Nationaal Coördinator Terrorismebestrijding en Veiligheid geeft inzicht in dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Voor een actueel beeld van de huidige dreigingen is het raadzaam om het CSBN te raadplegen. De Informatie Beveiligingsdienst (IBD) stelt jaarlijks ook een lokaal dreigingsbeeld op, het 'IBD Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten', dat onlinewordt gepubliceerd door de Vereniging van Nederlandse Gemeenten.

1.3 Impact van een cyberincident

De impact begrijpen van een digitale verstoring is lastig. Dit 'begrijpen' noemen we het duiden van de impact. Een cybercrisis veroorzaakt door een bewuste cyberaanval heeft bijvoorbeeld een andere impact dan een technische storing. En een cyberaanval gericht op de gemeente heeft weer een andere impact dan een cyberaanval gericht op heel Nederland. Denk hierbij aan de wijze van respons, de communicatie en de escalatiemogelijkheden.

Om als crisisteam in staat te zijn deze impact te duiden is digitale expertise essentieel. Iedereen in een crisisteam moet een bepaalde basiskennis hebben van digitale processen en terminologie. Zonder deze basiskennis is het lastig om de experts te begrijpen die het crisisteam kunnen ondersteunen.

Digitale expertise ter ondersteuning van het crisisteam kan verschillende vormen aannemen:
• Kennis van oplossen *technisch component* (ver)storing
• Duiden impact *technische verstoring* op organisatieprocessen (bijvoorbeeld gemeentelijke dienstverlening)
• Duiden impact van de *verstoring op het maatschappelijk leven*

Kennis van de **technische kant** van de verstoring zit primair bij de leverancier van het geraakte systeem, maar zeker ook bij de gemeenten zelf. Deze informatie is vooral relevant voor de teams die zich met het oplossen van de verstoring bezighouden. De gemeente Aalsmeer en Amstelveen zijn zelf verantwoordelijk voor het oplossen van de technische verstoring (al dan niet met behulp van de leverancier) en het continueren van de eigen dienstverlening. Het helpt als vooraf contractuele afspraken zijn gemaakt tussen leverancier en afnemer over informatieoverdracht vanuit de leverancier naar de getroffen organisatie ten behoeve van de crisisbeheersing.

Kennis van impact van de **technische verstoring** op organisatieprocessen zit primair bij de CISO van de gemeente. Het betrekken van een CISO in het crisisteam kan daarmee beeld- en oordeelsvorming vergemakkelijken. Indien er meerdere crisisteams actief zijn die een beroep op aanwezigheid van de CISO doen, zal deze goed moeten uitvragen welke informatiebehoefte er ligt

vanuit deze crisisteams. Om zo een goede afweging te kunnen maken omtrent aanwezigheid en advies.

Het inschatten van de impact van **verstoringen op de maatschappij** ligt primair bij de veiligheidsregio's. De veiligheidsregio's bereiden zich vanuit van hun wettelijke taak voor op het verkleinen van effecten van verstoringen van het maatschappelijk leven. Dit is een rol die veiligheidsregio's vervullen voor allerlei soorten crises en hier zit expertise omtrent maatschappelijke continuïteit. Bij de afdelingen OOV van de gemeenten is daarnaast expertise aanwezig over de specifieke maatschappelijke vraagstukken in de betreffende gemeente en wijken. Ook deze expertise is noodzakelijk voor een goede impactanalyse van de verstoring op het maatschappelijk leven en zal in de analyse een plek moeten krijgen.

Voor cybercrises in de gemeentelijke organisatie kan de gemeentelijke calamiteitenorganisatie ondersteuning vragen aan de IBD als het gaat om de inschatting van de aard, omvang en ernst van de situatie. De IBD adviseert over te nemen maatregelen en acties en heeft een directe verbinding met onder andere belangrijke ICT-leveranciers, Computer Emergency Response Teams (CERT's) van andere organisaties, het NCSC en internationale CERT's.

De politie zal adviseren vanuit het oogpunt van opsporing en vervolging. Binnen de politie zijn verschillende cyberteams actief, waaronder het cybercrimeteam vanuit de regionale eenheid, die een mogelijk opzettelijke cybercrisis technisch kunnen duiden op oorzaak en bron en de mogelijkheden van opsporing en vervolging.

II. Crisisorganisatie

Als binnen de gemeente zich een crisis voordoet die vooral de interne organisatie raakt, wordt deze afgehandeld langs de lijnen zoals beschreven in de bedrijfscontinuïteitsplannen van de gemeente Aalsmeer en Amstelveen. Globaal gezegd gebeurt dit door een intern calamiteitenteam onder aansturing van de gemeentesecretaris en verantwoordelijkheid van het college. De CISO heeft daarin een belangrijke coördinerende rol voor de continuïteit van het digitale domein. Daarnaast geldt als uitgangspunt dat bij elke opzettelijke activiteit aangifte wordt gedaan door de gemeente.
Indien blijkt dat de crisis ook (grote) effecten heeft op de openbare orde en veiligheid, of dat er behoefte is aan extra opsporingsbevoegdheden om de actor te achterhalen, komt de driehoek bij elkaar. Mochten de hulpverleningsdiensten worden ingezet en daarbij (multidisciplinaire) afstemming nodig zijn, of is er sprake van crisisbeheersing of rampenbestrijding, dan kan gebruik worden gemaakt van de GRIP-structuur, waarbij heldere besluitvormings- en informatielijnen zijn afgesproken met multidisciplinaire crisisteams in het veld (CoPI) op tactischniveau (ROT) en op bestuurlijk niveau (BT). In geval van een dreigende situatie, er is nog geen sprake van daadwerkelijke inzet van de hulpverleningsdiensten, wordt deze dreiging geanalyseerd in een informele ROT-setting. De naam voor veiligheidsregio Amsterdam-Amstelland is "voorbereidend ROT".

Het kan zijn dat er wel sprake is van een cybercrisis en dat de effecten zichtbaar zijn in domeinen waar de hulpdiensten nog geen rol hebben. Vaak zal dan het informele ROT wel bij elkaar komen om de situatie te analyseren en scenario's te bespreken. Ook zal indien nodig het gemeentelijk crisisteam worden ingericht.

In theorie kunnen de teams tegelijkertijd actief zijn in hun eigen rol waarbij de focus van het gemeentelijke team zich richt op de eigen organisatie. De focus van ROT en BT richt zich op het bestrijden van de effecten in het fysieke domein, het gemeentelijk crisisteam richt zich op de effecten in het niet-fysieke domein. De driehoek richt zich op opsporingsvraagstukken. Hiernavolgend worden deze teams kort beschreven.

2.1 Gemeentelijk calamiteitenteam

Bij een cyberincident binnen de gemeentelijke organisatie kan het gemeentelijk calamiteitenteam, onder verantwoordelijkheid van de gemeentesecretaris, worden ingesteld. Naast de gemeentesecretaris nemen aan dit calamiteitenteam functionarissen deel binnen de gemeente met expertise op het gebied van facilitaire zaken (zoals ICT inclusief telefonie/andere communicatiemiddelen, gebouwbeheer en beveiliging) en crisiscommunicatie. In bijlage VII, stap 3, staat onder andere beschreven welke functionarissen bij ICT-storingen of uitval belast zijn met het reduceren van de effecten van een calamiteit en het continueren van de bedrijfsprocessen van de gemeente.

Samenvattend: dit team houdt zich bezig met het borgen van de gemeentelijke organisatiecontinuïteit en effectbestrijding bij gevolgen binnen de gemeentelijke beleidsdomeinen.

2.2 De Driehoek

Driehoeksoverleg (artikel 13 Politiewet 2012): De politie staat onder duaal gezag: voor de handhaving van de openbare orde en voor de hulpverlening ligt het gezag bij de burgemeester en voor de strafrechtelijke handhaving ligt het gezag bij de officier van justitie. Dit overleg tussen politie, burgemeester en OM is de lokale gezagsdriehoek. De burgemeester is meestal de voorzitter van het driehoeksoverleg. In het geval van een cybercrisis kan het zijn dat de politie extra opsporingsmiddelen vraagt om zo de actor op te sporen. Dit moet in overleg met het OM vanuit strafrechtelijk oogpunt, maar ook overleg met de burgemeester is relevant omdat de uitkomst invloed kan hebben voor een snelle(re) afhandeling van de crisis. Er is dan zowel een strafrechtelijke afweging als een afweging in het kader van openbare orde. De driehoek neemt hier in gezamenlijkheid een besluit over zodat de politie altijd kan blijven voldoen aan haar gezagsrelatie met zowel OM als burgemeester. De informatie uit het driehoeksoverleg wordt waar relevant voor de crisisbeheersing gedeeld met het beleidsteam op basis van need to know.

Het driehoeksoverleg is daarmee een ander type crisisoverleg dan dat van het interne calamiteitenteam en dat van het beleidsteam.

2.3 De GRIP-structuur

Bij een cybercrisis in het geografisch gebied van de gemeente kan de gemeente als bevoegd gezag gebruik maken van de crisisbeheersingsstructuur. Er wordt dan via de GRIP-structuur opgeschaald en de burgemeester laat zich in het GBT adviseren over de consequenties van de digitale verstoring op het maatschappelijk leven en de te nemen maatregelen omtrent de effectbestrijding. Deze opschaling vindt plaats als de effecten van deze cybercrisis leiden tot (grootschalige) inzet van de hulpverleningsdiensten. Er wordt dan binnen de GRIP-structuur opgeschaald om snel een crisisteam te formeren en heldere informatie-besluitvormingslijnen te creëren.

De GRIP-structuur is ontwikkeld om bij crises die één of meerdere gemeenten treffen om de crisisbeheersing te structureren. Binnen deze structuur overleggen de hulpverleningsdiensten (brandweer, politie, geneeskundige zorg en bevolkingszorg) onder gezag van de burgemeester of voorzitter veiligheidsregio om de crisis zo effectief mogelijk te bestrijden en de effecten te beperken. Afhankelijk van de omvang van een incident vallen deze diensten onder het bevoegd gezag van de burgemeester van de getroffen gemeente (GRIP-1 tot en met 3) óf van de voorzitter van de veiligheidsregio (GRIP-4).

Ten behoeve van effectieve afhandeling is er een aantal ondersteunende secties ingericht:informatiemanagement, operationele leiding en crisiscommunicatie. Deze zijn onafhankelijk van het soort crisis te gebruiken.

2.4 Gemeentelijke crisisorganisatie

Er zijn cybercrises denkbaar waar het lokaal bestuur effecten van ondervindt, maar die buiten het traditionele domein van de veiligheidsregio vallen en ook de eigen gemeentelijke dienstverlening niet direct raken. Denk bijvoorbeeld aan het uitvallen van diensten die door een gemeenschappelijke regeling worden geleverd. Voor dit type (cyber)crisis is gemeente ook aan zet om zich met de gevolgen bezig te houden.

Het is aan de gemeenten en de veiligheidsregio samen om te bepalen of onderdelen van de regionale crisisorganisatie ingezet kunnen worden binnen de gemeentelijke crisisorganisatie. Mocht deze wens er zijn dan moet dat formeel op regionaal niveau onder verantwoordelijkheid van het bestuur van de veiligheidsregio's worden besloten.

Enkele aandachtspunten:

- Kennis van de technische kant van de verstoring zit primair bij de leverancier van het geraakte systeem. Daarnaast is er ook technische kennis bij de gemeentelijke organisatie. Deze informatie is vooral relevant voor de teams die zich met het oplossen van de verstoring bezighouden.
- Kennis van impact van de technische verstoring op organisatieprocessen zit primair bij de CISO van de geraakte organisatie. Het betrekken van een CISO in het crisisteam kan daarmee beeld- en oordeelsvorming vergemakkelijken.
- Kennis van impact van verstoringen op het maatschappelijk leven zit bij de veiligheidsregio's en de afdelingen OOV van de gemeente Aalsmeer en Amstelveen.
- Per crisis moet worden gekeken welk domein en systemen geraakt zijn om zo de juiste inhoudelijk adviseurs aan tafel te krijgen.
- Een cybercrisis vraagt om een specialistische aanpak en daarmee inhoudelijke kennis aan tafel. Het zal voor deelnemers die standaard een rol hebben binnen de gemeentelijke crisisorganisatie onwennig zijn als ze bij dit type crisis geen rol hebben. Het helpt om dit vooraf goed af te spreken en tijdens de crisis op te blijven reflecteren.
- Zorg dat de processen informatiemanagement, crisiscommunicatie en leiding- en coördinatie georganiseerd zijn.

2.5 Nationaal versus regionaal

In het Nationaal Crisisplan Digitaal wordt de landelijke reactie op een cybercrisis beschreven. Tegelijkertijd is er ook een regionale rol bij het bestrijden van een landelijke cybercrisis.

Vanzelfsprekend blijft het lokale of regionale gezag verantwoordelijk voor effectbestrijding conform de Wet veiligheidsregio's (Wvr).

Wanneer er sprake is van een cybercrisis binnen de gemeentelijke organisatie is de IBD de partij die informatie over het cybercomponent en de oplossingsstrategie kan delen met de getroffen gemeenten. Ook is de IBD de liaison namens de gemeenten richting het NCSC om eventuele lokale oplossingen en vraagstukken te delen.

Politie en OM zijn landelijk georganiseerd, daarmee wordt de opsporingstaak bij een landelijke cybercrisis ook vanuit die partijen landelijk gecoördineerd. Het staat niet specifiek beschreven hoe dit zich verhoudt tot de getroffen lokale partijen en de driehoeken. Lokale bestuurders zullen zich bij een crisis op landelijke schaal vooral laten informeren vanuit OM en politie voor wat betreft de opsporingstaak en afweging.

Indien de cybercrisis beperkt blijft tot een gemeente of regio is het nationale niveau vooral ondersteunend. Indien de gemeente zelf getroffen wordt zal de IBD ondersteunen en de link vormennaar het NCSC. Indien de gemeentelijke organisatie niet zelf getroffen is zal de informatie van het NCSC via de politie en en verantwoordelijkheden van de verschillende (nationale) partijen verder toegelicht.
Indien de effecten zodanig bovenregionaal zijn dat er landelijk wordt opgeschaald (meerdere veiligheidsregio's zijn geraakt) zullen het NCC en het LOCC-bovenregionaal zich vooral richten op informatiedeling en het landelijk informatiebeeld. De informatiemanagers vanuit het ROT hebben inzicht in het landelijk beeld zoals dat binnen het Landelijk Crisismanagement Systeem (LCMS) wordt bijgehouden.

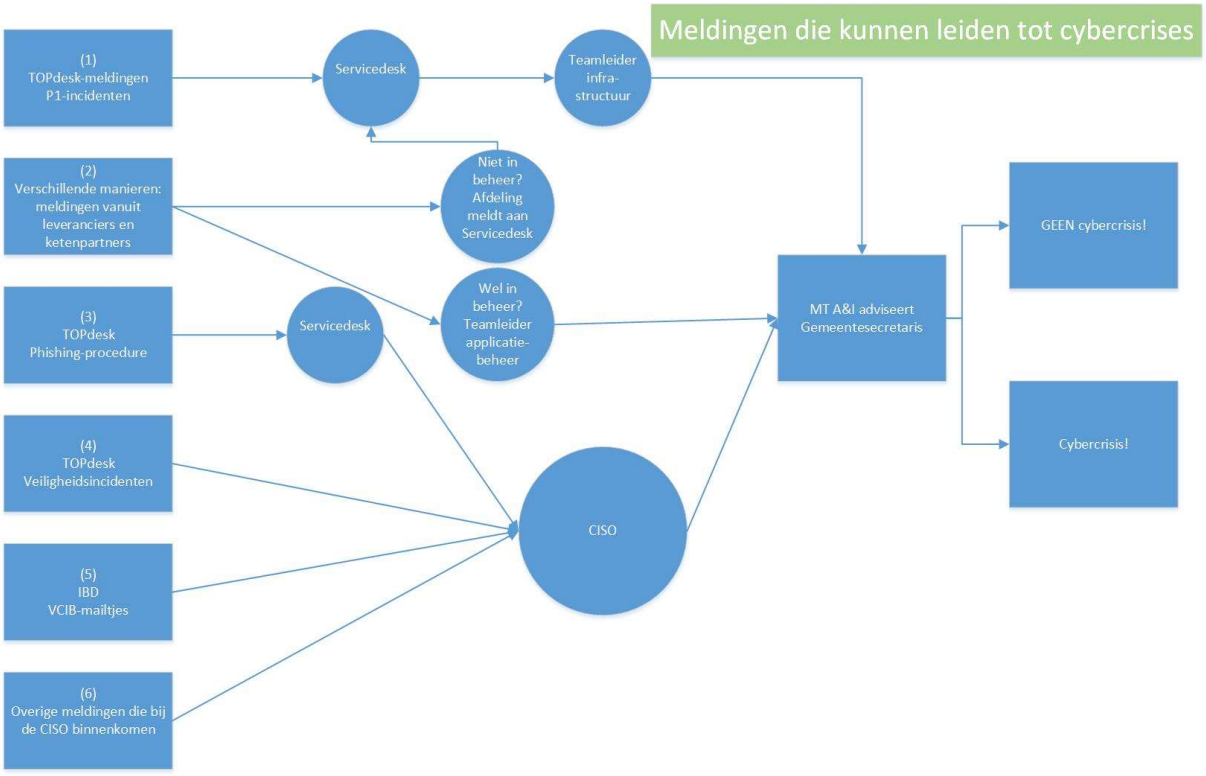
III. Opstart Cybergevolgbestrijding

Bij een (cyber)crisis is het van groot belang dat betrokken partijen zo snel als mogelijk op de hoogte raken van de situatie. Dit geldt zowel voor crises die door opzettelijk handelen zijn veroorzaakt als voor andere verstoringen. Vanwege de snelheid waarmee een cybercrisis zich kan verspreiden, kan het aantal betrokken partijen snel veranderen. Daarom is het belangrijk om heel snel de partijen te informeren die als informatieknooppunt fungeren, zoals de IBD en het NCSC.

3.1 Melding

Crisisbeheersing start pas als de getroffen organisatie weet dat er een crisis is. Hiervoor is bewustwording bij alle medewerkers randvoorwaardelijk: zij moeten weten hoe ze een cybercrisis herkennen en spelen daarnaast een belangrijke rol in het voorkomen van een crisis. Er moet een melding plaatsvinden bij de partij die de crisis kan aanpakken. Dat kan een interne (cyber)crisisorganisatie zijn, maar ook een externe partij die daarbij ondersteunt. Naast de reguliere meldingsprocessen gelden er aandachtspunten in het geval van een cybercrisis. Deze aandachtspunten verschillen per domein dat geraakt wordt en staan beschreven in bijlage V.

Binnen de organisatie van de gemeente Aalsmeer en Amstelveen zijn er diverse kanalen waarbij er meldingen binnen kunnen komen met incidenten die tot mogelijke cybercrisis kunnen lijden. Het uiteindelijke besluit ligt bij het hoofd van Automatisering en informatiemanagement die de gemeentesecretaris adviseert of de melding een cybercrisis is of niet.



Er zijn meerdere meldingen die kunnen uitmonden in de classificatie “Cybercrisis”. Dit komt omdat een cybercrisis niet altijd door iedereen wordt herkend als een cybercrisis, én omdat een melding zowel vanuit intern (van een medewerker) als extern (van een ketenpartner, een leverancier, een CERT of op een andere manier) binnen kan komen.

Interne meldingen
Hieronder worden de interne meldingen zoals benoemd in bovenstaand schema uitgewerkt. De nummers tussen haakjes corresponderen met de nummers in de blokjes in dit schema.

- (4) Als een medewerker weet dat er (mogelijk) sprake is van een cybercrisis, geldt de "veiligheidsincidenten-procedure". In deze procedure staat het proces van veiligheidsincidenten, incl. melden en opvolgen, nauwkeurig beschreven. Indien een medewerker een mogelijk veiligheidsincident constateert, meldt hij dit via het Self Service Portal van TOPdesk. Deze melding komt terecht bij de Chief Information and Security Officer (CISO) van de organisatie die de afweging maakt en het besluit neemt of dit een serieuze melding is voor een mogelijke cybercrisis. Indien dit wél het geval is, neemt de CISO contact op met het MT A&I die de gemeentesecretaris adviseert. Deze neemt het uiteindelijke besluit.
- (1) Bij de Servicedesk komen dagelijks allerlei ICT-gerelateerde meldingen voorbij vanuit de gehele organisatie. Als de Servicedesk vermoedt dat één zo'n melding wijst op een Cybercrisis, escaleert deze aan de verantwoordelijk Teamleider (Infrastructuur). Indien deze het met die vermoedens eens is, neemt zij contact op met het MT A&I die de gemeentesecretaris adviseert. Deze neemt het uiteindelijke besluit.
- (3) Medewerkers kunnen meldingen doen van phishingmail bij de Servicedesk. Het is mogelijk dat een phishingmail een cybercrisis tot gevolg heeft. Deze onderzoekt de phishingmail op een iPad die geen verbinding heeft met het netwerk. Indien het een serieuze dreiging is wordt de mail doorgezet naar een escalatiegroep waarin o.a. de CISO zit. Deze maakt het besluit of de phishing mail wijst op een cybercrisis. Indien dit wél het geval is, neemt de CISO contact op met het MT A&I die de gemeentesecretaris adviseert. Deze neemt het uiteindelijke besluit.

Voor de interne meldingen geldt dat (indien er een cybercrisis wordt uitgeroepen) de veiligheidsincidenten procedure op een gegeven moment in werking treedt. Hierin wordt het proces van de melding aan de IBD, de AP en politie (indien nodig) beschreven. Snelle informatiedeling met de IBD houdt eventuele verdere verspreiding tegen.

Melding(en) vanuit leveranciers/ketenpartners
(2) Als de melding komt vanuit leveranciers en ketenpartners waarvan de systemen in beheer zijn bij A&I, komt deze in eerste instantie terecht bij de beheerder van de applicatie/het systeem. Indien de dreiging serieus is, escaleert deze naar zijn teamleider. Deze beoordeelt of de melding verder moet naar het MT A&I, die vervolgens de gemeentesecretaris adviseert.

Als de melding komt vanuit leveranciers en ketenpartners waarvan de systemen níét in beheer zijn bij A&I, komt de melding terecht bij de functioneel beheerder/contactpersoon op de afdeling. Deze dient een melding in bij de servicedesk of een veiligheidsincident, waarna de route loopt volgens de hierboven beschreven route.

Melding(en) vanuit IBD en VCIB en overige meldingen bij de CISO
(5) (6) Bij de CISO komen ook meldingen van de IBD en VCIB binnen. Voor iedere meldingen wordt na afweging het besluit genomen of dit verder opgepakt moet worden als een mogelijke cybercrisis. Hetzelfde geldt voor overige meldingen die via onofficiële kanalen binnenkomen. Uiteindelijk maakt die de afweging en neemt het besluit of dit een serieuze melding is voor een mogelijke cybercrisis. Indien dit wél het geval is, neemt de CISO contact op met het MT A&I die de gemeentesecretaris adviseert. Deze neemt het uiteindelijke besluit.

3.2 Hoe werkt de afdeling A&I in geval van een cybercrisis?

In hoofdstuk 3.1 is beschreven vanuit welke richtingen een melding kan komen die leidt tot een cybercrisis. De afdeling A&I is vaak aan zet om deze op te lossen. In dit hoofdstuk staat kort beschreven hoe deze afdeling te werk gaat.

First line of defence
De ICT-specialisten (netwerkbeheer, systeembeheer, applicatiebeheer, informatiebeheer en servicedesk ICT) vormen de 'first line of defence'.[1] Iedere I(CT) specialist heeft de

[1] De 'second line of defence' wordt gevormd door interne controles die gericht zijn op het functioneren van de operationele controls. Deze 'second line of defence' kijkt mee over de schouders van de ICT specialisten en ICT managers om er zeker van te zijn dat de ICT beheersingsmaatregelen goed worden toegepast. De 'third line of defence' wordt gevormd door onafhankelijke toetsing (audits, vulnerability testen, PEN testen of concern control)

verantwoordelijkheid (en zelfs de plicht) om bij constateren van dreiging of risico, direct in te grijpen. Dit mandaat behoort bij de primaire beheerverantwoordelijkheid. Dit ingrijpen kan natuurlijk alleen indien de specialist een behoorlijk vermoeden of zekerheid heeft over hetgeen plaatsvindt en zicht heeft op de risico's. De ingreep kan zelfstandig plaatsvinden of in directe afstemming met de teamleider. Deze 'first line of defence' is continu actief, handelt direct indien de ICT-specialist een voorval constateert of uit de monitoringsystemen (met opvolgingsafspraken) een signaal ontvangt.

Vervolg – na ingrijpen

1. Indien met het ingrijpen het risico is afgewend, wordt achteraf door de ICT lijnmanager / incidentmanager een rapportage met evaluatie opgeleverd.

2. Indien opgeschaald moet worden over de (vervolg)aanpak, de impact, de urgentie of de oplossing van de dreiging, dan wordt (om geen tijd te verliezen) direct opgeschaald in twee sporen:

    a. **Gemeentelijke Operationeel team** wordt ingericht. Dit team wordt samengesteld afhankelijk van de geconstateerde dreiging en kan bestaan uit de incidentmanager, (vooraf gecontracteerde) externe specialisten, specialisten netwerkbeheer, specialisten systeembeheer en/of specialisten applicatiebeheer. Dit team gaat direct gericht aan de slag met de analyse en voorstel voor aanpak. Dit team staat onder leiding van de teamleider van het team dat het grootste aandeel (lijkt) te hebben in de dreiging (deze teamleider is tegelijkertijd de linking pin/liaison naar het Gemeentelijke cybercrisisteam (GCC)). Het gemeentelijke operationeel team legt verantwoording af aan het Gemeentelijke cybercrisisteam (GCC).
    b. **Gemeentelijk cybercrisisteam (GCC)** wordt ingericht. Dit team coördineert de aanpak, acties en communicatie, zowel naar het gemeentelijk operationeel team als naar de organisatie c.q. directie. De inzet van dit team wordt uitgewerkt in hoofdstuk 3.3. In de bijlagen staat andere informatie over dit team: De samenstelling (I), een concept-agenda (II), een Format voor de actie-en besluitenlijst (III), Bereikbaarheidsgegevens (IV), een Organisatieschema (V) en een Stappenplan bij het bestrijden van een cybercrisis (VI).

Voorwaarden Afdeling A&I

Er zijn een aantal voorwaarden waaraan moet worden voldaan om Afdeling A&I op bovenstaande manier optimaal te laten functioneren. Deze staan beschreven in bijlage XI.

3.3 Alarmering, activering en inzet Gemeentelijk Cybercrisisteam (GCC)

Om de alarmering en vervolgstappen compleet en secuur te laten verlopen is het noodzakelijk hiervoor deze 6 stappen te doorlopen:

- Stap 1. Informatie verzamelen
- Stap 2. Juiste team(s) alarmeren
- Stap 3. Juiste bezetting van het team
- Stap 4. Vergadering cybercrisisteam
- Stap 5. Informatiedeling – Netwerkkaart
- Stap 6. Oordeels- en Besluitvorming – Checklist sleutelbesluiten

Omdat bij een cybercrisis extra en andere expertise nodig is, zijn er voor alarmering enkele aandachtspunten in de te zetten stappen. Het gaat om de onderstaande stappen waarvan hier enkel wat aandachtspunten benoemd staan. De uitwerking staat beschreven in bijlage VII.

DEEL 2: Bijlagen

I. Bezetting Gemeentelijk Cybercrisisteam (GCC)

De rollen en aanwezigen zijn voorbeelden. Elke crisis is anders en het is per crisis noodzakelijk om te kijken wie er aanwezig dient te zijn. Een voorzitter, een beslissingsbevoegde en de CISO (de eerste drie rollen) zijn sowieso altijd een onderdeel van het GCC.

V.w.b. de bestuurlijke betrokkenheid (directie, burgemeester, wethouder ICT en eventueel overige wethouders) wordt aangehaakt bij de constructie zoals geregeld in een GRIP situatie.

Rol	**Aanwezig en nodig**
Voorzitter Rapporteert aan directie, wethouder ICT en evt. vakwethouder en burgemeester	Een lid van het MT A&I, in volgorde: Afdelingshoofd Teamleider Infra Teamleider Applicaties Teamleider A&P Teamleider IV Teamleider Basisinformatie
Beslissingsbevoegde verantwoordelijke	Zie voorzitter
Verbinding met IBD, FG/AP, regionale CISO's e.d. en kennis van impact van de technische verstoring op organisatieprocessen	CISO
Adviseur crisiscommunicatie	Team communicatie (piket)
Informatiemanager Deze zorgt voor een gedegen beeld. Haalt informatie op en verspreidt deze. Vertaalt de informatie naar het incident	Incidentmanager (ook schakel naar het gemeentelijk operationeel team)
Secretaris/notulist/plotter	Voorzitter benoemt de secretaris. Bijv. binnen A&I iemand van het PMO.
Inhoudelijk deskundige technische verstoring	Systeem- en/of netwerkbeheer Applicatiebeheerder Changemanager Leverancier
Duiden impact technische verstoring op organisatie-processen	Enterprise/Solution architect, informatiemanagers afhankelijk van afdeling.
Duiden impact van de verstoring op het maat-schappelijk leven	Afdelingshoofden/teamleiders, afhankelijk van getroffen afdelingen/teams
Inhoudelijk deskundige effect eigen organisatie	Afdelingshoofden/teamleiders, afhankelijk van getroffen afdelingen/teams
Inhoudelijk deskundige maatschappelijk effect 1	Experts op het getroffen gebied. Wordt op basis van maatwerk ingevuld.
Inhoudelijk deskundige op het gebied van gegevensbescherming 2	Functionaris Gegevensbescherming en Controller Informatieveiligheid
Liaison voor verbinding andere teams	OOV

II. Concept agenda

1. Opening en aanleiding
- 1.1 Check: iedereen hetzelfde beeld bij aanleiding en doel vergadering
- 1.2 Check: iedereen hetzelfde beeld bij verantwoordelijkheden team
- 1.3 Check: vergaderafspraken

2. Voorstelronde, juiste expertise/partijen aan tafel
- 2.1 Check: indien voor team relevant: voldoende kennis op gebied van de technische component van de verstoring aan tafel
- 2.2 Check: indien voor team relevant: voldoende kennis van impact verstoring op bedrijfsprocessen aan tafel
- 2.3 Check: indien voor team relevant: voldoende kennis van impact verstoring op maatschappelijk leven aan tafel
- 2.4 Check: zijn alle partijen aan tafel ook voor deze crisis relevant, missen we iemand

3. Beeldvorming (Bob**)**
- 3.1 Informatiemanager deelt beeld over verstoring en effecten
- 3.2 Check: welke teams zijn opgeschaald
- 3.3 Check: aanvulling vanuit deelnemers
- 3.4 Check: de tien vragen uit de Cyber-Crisis-Cirkel (welke blinde vlekken zijn er nog)
- 3.5 Check: wie is verantwoordelijk voor ophalen informatie
- 3.6 Check: zijn er nog andere crises/ontwikkelingen waar rekening mee gehouden moet worden
- 3.7 Vat beeld samen
- 3.8 Apart voor beeld omtrent eigen organisatie verstoring en effecten
- 3.9 Apart voor beeld omtrent maatschappelijke verstoring en effecten en omgevingsbeeld crisiscommunicatie

4. Oordeelsvorming (b**O**b**)**
- 4.1 Definieer thema's ter bespreking
- 4.2 Check met team welke thema's geraakt zijn
- 4.3 Check welke andere teams ook bezig zijn en hoe de informatie uitwisseling plaatsvindt
- 4.4 Check waar de maatschappelijke impact het grootst is en prioriteer aandachtsgebieden
- 4.5 Check welke effecten er zijn op eigen organisatie(continuïteit)
- 4.6 Bespreek mogelijke escalatiescenario's/gebruik hierbij de tien vragen uit de Cyber-Crisis-Cirkel
- 4.7 Identificeer welke maatregelen vanuit dit team hierop genomen kunnen worden en wie dat doet
- 4.8 Check welke bestuurlijke besluiten/dilemma's relevant zijn

5. Besluitvorming (bo**B) (zie checklist sleutelbesluiten)**
- 5.1 Inhoudelijke besluiten (wie voert welke actie uit om effecten te reduceren, crisiscommunicatie)
- 1.2 Proces besluiten (wie informeert wie, wanneer vergaderen, nog extra expertise aan tafel nodig)
- 5.3 Check welke besluiten bij ander teams worden voorgelegd.

III. Format Actie- en Besluitenlijst Cybergevolgbestrijding (CGB)

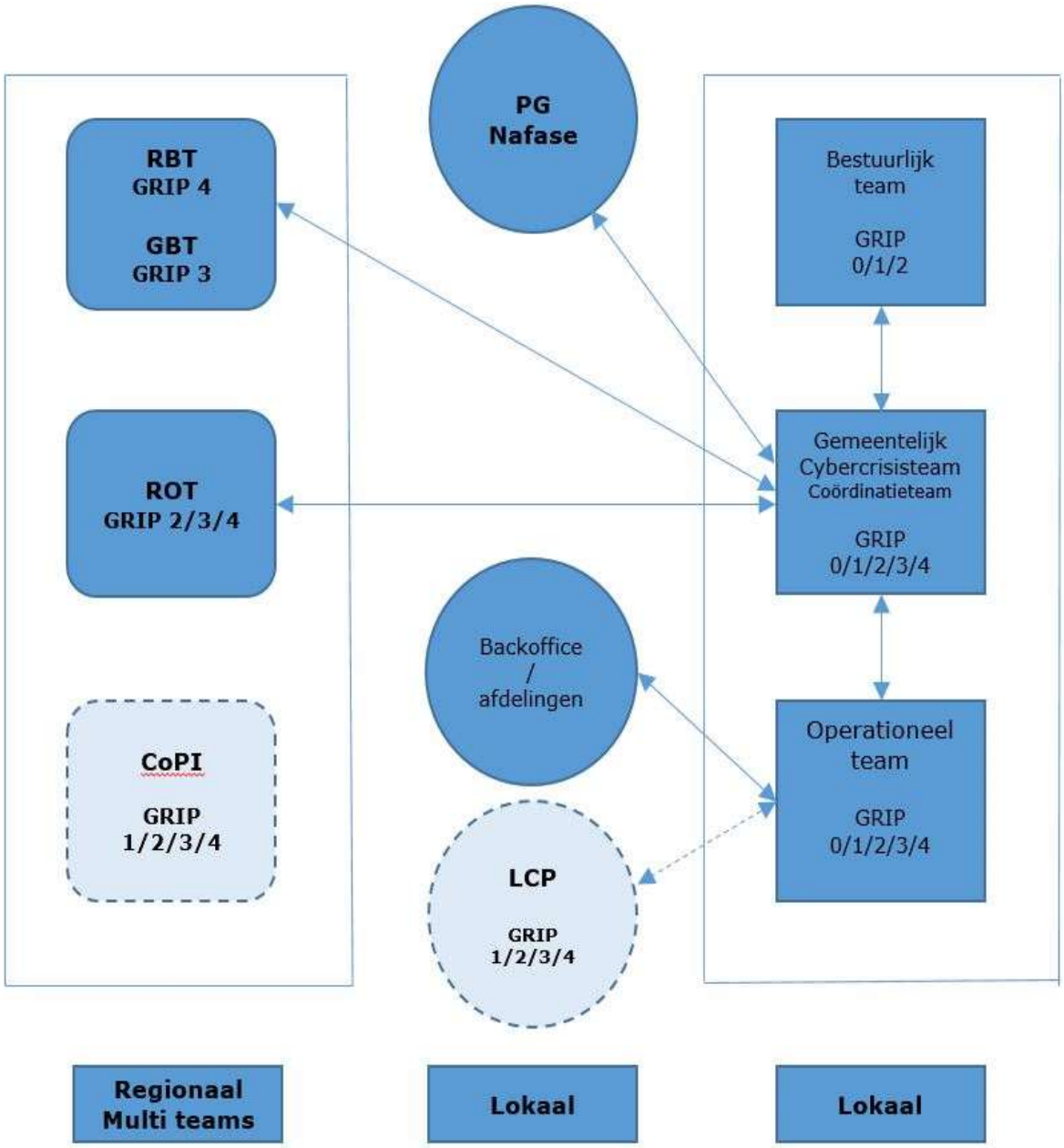
ACTIE- EN BESLUITENLIJST CGB d.d --/--/----

NR.	ACTIE/BESLUIT	OMSCHRIJVING	ACTIEHOUDER	AFGEROND

IV. Cybercrisiskaart gemeente AA

Zie bijlage "Cybercrisiskaart gemeente AA" voor:
Telefoonlijst intern
Telefoonlijst interne applicatiebeheerders
Telefoonlijst extern

V. Organisatieschema



Multi teams: o.a. gemeente, politie, brandweer, geneeskundige hulpverlening (GHOR), Openbaar Ministerie, Defensie.
Regionaal: 6 gemeenten binnen de Veiligheidsregio Amsterdam-Amstelland (VrAA) (Aalsmeer/ Amstelveen/ Amsterdam/ Diemen/ Ouder-Amstel/ Uithoorn)
Lokaal: brongemeente (Aalsmeer en/of Amstelveen)
GRIP: Gecoördineerde Regionale Incidentenbestrijding Procedure (altijd multi)
RBT: Regionaal beleidsteam, meerdere gemeenten bij betrokken (fysiek in Amsterdam)
GBT: Gemeentelijk beleidsteam, getroffen gemeente (fysiek in eigen raadhuis)
ROT: Regionaal Operationeel Team (fysiek in Amsterdam)
CoPI: Commando Plaats Incident (fysiek op plaats incident)
PG Nafase: Projectgroep nafase (organisatie
LCP: Lokaal Coördinatie Punt (gemeentelijk Actiecentrum, ondersteunend aan gemeentelijke crisisorganisatie tijdens een GRIP incident) (fysiek in eigen raadhuis)

VI. Aandachtspunten meldingsprocessen per domein

Crisisbeheersing start pas als de getroffen organisatie weet dat er een crisis is. Er moet een melding plaatsvinden bij de partij die de crisis kan aanpakken. Dat kan een interne (cyber)crisisorganisatie zijn, maar ook een externe partij die daarbij ondersteunt. Naast de reguliere meldingsprocessen gelden de volgende aandachtspunten in het geval van een cybercrisis. Deze aandachtspunten verschillen per domein dat geraakt wordt.

Indien een interne gemeentelijke organisatie is geraakt (zowel ICT-domein als gemeentelijke dienstverlening):

• Aandachtspunt 1: er zijn interne meldingsprotocol en opvolging zodat werknemers snel melden en weten waar ze moeten melden en dat de interne organisatie snel opvolgt met acties en delen van informatie. Zie hiervoor hoofdstuk 3.1.

• Aandachtspunt 2: draag zorg voor snelle informatiedeling met IBD zodat deze eventueel kunnen adviseren en ook overzicht houden over eventuele verdere verspreiding. Zie ook de veiligheidsincidenten-procedure.

• Aandachtspunt 3: tenzij duidelijk is dat het geen bewuste actie is gelijk de politie informeren zodat deze geen tijd verliest voor mogelijke aanpak van de bron. Zie ook de veiligheidsincidenten-procedure.

Indien de maatschappij is geraakt:

• Aandachtspunt 1: inventariseer voor jouw specifieke gemeente/regio welke organisaties cruciaal zijn voor maatschappelijke continuïteit. Maak met deze organisaties afspraken over het delen van informatie omtrent cyberincidenten/crisis. Doe dit vanuit het perspectief dat de overheid gevolgbestrijding moet organiseren bij uitval van de organisatie en dat er mogelijk escalatierisico is. De AA-organisatie is aangesloten bij het SOC van MOTIV. Momenteel zijn we aan het onderzoeken hoe we SIEM SOC kunnen organiseren binnen onze organisatie.

• Aandachtspunt 2: de politie/OM is goed gepositioneerd voor cyberincidenten, zowel vanuit haar rol in de ISACs als in het kader van afspraken met mogelijke externe deskundigen omtrent forensisch onderzoek en analyse.

VII. Stappenplan bij het bestrijden van de cybercrisis

Stap 1. Informatie verzamelen

De eerste vragen bij elke crisis zijn: wat is er aan de hand en welk effect heeft het? Bij een digitale verstoring is het zinvol om steeds het onderscheid te maken tussen de digitale verstoring zelf en het effect dat deze heeft op het maatschappelijk leven. Om meer zicht te krijgen op de verstoring en het effect helpt het de volgende vragen te stellen:

VERSTORING
- Welk systeem is geraakt?
- Hoe lang gaat de verstoring duren?
- Is dit systeem geïsoleerd of verbonden met andere digitale systemen?
- Betreft het een opzettelijke verstoring?
- Is er een (technisch) oplossingsperspectief?

EFFECTEN
- Welk maatschappelijk domein wordt hiermee verstoord?
- Wat is de maatschappelijke impact?
- Zijn er mogelijkheden om het effect te reduceren of is er kans op escalatie van effecten?
- Hoe lang gaat de maatschappelijke verstoring duren?
- Welk geografisch gebied is geraakt?

Stap 2. Juiste team(s) alarmeren

Alarmeer het Gemeentelijk Cybercrisisteam (GCC) dat verantwoordelijk is voor het herstel van bedrijfsprocessen. Zodra er overtuiging is dat er opzet in het spel is, is alarmering van politie een belangrijke stap die snel gezet moet worden zodat deze zich op de opsporing van de (mogelijke) actor kan richten.

Voor elk team is het relevant zich de volgende vragen te stellen:
- Waar ben ik verantwoordelijk voor?
- Welke andere teams zijn actief en waar zijn die verantwoordelijk voor?
- Hoe gaan we deze crisis samen (met de andere betrokken teams) zo effectief mogelijk bestrijden?

De belangrijkste **afbakening** loopt daarbij langs drie lijnen.
- Wie is eigenaar/gebruiker van het systeem dat verstoord is?
- Waar ligt de bestuurlijke verantwoordelijkheid voor de effectbestrijding?
- Zijn er relevante opsporingsdilemma's ten opzichte van openbare orde?

De beantwoording van deze vragen leidt tot het alarmeren van één of meerdere teams met elk hun eigen taken en verantwoordelijkheden (tabel 1). Een dreiging op effecten kan genoeg zijn om betreffende organisatie(s) vanuit hun verantwoordelijkheid te laten handelen.

Verantwoordelijke organisatie(s)	**Verantwoordelijke team/overleg**	**Hoofdtaken en verantwoordelijkheden**
Eigenaar verstoorde systeem	Incidentmanagementteam	Eventuele aanpassingen aan het systeem, functionerende software.
Bedrijf/ instelling waar digitale systeem is verstoord (gebruiker)	Calamiteitenteam	Oplossen verstoring digitale systeem/ technische oplossing probleem/ bedrijfscontinuïteit
Gemeente, politie en Openbaar Ministerie	Driehoeksoverleg	Opsporingsvraagstukken en afwegen opsporing versus openbare orde en veiligheid.

Gemeente, Veiligheidsregio	GRIP-structuur (ROT/BT)	Effectbestrijding bij gevolgen voor maatschappelijke ontwrichting/ inzet van hulpdiensten.
Gemeentelijke organisatie	Gemeentelijk calamiteitenteam/ Gemeentelijk crisisteam	Effectbestrijding bij gevolgen binnen gemeentelijke beleidsdomeinen (bijvoorbeeld sociale domein)/gemeentelijke organisatie continuïteit.
Rijksoverheid (Nationaal Cyber Security Centrum (NCSC) en Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)	Nationale crisisbeheersingsstructuur	Effectbestrijding bij bovenregionale effecten

N.B. Na een eerste analyse van welk team of welke teams gealarmeerd zouden moeten worden, controleer of dit ook gebeurd is. Zo niet, zet dit in werking.

Stap 3. Juiste bezetting van het team binnen de gemeenten Amstelveen en Aalsmeer

Zie voor de uitwerking bijlage I.

Daarnaast is de AA-organisatie bezig om afspraken te maken met een externe partij. Dit zal in een aparte notitie worden beschreven.

Stap 4. Vergadering crisisteam

De meeste crisisteams hebben een vaste vergaderagenda. Deze verschilt per gemeente en Veiligheidsregio en crisisteam. Als bijlage I is een conceptagenda opgenomen die gebruikt kan worden bij een cybercrisis, of, indien gewenst, gebruikt kan worden om de reeds bestaande vergaderagenda's aan te passen.

Stap 5. Informatiedeling – Netwerkkaart

In het geval van een digitale verstoring zijn er meerdere partijen die betrokken (kunnen) worden ten behoeve van ondersteuning of waarmee informatie kan worden gedeeld.
Belang van een netwerkkaart is dat die inzicht geeft in de belangrijkste partijen die benaderd kunnen worden of die contact kunnen zoeken. Het is goed om in de beeldvormingsfase op basis van deze netwerkkaart te bepalen welke partijen betrokken en/of geïnformeerd moeten worden.

Stap 6. Oordeels- en Besluitvorming – Checklist sleutelbesluiten

Enkele bestuurlijke dilemma's die tijdens de oordeelsvorming aan bod kunnen komen zijn in de volgende tabel samengevat:

Thema's	**Dilemma**
Maatschappelijke impact en stakeholdermanagement	Welke rol heb je als bestuurder richting maatschappelijke partijen waar de oorzaak van de verstoring ligt, terwijl het openbaar bestuur de maatschappelijk impact moet managen?
Dreiging van escalatie en duiding en communicatie	Cyberincidenten kunnen razendsnel escaleren van dreiging naar crisis. Tegelijkertijd kan een dreiging ook

	een dreiging blijven. Communiceer je over die dreiging of niet?
Techniek en maatschappij	Welke onderdelen van een systeem worden geïsoleerd of uitgeschakeld terwijl ze nog niet geraakt zijn, maar die mogelijk wel geraakt zouden kunnen worden?
Betrouwbare overheid	Wie communiceert er over de crisis en wat is de belangrijkste boodschap? Op welke manier wordt communicatie afgestemd met de direct getroffen organisatie en op welke manier wordt afgestemd met het NKC?
Ketenbetrouwbaarheid	Op welk moment, door wie en wanneer kan worden besloten om systemen weer op te starten zonder 100% garantie dat de keten of het systeem veilig is?
Continuïteit crisisbeheersing (lokaal, regionaal, landelijk)	I. Rolverdeling lokaal bestuur versus driehoek versus Veiligheidsregio. II. Rolverdeling tussen lokaal/regionaal versus landelijk.
Continuïteit dienstverlening	Duur van monitoring van het systeem ten opzichte van vrijgeven van het systeem. Hoe langer je monitort, hoe kleiner de kans op infectie maar hoe hoger de kosten van de verstoring.
Opsporing en vervolging en continuïteit dienstverlening	Vanuit algemeen belang is het onwenselijk om te betalen. Indien opsporing realistisch is zou hier nadruk op moeten liggen. Hiermee wordt het criminele verdienmodel verstoort. Tegelijkertijd ligt er ook een maatschappelijke verantwoordelijkheid bij het openbaar bestuur voor de dienstverlening die het levert.

VIII. Relevante wet- en regelgeving

 # Wet veiligheidsregio's en gemeentewet
Indien zich een cybercrisis voordoet met fysieke effecten op de openbare orde en veiligheid, is er voor de burgemeester een centrale rol weggelegd. Artikel 172, eerste lid, van de Gemeentewet bepaalt namelijk dat de burgemeester belast is met de handhaving van de openbare orde. Een burgemeester kan vanuit zijn rol verschillende verantwoordelijkheden hebben, waaronder als burgemeester van een gemeente en als voorzitter van de veiligheidsregio. Volgens de Wet veiligheidsregio's heeft de burgemeester een aantal bevoegdheden:

- De burgemeester heeft het gezag bij brand alsmede bij ongevallen anders dan bij brand voor zover de brandweer daarbij een taak heeft (artikel 4).
- De burgemeester heeft het opperbevel in geval van een ramp of van ernstige vrees voor het ontstaan daarvan (artikel 5).
- De burgemeester kan de leiding van het ambulancevervoer aanwijzingen geven ten behoeve van de openbare orde (artikel 6).
- De burgemeester is belast met de informatievoorziening tijdens de ramp of crisis (crisiscommunicatie) naar bevolking en hulpverleners (artikel 7).

In het veiligheidsberaad is daarnaast ook gesproken over de rol van de veiligheidsregio's bij digitale ontwrichting. Dit is nog geen vastgestelde landelijke beleidslijn, maar geeft wel een indicatie hoe hier in de veiligheidsregio's naar gekeken kan worden. Met het toenemen van het aantal digitale verstoringen zal deze beleidslijn zich steeds verder uitkristalliseren. 'Aangezien de oorzaak van branden, rampen en crises ook in de digitale omgeving kan liggen, zullen de veiligheidsregio's moeten anticiperen op het voorkomen van digitale ontwrichting dan wel het verklei-nen van de kans erop. De burgemeester heeft een verantwoordelijkheid als het gaat om de verschillende aspecten van de digitale veiligheid van een gemeente of de regio:
• Informatieveiligheid (eigen organisatie).
• Risicoanalyse en -beheersing.
• Openbare orde en veiligheid.
• Bestrijding van digitale criminaliteit.
• Cybergevolgbestrijding.

De gemeente en veiligheidsregio (onder gezag van de burgemeester) hebben bij een digitale verstoring ook de verantwoordelijkheid om burgers te beschermen en voor te lichten. Een burgemeester is echter niet verantwoordelijk voor de verlening van continuïteit binnen vitale sectoren of de aanpak van een cyberincident zelf. Binnen de AA-gemeenten is hiervoor de directie en eventueel de wethouder ICT bestuurlijk verantwoordelijk.

 # Wet beveiliging netwerk- en informatiesystemen (Wbni)
De Wet beveiliging netwerk- en informatiesystemen (Wbni), ook wel de Cybersecuritywet genoemd, en het besluit Bbni is in essentie de Nederlandse implementatie van de Europese richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn), die een hoger niveau van cybersecurity binnen de EU beoogt. De Wbni en bijbehorend besluit regelen onder meer een meldplicht voor vitale sectoren en is dus relevant in het geval een organisatie in één van de aangewezen vitale sectoren geraakt is. Onder de Wbni vallen als (andere aangewezen) vitale aanbieder (AED of AAVA) of digitale dienstverlener (DSP). NCSC geldt volgens de Wbni als het CSIRT voor vitale diensten, de minister van EZK als CSIRT voor de DSP's. Omdat gemeenten en veiligheidsregio's vooralsnog geen vitale aanbieder zijn, kunnen zij tijdens een cybercrisis niet direct gebruik maken van de kennis en expertise van het NCSC. Ook zal de ICT Response Board niet direct worden geactiveerd als er sprake is van een (dreigende) cybercrisis. De gemeente of veiligheidsregio vallen volgens het besluit niet onder de Wbni. Het NCSC attendeert veiligheidsregio's en gemeenten niet direct op risico's en dreigingen, terwijl ze hier vanuit hun wettelijke taak wel een verantwoordelijkheid in hebben. De gemeente kan wel indirect te maken krijgen met de werking ervan, als een organisatie in de vitale sector binnen de gemeente of regio geraakt is. Dan geldt het NCSC als aanspreekpunt.

Omdat het NCSC niet direct verbonden is aan gemeenten, bestaat er de IBD. De IBD is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten en daarmee ook het aanspreekpunt voor cyberincidenten die plaatsenvinden binnen de bedrijfscontinuïteit van gemeenten. De IBD zorgt er daarnaast voor dat kennis over cybersecurity bij de gemeenten onderling wordt gedeeld, maar ook met leveranciers en vitale sectoren. Dit doen zij als schakelpunt naar het NCSC.

 # Politiewet
Volgens de politiewet wordt de taak van de politie als volgt omschreven:

'De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.'

De politie heeft, ter uitvoering van zijn taak, de bevoegdheid om geweldsmiddelen en vrijheidsbeperkende middelen toe te passen (Politiewet 2012, artikel 7). Cybercrime kan de openbare orde en veiligheid verstoren en valt daardoor onder de reguliere opsporingsverantwoordelijkheid van politie en OM. De politie voert deze taak uit middels cybercrimeteams in de eenheden en het THTC. Dit team richt zich op de meest geavanceerde vormen van cybercrime. Daarnaast bestaat er binnen de politie het Landelijk Meldpunt Internet Oplichting en een samenwerkingsverband met banken. De politie voert, vanwege de aard van cybercrime, zijn opsporingstaak uit in samenwerking met andere internationale politieorganisaties (onder andere Europol). Dit doen zij ook in samenwerking met de nationale inlichten- en veiligheidsdiensten.

Voor gemeenten en veiligheidsregio's geldt dat hierin een belemmering bestaat om te handhaven in de online wereld. Het gemeenterecht is geschreven vanuit een offline oogpunt en is dus niet direct toepasbaar in de online wereld. Politie en Openbaar Ministerie zijn de bevoegde organen als het gaat om optreden achteraf. 'Voor bestuursrechtelijk optreden door de burgemeester in zijn hoedanigheid van handhaver van de openbare orde is dan geen ruimte. Wel kan de burgemeester op de hoogte worden gesteld van dergelijke zaken in het driehoeks-overleg, zeker indien de uitingen gepaard gaan met een bedrei-ging van de openbare orde.

 # Wet op de inlichtingen- en veiligheidsdiensten (WIV)
Op 1 mei 2018 is de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) ingegaan, die geldt voor de AIVD en MIVD. De Wiv is een belangrijk instrument om de toenemende dreigingen rondom cyber tegen te gaan. De gemoderniseerde wet vergemakkelijkt onderzoek naar cyberdreigingen en dreigingsbeelden in het cyberdomein. De Wiv maakt het mogelijk om de volgende acties uit te voeren: onderzoeksopdrachtgerichte interceptie (art. 48-50), (2) de hackbevoegdheid (art. 45), (3) het stelselmatig vergaren van gegevens omtrent personen uit open bronnen (art. 38) en (4) de informantenbevoegdheid (art. 39).

'Voor de AIVD en de MIVD is een belangrijke taak weggelegd deze vorm van spionage vroegtijdig te detecteren en waar mogelijk te voorkomen. Om dat mogelijk te maken wordt gezocht naar de kenmerken van ongewenste activiteiten (bijv. signatures van kwaadaardige software) en naar verkeer dat ongebruikelijke afwijkingen vertoont (anomaliedetectie).'

 # Baseline Informatieveiligheid Overheid (BIO)
Overheden hebben een grote verantwoordelijkheid om hun informatievoorziening te beveiligen en veilig te houden. De Baseline Informatiebeveiliging Overheid (BIO) beschrijft de controls en maatregelen die minimaal benodigd zijn om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(systemen) te waarborgen. Hiermee verhogen we de digitale weerbaarheid. Informatiebeveiliging is een proces van plannen, uitvoeren, controleren en bijstellen (Plan-Do-Check-Act). Gemeenten groeien in volwassenheid van informatiebeveiliging. De focus verschuift van reageren op incidenten naar het herkennen en voorkomen van incidenten. Een digitaal weerbare gemeente kan potentiële incidenten vroegtijdig signaleren en de gevolgen ervan beperken, omdat de juiste maatregelen zijn getroffen. Als de basis door implementatie van de BIO op orde is, verhoogt dit de digitale weerbaarheid van gemeenten.

 # Algemene Verordening Gegevensbescherming (AVG)
De Europese Algemene Verordening Gegevensbescherming (AVG) regelt de bescherming van persoonsgegevens en het vrije verkeer van persoonsgegevens binnen de Europese Unie.
De AVG versterkt rechten en plichten rondom privacy en regelt onder meer een meldplicht in geval van datalekken. De verordening geldt voor alle bedrijven en organisaties die zich met persoonsgegevens bezighouden. De AVG is bij een cybercrisis relevant in het geval persoonsgegevens zijn gelekt of gestolen, in het bijzonder de meldplicht datalekken. De getroffen gemeente meldt de datalek bij de Autoriteit Persoonsgegevens.

Telecommunicatiewet

Telecommunicatie is momenteel niet meer weg te denken. Iedereen moet tegenwoordig toegang kunnen hebben tot betrouwbare en moderne telecommunicatie. Om deze groeiende markt te reguleren bestaat de Telecommunicatiewet. Deze wet is gebaseerd op regels van Europese verordeningen en Nederlandse wetten.

De Telecommunicatiewet regelt onder andere:
- frequentiebeleid
- beleid van telefoonnummers
- consumentenbescherming
- privacybescherming.

Voor crisisbeheersing in telecommunicatie speelt de Telecommunicatiewet een belangrijke rol. 'Voor crisisbeheersing ten aanzien van het internet gelden geen bijzondere bepalingen in aanvulling op de algemene regeling in de Telecommunicatiewet. Het aanbieden van internettoegang valt onder 'het aanbieden van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten' in de zin van die wet'.

De Telecommunicatiewet regelt het bevoegd gezag. De minister van EZK is bevoegd om maatregelen jegens de telecomsector te nemen, de minister van J&V jegens computercriminaliteit en persoonlijke levenssfeer en de burgemeester of voorzitter veiligheidsregio alleen ten aanzien van de gevolgen van onbereikbaarheid. De Telecommunicatiewet regelt ook de continuïteit van telecommunicatie. Om de continuïteit van telecommunicatie veilig te stellen stelt artikel 11a. 1 uit de Telecommunicatiewet dat aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten passende technische en organisatorische maatregelen nemen om de risico's voor de veiligheid en de integriteit van hun netwerken en diensten te beheersen. Indien de continuïteit van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten wordt onderbroken geldt dat bij een inbreuk op de veiligheid en/of een verlies van inte-griteit de minister in kennis wordt gesteld.

De Telecommunicatiewet (artikel 14) regelt ook dat in bijzondere omstandigheden de minister van EZK aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten aanwijzingen kan geven om de telecommunicatie van en naar het buitenland te verzorgen (in overeenstemming met de minister van BZ). Ook regelt de wet dat in bijzondere omstandigheden aanwijzingen kunnen worden gegeven aan aanbieders om bij mededelingen van overheidsinstanties om het publiek te waarschuwen voor dreigende rampen of noodsituaties en om de gevolgen van rampen of noodsituaties te verzachten, gebruik te maken van de diensten.

Wet computercriminaliteit

Per 1 maart 2019 is de Wet computercriminaliteit III in werking getreden. Deze wet versterkt de opsporing en vervolging van computercriminaliteit. Hier zijn wijzigingen in het Wetboek van Strafrecht en het Wetboek van Strafvordering aan vooraf gegaan. Politie en Justitie kunnen middels deze wet heimelijk en online onderzoek doen in computers (pc, mobiele telefoon of server). Ook zijn er meer handelingen beschikbaar om onder-zoek te doen naar ernstige delicten. Ambtenaren kunnen bij een zeer ernstig misdrijf gegevens ontoegankelijk maken of kopiëren en als het gaat om een ernstig misdrijf communicatie aftappen of observeren.

Coordinated vulnerability disclosure beleid

Een Coordinated Vulnerability Disclosure (CVD), eerder bekend als Responsible Disclosure, is 'het op een gecoördineerde wijze bekend maken van een kwetsbaarheid') en wordt opgesteld door een organisatie zelf. Een melder maakt in gezamenlijkheid met een organisatie ICT-kwetsbaarheden openbaar. De organisatie waar de kwetsbaarheden zijn aangetroffen hebben in zo een geval tijd om de kwetsbaarheid op te lossen. Het beleid stelt dat er bijvoorbeeld geen aangifte wordt gedaan van inbreuk indien de melder zich aan de spelregels heeft gehouden.
Een CVD helpt de veiligheid van ICT-systemen te vergroten en ICT-kwetsbaarheden eerder te melden om de kans op schade zoveel mogelijk te beperken. De gemeenten Aalsmeer en Amstelveen hebben een CVD gepubliceerd op hun websites.

IX. Opstartinstructie vergaderruimte 24/7

Instructielijst en checklist opstarten kamer 130/131

Activiteit	Actie door
Openstellen raadhuis 24/7 Buiten kantooruren opent de mobiele surveillance van Securitas het raadhuis. Deze kan worden gealarmeerd via de piketambtenaar OOV AM of via piket Vastgoed. ***Procedure alarmeren Securitas*** - De dienstdoende collega OOV AM stemt met de voorzitter van het Gemeentelijk Cybercrisisteam (Vz GCC) af m.b.t. openstellen raadhuis en belt met de alarmcentrale Securitas. - Bericht aan de meldkamer Securitas: Betreft "Assistentie bij Calamiteitendienst", Openen binnen 30min. Verzoeken om een surveillant aan te sturen om het raadhuis Amstelveen te openen binnen een half uur. - De dienstdoende collega OOV AM stemt met Coördinator LCP af om daarnaast contact op te nemen met D&B om 2 medewerkers van D&B te sturen, tot die tijd zal de surveillant Securitas t.p. moeten blijven.	OOV/ Vz GCC
Beveiliging (D&B) ***Afspraken gemeente Amstelveen/D&B Beveiliging m.b.t. ondersteuning*** Bij calamiteiten binnen de gemeente Amstelveen kan besloten worden om in het Raadhuis het Gemeentelijk Cybercrisisteam in te richten. Bij de inrichting van het Cybercrisisteam moeten 2 diensten door D&B Security worden geleverd. D&B levert deze diensten hetgeen betekent dat er tijdens kantooruren 1 en buiten kantooruren 2 extra Security moeten worden ingezet. Deze medewerkers dienen binnen 1 uur na de aanvraag van de dienst inzetbaar te zijn. De medewerkers van de gemeente die in het crisisteam hun werk moeten doen zijn voorzien van een identiteitsbewijs waarmee zij zich kunnen legitimeren. Alleen deze personen worden toegelaten tot het raadhuis. Anderen worden pas toegelaten na ruggespraak met OOVAM en/of de voorzitter van het crisisteam. Bij de inzet van het crisisteam wordt aan de Security een aanspreekpunt en telefoonnummer bekend gemaakt waar zij met vragen terecht kunnen. ***Tijdens kantooruren*** wordt de extra inzet aangevraagd via een adviseur Facilitaire Zaken. ***Buiten kantooruren*** kan door OOV AM of een van de leden van het crisisteam rechtstreeks contact opgenomen worden met D&B Security. Bij een inzet buiten kantooruren zorgen de extra medewerkers van D&B ervoor dat het	OOV/ Vz GCC

Raadhuis na sluiting van het crisisteam, op de gebruikelijke wijze wordt gecontroleerd en afgesloten. Tijdens kantooruren wordt dit door de reguliere middagdienst gedaan.	
Vergaderruimte Kamer 130/131 is aangewezen als vergaderruimte ten tijde van een crisis of groot incident. Haal de sleutel van kamer 130-131 op bij de beveiliging. Vraag naar sleutel nummer 10. • Deze sleutel opent ook de kasten in kamer 130-131. (Is de sleutel niet bij de beveiliging? – heeft iemand deze al opgehaald?)	Allen; De eerste aanwezige krijgt de sleutel mee.
Regelen van koffie, thee, water en eten Broodmaaltijd en/of warme maaltijd bestellen via facilitaire zaken.	Vz GCC
Breng naderhand de sleutel terug bij de beveiliging.	OOVAM/ Vz GCC

X. Relevante gerelateerde documenten

Deze documenten worden allemaal toegevoegd aan de app *CrisisConnect*. Verder zijn ze te vinden op Atlas. Daarnaast liggen ze uitgeprint in de Crisiskamer in het raadhuis van Amstelveen.

Veiligheidsincidenten-procedure
In dit document staat beschreven hoe de AA-organisatie omgaat met veiligheidsincidenten en datalekken, incl. termijnen en meldingen aan derden (AP, IBD etc.)

BIA's
In dit document zijn de Business Impact Analyses (BIA's) opgenomen die de AA-organisatie heeft uitgevoerd. De AA-organisatie voert deze risico-analyses op beschikbaarheid uit op processen (dus niet afdelingen of applicaties)

Continuïteitsplan
In dit document staat beschreven wat ondersteunende afdelingen (kunnen) doen in geval van een crisis. Hierbij gaat het om Facilitaire zaken, Bouwzaken en ICT. Voor ICT staat erin beschreven wat er gebeurt en in welke volgorde als er sprake is van een uitwijk/herstel van de gemeente Amstelveen/Aalsmeer.

Regionaal Crisisplan 2021-2024
Het Regionaal Crisisplan beschrijft de gehele aanpak van alle mogelijke crisissituaties in de Veiligheidsregio, de interregionale samenwerking en samenwerking met het landelijke niveau. In het Regionaal Crisisplan zijn de bevoegdheden, taken en verantwoordelijkheden vastgelegd en afspraken vastgelegd over randvoorwaardelijke processen als alarmering, opschaling, leiding, coördinatie, crisisdiagnose en informatievoorziening.

Draaiboek Lokaal Coördinatiepunt (LCP) Gemeente Aalsmeer-Amstelveen
Dit draaiboek beschrijft op welk moment, op welke wijze en met welke opdracht het gemeentelijk actiecentrum wordt opgestart ter ondersteuning van de gemeentelijke crisisorganisatie binnen de crisistructuur.

Draaiboek Nafase gemeente Aalsmeer-Amstelveen
In dit draaiboek is beschreven op welke wijze de gemeenten Aalsmeer en Amstelveen zich hebben voorbereid op de nazorg na een crisis en hoe de gemeente omgaat met de fase na een crisis. Dit kan betrekking hebben op nazorg na een GRIP-crisis of een crisis waar geen GRIP-opschaling aan vooraf gaat. Het draaiboek bevat een beschrijving van de taken en verantwoordelijkheden, de organisatiestructuur alsmede een invulling op hoofdlijnen van een aantal thema's dat in de nafase aan de orde kan komen.
Toekomst: afspraken/contracten met een externe partij die zal helpen in het geval van een cybercrisis.

XI. Voorwaarden Afdeling A&I

Voorwaardelijke ontwikkeldoelen
Deze (gelaagde) aanpak van cybersecurity vraagt van het Kernteam A&I een stevige ontwikkeling van organisatie- en techniek:

1. Trainen, en opleidingen en coachen van de ICT medewerkers op kennis, vaardigheden, maar ook op verantwoordelijkheid en mandaat
2. Goede voorlichting van procedures en afspraken rond cybersecurity
3. Inplannen van een oefening op gebied van cybersecurity
4. Succesvol afronden van het project ICT informatiebeveiliging, om de technische risico's zo klein mogelijk te maken en een dreiging te beheersen
5. Continueren van gebruikersvoorlichting over cyberrisico's en de acties die gebruiker moet ondernemen in geval van constateren van een dreiging
6. Vooraf contracteren van externe ICT specialisten
7. Inrichten monitor systemen (waaronder SIEM/SOC en externe partijen) voor een snelle en vroegtijdige signalering en vastleggen van opvolgingsafspraken naar ICT specialisten
8. Bellijsten en/of appgroepen samenstellen voor gemeentelijk operationeel team
9. Communicatieplatforms voor crisiscommunicatie aanwijzen (Teams, Telefoon, Whatsapp, CrisisConnectApp)
10. Procedure voor besluitvorming over noodprocedures die grote impact hebben, zoals overgaan tot een uitwijk of het terugzetten van backup, incl. opschalen naar IBD
11. Bereikbaarheid en beschikbaarheid van AA medewerkers na reguliere kantoortijden (piket)

XII. Afkortingenlijst

AED Aanbieder van een essentiële dienst
AIVD Algemene Inlichtingen en Veiligheidsdienst
AP Autoriteit Persoonsgegevens
AVG Algemene Verordening Gegevensbescherming
BT Beleidsteam
BZ Ministerie van Buitenlandse Zaken
CERT Computer Emergency Response Team
CGB Cybergevolgbestrijding
CISO Chief Information Security Officer
CoPI Commando Plaats Incident
CSBN Cybersecuritybeeld Nederland
CSIRT Computer Security Incident Response Team
CVD Coordinated Vulnerability Disclosure
DDoS Distributed Denial of Service
EZK Ministerie van Economische Zaken en Klimaat
FG Functionaris Gegevensbescherming
GBT Gemeentelijk Beleidsteam
GCC Gemeentelijk Cybercrisisteam
GOT Gemeentelijke operationeel team
GRIP Gecoördineerde Regionale Incidentbestrijdings Procedure
IBD Informatiebeveiligingsdienst
ICT Informatie- en communicatietechnologie
ISAC Information Sharing and Analysis Center
LCMS Landelijk Crisis Management Systeem
LOCC Landelijk Operationeel Coördinatiecentrum
MIVD Militaire Inlichtingen- en Veiligheidsdienst
NCC Nationaal Crisiscentrum
NCP-Digitaal Nationaal Crisisplan Digitaal
NCSC Nationaal Cyber Security Centrum
NCTV Nationaal Coördinator Terrorismebestrijding en Veiligheid
OM Openbaar Ministerie
OOV Openbare Orde en Veiligheid
RBT Regionaal Beleidsteam
ROT Regionaal Operationeel Team
SIEM Security Information & Event Management
SOC Security Operations Center
THTC Team High Tech Crime Politie
Wbni Wet Beveiliging Netwerk- en Informatiesystemen
Wiv Wet op inlichtingen en veiligheidsdiensten