Den Haag

Cyber- en IT-crisisplan

Voorbereid op digitale noodsituaties

Inhoud

Voorwoord

Dit cyber- en IT-crisisplan publiceren wij vanuit toewijding en de overtuiging dat transparantie bijdraagt aan een betere digitale weerbaarheid. Binnen de gemeente Den Haag waren er veel uiteenlopende initiatieven om (digitale) incidenten en crises te beheersen, verspreid over de organisatie. De Citrix crisis van 2019 is een van de belangrijke aanleidingen geweest om alle voorbereidingen, maatregelen en activiteiten op het gebied van cyber- en IT-crises gebundeld in een plan samen te vatten. Het plan geeft kort samengevat inzicht in wie wat moet doen tijdens een digitale noodsituatie.

Na enkele jaren ervaring met cyber- en IT-crises, willen wij onze kennis delen met iedereen die eenzelfde uitdaging heeft en op zoek is naar voorbeelden die in de praktijk werken. Niet omdat wij denken dat dit plan het beste antwoord is op hoe een organisatie zich voorbereid op digitale crises, maar om inzicht te geven in onze aanpak. Wij hebben ervaren dat het oplossen van crises ingewikkeld is, maatwerk behoeft en continu aan verandering onderhevig is. De crisisvoorbereidingen en het plan zijn nooit af. Na elke oefening, incident of grote crisis vergaren wij weer nieuwe inzichten die ons beter voorbereiden op de volgende crisis. Dit plan is dan ook slechts een momentopname en zal op het moment van publicatie mogelijk alweer aan verandering onderhevig zijn. Toch vinden wij het belangrijk om het plan te delen om elkaar te helpen inzicht te geven hoe wij ons voorbereiden op digitale crises.

Wij hopen collega's van andere gemeenten of organisaties die zich bezighouden met (digitale) crisisbeheersing te bereiken en hebben twee doelstellingen met deze publicatie:

1. Door middel van het delen van dit plan beogen wij andere organisaties te helpen met het geven van inzicht in hoe een plan voor digitale crisisbeheersing eruit kan zien.
2. De dialoog aan gaan met collega's/lotgenoten over de voorbereiding op digitale crises op basis van dit plan en ook van jullie te leren.

Graag nodigen wij u uit om vragen en verbetersuggesties met ons te delen. Tot slot hopen wij u te inspireren om kennis te blijven delen op het gebied van digitale crisisbeheersing. Zo kunnen wij gezamenlijk de digitale weerbaarheid blijven vergroten.

Jeroen Schipper
Chief Information Security Officer, gemeente Den Haag

Voorjaar 2023

1 Inleiding en reikwijdte

Digitalisering biedt de gemeente en de stad veel kansen. Bijvoorbeeld bij het aanbieden van dienstverlening voor inwoners en bedrijven in de stad, voor het aanjagen van de (digitale) economie, maar ook bij het ontwikkelen van innovatieve projecten op het gebied van zorg.

Naast dat digitalisering veel en diverse kansen biedt, zorgt het echter ook voor nieuwe uitdagingen en afhankelijkheden. De gemeente Den Haag wordt steeds afhankelijker van digitale middelen en daarbij nemen de digitale dreigingen toe. Er zijn in de afgelopen jaren diverse voorbeelden geweest van gemeenten die getroffen zijn door cyberaanvallen, zoals de gemeente Hof van Twente[1] en de gemeente Lochem[2]. Eind 2021 is gemeente Den Haag zelf getroffen door een DDoS-aanval[3]. Bovendien blijkt uit diverse onderzoeken en rapporten dat de meeste organisaties, waaronder gemeenten in Nederland, onvoldoende voorbereid zijn op een digitale crisis[4]. Het is niet te voorkomen dat cyberaanvallen de gemeente Den Haag raken, maar het is wel mogelijk om een cyberaanval snel te herkennen en adequaat en effectief te reageren.

Onder digitale dreigingen vallen ook IT-verstoringen waar geen kwaadwillend handelen aan ten grondslag ligt. Incidenten zoals bijvoorbeeld een brand in een datacenter kunnen uitval van digitale dienstverlening veroorzaken. Een adequate en effectieve reactie is ook op deze digitale crisissen belangrijk.

De gemeente Den Haag bereidt zich daarom continu voor op digitale noodsituaties. In dit cyber- en IT-crisisplan (digitale crisisplan) wordt vastgelegd welke crisisbeheersingsmaatregelen de gemeente Den Haag kan nemen om adequaat te reageren op digitale crises en zo schade te beperken. Dit plan sluit aan bij de structuren en plannen van de bredere en al bestaande crisisbeheersing binnen de gemeente Den Haag.[5]

Reikwijdte cyber- en IT-crisisplan

In dit cyber- en IT-crisisplan worden de organisatie en activiteiten met betrekking tot een digitale crisis respons beschreven die van toepassing zijn op de interne gemeentelijke organisatie en de dienstverlening aan inwoners en de stad. Cyberaanvallen en IT-verstoringen die organisaties binnen de gemeentegrenzen raken, maar dus niet de gemeentelijke organisatie zelf, vallen buiten de reikwijdte van dit plan. Ook valt het organiseren van business continuïteitsmanagement buiten de reikwijdte van dit plan. Tot slot is dit plan uitsluitend gericht op de beheersing van crises waar digitale middelen centraal staan als oorzaak en/of gevolg van de crisis.

1 https://www.rtlnieuws.nl/tech/artikel/5201033/hacker-legt-gemeente-hof-van-twente-plat
2 https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/gemeente-lochem-door-het-oog-van-de-naald-bij-hack-2553
3 https://nos.nl/artikel/2409623-ddos-aanval-op-computersystemen-gemeente-den-haag
4 https://www.binnenlandsbestuur.nl/digitaal/geen-enkele-gemeente-echt-voorbereid-op-een-cybercrisis
5 Vakmanschap in verandering, Gemeentebrede Samenhangende Aanpak Gemeentelijk Team Incidentenbestrijding.

Leeswijzer

In dit cyber- en IT-crisisplan wordt de digitale crisisbeheersingsorganisatie van gemeente Den Haag uiteengezet. In het volgende hoofdstuk worden de relevante beleidsuitgangspunten gekoppeld met dit plan. Vervolgens zal inhoudelijk worden ingegaan op de definiëring van een digitale crisis, de digitale crisisstructuur, de rollen, verantwoordelijkheden en bevoegdheden van de digitale crisisteams, de impact bepaling, de communicatie, op- en afschalen, preparatie nafase, evaluatie en tot slot wordt de borging van dit plan beschreven.

2 Beleidsuitgangspunten en gerelateerde documenten

Dit beleid is gebaseerd op beleidsuitgangspunten die zijn ontleend aan het vigerend Strategisch Beleidskader Informatieveiligheid van gemeente Den Haag, de Baseline Informatiebeveiliging Overheid (BIO) en het NIST Cybersecurity Framework.

Uitgangspunten Strategisch Beleidskader Informatieveiligheid gemeente Den Haag 2019-2022
Binnen de door de gemeente gestelde doelen is nadrukkelijk aandacht voor de impact die de digitalisering op de samenleving heeft. De beschreven veranderingen spelen niet alleen in de stad, maar ook binnen de gemeentelijke organisatie. De gemeente is het dan ook, als stad van vrede, recht en veiligheid, aan haar stand verplicht om haar eigen digitale omgeving goed te beschermen en op dit vlak een voorbeeldrol te vervullen.

Uitgangspunten Baseline Informatiebeveiliging Overheid (BIO) & NIST Cybersecurity Framework
De Baseline Informatiebeveiliging Overheid (BIO) stelt de minimum set aan eisen op het gebied van informatiebeveiliging voor overheden. In de BIO worden in hoofdstuk 16, beheer van informatiebeveiligingsincidenten, diverse maatregelen beschreven.

Het NIST Cybersecurity Framework is een raamwerk waarin de samenhang van de organisatie-doelstellingen en activiteiten en de informatiebeveiliging worden weergegeven. Waaronder het omgaan met digitale incidenten en crises. In het NIST Cybersecurity Framework wordt dit beschreven in de onderdelen Respond & Recover.

De van toepassing zijnde BIO en NIST-normen zijn in bijlage D opgenomen.

Gerelateerde documenten
Het cyber- en IT-crisisplan is het overkoepelende document voor de beheersing van cyber- en IT-crises. Naast het cyber- en IT-crisisplan zijn er diverse documenten die ondersteunend zijn aan een cyber- en IT-crisis. Waaronder scenariokaarten, incidentenprocedures en handboeken.

3 Digitale crisisbestrijdingsprocedure

3.1 Wat is een digitale (Cyber & IT) crisis?

Digitale crisis is de overkoepelende naam voor cyber- en IT-crises. In dit plan wordt een cyber-crisis gedefinieerd als het hoogste escalatieniveau van een informatieveiligheidsgebeurtenis, waarbij kwaadwillend menselijk handelen ernstige schade veroorzaakt via digitale middelen en/of gericht is op digitale middelen of de digitale dienstverlening van de gemeente.

Indien er geen kwaadwillend menselijk handelen van toepassing is, spreekt men van een IT-crisis. Het onderscheid tussen een cyber- en IT-crisis bepaalt de betrokkenheid van security-experts van Expertisecentrum Security in de bestrijdingsprocedure. Dit wordt nader beschreven in paragraaf 3.4.

Niet elke digitale gebeurtenis is een digitale crisis. De drie niveaus in oplopende volgorde van ernst die hiervoor gehanteerd worden zijn; digitale gebeurtenis, digitaal incident en digitale crisis. Voor de leesbaarheid van dit document wordt de term digitale crisis, -incident, -gebeurtenis gebruikt voor zowel cyber- als IT-verstoringen. Deze staan hieronder gedefinieerd.

Wat	Wanneer
Digitale gebeurtenis	Een digitale gebeurtenis is een waarneembare op zichzelf staande gebeurtenis in een informatiesysteem die op een bepaald moment plaatsgevonden heeft. Een digitale gebeurtenis kan onderdeel zijn of leiden tot een digitaal incident of digitale crisis. Zorg dat goed in beeld is of de digitale gebeurtenis niet (potentieel) groter is dan dat het lijkt.
Digitaal incident	Een digitaal incident is een (mogelijke) IT-verstoring in de dienstverlening (beschikbaarheid van systemen of informatie) en/of het ongeoorloofd openbaren, verkrijgen en/of wijzigen van informatie (vertrouwelijkheid of integriteit van informatie of systemen)[6].
Digitale crisis	Een digitale crisis is een ernstig digitaal incident waarbij er een risico is dat de impact grote gevolgen heeft voor de (digitale) dienstverlening, significante schade (fysieke, financiële, imago, bestuurlijk, gezondheid) optreedt en/of geen standaardoplossing bekend is.

3.1.1 Verstoring vs. aanval

De gemeente Den Haag onderscheidt twee type oorzaken voor het uitvallen of veroorzaken van schade aan digitale middelen of dienstverlening van de gemeente. Verstoringen en aanvallen.

Verstoringen

Verstoringen worden veroorzaakt door technische fouten of problemen die geen opzettelijk of kwaadwillend handelen ten oorzaak hebben. Bijvoorbeeld een stroomstoring, problemen bij een leverancier, of het per ongeluk verkeerd uitvoeren van een proces door een persoon.

6 IBD

Aanval
Men spreekt van een aanval wanneer (vermoedelijk) kwaadwillend of opzettelijk handelen ten grondslag ligt aan uitval van of schade aan digitale middelen of dienstverlening. Bijvoorbeeld DDoS- of ransomware-aanvallen en bewuste datalekken met als doel de gemeente schade toe te brengen.

In het geval van verstoringen wordt het Expertisecentrum Security (ECS) weliswaar geïnformeerd, maar zal het initieel niet deelnemen in het crisisteam (CT)[7]. In het geval van kwaadwillend en opzettelijk handelen, of op verzoek van de voorzitter CT in andere gevallen zal security actief deelnemen in het CT.

Uitgebreide opschalingsdocumentatie wordt verder beschreven in het referentiekader opschaling (bijlage B).

3.2 Uitgangspunten van besluiten tijdens een digitale crisis

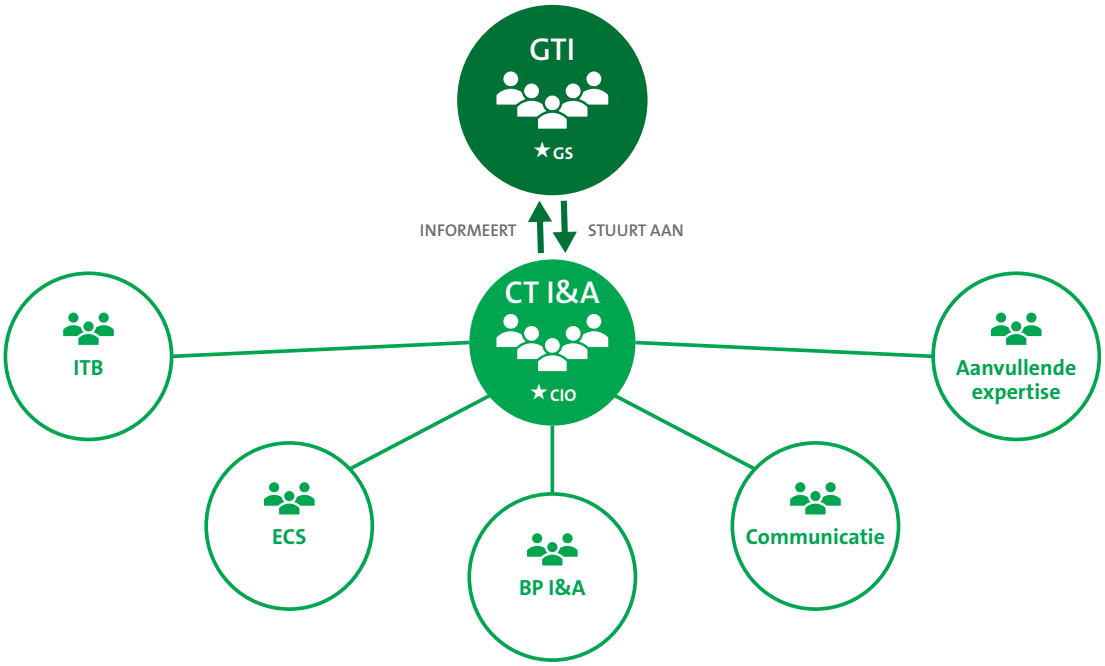
In de benadering van een digitale crisis staat een zestal uitgangspunten centraal bij het maken van beslissingen:

1. De veiligheid van mensen staat voorop.
2. We streven ernaar de betrouwbaarheid van de dienstverlening te herstellen.
3. We zijn transparant over onze crisisbestrijding.
4. Indien nodig, schakelen we z.s.m. specifieke expertise in (intern of extern).
5. We doen aangifte in geval van opzet.
6. We melden aan toezichthouder(s) conform wettelijke en interne eisen/procedures.

Deze uitgangspunten staan aan de basis van het advies en de keuzes die gemaakt worden ten behoeve van het bestrijden en voorkomen van een digitale crisis.

7 Het crisisteam (CT) wordt nader beschreven in paragraaf 3.3

3.3 Digitale crisisstructuur



Bovenstaande afbeelding geeft de digitale crisisstructuur weer van de gemeente Den Haag.

Het Crisisteam Informatisering & Automatisering (CT I&A, hierna afgekort als CT of crisisteam) coördineert de crisisbestrijding met alle relevante stakeholders. Het activeren van het CT gebeurt op het besluit van de Chief Information Officer (CIO die als voorzitter van het crisisteam de beslissingsbevoegde is. Het CT sluit aan op het Gemeentelijk Team Incidentenbestrijding (GTI). Bij de activering van het CT informeert de CIO, de Gemeentesecretaris (GS) als voorzitter van het GTI en de wethouder ICT als bestuurlijk verantwoordelijke.

Centraal in de digitale crisisstructuur staat het crisisteam, dit is het tactische team tijdens een digitale crisis. Indien de potentiële impact hoog/kritiek is, kan de CIO, als voorzitter van het CT, de GS adviseren om het GTI te activeren.
Als het CT wordt geactiveerd, informeert de voorzitter van het CT I&A (de CIO) de voorzitter van het GTI (de GS) en de wethouder ICT als bestuurlijke verantwoordelijke.

Binnen de digitale crisisstructuur is elke relevante stakeholder aangesloten. Iedere stakeholder heeft zijn eigen procedures voor de cyber- IT crisisbestrijding en is daar zelf verantwoordelijk voor. Het Expertisecentrum Security (ECS) vertegenwoordigt de belangen en behoeften vanuit cybersecurity en informatieveiligheid, IT Basisdiensten (ITB) vertegenwoordigt de ICT-dienstverlening, De Businesspartner Informatie en Automatisering (BP I&A) vertegenwoordigt de dienstverlening zelf. Communicatie is verantwoordelijk voor alle interne en externe communicatie. Daarnaast kunnen agendaleden worden gevraagd deel te nemen aan het CT zoals Juridische Zaken, Privacy of externe leveranciers. In Bijlage F is een begrippenlijst met daarin een beschrijving van deze stakeholders beschikbaar.

Hieronder wordt kort beschreven hoe het CT zich verhoudt tot het GTI. Verdere informatie over het GTI en de procedures rondom dit team staan beschreven in het Plan GTI en zullen hier niet volledig worden behandeld.

3.3.1 Gemeentelijk Team Incidentenbestrijding (GTI)

Het GTI komt samen op besluit van de gemeentesecretaris (GS) en is gericht op een gemeentebrede aanpak van incidenten. Het GTI is nadrukkelijk geen crisisorganisatie, maar regisseert en monitort de (samenhang van de) inzet en werkzaamheden van de gemeentelijke diensten conform de organisatie-, informatie en communicatiestructuur om verdere escalatie van een (dreigende) verstoring te voorkomen.

Hieronder volgen de belangrijkste uitgangspunten ten aanzien van de verhoudingen tussen het CT en het GTI.

- Als een digitale crisis een dusdanige impact heeft op de organisatie van de gemeente Den Haag dat burgers en organisaties in belangrijke mate worden getroffen, dan informeert de voorzitter van het CT de GS en zal hij hem adviseren om het GTI bijeen te roepen.
- Wanneer het GTI actief is ten tijde van een digitale crisis worden hier de besluiten met betrekking tot de digitale crisisbestrijding besproken en gemaakt.
- Als bij een andersoortige crisis door het GTI wordt vastgesteld dat er mogelijk ook een IT-verstoring kan plaatsvinden, dan wordt vanuit het GTI top-down het CT I&A geactiveerd. Dit gebeurt door de CIO te benaderen, die vervolgens in overleg met de CISO en/of manager ITB (afhankelijk van de aard van de crisis) besluit in welke vorm en met welke leden het CT geactiveerd wordt.

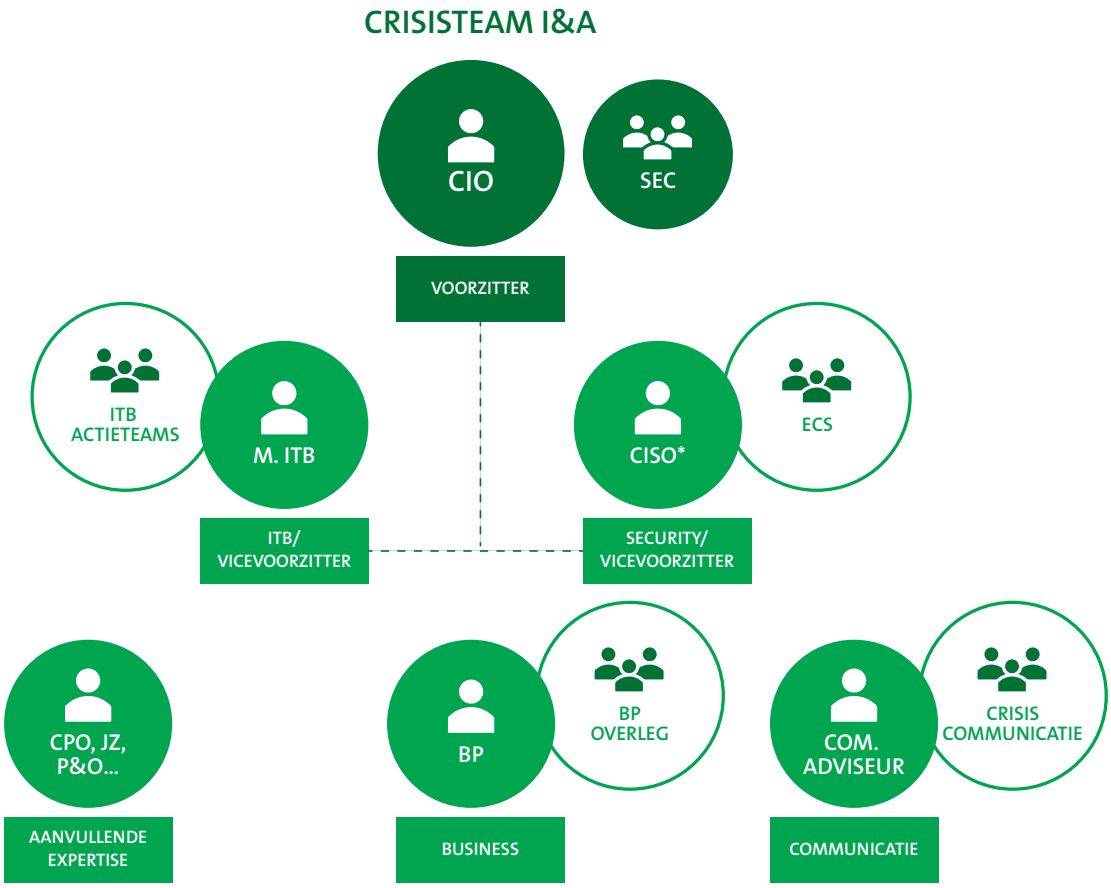
3.3.2 Beslissingsbevoegdheid digitale crisis

Ten tijde van een digitale crisis zijn er twee mogelijke interne beslissingsbevoegden, te weten de CIO en de GS. De eindverantwoordelijkheid ligt altijd bij de GS.

Hoogst actieve crisisteam	Beslissingsbevoegde[8]	Eindverantwoordelijk
Gemeentelijk Team Incidentenbestrijding (GTI)	Gemeentesecretaris (GS)	GS
CT I&A	CIO	GS

8 Met uitzondering van de noodprocedure, zie hoofdstuk 3.7

3.4 Crisisteam Informatisering & Automatisering (CT I&A)



3.4.1 Opzet CT I&A

Het CT is een multidisciplinair team waarin alle relevante stakeholders van een digitale crisis worden vertegenwoordigd door vaste leden en mogelijk aanvullende expertise. De voorzitter van het CT is de Chief Information Officer (CIO). Hij wordt in zijn rol ondersteund door een secretaris. Daarnaast sluiten de manager ITB en de Chief Information Security Officer (CISO) aan als vicevoorzitters. Gezamenlijk bepalen zij vervolgens de verdere bezetting van het CT op basis van de aard, omvang en reikwijdte van de crisis. Deze aanvullende bezetting kan bestaan uit een of meerdere Business Partners (BP), een communicatieadviseur (CA) en eventuele aanvullende experts (intern en extern).

De leden van het CT sturen ieder hun eigen teams aan en halen via die teams ook informatie op om te delen tijdens CT overleggen. De manager ITB stuurt de ITB productteams aan, de CISO stuurt het Expertise Centrum Security (ESC) aan, de Business Partner vertegenwoordigt het Business Partner Overleg en de communicatieadviseur stuurt het crisis communicatie-team aan. Zie de begrippenlijst uit bijlage F voor een nadere toelichting op deze rollen en functies.

Hieronder volgen de belangrijkste uitgangspunten ten aanzien van de samenstelling van het CT.

- De CIO is de voorzitter van het CT. Indien de CIO niet aanwezig is, wordt de voorzittersrol overgenomen door een van de vicevoorzitters (manager ITB/CISO).
- Het CT kan geactiveerd worden door de voorzitter en de vicevoorzitters. Dit gebeurt altijd in onderling overleg, waarbij het zwaartepunt tijdens een IT-crisis bij de manager ITB en de CIO zal liggen en tijdens een cybercrisis bij de CISO en de CIO.

- Bij een cybercrisis is de CISO de vicevoorzitter. Bij elk ander scenario is de manager ITB de vicevoorzitter. Deze rol kan in onderling overleg (af)gewisseld worden.
- Bij het activeren van het CT I&A wordt de voorzitter van het GTI direct geïnformeerd (de GS).
- De leden van het CT vertegenwoordigen elk hun eigen discipline. Zij zijn verantwoordelijk om de acties voor hun eigen discipline bij de juiste stakeholders te beleggen.
  - De manager ITB stuurt de ITB-productteams aan. Dit gebeurt in samenwerking met de aangewezen manager van dienst.
  - De CISO schakelt met het Expertisecentrum Security (ECS) en de Securityketen-partners zoals de IBD, G4, NCSC en externe cybersecuritybedrijven.
  - De BP stuurt zijn collega's aan via het BP-overleg en de onderliggende adviesteams per dienst.
  - De Communicatieadviseur (CA) geeft communicatieadvies aan het CT, coördineert interne en externe communicatieacties en schakelt indien nodig aanvullende expertise in.
- De secretaris komt voort uit de I&A organisatie en is verantwoordelijk voor:
  - Het maken en actueel houden van het informatiebeeld.
  - Het organiseren van de crisisvergaderingen.
  - Het bijhouden van de genomen besluiten.
  - Het bijhouden van welke acties er uitgezet, lopend en afgehandeld zijn en dit centraal en actief communiceren.

3.4.2 Kerntaken

Het CT heeft als kerntaak om inhoudelijk sturing te geven aan de crisisbestrijding. Het doel is om de daadwerkelijke verstoring te verhelpen en de impact van de verstoring zo beperkt mogelijk te houden. De taken van het CT kunnen onderverdeeld worden in de volgende vier thema's.

1. **Impactbepaling:** Het is belangrijk om een helder beeld te krijgen van de waargenomen effecten van de verstoring, maar ook van de dreigende effecten. Binnen het CT zijn de BP en ITB verantwoordelijk voor het bepalen van de impact bij een IT-crisis. Bij een cybercrisis zijn de BP, ITB en het ECS gezamenlijk verantwoordelijk voor het bepalen van de impact.
2. **Impactbeperking:** Het is belangrijk om een overzicht te krijgen van de acties die uitgevoerd kunnen worden om de (mogelijke) effecten van de verstoring te minimaliseren. Binnen het CT is met name de BP verantwoordelijk voor het opstellen en coördineren van de juiste actielijst. Dit gebeurt in samenspraak met het BP-overleg op basis van de Business Continuity plannen van de diensten.
3. **Oplossingsperspectief:** Tijdens een crisis wordt er gekeken naar de aard, oorzaak en scope van de verstoringen, maar bovenal naar wat er nodig is om de getroffen systemen te kunnen herstellen. In het geval een IT-crisis zal ITB dit organiseren, in het geval van een cybercrisis zullen ITB en het ECS hierin samen optrekken.
4. **Besluitvorming:** Op basis van de beschikbare informatie zullen regelmatig knopen doorgehakt moeten worden. De (vice)voorzitters dragen de verantwoordelijkheid voor het nemen van de beslissingen tijdens de crisisbestrijding. Daarnaast zijn zij verantwoordelijk voor het op- en afschalen van de crisisbestrijding.

Per thema zijn een aantal specifieke taken uiteengezet. Deze zijn in aparte tabellen opgenomen in bijlage E.

3.4.3 Informatiestromen en samenwerking

De verschillende relevante stakeholders die betrokken zijn bij de digitale crisis voeden het CT met informatie over de verstoring, zodat acties in de juiste volgorde kunnen worden uitgezet.

Er zijn vier belangrijke lijnen van informatiestromen: **ITB, Security, Business en communicatie**.

- **ITB-lijn:** de manager ITB wisselt informatie direct uit met de aangewezen manager van Dienst. De manager van Dienst staat in direct contact met de product owners van de ITB-productteams.
- **Security-lijn:** de CISO en de Information Security Manager (ISM) wisselen informatie direct uit met het Expertise Centrum Security (ECS).
- **Business-lijn:** de BP die in het CT plaatsneemt, communiceert direct met de overige BPs via het BP-overleg. In dit overleg wordt de samenwerking tussen de BPs en de directies en lijnverantwoordelijken van de verschillende diensten afgestemd.
  - Het is belangrijk dat alle informatie eerst gedeeld wordt met het CT, alvorens er gecommuniceerd wordt richting een sectordirecteur of algemeen directeur.
- **Communicatielijn:** De communicatieadviseur CT is verantwoordelijk voor de coördinatie van informatiestromen op het gebied van communicatie binnen de organisatie ten tijde van de crisis.

Met het oog op snelle en effectieve communicatie, zal er ook buiten het CT om gecommuniceerd worden. Zo zal de manager van Dienst wanneer nodig rechtstreeks schakelen met securityspecialisten en andersom. Het uitgangspunt blijft wel dat alle relevante informatie tijdig in het CT wordt besproken en dat het CT op de hoogte wordt gehouden van relevante overleggen en samenwerkingen om een eenduidig crisisbeeld te behouden.

3.4.4 Communicatieafspraken

Het uitgangspunt van het delen van informatie is dat alle informatie moet bijdragen aan het besluit dat binnen het CT I&A wordt opgesteld. De inhoud van het besluit voldoet minimaal aan een aantal inhoudelijke punten. Dit zijn onder meer de oorzaak, indien bekend, de (mogelijke) impact als systemen getroffen zijn of als wordt besloten systemen uit te schakelen en de hersteltijd -kosten. Dit besluit is als procedure beschreven en is intern beschikbaar voor de digitale crisisorganisatie.

- De voorzitter van het CT beslist vanwege zijn centrale positie tussen de IT en de Business over de definitieve inhoud van het besluit.
- De CISO is verantwoordelijk voor de afstemming met ketenpartners binnen de nationale crisisstructuur (bijv. IBD, NCSC, NCC, NCTV, BZK).
- De communicatieadviseur ondersteunt de interne en externe communicatie (zie 3.6 communicatie).
- De voorzitter van het CT is verantwoordelijk voor de communicatie richting de GS, de sectordirecteuren en de algemeen directeuren van de business. Hij kan er echter voor kiezen om dit (deels) te delegeren aan de BPs.
- De GS bepaalt op welke wijze en frequentie het Gemeentelijke Management Team (GMT) wordt geïnformeerd
- De secretaris informeert het hoger management van de I&A afdeling.

3.5 Opschalen en impact bepaling

Een melding kan via diverse kanalen en bronnen binnenkomen en kan zodoende bij verschillende ontvangers belanden. Bekende bronnen zijn: werknemers, leidinggevenden, directies, leveranciers en partners van de gemeente Den Haag. Bekende ontvangers zijn: de servicedesk (via officiële procedure), adviseurs binnen DBV, de CISO, de Vertrouwde Contactpersoon Informatiebeveiliging (VCIB).

Wanneer een melding potentie heeft om het CT I&A te activeren wordt dit besloten binnen de kernbezetting; de manager ITB, CISO en de CIO. Deze rollen kunnen besluiten tot opschalen.

Meldingsplicht

Om ervoor te zorgen dat meldingen tijdig in beeld komen bij de juiste personen, geldt de volgende meldingsplicht:

- Alle medewerkers zijn verplicht om een potentiële digitale crisis te melden bij de servicedesk volgens de reguliere procedures.
- Alle leveranciers van de gemeente Den Haag dienen een potentiële digitale crisis te melden bij hun vaste contactpersoon.
- Alle partners van de gemeente Den Haag melden een potentiële digitale crisis direct bij het ECS bij de bekende contactpersonen.
- De IBD houdt vast aan de contacten met de VCIB. De VCIB meldt vervolgens het incident volgens de reguliere procedure.

Uitgangspunten opschalen

Aangezien er bij een dreigende digitale crisis geen tijd te verliezen valt, gelden de volgende uitgangspunten voor opschalen:

- Is er potentieel veel schade of dreigen er andere ernstige gevolgen bij niet direct handelen?
  ► OPSCHALEN
- Is er sprake van opzettelijk handelen?
  ► OPSCHALEN

Specifiekere triage met betrekking tot opschaling is beschreven in het referentiekader opschaling in bijlage B.

3.6 Communicatie

3.6.1 Algemene uitgangspunten

Tegenwoordig is veel informatie realtime beschikbaar en zijn mensen via nieuwsapps en social media binnen enkele minuten op de hoogte van rampen en crises. Het is daarom van belang om als de gemeente Den Haag een plan te formuleren met betrekking tot de digitale communicatie ten tijde van een ramp of crises. Communicatie van bestuurders kan immers de samenleving verbinden door een beroep te doen op de veerkracht van individuele burgers en zodoende ook de samenleving als geheel.De volgende uitgangspunten dienen als startpunt van de communicatie van de afdeling I&A.

- Het voornaamste doel is het helder communiceren van en over de crisis.
- Communicatie is omgevingsbewust, proactief, transparant, tijdig en consistent.
- Communicatie is gericht op schadebeperking, door het beantwoorden van de maatschappelijke informatiebehoefte en betekenisgeving.

- Communiceer over het proces: wat is er al bekend en wat nog niet?
- Communiceer over zichtbare maatregelen en indien wenselijk/mogelijk ook over onzichtbare maatregelen.
- Communiceer wat de burger moet doen of laten.
- Communiceer ook wanneer informatie bewust niet gedeeld wordt vanwege veiligheidsoverwegingen. Bijvoorbeeld over technische en operationele kwetsbaarheden en/of maatregelen.
- Communiceer niet over mogelijke oorzaken, duur en omvang, zolang dit niet zeker is, of indien er sprake is van opzettelijk handelen.
- Communiceer niet over slachtoffers, identiteiten, scenario's, of schade.
- Betrek technische experts bij het communicatieproces.

3.6.2 Communicatie afspraken

Tijdens een digitale crises gelden een aantal afspraken met betrekking tot de communicatie.

- Als het GTI het hoogst actieve crisisbestrijdingsteam is, sluit communicatie aan bij het GTI en wordt daar communicatie aangestuurd.
- Als het CT het hoogst actieve crisisbestrijdingsteam is, organiseert de communicatieadviseur van het CT de interne en externe communicatie.
- Communicatie met partners over de inhoudelijke aspecten van de digitale crisis (G4-gemeenten, IBD, NCSC, AIVD, etc.) worden gecoördineerd door het CT.
- De CA kan voor ondersteuning de directie Communicatie & Citybranding (dCC) inschakelen, vanuit daar kan indien nodig een communicatieteam worden geformeerd. De beschrijving en verantwoordelijkheid hiervan ligt buiten de scope van dit plan.
- De verantwoordelijkheid van communicatie over dienst specifieke gevolgen (business impact) van de crisis ligt primair bij de AD/dienst zelf en niet het CT. Het CT richt zich uitsluitend op de communicatie van de oorzaken en de crisisbeheersing van de IT- of cybercrisis.

3.7 Praktische zaken

Hieronder worden een aantal praktische zaken in bulletpoints uiteengezet.

3.7.1 Kernbezetting CT

- De kernbezetting van het CT bestaat uit de CIO, CISO en manager ITB
- De kernbezetting CT wordt ten minste ondersteund door de CA, BP en secretaris.
- De voorzitter van het CT kan besluiten om aanvullende expertise te laten aansluiten bij het CT.

3.7.2 Alarmering kernbezetting:

- De CIO besluit, als voorzitter CT, tot het alarmeren en bijeenkomen van de kernbezetting CT.
- De kernleden van het CT worden geacht binnen een half uur (digitaal) beschikbaar te zijn voor een CT-overleg, binnen kantooruren.
- De ondersteuners van het CT worden geacht binnen een uur (digitaal) beschikbaar te zijn voor een CT-overleg, binnen kantooruren.

3.7.3 Afwezigheid, aflossing en overdracht

- De kernleden en ondersteuners van het CT dienen minimaal twee vervangers te hebben om de rol te kunnen overnemen.
- Indien de inzet en aanwezigheid van de kernbezetting, ondersteuners en opgeroepen specialisten nodig is tot buiten reguliere kantoortijden en langer dan 24 uur, dan moet er nagedacht worden over aflossing en overdracht aan de plaatsvervangers. Bijvoorbeeld, er zijn twee shifts van 12 uur per dag en deze worden afgewisseld door de functionaris en de plaatsvervanger.
- De kernleden en ondersteuners van het CT dragen zelf zorg voor aflossing en overdracht van de eigen rol, maar stemmen dit wel af met de voorzitter van het CT.

3.7.4 Bijeenkomsten en vergaderen CT

- De voorzitter van het CT kan besluiten om fysiek of digitaal te vergaderen, afhankelijk van wat het beste past bij de situatie.
- De secretaris van het CT draagt zorg voor de faciliteiten van het CT.
  - Het digitaal bijeenkomen, wordt georganiseerd via voorbereide digitale middelen.
  - De secretaris richt volgens een vooropgezet stappenplan de digitale omgeving in voor het CT om in te vergaderen en draagt zorg dat alle relevante documentatie beschikbaar is voor de leden van het CT.

3.7.5 Noodprocedure

- Indien er bij een digitale crisis noodzakelijke maatregelen zijn die direct uitgevoerd moeten worden (e.g. het uitzetten van een applicatie), dan is de voorzitter van het CT of diens plaatsvervanger bevoegd om direct te handelen. De voorzitter van het CT is verantwoordelijk voor de communicatie met betrekking tot de noodprocedure naar de beslissingsbevoegde.

3.8 Nazorgfase en evaluatie

In dit hoofdstuk worden drie onderwerpen beschreven, het afschalen, de nazorgfase en evaluatie van de crises. Het doel van dit hoofdstuk is het uiteenzetten van mogelijkheden voor een soepele overdracht van de crisisbeheersingsorganisatie tijdens de crisis naar de nazorgfase.

3.8.1 Besluit tot afschalen

De voorzitter van het hoogste actieve crisisteam maakt het besluit tot afschalen. Op basis van de huidige crisisteams zijn er twee mogelijkheden.

- De GS als voorzitter van het GTI (indien het GTI actief is).
- De CIO als voorzitter van het CT I&A (indien het GTI niet actief is).

3.8.2 Nazorgfase

Na afschalen is het belangrijk dat er een goede overdracht wordt gedaan van het actieve CT naar de verantwoordelijken van de reguliere lijn in de nazorgfase.

- De voorzitter van het CT is verantwoordelijk voor een warme overdracht naar de verantwoordelijken voor de nazorgfase.
- In geval van een digitale aanval is de CIO verantwoordelijk voor het doen van de aangifte namens de gemeente Den Haag.

In bijlage C is een voorbeeld weergegeven van een overdrachtsdocument die kan worden gebruikt voor de overdracht naar de verantwoordelijken van de nazorgfase.

3.8.3 Evaluatie

Om te leren van zowel de oorsprong van de crisis, en ook de handelwijze van de crisisorganisatie tijdens de crisis is het belangrijk om te evalueren.

- De gemeente Den Haag streeft ernaar alle digitale crises te evalueren, waarin het CT geactiveerd is.
- De aard en omvang van de crisis bepalen hoe de evaluatie wordt vormgegeven.
- De voorzitter van het CT kan besluiten om af te zien van evaluatie of om de evaluatie geheim te houden. Reden hiervoor kan zijn dat het handelen van specifieke functionarissen in de evaluatie is opgenomen. Dit besluit dient genomen te worden alvorens het nazorgfase-team aan de slag gaat met de evaluatie.
- Dit besluit moet genomen worden met in acht neming van de Wet Openbaarheid van Bestuur. De voorzitter van het CT wordt daarom geboden om juridisch en bestuurlijk advies in te winnen voor de rechtmatigheid en doelmatigheid van dit besluit.

Evaluatievormen
Interne evaluatie door betrokkenen crisisteam en team nafase zonder bindend advies.
Interne evaluatie met bindend advies.
Externe evaluatie zonder bindend advies.
Externe evaluatie met bindend advies.

4 Borging

In bovenstaande hoofdstukken is de digitale crisisorganisatie beschreven. Een belangrijk element voor de borging van de kwaliteit van de digitale crisisorganisatie is het opleiden, trainen en oefenen van digitale crises met de functionarissen die actief zijn binnen de digitale crisisorganisatie. Het tweede belangrijke element voor de borging is de doorontwikkeling van dit plan. In dit hoofdstuk komen beide onderwerpen aan bod.

4.1 Opleiden, trainen en oefenen

Alle betrokken partijen en leden van actieve crisisteams dienen bekend te zijn met dit plan. Daarvoor is het belangrijk dat zij opgeleid worden, dat zij periodiek trainen op specifieke rollen en dat zij binnen het team periodiek oefenen met een realistisch scenario. De combinatie van de opleiding voor het plan, de training met de rollen en het team en het oefenen met een scenario leidt tot een professionele crisisorganisatie. Het ECS is verantwoordelijk voor het getraind en geoefend houden van de leden van het CT.

- De actieve rollen van het CT dienen opgeleid te worden om de rol binnen de crisisorganisatie professioneel te kunnen uitvoeren.
- Het CT zal ten minste een keer per jaar een digitale crisisrespons oefening doen met een realistisch scenario.
- Er zal minimaal eens per twee jaar een bestuurlijke oefening worden georganiseerd, waarin een digitale crisisrespons wordt geoefend met het bestuur en het CT.

4.2 Borging plan

Jaarlijks dient dit plan te worden herzien en aangepast. Voorgestelde wijzigingen op basis van trainingen, oefeningen en evaluaties na daadwerkelijke inzet, worden voorgelegd aan het ECS.

Bijlage A Onderliggende en gerelateerde documentatie

Relevante gerelateerde documenten:

ID	Titel	Versie
1	Raamwerk Digitale crisisplan gemeente Den Haag	12-11-2020
2	P1 Procedure	01-12-2021
3	Gemeentebrede samenhangende aanpak Gemeentelijk Team Incidentenbestrijding (GTI)	12-10-2020

Bijlage B Referentiekader opschaling

Zodra er binnen de gemeente een vermoeden van een beveiligingsincident is zal dit bij de Servicedesk gemeld worden. De servicedeskmedewerker bepaalt of de melding een beveiligingsincident of een datalek is volgens het 'Prio 1 Procedure' en de Incident Response Procedure. Via andere wegen is het ook belangrijk dat potentiële incidenten en meldingen met opzettelijk of kwaadwillend handelen in het digitale domein worden gemeld bij het expertise centrum security.

Als de melding wordt geclassificeerd als beveiligingsincident met opzettelijk of kwaadwillend handelen komt deze terecht bij het Expertisecentrum Security.

Binnen het ECS wordt bepaald wat de omvang is van de melding aan de hand van vier impact categorieën vanuit het NIST Framework zoals deze worden gebruikt in de crisisprocedure[9] die wordt gebruikt binnen het drie stappenplan:

Drie stappenplan voor opschaling

Om tot een korte en adequate impact bepaling te komen, dienen drie stappen gevolgd te worden:

1. Bepaal de betrouwbaarheid van de melding
2. Bepaal de (potentiële) impact op basis van beschikbare informatie
3. Adviseer en informeer tijdig de juiste personen

1. Bepaal de betrouwbaarheid van de melding

- Controleer of de feiten van de melding kloppen bij de melder
- Vraag door bij onduidelijkheden
- Noteer onzekerheden en aannames
- Vraag een collega om een second opinion.

2. Bepaal de (potentiële) impact op basis van beschikbare informatie

- Bepaal impact op basis van de vier onderstaande categorieën.

Impact op functionaliteit

In welke mate kunnen de diensten van de gemeente nog geleverd worden?

De gemeente kan diensten leveren zonder nadelige gevolgen	Lage impact
Kritieke diensten kunnen geleverd worden maar de effectiviteit is gedaald	Middel impact
De gemeente kan enkele kritieke diensten niet meer leveren aan een groep gebruikers	Grote impact
De gemeente kan een of meerdere kritieke diensten niet meer leveren aan alle betrokkenen	Kritieke impact

9 Zie Incidentenprocedure & https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf p. 32-33. Hieraan is toegevoegd de inschatting van de Schade.

Vertrouwelijkheid

Wat is de vertrouwelijkheid van de informatie in kwestie?

Openbaar	Lage impact
Intern	Middel impact
Vertrouwelijk	Grote impact
Geheim	Kritieke impact

Hersteltijd en kosten

Wat is de hersteltijd en wat zijn de kosten voor herstel met de huidige capaciteit?

Hersteltijden en kosten zijn haalbaar en inzichtelijk met de huidige capaciteit	Lage impact
Hersteltijd en kosten zijn haalbaar en inzichtelijk met inzet van extra interne capaciteit	Middel impact
Hersteltijd en kosten zijn niet inzichtelijk of haalbaar met inzet van extra capaciteit. Externe hulp is nodig.	Grote impact
Hersteltijd en kosten zijn niet bekend.	Kritieke impact

Schade

Welke schade kan het incident veroorzaken?

	Gezondheids-schade	Fysieke schade	Imagoschade	Bestuurlijke schade	Financiële schade
Lage impact					
Middel impact					
Grote impact					
Kritieke impact					

3. Adviseer en informeer tijdig de juiste personen

- Wanneer één van de categorieën op laag komt te staan, is het advies om niet op te schalen.
- Wanneer één van de categorieën op middel komt te staan, is het advies om eventuele opschaling in ieder geval met de CISO en/ of de manager ITB te bespreken.
- Wanneer één van de categorieën op hoog komt te staan, is het advies om eventuele opschaling in ieder geval met de CIO te bespreken.
- Wanneer één van de categorieën op kritiek komt te staan, is het advies om op te schalen naar CT en/ of GTI.

Maak gebruik van de uitgangspunten voor opschaling in het advies. De uitgangspunten voor het opschalen zijn:

- Is er potentieel veel schade of andere ernstige gevolgen bij niet direct handelen? OPSCHALEN
- Is er sprake van opzettelijk handelen? OPSCHALEN?

Bijlage C Overdrachtsdocument nafase

Overdrachtsdocument

In het crisisteam kan een overdrachtsdocument worden gemaakt, die als basis dient voor het team nafase. Dit overdrachtsdocument. Onderwerpen die beschreven staan in het overdrachtsdocument zijn verschillend per crisis, maar kan de volgende onderwerpen bevatten:

Thema's	Acties (voorbeelden)
Informatie en coördinatie	Helder overzicht van stand van zaken van crisis en openstaande actiepunten.
	Officiële overdracht van coördinatie van crisisteam naar team nafase.
	Overzicht impact crisis/ onrust intern en extern
Communicatie	Communicatieplan intern en extern (inclusief mediastrategie)
Herstelwerkzaamheden	Actielijst herstelwerkzaamheden + verantwoordelijken
	Plan van aanpak herstel
Schademanagement	Juridische afwikkeling
	Financiën
Onderzoek en evaluatie	Strafrechtelijk onderzoek?
	Plan van aanpak evaluatie
	Verslaglegging en archivering crisis
Security specifieke nazorg	Indien er sprake is van een cybercrisis zal er in de nazorgfase aandacht besteed moeten worden in het verzamelen en ordenen van het bewijsmateriaal. Het bewijsmateriaal is belangrijk voor de evaluatie van de respons en voor het doen van aangifte.

Bijlage D Normen BIO & NIST CSF

Normen Baseline Informatiebeveiliging Overheid (BIO)

ID	BBN	Verantwoordelijke	Omschrijving
16.1.1	1	Secretaris/Algemeen directeur Proceseigenaar	Verantwoordelijkheden en procedures Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
16.1.2	1	Secretaris/ Algemeen directeur Proceseigenaar Dienstenleverancier	Rapportage van informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
16.1.4	1	Proceseigenaar Dienstenleverancier	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.
16.1.5	2	Proceseigenaar Dienstenleverancier	Respons op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
16.1.6	2	Secretaris/ Algemeen directeur Proceseigenaar Dienstenleverancier	Lering uit informatiebeveiligingsincidenten. Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
16.1.7	2	Secretaris/ Algemeen directeur Proceseigenaar Dienstenleverancier	Verzamelen van bewijsmateriaal. De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

Normen NIST cybersecurity framework (NIST CSF)

RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed
		RS.CO-2: Incidents are reported consistent with established criteria
		RS.CO-3: Information is shared consistent with response plans
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated
		RS.AN-2: The impact of the incident is understood
		RS.AN-3: Forensics are performed
		RS.AN-4: Incidents are categorized consistent with response plans
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained
		RS.MI-2: Incidents are mitigated
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned
		RS.IM-2: Response strategies are updated
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned
		RC.IM-2: Recovery strategies are updated
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed
		RC.CO-2: Reputation is repaired after an incident
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Bijlage E Taken en verantwoordelijkheden matrix Crisisteam I&A

Elk thema bevat een aantal kerntaken die onder een discipline vallen. Hieruit komt naar voren welke rol in het CT I&A verantwoordelijk is voor deze taak.

OPLOSSINGSPERSPECTIEF		
TAAK	DISCIPLINE	PRIMAIR VERANTWOORDELIJK
Achterhalen oorzaak en bron	ITB/SECURITY	MANAGER ITB/CISO
Detecteren en analyseren van het incident.	SECURITY/ITB	CISO
Verzamelen forensisch bewijsmateriaal	SECURITY	CISO
Geraakte processen isoleren van de rest van het gemeentelijk netwerk	ITB/SECURITY	MANAGER ITB
Geven oplossingsperspectief	ITB	MANAGER ITB
Opstellen vernietigingsplan voor onschadelijk maken van de aanval	SECURITY/ITB	CISO
Uitvoeren vernietigingsplan	ITB	MANAGER ITB
Bepalen hersteltijd en kosten	ITB	MANAGER ITB
Uitvoeren Herstelplan	ITB	MANAGER ITB

IMPACTBEPALING		
TAAK	DISCIPLINE	PRIMAIR VERANTWOORDELIJK
Achterhalen geraakte processen	BUSINESS / ITB	BP
In welke mate kunnen de diensten van de gemeente nog geleverd worden?	BUSINESS / ITB	BP
Welke systemen zijn geraakt of kwetsbaar?	BUSINESS / ITB	MANAGER ITB
Welke impact kan het incident veroorzaken voor de dienstverlening?	BUSINESS/SECURITY	BP
Actuele update van aanvalsscope communiceren naar leden CT I&A	SECURITY	CISO

IMPACTBEPERKING		
TAAK	DISCIPLINE	PRIMAIR VERANTWOORDELIJK
Coördineren contact met directie & lijnverantwoordelijken getroffen processen binnen diensten	BUSINESS	BP
Inzichtelijk maken & prioriteren getroffen processen in samenwerking met directie en lijnverantwoordelijken.	BUSINESS	BP

BESLUITVORMING		
TAAK	DISCIPLINE	PRIMAIR VERANTWOORDELIJK
Besluit tot opschaling crisisbestrijding CT	Voorzitter/Vicevoorzitters	CIO (CISO/M. ITB bij afwezigheid CIO)
Besluit tot afschalen crisisbestrijding	Voorzitter/Vicevoorzitters	CIO (CISO/M. ITB bij afwezigheid CIO)
Vaststellen acties CT I&A	Voorzitter/Vicevoorzitters	CIO (CISO/M. ITB bij afwezigheid CIO)

Bijlage F Begrippenlijst

BP	Businesspartner behoudt het contact tussen de verschillende afdelingen en het vakgebied waar die aan verbonden is. Zo is de BP I&A de schakel tussen de verschillende afdelingen binnen I&A en die binnen de dienstverlening. (functionaris)
BP overleg	Periodiek overleg tussen de businesspartners.
CPO	Chief Privacy Officer. Deze functionaris houdt zich bezig met de privacy strategie van de gemeente Den Haag en geeft leiding aan het Expertisecentrum Privacy.
Crisisteam (CT) I&A	Crisisteam Informatisering & Automatisering. Ook wel beschreven als het 'CT'.
Cybercrisis	Het hoogste escalatieniveau van een informatieveiligheidsgebeurtenis, waarbij kwaadwillend menselijk handelen ernstige schade veroorzaakt via digitale middelen en/of gericht is op digitale middelen en dienstverlening van de gemeente.
DBV	Dienst Bedrijfsvoering (gemeentelijke dienst)
directie Communicatie & Citybranding (dCC)	De directie Communicatie en Citybranding is de afdeling die de voert regie over alle gemeentelijke communicatie en daarmee ook de crisiscommunicatie.
Expertisecentrum Security (ECS) Soms verkort tot "Security"	Expertise team binnen de gemeente die zich ontfermt over Informatieveiligheid en Cyber Security. (afdeling)
GMT	Gemeentelijk Management Team (team)
GS	Gemeentesecretaris (functionaris)
GTI	Gemeentelijk Team Incidentbestrijding kan kan worden ingezet bij zowel het afschalen van een crisis door de Veiligheidsregio en de overdracht ervan aan de gemeente als voor andere calamiteiten met een grote impact voor onze stad. (team)
I&A	Afdeling Informatisering & Automatisering.
IBD	Informatiebeveiligingsdienst, sectorale CERT voor gemeenten (extern)
ISM, Information Security Manager	Rol binnen de cybercrisisorganisatie die meerwaarde levert op het gebied van kennis van de organisatie, primaire processen en IT omgeving vanuit een security perpectief. (functionaris)
ITB	IT Basisdiensten is een afdeling binnen Bedrijfsvoering die zich bezighoudt met ICT-dienstverlening (afdeling)
ITB Productteams	IT Basisdiensten is verdeeld in teams met elk een eigen expertise (zoals: Netwerk, Unix, Windows, Databases, enz.) (team)
IT crisis	Zie "cybercrisis", met het verschil dat indien er geen kwaadwillend menselijk handelen van toepassing is, het gedefinieerd wordt als IT-crisis.
JZ	Juridische Zaken (afdeling)
Manager van Dienst	Operationeel aanspreekpunt bij ITB (24x7) (rol binnen ITB)
P&O	Afdeling Personeel en Organisatie.
Security-specialisten	Groep binnen het Expertisecentrum Security: functionarissen met technische kennis van informatiebeveiliging.
Servicedesk	Servicedesk Automatisering
Strategisch Beleidskader Informatieveiligheid gemeente Den Haag	Dit bestuurlijk beleidskader is richtinggevend en kaderstellend voor Informatieveiligheid.
Team Respond	Subteam binnen het Expertisecentrum Security verantwoordelijk voor de ontwikkeling van de cybercrisisorganisatie (team).
Vertrouwde Contactpersoon Informatiebeveiliging (VCIB)	Contactpersoon voor informatie vanuit IBD (Rol)

Colofon

Cyber- en IT-crisisplan
Gemeente Den Haag

Versiebeheer en eigenaarschap
Het voorliggende document betreft versie 1.0. De eigenaar van dit document is de Chief Information Security Officer (CISO) van gemeente Den Haag. Het beheer van dit document berust bij het team Respond van het Expertisecentrum Security van de gemeente Den Haag.

Geldigheid
Dit document is geldig voor een jaar vanaf de datum van vaststelling. Review zal plaatsvinden bij grote relevante wijzigingen op het onderwerp en ten minste jaarlijks na de vaststellingsdatum. Als een nieuw plan binnen deze termijn nog niet is vastgesteld, dan blijft het huidige plan tot dat moment van toepassing.

Beleidshiërarchie
Dit document valt in de categorie tactisch beleid. De vertrouwelijkheid is vastgesteld op classificatie openbaar.
Goedkeuring en opvolging
Dit document is gebaseerd op het interne cyber- en IT-crisisplan en aangepast om openbaar te delen.

Warme documentatie
Na vaststelling en publicatie van dit document wordt het uitgebreid met warme documentatie die operationeel gebruikt kan worden tijdens een incident of crisis. Hierin worden handreikingen opgenomen voor verschillende functionarissen met verschillende onderwerpen.