Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoring)

Introductie

De NCTV geeft aan: “Cybersecurity (digitale veiligheid), het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT, is noodzakelijk voor het functioneren van onze sterk gedigitaliseerde samenleving, economie en nationale veiligheid”.[1] Er is sprake van een nationale crisis wanneer een cyberincident een ontwrichtend effect heeft op de samenleving of als één of meer van de vitale belangen wordt aangetast.

Cybergevolgbestrijding behelst alle activiteiten in het kader van bestrijden van de effecten van een incident waarvan de oorzaak en/of gevolg in het digitale domein ligt. Cyber kan als vraagstuk spelen voor:

- de eigen organisatie (continuiteit van eigen kritische processen; bedrijfscontinuiteit)
- de hulpverleningsketen (continuiteit van de hulpverlening)
- de regionale crisisbeheersing (denk aan uitval van vitale infrastructuur: het beheersen van gevolgeffecten en het stimuleren van zelfredzaamheid en samenredzaamheid).

Er zijn verschillende verschijningsvormen van digitale verstoringen (COT, 2017[2]):

Mogelijke effecten van digitale verstoringen zijn:

- reputatieschade oftewel het verlies aan vertrouwen in de berichtgeving van de overheid
- uitval/niet meer beschikbaar zijn van communicatieaccounts (twitter, website, etc.)
- uitval van telefonie
- digitale diefstal van gegevens of het verlies van gegevens
- afpersing (ransomware)
- (langdurige) verstoring van systemen en primaire processen door uitval van computersystemen; dit kan weer leiden tot nevenschade (ketenafhankelijkheid)
- stagneren van dienstverlening of het verlies van productiviteit.

[1] Hoofdstuk 3 Cybersecuritybeeld Nederland CSBN 2018.

[2] https://www.linkedin.com/pulse/de-veiligheidsregio-en-cyberagenda-2017-2020-abderrahman-kaouass/?trk=v-feed

Dit zijn slechts enkele voorbeelden; de grote complexiteit van cyberincidenten en de verwevenheid van het digitale domein met het fysieke domein maken het bepalen van gevolgen van cyberincidenten lastig. Snelle, open, transparante en heldere communicatie kan eraan bijdragen dat de beschadiging van vertrouwen in de overheid en betrokken ketenpartners wordt beperkt en dat verloren vertrouwen wordt hersteld.

Rolverdeling crisiscommunicatie

Uitgangspunt is en blijft dat we vasthouden aan bestaande structuren, rollen en werkwijzen, met oog voor het bijzondere dat een cybercomponent met zich meebrengt. Iedere betrokken partij communiceert vanuit eigen verantwoordelijkheid over eigen onderwerpen, maar stemt centraal af over timing en inhoud van de boodschap.

Nationaal Cyber Security Center (NCSC)	> Vergroten van de digitale weerbaarheid, primair via organisaties binnen de rijksoverheid en vitale processen. Publiek-private samenwerking is uitgangspunt. > Coördinerende rol (op inhoud) bij een nationale cybercrisis in samenwerking met het NCC. > Delen van informatie om de digitale weerbaarheid van Nederland te versterken. > Aanjagen van zelforganisatie door andere partijen, helpen bij het opzetten van samenwerkingsverbanden (bijv. Information Sharing and Analysis Centre (ISAC) en Computer Security Incident Response Team (CSIRT)). > Database beschikbaar stellen met beveiligingsadviezen, factsheets, checklists, handreikingen etc.
NCTV / NCC	> 24/7 beschikbaar voor hulp, vragen en afstemming. > Kan op verzoek van de betrokken regio's een coördinerende rol oppakken richting betrokken veiligheidsregio's en landelijke partners. > Nationaal Kernteam Crisiscommunicatie is actief bij incidenten met effect op nationale veiligheid of met grote maatschappelijke impact[3]. Afstemming met taakorganisatie crisiscommunicatie, lokaal via liaisons over de timing en inhoud van de communicatieboodschap.
Veiligheidsregio	> Afhankelijk van de (verwachte) ernst van de situatie, synchroon of asynchroon opschalen van (onderdelen van) de crisisorganisatie en de crisiscommunicatieorganisatie. > Indien er sprake is van meerdere betrokken veiligheidsregio's en er geen duidelijke aanwijsbare incidentregio is, wordt (in overleg) een coördinerende veiligheidsregio aangewezen, waarbij de communicatieadviseurs van betrokken partners kunnen aansluiten. > Eventueel kan het LOCC-B op verzoek van de betrokken veiligheidsregio's operationeel advies uitbrengen.
Gemeente / Burgemeester	> De burgemeester of voorzitter veiligheidsregio is verantwoordelijk voor de aanpak van de effecten van de verstoring op de openbare orde en veiligheid.
Informatie-beveiligingsdienst voor gemeenten (IBD)	> De Informatiebeveiligingsdienst (IBD) is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten en onderdeel van de VNG. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het NCSC. > Het Computer Emergency Response Team (CERT) van de Informatie-beveiligingsdienst voor gemeenten (IBD) kan de gemeente ondersteuning leveren in geval van (dreigende) incidenten en crisissituaties op het vlak van informatiebeveiliging. > Ook voor woordvoering en communicatieadvies is de IBD 24/7 bereikbaar.

[3] Het NKC is gekoppeld aan opschalen nationale crisisstructuur. Maar afstemming over de communicatie kan natuurlijk in de fase daaraan voorafgaand plaatsvinden via het NCC.

Politie	> De politie is verantwoordelijk voor communicatie over opsporing, indien er sprake is van (verdenking) van moedwillig veroorzaken van een digitale verstoring. Wanneer er een vermoeden is van een mogelijk terroristisch motief, gelden de CTER[4] samenwerkingsafspraken. > De politie is tevens verantwoordelijk voor communicatie over incidenten (met een openbare orde- of opsporingscomponent) die ten gevolge van het cyberincident ontstaan.
Openbaar Ministerie	> Vanaf het moment dat een verdachte wordt voorgeleid aan de rechter-commissaris neemt het OM de woordvoering voor zijn rekening. > Het OM stemt hierover af met de politie en bespreekt dit eventueel in de driehoek en/of op landelijk niveau.
Vitale partners	> Aanbieders van vitale processen in de sectoren energie, drinkwater, keren en beheren, telecom en financiën, als ook de mainports Rotterdam en Schiphol zijn verplicht om ernstige ICT-incidenten in hun vitale processen te melden aan het NCSC[5]. > Aanbieders van vitale processen communiceren via de eigen communicatiemiddelen over de storing, de verwachte duur daarvan, herstelwerkzaamheden en handelingsperspectieven (zie ook Crisiscommunicatietips voor uitval van vitale voorzieningen).
Autoriteit Persoons-gegevens	> Als een datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen, zijn organisaties verplicht om een datalek onverwijld te melden[6].

Doelstellingen crisiscommunicatie

Crisiscommunicatie bij cyberincidenten is voornamelijk gericht op informatievoorziening, het bieden van handelingsperspectief en duiding. Vaak duurt het enige tijd voordat de precieze oorzaak en effecten bekend zijn. In dat geval is het belangrijk om procesinformatie te geven:

1. Wat is er aan de hand?
   - > De (mogelijke) gevolgen van een cyber incident zijn soms (lange) tijd niet of nauwelijks zichtbaar.
   - > Zichtbare gevolgen zijn soms maar het topje van de ijsberg; het kan lang duren voordat de oorzaak van de uitval achterhaald is en in die tijd kunnen zich nog allerlei cascade-effecten voordoen.
   - > Het incident kan zelf de voorbode zijn van iets wat nog moet komen. Het gaat vaak niet om de aardbeving, maar om de tsunami die daarop volgt.
2. Wat is de oorzaak?
   - > Man-made: er is moedwillig een aanval op systemen uitgevoerd. Dit kan vanuit een crimineel of een terroristisch motief zijn. In dat geval komen andere partijen en aspecten in beeld: OM, politie, strafrechtelijk onderzoek, plaats delict.
   - > Technisch. De stroomstoring op Schiphol zorgde voor fysieke problemen omdat ICT-systemen uitvielen en borden met reizigersinfo niet werkten. Hierdoor ontstond voor zowel reizigers als carriers een behoorlijke fysieke chaos.
   - > Natuurlijke oorzaak: een fysiek incident/ natuurlijke oorzaak zorgt voor uitval van systemen. Denk bijv. aan een brand in een datacenter.
   - > Informatie over oorzaak en omvang kun je in een vroeg stadium vaak nog niet geven, wel procesinformatie dat je het nog niet weet.
3. Wat zijn de effecten?
   Een cyberincident kan gevolgen hebben voor:
   - > de eigen organisatie
   - > andere organisaties
   - > de fysieke omgeving

[4] CTER: Contra Terrorisme Extremisme en Radicalisering. Specifiek gelden de afspraken die landelijk en interregionaal zijn gemaakt met betrekking tot leiding en coördinatie, informatiedeling en communicatie bij een dreiging of aanslag.

[5] Bestuurlijke netwerkkaart 21: Telecommunicatie & Cybersecurity

[6] Voor nadere informatie zie ook: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

- vitale processen, dienstverlening
- de samenleving.

4. Hoe lang gaat het duren en wat is het handelingsperspectief?
   Dit kan wisselen per doelgroep en met verloop van tijd.

Doelgroepen

- Interne doelgroepen:
  medewerkers, bestuurders, ICT-professionals, het crisisteam en juristen. Denk ook aan: betrokken leveranciers en andere partijen, getroffen organisaties uit de keten.
- Externe doelgroepen:
  media, publiek, actiegroepen en belangenpartijen.

Communicatiepartners (partijen om mee af te (laten) stemmen)

- Getroffen vitale partner:
  netbeheerder, drinkwaterbedrijf, beheerders van andere vitale processen (bijv. toegang tot internet en betalingsverkeer).
- (Boven)regionale partijen:
  getroffen gemeenten, buurregio's, provincies, waterschappen, meldkamers/alarmcentrales.
- Landelijke partijen (als sprake is van een bovenregionale crisis):
  Ministerie van Justitie en Veiligheid (NCSC, NCC, NCTV, LOCC en met name het Nationaal Kernteam Crisiscommunicatie)

Handelingsperspectieven voor communicatieadviseurs

Hier worden kort de belangrijkste lessen gedeeld met betrekking tot cyberincidenten. De lessen zijn voornamelijk naar voren gekomen uit eigen ervaringen en incidentevaluaties**.**

Risicocommunicatie

- Stimuleer cyberbewustwording, het verhogen van maatschappelijke alertheid en digitale weerbaarheid.
- Maak een onderscheid in doelgroepen: publieke partijen - private partijen - algemeen publiek.
- Gebruik communicatiemateriaal dat door de rijksoverheid gratis ter beschikking wordt gesteld, zoals het logo van AlertOnline, video's, bannermateriaal, posters, etc. Deze zijn te downloaden via https://www.alertonline.nl/toolkit.
- Andere voorbeelden van risicocommunicatie op dit vlak zijn te vinden op:
  - https://crisis.nl/wees-voorbereid/cyberaanval/
  - https://veiliginternetten.nl/
  - https://www.meldknop.nl/
  - https://www.digitaltrustcenter.nl/ (doelgroep ondernemers)

Preparatie op de crisiscommunicatie

1. Zorg voor aansluiting bij de crisiscoördinatiecollega's, die zich met dit type incidenten bezighouden.
2. Zorg (via hen) dat je inzicht hebt (voor zover mogelijk) in de ICT-uitvalscenario's die jouw organisatie/domein zouden kunnen treffen.
3. Zoek uit aan welke specifieke expertise je behoefte hebt, welke kennis je nu mist, wat je nodig hebt om te kunnen communiceren. Crisiscommunicatie bij incidenten met een cybercomponent vraagt meestal om een vertaling van technische termen en uitleg van processen. De vragen van pers en media gaan vaak over technische details, kennis die communicatieadviseurs vaak niet in huis hebben, terwijl de eigen informatiebeveiligers druk zijn met het beheersen van het incident. Zorg daarom waar mogelijk voor een lijstje met externe experts/deskundigen, die het woord kunnen voeren tijdens een incident
4. Zorg ervoor dat je per scenario weet wie je communicatiepartners zijn.
5. Maak goede afspraken over (tijdige) opschaling en de wijze van afstemming.
6. Zorg voor communicatievertegenwoordiging in de crisisteams.
7. Verkrijg inzicht in communicatieve vraagstukken, dilemma's en beslispunten.
8. Beoefen en doorleef de verschillende scenario's.

Crisiscommunicatie tijdens de warme fase

1. Escaleer op tijd en wees snel zichtbaar: ook als je nog niet precies weet hoe het zit, kun je al wel vertellen wat er aan de hand is.
2. Geef procesinformatie: wat zijn we aan het doen, waarom en wanneer verwachten we meer informatie te hebben.
3. Doe geen toezeggingen die je niet kunt nakomen, bijv. zeggen dat de systemen snel weer op orde zullen zijn.
4. Laat de perceptie van de buitenwereld leidend zijn voor je communicatie; maak omgevingsanalyses.
5. Zorg voor een direct lijntje met de juiste communicatiepartners. Maak bijv. meteen een app-groep aan.
6. Zorg voor afstemming op timing en inhoud van boodschappen. Ieder communiceert vanuit de eigen verantwoordelijkheid over eigen onderwerpen, maar stemt af over timing en inhoud en verwijs naar elkaar waar mogelijk.
7. Pas je boodschap aan op je doelgroep; gaat het om een technische professional of een onwetende burger?
8. Maak ingewikkelde informatie toegankelijk; visualiseer of zorg voor woordvoerders die technische informatie kunnen vertalen naar gewone mensentaal.
9. Wees voorzichtig met de term ‘aanval’; spreek liever over digitale verstoring en stem dit af met de betrokken regio’s en partners.

Crisiscommunicatie in (de preparatie van) de nafase

1. Start direct de communicatieve kant van de nafase op. Dit betreft de fase van:
   - verantwoording en schadeafwikkeling: (strafrechtelijk) onderzoek naar oorzaak
   - (politisering van) de schuldvraag: hoe heeft dit kunnen gebeuren en hoe gaan we dit in de toekomst voorkomen?
   - herstel van systemen, schadevergoedingen etc.
2. Beheersen van gevolgen: veranderingen in klantcontacten, reputatieschade, gevolgen voor processen.

Crisiscommunicatiemiddelen

Algemene middelen (afhankelijk van het mandaat):

- Publiek: (crisis)website veiligheidsregio of gemeente(n), crisis.nl (via NCC), Twitter, Facebook, persconferentie burgemeester, publieksinformatienummer, persinformatienummer woordvoerder.
- Intern: intranet, SMS, WhatsApp, LCMS.

Analoge middelen:

- Publiek: geluidswagens politie, fysieke informatiepunten op het gemeentehuis en/of brandweerposten, bewonersbrief, flyer, of een bericht in het lokale weekblad.
- Intern: noodcommunicatievoorziening (NCV), C2000-netwerk, centrale informatiepunten en/of nieuwsbrieven voor medewerkers

Omgang met de media

1. Neem de tijd en geef serieus aandacht aan de vragen van journalisten.
2. Vraag voordat je contact hebt met de media aan specialisten in de organisatie hoe het precies zit.
   - Vraag vooral om het in jip-en-janneketaal uit te leggen.
   - Vraag naar de realistische scenario’s (kans en impact).
   - Vraag een controle op de feiten als er een conceptartikel wordt voorgelegd.
3. Wees open en transparant waar dan kan en besef dat men ook op een andere manier aan de informatie kan komen (een expert die dingen over het incident of de betrokken organisaties beweert, kan erg schadelijk zijn)
4. Vermijd aantallen en data wanneer deze niet strikt noodzakelijk zijn.
5. Vermijd waardeoordelen over situaties; zeg nooit dat het wel meevalt.
6. Houd je aan de feiten die verband houden met het specifieke incident.
7. Maak het incident niet groter door het in verband te brengen met iets anders/groters.
8. Vraag bij waardeoordelen van de ander zo mogelijk door: wat bedoelt u daar precies mee, waar baseert u dat op, wie vindt dat, waaruit blijkt dat?)

Voorbeeldcases

- Fysiek incident met ICT-effect: Vodafonebrand Rotterdam; brand bij dataterminal (april 2012)
- ICT-uitval zonder moedwillig motief maar met fysiek effect: Uitval inchecksystemen Schiphol (april 2018)
- Cyberincidenten met een moedwillig motief en fysiek effect:
  - Aanval NotPetya-malware, waarbij ook twee terminals van de dochteronderneming van het Deense Maersk in de Rotterdamse haven werden getroffen (juni 2017). Volkskrant, Wikipedia
  - Aanval WannaCry (mei 2017)
- Cyberincident in de eigen organisatie
  - Hack bij DigiNotar (juli 2011) Wikipedia, IVenJ
  - Dorifel-virus (augustus 2012)
  - Zware DDoS-aanvallen: wie, wat, waar en waarom? (januari 2018)

Interessante links

IFV

- Crisiscommunicatietips voor uitval van vitale voorzieningen
- Een kennisdossier op IFV Kennisplein is in ontwikkeling.

Ministerie van Justitie en Veiligheid / NCTV en Ministerie van Economische Zaken

- https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html
- https://www.ncsc.nl/
- https://www.alertonline.nl/
- https://veiliginternetten.nl/
- https://crisis.nl/wees-voorbereid/cyberaanval/
- https://www.digitaltrustcenter.nl/

Nationale Politie

- https://veiliginternetten.nl/
- https://www.meldknop.nl/

VNG / Informatiebeveiligingsdienst

- https://www.informatiebeveiligingsdienst.nl/thema/communicatie/
- Factsheet crisiswoordvoering / Leidraad communicatie IBD

Colofon

Instituut Fysieke Veiligheid, april 2019.

Om de publicatie te kunnen blijven ontwikkelen en verbeteren, ontvangen wij graag commentaar en suggesties ter verbetering. Vragen of opmerkingen kunt u sturen naar info@ifv.nl, onder vermelding van ‘Crisiscommunicatietips voor incidenten met een cybercomponent’.

Achtergrondinformatie over crisiscommunicatie is te vinden in het dossier Crisiscommunicatie op www.ifv.nl/kennisplein.

Opdrachtgever : Monique Polder, Portefeuillehouder crisiscommunicatie Landelijk Netwerk Bevolkingszorg
Auteur : Ellis Hazendonk, Svenja Westerduin (NCTV), Susan van Petten (IFV)
Projectleider : Susan van Petten (IFV)
Review : Marije Bakker (IFV), Sanne Kuypers (Politie), Wouter Jong (NGB), Remco Groet (VNG/IBD)