centrum informatiebeveiliging en privacybescherming

Ketencommunicatie bij Crises

Een handreiking

Maart 2020 [v1.1]

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan echter voorkomen dat er toch sprake is van omissies, onjuistheden, of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag foutmeldingen, commentaar of suggesties.

© Centrum Informatiebeveiliging en Privacybescherming.
Voor dit werk geldt een Creative Commons Naamsvermelding GelijkDelen 4.0 licentie, verleend door het CIP. Zie https://creativecommons.org/licenses/by-sa/4.0/

Titel	Ketencommunicatie bij Crises
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Status	Versie 1.1 Becommentarieerde praktijk
Auteurs en reviewers	Ton Bosman, KvK / Mirjam Deelen, Kadaster / Marthe Fuld, i-Interim Rijk / Jaap Halfweeg, SVB / Margreet Heida, UWV / Elleke Oosterwijk, CIP-UWV / Ad Reuijl CIP-UWV. Versie 1.1 update door CIP
Bijdrage van	
Datum	25-3-2020
Filenaam	Handreiking Ketencommunicatie.docx

Considerans

Met het doel informatie-uitwisseling en kennisdeling te bevorderen wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen uit de CIP-netwerk, maar het kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd. De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de opstellers en deelnemende reviewers en/of het idee dat wat in één organisatie goed werkt, ook voor andere organisaties nuttig kan zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden. CIP heeft categorieën geformuleerd waarmee reikwijdte, intentie, status en/of draagvlak van CIP-publicaties wordt aangegeven. Een nadere uitleg hiervan staat op www.cip-overheid.nl.

De CIP-documenten hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als de besloten community site cip.pleio.nl.

Managementsamenvatting

Vrijwel alle overheidsdienstverlening komt tot stand in ketens en netwerken van organisaties. De betrouwbaarheid van gegevensuitwisseling en in het bijzonder die van de basisregistraties is van groot belang voor die dienstverlening.

Zodra er iets mis gaat, bijvoorbeeld als gevolg van geslaagde hacks, DDOS-aanvallen, maar ook door 'gewone' technische storingen is effectieve (crisis)communicatie noodzakelijk.
Naast deze noodzaak voor communicatie omtrent reële onbeschikbaarheid, ontstaat in het huidige tijdsgewricht met nepnieuws en klankversterking binnen sociale media, toenemende urgentie om communicatie te organiseren ter beheersing van de opiniëring over onze organisaties. Ofwel: crisiscommunicatie is ook nodig wanneer er alleen vermoedens of verdachtmakingen over de organisatie worden geuit.

Als een incident zich voordoet, is het van groot belang een aantal zaken op orde te hebben. Vooral moeten dan de afhankelijkheden tussen systemen en organisaties, die inzicht verschaffen in de consequenties van verstoringen voor ketenpartners, afnemers etc., duidelijk zijn. Daarnaast is het van belang dat de verantwoordelijken voor de (crisis)communicatie binnen de organisaties elkaar snel weten te vinden. Dat gaat altijd gemakkelijker wanneer deze medewerkers elkaar vooraf kennen (en ook samen regelmatig oefenen).

Deze handreiking biedt een generieke opzet voor een ketencrisiscommunicatieprotocol. De organisaties kunnen de handreiking invullen en aanvullen met proces-eigen kenmerken. Zo ontstaat een communicatieprotocol, dat kan worden gebruikt voor de communicatie met keten/netwerkpartners en overige stakeholders. Als alle keten-/netwerkpartners dit hanteren (en er ook mee oefenen), ontstaat grotere transparantie en eenduidigheid in de onderlinge communicatie en in de communicatie met klanten, burgers, media, etc.

Deze handreiking bevat twee niveaus van invulling:

1. Inrichtingsfase. Een invulling van de organisatie-specifieke gegevens (zoals stakeholders, bezetting crisisteam, bereikbaarheidsgegevens, etc.). Deze invulling is nodig voordat ordentelijke ketencommunicatie mogelijk is. Dit onderdeel moet actueel worden gehouden aan de wijzigingen die zich voordoen in de organisaties. Dus periodieke update is vereist.
2. Verrichtingsfase. Aangezien elk incident eigen karakteristieken en een eigen verloop heeft, moet situationeel bepaald worden welke communicatie noodzakelijk is. Voor de invulling op het verrichtings-niveau biedt de handreiking een vraagstructuur met daarin de belangrijkste keuzes die gemaakt moeten worden bij het bepalen van de noodzakelijke communicatie met ketenpartners en overige stakeholders.

NB. De scope van deze handreiking is beperkt tot de communicatieaspecten. Mechanismen die nodig zijn voor de detectie, het bestrijden en oplossen van de incidenten vallen buiten de scope van dit document.

Inhoudsopgave

1 Inrichtingsfase

Voor een effectieve crisiscommunicatie is het nodig een compleet en actueel beeld te hebben bij de volgende onderwerpen.

De primaire processen en informatiesystemen

- Overzicht van systemen die een rol spelen bij de cruciale processen van de organisatie met hun onderlinge samenhang en in- en externe afhankelijkheden.
- Overzicht van belangrijke medewerkers die deze processen goed kennen (met hun contactgegevens tijdens en buiten kantoortijd).
- Business Continuity Plan voor de zekerstelling van de continuïteit van de dienstverlening bij ernstige verstoringen.

Stakeholders en hun rol

Informatie over contactpersonen (contactgegevens zakelijk en privé), communicatie-afspraken, contractuele verplichtingen, etc. m.b.t:

- Keten/netwerkpartners in de dienstverleningsketen.
- Uitbestedingspartners (zoals ICT service providers, websitebeheerders, clouddiensten, telefonie, etc).
- Overige stakeholders (zoals ministerie, Autoriteit Persoonsgegevens, politie en NCSC).

Crisisorganisatie

Informatie over de volgende contactpersonen en/of dienstdoende functies:

- Eindverantwoordelijke voor het crisismanagement.
- Eindverantwoordelijken voor zowel in- als externe communicatie.
- Eindverantwoordelijken voor ICT, Informatieveiligheid en SOC (CIO en CISO).
- Leden crisisteam Businessmanagement eigen organisatie.
- Leden crisisteam ketenpartners.
- Leden crisisteam uitbestedingspartners.

Communicatiekanalen

Per stakeholder een overzicht van de mogelijk in te zetten kanalen.

Monitoring publieke communicatie

De publieke media worden op permanente basis gemonitord op wat er over de organisatie gecommuniceerd wordt. Per kanaal/medium is duidelijk wie daarvoor verantwoordelijk is.
Het betreft in ieder geval:

- De pers.
- Sociale media (zoals Facebook, Twitter, nieuwssites, vloggers/bloggers, etc).
- Nieuwssites.
- Radio/TV.
- Interne websites.

Monitoring beschikbaarheid en veiligheidsincidenten

Met de CIO en de CISO zijn afspraken vastgelegd over de voorwaarden waaronder incidenten worden opgeschaald naar het ketenniveau, en die dus leiden tot communicatie in de zin van het op deze handreiking gebaseerde protocol.

Oefening en actualisering
Minimaal eens per jaar wordt geoefend met crisiscommunicatie, waarbij ook combinaties van stakeholders meedoen. Rond de jaarlijkse oefening wordt ook het protocol geactualiseerd.

NB. Gebruik bijlage I als instrument voor nadere verdieping en invulling voor zover deze informatie al niet voorhanden is in bijvoorbeeld een Business Continuïty Management (BCM) plan.

2 Verrichtingsfase

De noodzaak tot crisiscommunicatie kan worden veroorzaakt door verschillende soorten gebeurtenissen. Afhankelijk van de ernst, de betrokken of geraakte groepen/personen en de fase waarin het inzicht in het probleem zich bevindt, moeten er verschillende accenten worden gelegd en doelgroepen worden benaderd.

Voor het doel van deze handreiking hanteren we de onderstaande onderscheidende kenmerken voor het bepalen van de benodigde communicatie.

Aard van het incident/probleem
- Onthullende of negatieve publieke uitingen over onze organisatie.
- Algemene dreiging voor (ook) onze organisatie.
- Gerichte dreiging/aanval op onze organisatie.
- Incident met onbeschikbaarheid.
- Incident met datalek.
- Incident met manipulatie van (persoons)gegevens.

Zichtbaarheid/merkbaarheid van het probleem
- Binnen de organisatie.
- Bij uitbestedingspartners.
- Bij keten/netwerkpartners.
- Bij klanten/afnemers.
- Bij het publiek.

(Meestal komen combinaties voor van deze groepen).

Mate van inzicht in het probleem/fase probleemanalyse
- Probleem betreft uitsluitend negatieve publiciteit.
- Probleem onduidelijk.
- Probleem duidelijk.
- Oplossing duidelijk.
- Oplossing en evt. herstelacties doorgevoerd.
- Nazorg.

NB. Gebruik bijlage II als instrument om in voorkomende situaties de aard en de doelgroepen van communicatie te bepalen. Deze matrix maakt alle relevante combinaties van de hierboven beschreven kenmerken inzichtelijk en koppelt die aan type communicatie en doelgroepen waarop die gericht kan zijn.

De matrix leent zich ervoor om gedurende het verloop (de 'levenscyclus') van het probleem steeds opnieuw te bepalen welke communicatie nodig is als de situatie verandert.

3 Algemene tips bij mediacommunicatie

In het geval dat communicatie leidt tot interactie met de media, zijn hier nog enkele tips.

- Vraag voordat u contact heeft met de media aan de specialisten in uw organisatie hoe het precies zit.
    - Vraag vooral om het in jip-en-janneke-taal uit te leggen.
    - Vraag naar de realistische risico's (kans en de impact) – zoek uit wat u kunt doen om de gevolgen voor betrokkenen zoveel mogelijk te beperken.
    - Vraag een controle op de feiten indien er al een conceptpersbericht is.
- Wees open en transparant waar mogelijk. Realiseer je dat men veelal ook via andere wegen aan de informatie kan komen.
- Vermijd aantallen en data wanneer deze niet strikt noodzakelijk zijn.
- Vermijd waardeoordelen over situaties – zeg nooit dat het wel meevalt.
- Blijf bij de feiten die verband houden met het specifieke incident.
- Maak het incident niet groter of kleiner door het in verband te brengen met iets anders / groters.
- Vraag bij waardeoordelen of aannames van de ander zo mogelijk door (wat bedoelt u daar precies mee, waar baseert u dat op, wie vindt dat, waaruit blijkt dat)?
- Maak zaken transparant.

Bijlage I: Invulling inrichtingsfase

1. De primaire processen en informatiesystemen

Cruciale informatiesystemen (dan wel applicaties of applicatieclusters) voor de dienstverlening, met hun contactpersonen.

Informatiesysteem	Naam en rol verantwoordelijke	Functie/ bedrijfsonderdeel	Telnrs (werk en privé)	Email adres	Naam vervanger	Telnrs (werk en privé)	Email adres

Ketenafhankelijkheden tussen de processen / informatiesystemen binnen de organisatie.

<hier informatie opnemen over de afhankelijkheden die vitaal zijn voor de goede werking van de gehele dienstverlening van de organisatie>

Business Continuity Plan.

<hier een verwijzing opnemen naar het BCM-plan (dan wel BCM-verantwoordelijke) van de organisatie>

2. Stakeholders

Keten/netwerkpartners (toeleveranciers en afnemers in de dienstverleningsketen)

Keten/netwerkpartner	Naam en rol verantwoordelijke	Functie/ bedrijfsonderdeel	Telnrs (werk en privé)	Email adres	Naam vervanger	Telnrs (werk en privé)	Email adres

Afhankelijkheden bij stakeholders en eisen aan tijdigheid communicatie

<Hier informatie opnemen over de consequenties bij ketenpartners van uitval van onze dienstverlening>

Uitbestedingspartners (leveranciers en dienstverleners waaraan onderdelen van de bedrijfsprocessen zijn uitbesteed).

Uitbestedingspartner	Naam en rol verantwoordelijke	Functie/ bedrijfsonderdeel	Telnrs (werk en privé)	Email adres	Naam vervanger	Telnrs (werk en privé)	Email adres

Overige Stakeholders (toezichthouder, ministerie, etc.)

Overige stakeholders	Naam en rol verantwoordelijke	Functie/ bedrijfsonderdeel	Telnrs (werk en privé)	Email adres	Naam vervanger	Telnrs (werk en privé)	Email adres
Ministerie							
AP							
Politie							
NCSC							
…							
…							

3. Crisisorganisatie

Samenstelling van de crisisorganisatie. NB. Voor telefoonnummers bij voorkeur 06-nummers gebruiken.

Betrokken organisatie-onderdelen in crisisteam	Naam verantwoordelijke	Functie/ bedrijfsonderdeel	Telnrs (werk en privé)	Email adres	Naam vervanger	Telnrs (werk en privé)	Email adres
Teamleiding							
RvB-lid							
Business							
Communicatie							
ICT							
IB&P							
…							

Betrokken keten/netwerkpartners in crisisteam	Naam verantwoordelijke	Functie/ bedrijfsonderdeel	Telnrs (werk en privé)	Email adres	Naam vervanger	Telnrs (werk en privé)	Email adres

Betrokken uitbestedings partners in crisisteam	Naam verantwoordelijke	Functie/ bedrijfsonderdeel	Telnrs (werk en privé)	Email adres	Naam vervanger	Telnrs (werk en privé)	Email adres

In te zetten communicatiekanalen per type stakeholder

Stakeholder	telefoon	Email	brief	nieuwsbrief	social media
Ministerie	x	x	x		
AP	x	x	x		
Politie	x	x			
NCSC	x	x			
...					
...					

4. Monitoring van publieke communicatie

Per medium is duidelijk wie verantwoordelijk is voor het volgen wat over ons in het publieke domein gecommuniceerd wordt.

Soort medium	Naam verantwoordelijke	Functie/ bedrijfsonderdeel	Telnrs (werk en privé)	Email adres	Naam vervanger	Telnrs (werk en privé)	Email adres
Pers							
Social media							
Nieuwssites							
Radio/TV							
Interne websites							

De verantwoordelijke heeft als taak:

- Volgen wat er over ons in de media verschijnt.
- Daarvan periodiek (bijv. wekelijks) een ingedikt beeld te schetsen en te publiceren in de organisatie.
- Bij plotselinge toename van negatieve pers, tussentijds de lijn te informeren/alarmeren.

5. Monitoring van beschikbaarheid en veiligheidsincidenten.

De CIO en CISO dragen de verantwoordelijkheid voor de ICT en Informatiebeveiliging. Logging en Monitoring zijn absolute voorwaarden om problemen tijdig te signaleren en op te lossen.
Dit proces wordt op deze plaats niet verder uitgewerkt.

Met de CIO en de CISO zijn afspraken vastgelegd over de voorwaarden waaronder incidenten worden opgeschaald naar het ketenniveau, en die dus leiden tot communicatie in de zin van dit protocol.

<Hier afspraken vastleggen over condities voor opschaling van incidenten>

6. Oefening

Minimaal eens per jaar wordt geoefend met crisiscommunicatie, waarbij dit protocol wordt gevolgd en ook combinaties van stakeholders meedoen.
Bij deze gelegenheid wordt tevens het protocol weer geactualiseerd. Oefening op een vaste dag in het jaar/kwartaal geeft de meeste kans op succes.

Datum laatste oefening en actualisering: <invullen>
Datum eerstkomende oefening en actualisering: <invullen>

Bijlage II: Invulling verrichtingsfase

Zie op de volgende twee bladzijden welk type communicatie gedaan moet worden:

- aan welke doelgroep;
- in welke fase van de probleemanalyse/het oplossingstraject;
- bij welk type incident.

		Aard incident/probleem					
Zeker of waarschijnlijk zichtbaar/merkbaar bij: (de doelgroepen)	**Mate van inzicht in het probleem / fase probleemanalyse**	**Onthullende of negatieve publieke uitingen over ons**	**Algemene dreiging voor (ook) onze organisatie**	**Gerichte dreiging/aanval op onze organisatie**	**Incident met onbeschikbaarheid**	**Incident met datalek**	**Incident met manipulatie van (persoons)gegevens**
Binnen organisatie	Uitsluitend negatieve publiciteit	Actie 1					
	Probleem onduidelijk	Actie 1	Actie 1	Actie 1	Actie 1	Actie 1	Actie 1
	Probleem duidelijk	Actie 2	Actie 2	Actie 2	Actie 2	Actie 2, 6	Actie 2, 6
	Oplossing duidelijk		Actie 2	Actie 2	Actie 2, 5	Actie 2, 6	Actie 2, 5, 6
	Oplossing en evt herstelacties doorgevoerd		Actie 7	Actie 7	Actie 8, 9	Actie 7	Actie 8, 9
	Nazorg				Actie 10	Actie 10	Actie 10
Bij uitbestedingspartners	Uitsluitend negatieve publiciteit	Actie 1					
	Probleem onduidelijk	Actie 1	Actie 1	Actie 1	Actie 1	Actie 1	Actie 1
	Probleem duidelijk	Actie 2	Actie 2	Actie 2	Actie 2	Actie 2, 6	Actie 2, 6
	Oplossing duidelijk		Actie 2	Actie 2	Actie 2, 5	Actie 2, 6	Actie 2, 5, 6
	Oplossing en evt herstelacties doorgevoerd		Actie 7	Actie 7	Actie 8, 9	Actie 7	Actie 8, 9
	Nazorg				Actie 10	Actie 10	Actie 10
Bij keten/netwerkpartners	Uitsluitend negatieve publiciteit	Actie 1					
	Probleem onduidelijk	Actie 1	Actie 1	Actie 1	Actie 1	Actie 1	Actie 1
	Probleem duidelijk	Actie 2	Actie 2	Actie 2	Actie 2	Actie 2, 6	Actie 2, 6
	Oplossing duidelijk		Actie 2	Actie 2	Actie 2, 5	Actie 2, 6	Actie 2, 5, 6
	Oplossing en evt herstelacties doorgevoerd		Actie 7	Actie 7	Actie 8, 9	Actie 7	Actie 8, 9
	Nazorg				Actie 10	Actie 10	Actie 10
Bij klanten/afnemers	Uitsluitend negatieve publiciteit	Actie 3					
	Probleem onduidelijk	Actie 3	Actie 3	Actie 3	Actie 3	Actie 3	Actie 3
	Probleem duidelijk	Actie 4	Actie 4	Actie 4	Actie 4	Actie 4, 6	Actie 4, 6
	Oplossing duidelijk		Actie 4	Actie 4	Actie 4, 5	Actie 4, 6	Actie 4, 5, 6
	Oplossing en evt herstelacties doorgevoerd		Actie 7	Actie 7	Actie 8, 9	Actie 7	Actie 8, 9
	Nazorg				Actie 10	Actie 10	Actie 10
Bij Publiek	Uitsluitend negatieve publiciteit	Actie 3					
	Probleem onduidelijk	Actie 3	Actie 3	Actie 3	Actie 3	Actie 3	Actie 3
	Probleem duidelijk	Actie 3	Actie 3	Actie 3	Actie 3	Actie 3	Actie 3
	Oplossing duidelijk		Actie 3	Actie 3	Actie 3	Actie 3	Actie 3
	Oplossing en evt herstelacties doorgevoerd		Actie 3	Actie 3	Actie 3, 8	Actie 3, 8	Actie 3, 8
	Nazorg						

Communicatie acties in kernwoorden.	
Actie 1	Informeer de desbetreffende doelgroep met procesinfo over de aanpak van het onderzoek.
Actie 2	Informeer de desbetreffende doelgroep over de inhoudelijk kant. Geef feiten.
Actie 3	Publiceer nieuwsberichten/flitsen in de pers en/of op Sociale Media. Beperk tot procesinfo.
Actie 4	Publiceer nieuwsberichten/flitsen in de pers en/of op Sociale Media. Procesinfo + inhoudelijke feiten. Ook evt. prognose en aankondiging nieuwsupdates
Actie 5	Geef de desbetreffende doelgroep aan hoe zijn in kennis wordt gesteld van hernieuwde beschikbaarheid. Indien voldoende zekerheid over de oplostijd: geeft prognose met slag om de arm.
Actie 6	Als dit nog niet gedaan is: start procedure melding datalek. (bij 'echt'datalek: licht getroffenen in en meld bij AP).
Actie 7	Meld aan desbetreffende doelgroep welke maatregelen zijn getroffen om de dreiging te mitigeren
Actie 8	Meld aan desbetreffende doelgroep dat het probleem is opgelost.
Actie 9	Zonodig: instrueer de doelgroep over specifieke zaken bij het hervatten van het gebruik.
Actie 10	Informeer (evt. bij steekproef) of bij de doelgroep nog onduidelijkheden resteren.