Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

CRISISMANAGEMENT EN CRISISCOMMUNICATIE BIJ DIGITALE INCIDENTEN

MAART 2022

NCSC

Praktische informatie en tips voor crisismanagement en crisiscommunicatie bij digitale incidenten

Alertheid en paraatheid

Inleiding

Digitale incidenten zijn een groot risico voor de maatschappelijke continuïteit. Het NCSC waarschuwt dagelijks voor mogelijk digitale dreigingen en incidenten (zie www.ncsc.nl). Een goede en doordachte voorbereiding is essentieel. Immers, zowel incidenten als de maatregelen hierop kunnen grote impact hebben op de continuïteit van processen en diensten. Een gecoördineerde en goed voorbereide digitale respons moet helpen het risico te beperken.

Dit document draagt bevat praktische informatie voor crisismanagement en crisiscommunicatie om zo de respons bij digitale incidenten zo goed mogelijk te organiseren.

Aandachtspunten

- Het belang van monitoring en het treffen van technische maatregelen zoals geadviseerd
- Om de mogelijke impact te verkleinen is het van belang om ook voorbereidingen te treffen gericht op; de incident respons op een eventuele aanval; het borgen c.q. herstellen van de continuïteit; passende interne en externe communicatie; het bijbehorende crisismanagement
- Naarmate de individuele organisatie er in slaagt de impact te beperken, blijft ook de bredere maatschappelijke impact beperkt. Aanvullend op de tips vanuit het NCSC deelt de NCTV tips over crisismanagement en crisiscommunicatie.

Ieder incident- en crisistype heeft bijzonderheden die van invloed kunnen zijn op de voorbereiding en respons.

Bij digitale crises zijn dit onder meer:

- De snelheid waarmee dergelijke incidenten zich manifesteren;
- door complexe ketenafhankelijkheden kan de bron soms lastig te achterhalen zijn, waardoor respons wordt bemoeilijkt;
- de crisisorganisaties worden zelf mogelijk ook zwaar geraakt in hun functioneren;
- bij de bronbestrijding is de overheid grotendeels afhankelijk van het handelen van private partijen;
- bronbepaling en attributie zijn moeilijk. Het is complex om te bepalen waar een incident vandaan komt, wie er achter een eventuele aanval zit en wat het eventuele doel van de aanval is;
- een incident in de netwerk- en informatiesystemen treft zelden alleen het digitale domein. Vaak treden er ook ongewenste effecten op in het fysieke domein;
- er is mogelijk een tekort aan specifieke deskundigen;
- het mogelijke intensieve en langdurige herstel.

Zie ook het Nationaal Crisisplan Digitaal voor onder meer uitgewerkte scenario's.

VOORBEREID ZIJN

1. Blijf de updates vanuit het NCSC volgen: www.ncsc.nl
2. Ken de eigen technische mogelijkheden en onmogelijkheden in de incidentrespons
3. Zorg dat uw *forensic readiness* op orde is. https://www.ncsc.nl/actueel/weblog/weblog/2021/bent-u-al-klaar-voor-forensic-readiness
4. Ken de bestaande hulplijnen voor de eigen branche/sector (zoals de sectorale CERT's, het Digital Trust Center, etc.) en andere relevante cyberloketten. Ken ook de eventuele meldingsplichten. Een overzicht van de relevante cyberloketten is te vinden op de website van de NCTV: www.nctv.nl/onderwerpen/overzicht-cyberloketten
5. Maak in de eigen organisatie afspraken over escalatiecriteria: van IT naar de crisisorganisatie. Trek samen op in de voorbereiding
6. Doordenk een *best*, *realistic* en *worst case* scenario. Doorleef deze scenario's met sleutelfunctionarissen die een rol kunnen hebben in het incident- en crisismanagement. Denk aan de volgende disciplines: IT, operatie/uitvoering, HR, juridisch, privacy, communicatie en bestuur/directie
7. Bereid mogelijke ingrijpende maatregelen voor: wie neemt het besluit en wat is hiervoor nodig?
8. Denk na over de wijze van organiseren bij een incident of crisis. Zorg voor een goede rolverdeling qua IT respons, omgaan met impact / continuïteit en communicatie. Ken de eigen positie binnen het netwerk en ga na welke eventuele keten-/sectorale afspraken en afhankelijkheden er zijn
9. Verken mogelijke dilemma's: waar kunnen belangen gaan botsen? En hoe hier mee om te gaan (uitgangspunten)?
10. Ga na welke bestaande voorzieningen en plannen er zijn rond continuïteit: bekijk deze door de bril van de huidige kwetsbaarheid. Worden er zaken gemist voor de belangrijkste toepassingen? Zijn er alternatieven?
11. Maak afspraken over bereikbaarheid en beschikbaarheid, ook (of juist) in de vakantieperiode

REAGEREN

1. Bij overwegen van ingrijpender maatregelen: houd oog voor de impact in de keten en informeer partners tijdig
2. Denk bij mogelijke ingrijpende maatregelen ook na over criteria voor het weer beperken of beëindigen van deze maatregelen
3. Houd rekening met de ‘taalbarrière’: terminologie uit de IT wereld is waarschijnlijk minder goed bekend bij anderen en vice versa
4. Benut bestaande crisisvoorbereidingen en ervaren crisisfunctionarissen: ga na wat er ‘bijzonder’ is voor de specifieke situatie en wat dit betekent voor te betrekken functionarissen/te benutten expertise.
5. Meld het incident (o.a. bij NCSC). Doe aangifte. Zie onder andere voor informatie over de politie het overzicht cyberloketten: www.nctv.nl/onderwerpen/overzicht-cyberloketten
6. Let op het welzijn van betrokken professionals en zorg voor goede begeleiding. Ook digitale incidenten kunnen grote impact hebben

CRISISCOMMUNICATIE

Tips voor de voorbereiding

- Maak een overzicht van je communicatiepartners. Deze zijn vaak anders dan bij een fysieke crisis. Wellicht zijn het er meer, vanwege digitale en fysieke effecten.
- Zorg voor aansluiting bij de operationele collega's die zich met digitale incidenten bezig houden.
- Bereid een lijstje met (in-en externe) experts/deskundigen voor die technische informatie kunnen duiden tijdens een incident. Want crisiscommunicatie bij incidenten met een cyber component vraagt veelal om de vertaling van technische termen en uitleg van processen.
- Zoek uit aan welke specifieke expertise je behoefte hebt, welke kennis je nu mist, wat je nodig hebt om te kunnen communiceren.
- Maak goede afspraken over (tijdige) opschaling en wijze van afstemming.
- Zorg voor communicatievertegenwoordiging in de crisisteams van de eigen organisatie.
- Verkrijg inzicht in communicatieve vraagstukken, dilemma's en beslispunten.
- Maak een plan B uitval van digitale communicatiemiddelen.
- Denk na over hoe beeld (visuals, infographics etc.) kan bijdragen om duiding, en handelingsperspectief over vaak ingewikkelde technische materie, begrijpelijk te communiceren.

Aandachtspunten voor crisiscommunicatie bij een digitaal incident

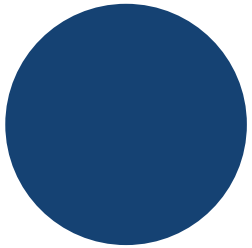
- Denk na over de timing van je boodschap. Breng zoveel mogelijk zelf het nieuws naar buiten.
- Deel wat je al wél weet (procesinformatie) - Cyberanalyses kosten relatief meer tijd dan analyses in de fysieke wereld. Het duurt vrij lang om scenario's te kunnen wegstrepen.
- Beschrijf wat er anders is bij een ICT-crisis:
  - Attributie
  - Analyse / duiding
  - Bestrijden verdere verspreiding (domino-effecten)
  - Zie ook het Nationaal Crisisplan Digitaal
  - Geef zodra het kan een handelingsperspectief
- Visualiseer ingewikkelde technische materie
- Formuleer een kernboodschap. Maak hierbij – indien nodig- je communicatiedilemma's bekend.
- Houd direct rekening met het ergste:
  - Bij uitval van digitale middelen is de maatschappelijke impact / ontwrichting al snel groot.
  - Heb oog voor de mogelijke domino-effecten / cascade effecten. Deze zijn al snel merkbaar.
- Gebruik beeld om je technische verhaal te ondersteunen. Denk hierbij aan visuals en infographics, afgestemd per doelgroep.
- Vergeet interne communicatie niet: ook medewerkers communiceren mogelijk naar buiten/partners.
- Zie ook de Koepelnotitie crisiscommunicatie bij digitale incidenten.

DIGITALE BRONNEN

- Nationaal crisisplan digitaal:
  www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal
- Overzicht cyberloketten:
  www.nctv.nl/onderwerpen/overzicht-cyberloketten
- Evaluatie verslag cyberoefening ISIDOOR:
  Leerpunten cyberoefening ISIDOOR 2021 | Rapport | Rijksoverheid.nl
- Cybersecurity woordenboek:
  https://www.cybersecurityalliantie.nl/ecp_images/2021/05/VCNL-Woordenboek-2eDruk-webversie-Final-2.pdf
- NCSC-website:
  www.ncsc.nl
- Koepelnotitie crisiscommunicatie:
  www.nctv.nl/onderwerpen/crisiscommunicatie/documenten/publicaties/2021/02/23/koepelnotitie-communicatie-bij-digitale-incidenten
- NAC/NCSC webinar masterclass voor crisisbeheersers:
  ISIDOOR 23-03-2021 9:30 (vimeo.com)
- NAC/NCSC webinar masterclass voor cyberspecialisten:
  Isidoor 25-03-2021 14:00 (vimeo.com)
- Digitale overheid:
  Wees voorbereid Toolbox Cyberincident - Digitale Overheid

Escalatieladder digitaal incident

Uw organisatie ervaart een digitaal incident



Effect op digitale organisatie

1. Behoort uw organisatie tot de rijksoverheid of vitale infrastructuur?
   - Nee → U meldt het incident bij uw sectorale CERT
   - Ja → U meldt het incident bij het NCSC
2. Neem contact op met uw IT-leverancier en (eventueel) uw cybersecurity provider
3. Meld het incident bij uw toezichthouder (indien van toepassing) en start aangifte bij de politie.

Effect op continuïteit dienstverlening

1. Informeer uw wettelijk meldpunt (indien van toepassing, bijvoorbeeld conform WBNI)
2. Informeer uw stelselverantwoordelijke partij, beleidsdepartement of DCC
3. Informeer afnemers en leveranciers in uw keten

Effect op fysieke veiligheid & openbare orde

1. Neem contact op met de meldkamer van de hulpdiensten
2. Indien uw organisatie behoort tot de overheid of vitale infrastructuur, contacteer direct de veiligheidsregio
3. Indien uw organisatie behoort tot de (landelijke) crisisorganisatie, contacteer het NCC