Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten

Handreiking

Deel 1: Warme fase

Praktische handvatten tijdens een cybercrisis

Gemeente Amsterdam

Den Haag

Gemeente Rotterdam

Gemeente Utrecht

Openbaar

1 mei 2020

Berenschot

Praktische handvatten bij een cybercrisis

De Handreiking Cybergevolgbestrijding is gericht op ondersteuning van het (verlengd) lokaal bestuur en haar directe adviseurs bij de gevolgbestrijding van een digitale verstoring. De handreiking is daarmee niet gericht op de digitaal specialisten die zich bezighouden met het oplossen van de technische verstoring zelf.

Deel 1 (voorliggend document) van de handreiking heet 'Warme fase' en is bedoeld om tijdens een digitale verstoring snel inzicht te krijgen in de verstoring en het mogelijk maatschappelijk effect daarvan. In deel 2 van deze handreiking, genaamd 'Koude fase', worden de onderdelen uit deel 1 verder uitgewerkt en wordt meer achtergrondinformatie gegeven. Deel 2 is daarmee meer geschikt om te gebruiken in de voorbereiding op een digitale verstoring of als naslagwerk tijdens of na een crisis. Hiernavolgend wordt stap voor stap de start van het crisisbeheersingsproces doorlopen. Een afkortingenlijst bevindt zich aan het eind van het document.

Stap 1. Informatie verzamelen

De eerste vragen bij elke crisis zijn: wat is er aan de hand en welk effect heeft het?

Bij een digitale verstoring is het zinvol om steeds het onderscheid te maken tussen de digitale verstoring zelf en het effect dat deze heeft op het maatschappelijk leven.

Om meer zicht te krijgen op de verstoring en het effect helpt het de volgende vragen te stellen:

VERSTORING

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

EFFECTEN

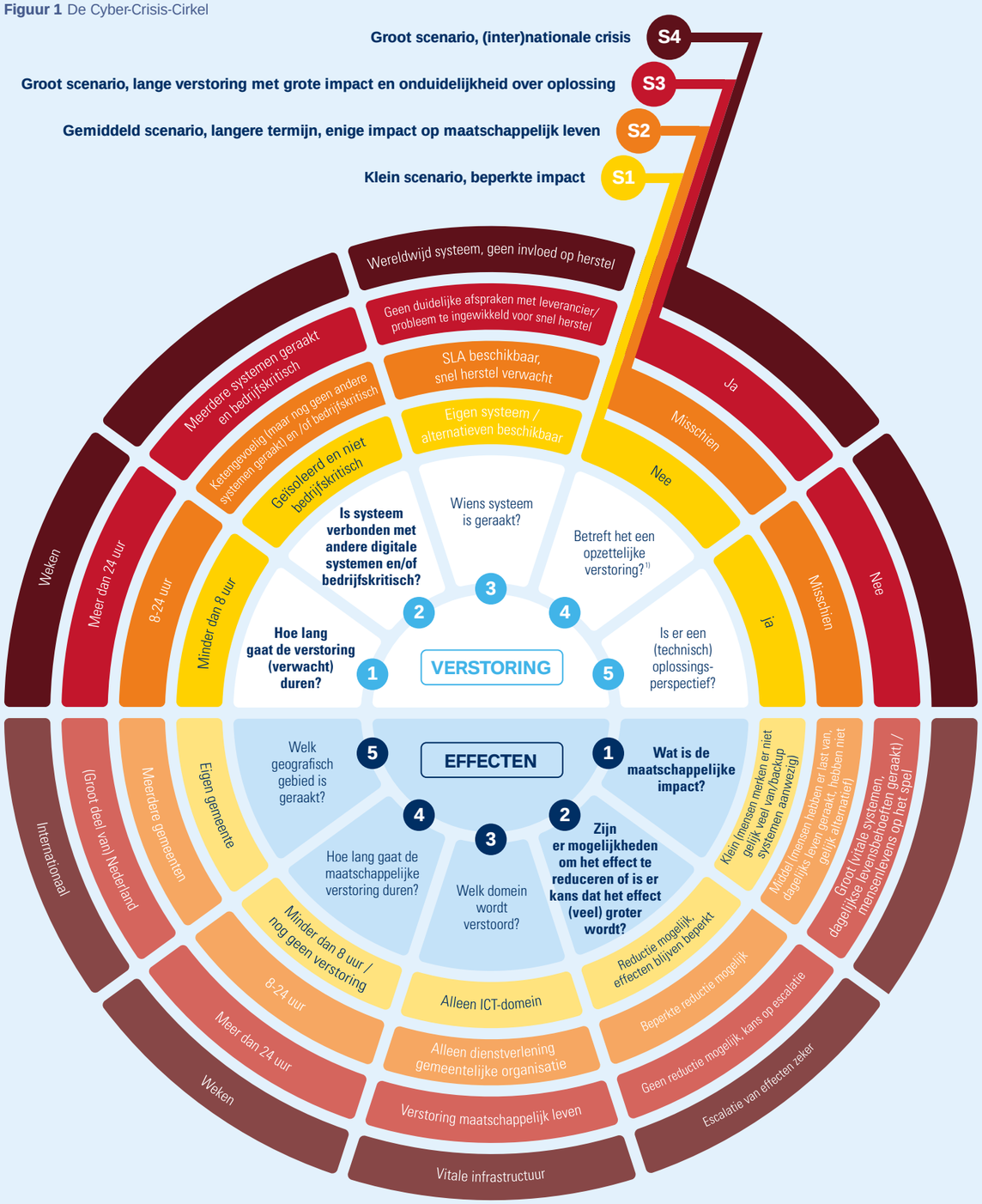
- Welk maatschappelijk domein wordt hiermee verstoord?
- Wat is de maatschappelijke impact?
- Zijn er mogelijkheden om het effect te reduceren of is er kans op escalatie van effecten?
- Hoe lang gaat de maatschappelijke verstoring duren?
- Welk geografisch gebied is geraakt?

De antwoorden op deze vragen zullen in het begin vaak niet aanwezig zijn, of veranderen gedurende de crisis. Het is belangrijk om deze vragen steeds te blijven stellen om dan op basis van de (gewijzigde) antwoorden actie te ondernemen. De antwoorden op deze vragen zijn medebepalend voor de inschatting van de ernst van de crisis. Vragen die niet kunnen worden beantwoord moeten ondertussen als 'uitzoekvragen' uitgezet worden binnen het crisisteam.

De Cyber-Crisis-Cirkel (figuur 1) op de volgende pagina helpt met het inzichtelijk maken van wat de antwoorden betekenen. De cirkel geeft een indicatie van de zwaarte van de crisis (Scenario 1-4) waar je mee te maken hebt.

Of het een klein, gemiddeld, groot of (inter)nationaal scenario is, wordt bepaald door de weging van alle beschikbare bouwstenen. Dat betekent bijvoorbeeld dat in een klein scenario (S1) ook elementen van een zwaarder (S2/S4) scenario kunnen zitten, of dat in een zwaar scenario (bijvoorbeeld S3) ook elementen van een lichter scenario kunnen zitten. De cirkel helpt het team doordat verbanden tussen bouwstenen zichtbaar worden gemaakt die in samenhang inzicht geven in de ernst van de situatie.

Figuur 1 De Cyber-Crisis-Cirkel



1) De politie gaat op voorhand uit van een opzettelijke verstoring tenzij duidelijk is dat dit niet zo is.

Stap 2. Juiste team(s) alarmeren

Tijdens een (cyber)crisis zullen veel mensen bezig zijn met zowel het oplossen van de digitale verstoring als met het beperken van de (maatschappelijke) effecten. We onderscheiden daarbij verschillende teams, met elk hun eigen taken en verantwoordelijkheden.

Voor elk team is het relevant zich de volgende vragen te stellen:

- Waar ben ik verantwoordelijk voor?
- Welke andere teams zijn actief en waar zijn die verantwoordelijk voor?
- Hoe gaan we deze crisis samen (met de andere betrokken teams) zo effectief mogelijk bestrijden?

De belangrijkste afbakening loopt daarbij langs drie lijnen.

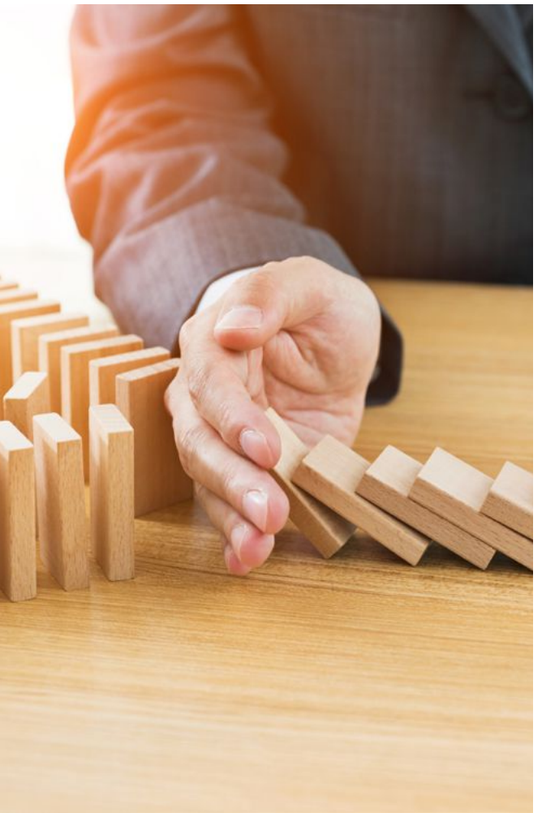
- Wie is eigenaar/gebruiker van het systeem dat verstoord is?
- Waar ligt de bestuurlijke verantwoordelijkheid voor de effectbestrijding?
- Zijn er relevante opsporingsdilemma's ten opzichte van openbare orde?

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

Verantwoordelijke organisatie(s)	Verantwoordelijke team/overleg	Hoofdtaken en verantwoordelijkheden
Eigenaar verstoorde systeem	Incidentmanagementteam	Eventuele aanpassingen aan het systeem, functionerende software.
Bedrijf/ instelling waar digitale systeem is verstoord (gebruiker)	Calamiteitenteam	Oplossen verstoring digitale systeem/ technische oplossing probleem/ bedrijfscontinuïteit.
Gemeente, politie en Openbaar Ministerie	Driehoeksoverleg	Opsporingsvraagstukken en afwegen opsporing versus openbare orde en veiligheid.
Gemeente, Veiligheidsregio	GRIP-structuur (ROT/BT)	Effectbestrijding bij gevolgen voor maatschappelijke ontwrichting/ inzet van hulpdiensten.
Gemeentelijke organisatie	Gemeentelijk calamiteitenteam/ Gemeentelijk crisisteam	Effectbestrijding bij gevolgen binnen gemeentelijke beleidsdomeinen (bijvoorbeeld sociale domein)/gemeentelijke organisatie continuïteit.
Rijksoverheid (Nationaal Cyber Security Centrum (NCSC) en Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)	Nationale crisisbeheersingsstructuur	Effectbestrijding bij bovenregionale effecten.

Tabel 1 Verantwoordelijke teams en overlegstructuren

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



Stap 3. Juiste bezetting van het team

Nu duidelijk is welke (crisis)team(s) betrokken is/zijn, is ook duidelijk wat de scope is van taken en verantwoordelijkheden van het team waar je zelf in zit. Vanuit die scope is het belangrijk om de juiste digitale expertise aan te laten sluiten. Daarbij zijn er enkele aandachtspunten.

Digitale expertise ter ondersteuning van de crisisbeheersing kan verschillende vormen aannemen:

- Kennis van oplossen technisch component(ver)storing.
- Duiden impact technische verstoring op organisatie-processen (bijvoorbeeld gemeentelijke dienstverlening).
- Duiden impact van de verstoring op het maatschappelijk leven.

Kennis van de technische kant van de verstoring zit primair bij de leverancier van het geraakte systeem, deze informatie is vooral relevant voor de teams die zich met het oplossen van de verstoring zelf bezighouden.

Kennis van impact van de technische verstoring op organisatieprocessen zit primair bij de CISO van de geraakte organisatie. Het betrekken van een CISO in het crisisteam kan daarmee beeld- en oordeelsvorming vergemakkelijken. Indien meerdere crisisteams een beroep doen op de CISO helpt het om duidelijk aan te geven welke expertise nodig is en waarom zodat de CISO goede afwegingen kan maken omtrent aanwezigheid en advies.

Kennis van impact van verstoringen op het maatschappelijk leven zit bij de veiligheidsregio's en afdelingen OOV van de gemeenten. Voor het gemak is de checklist bezetting crisisteam cybergevolgbestrijding toegevoegd zodat gelijk duidelijk is of benodigde expertise aan tafel zit (tabel 2).

Rol	Aanwezig en nodig
Voorzitter	
Beslissingsbevoegde verantwoordelijke	.
Informatiemanager	
Secretaris	
Adviseur crisiscommunicatie	
Inhoudelijk deskundige technische verstoring	
Duiden impact technische verstoring op organisatie-processen	
Duiden impact van de verstoring op het maatschappelijk leven	
Inhoudelijk deskundige effect eigen organisatie	
Inhoudelijk deskundige maatschappelijk effect 1	
Inhoudelijk deskundige maatschappelijk effect 2	
Inhoudelijk deskundige maatschappelijk effect x	
Liaison voor verbinding andere teams	
Notulist/plotter	

Tabel 2 Voorbeeld checklist bezetting crisisteam bij cybergevolgbestrijding

Stap 4. Vergadering crisisteam

De meeste crisisteams hebben een vaste vergaderagenda. Deze verschilt per gemeente en veiligheidsregio en crisisteam. Hier volgt een conceptagenda die gebruikt kan worden bij een cybercrisis, of, indien gewenst, gebruikt kan worden om de reeds bestaande vergaderagenda's aan te passen.

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

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

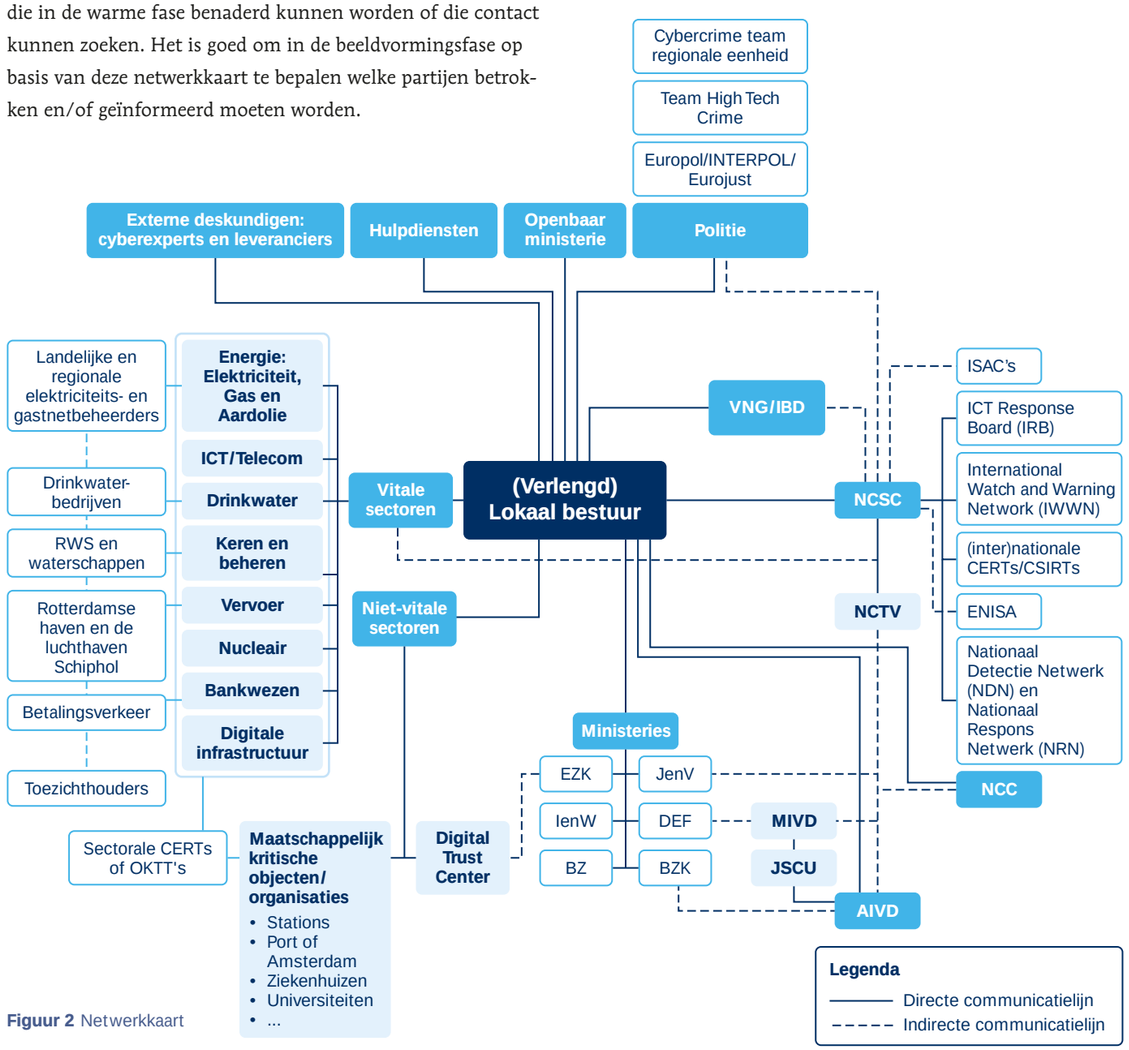
3. Beeldvorming
   - 3.1 Informatiemanager deelt beeld over verstoring en effecten
   - 3.2 Check: welke teams zijn opgeschaald (tabel 1: Verantwoordelijke teams en overlegstructuren en netwerkkaart)
   - 3.3 Check: aanvulling vanuit deelnemers
   - 3.4 Check: de tien vragen uit de Cyber-Crisis-Cirkel (figuur 1): welke blinde vlekken zijn er nog
   - 3.5 Check: wie is verantwoordelijk voor ophalen informatie
   - 3.6 Check: zijn er nog andere crises/ontwikkelingen waar rekening mee gehouden moet worden
   - 3.7 Vat beeld samen
   - 3.8 Apart voor beeld omtrent eigen organisatie verstoring en effecten
   - 3.9 Apart voor beeld omtrent maatschappelijke verstoring en effecten en omgevingsbeeld crisiscommunicatie

4. Oordeelsvorming
   - 4.1 Definieer thema's ter bespreking (tabel 3: strategische/bestuurlijke dilemma's)
   - 4.2 Check met team welke thema's geraakt zijn
   - 4.3 Check welke andere teams ook bezig zijn en hoe de informatie uitwisseling plaatsvindt
   - 4.4 Check waar de maatschappelijke impact het grootst is en prioriteer aandachtsgebieden
   - 4.5 Check welke effecten er zijn op eigen organisatie(continuïteit)
   - 4.6 Bespreek mogelijke escalatiescenario's/gebruik hierbij de tien vragen uit de Cyber-Crisis-Cirkel (figuur 1)
   - 4.7 Identificeer welke maatregelen vanuit dit team hierop genomen kunnen worden en wie dat doet
   - 4.8 Check welke bestuurlijke besluiten/ dilemma's relevant zijn

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

Stap 5. Informatiedeling - Netwerkkaart

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



Figuur 2 Netwerkkaart

In het midden van de netwerkkaart staat (Verlengd) Lokaal bestuur. Deze handreiking is bedoeld voor het lokaal bestuur (en haar directe adviseurs), lokale bestuurders zijn daarbij verantwoordelijk voor crisisbeheersing in hun gemeenten en de gemeenschappelijke regelingen waaraan zij deelnemen als verlengd lokaal bestuur. In de netwerkkaart is bij vitale sectoren gekozen voor die sectoren die zijn aangewezen als vitale sectoren onder de Wet Beveiliging Netwerk- en Informatiesystemen.

Stap 6. Oordeels- en Besluitvorming - Checklist sleutelbesluiten

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

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

Tabel 3 Strategische/bestuurlijke dilemma's

Vanuit de hiervoor genoemde dilemma's kunnen enkele sleutelbesluiten worden geïdentificeerd. Hierbij kan onderscheid gemaakt worden tussen inhoudelijke besluiten en procesbesluiten. Inhoudelijke besluiten zijn gericht op het effect van de crisisbeheersing. Procesbesluiten zorgen ervoor dat de crisisbeheersing niet hapert.

Mogelijk inhoudelijke besluiten:

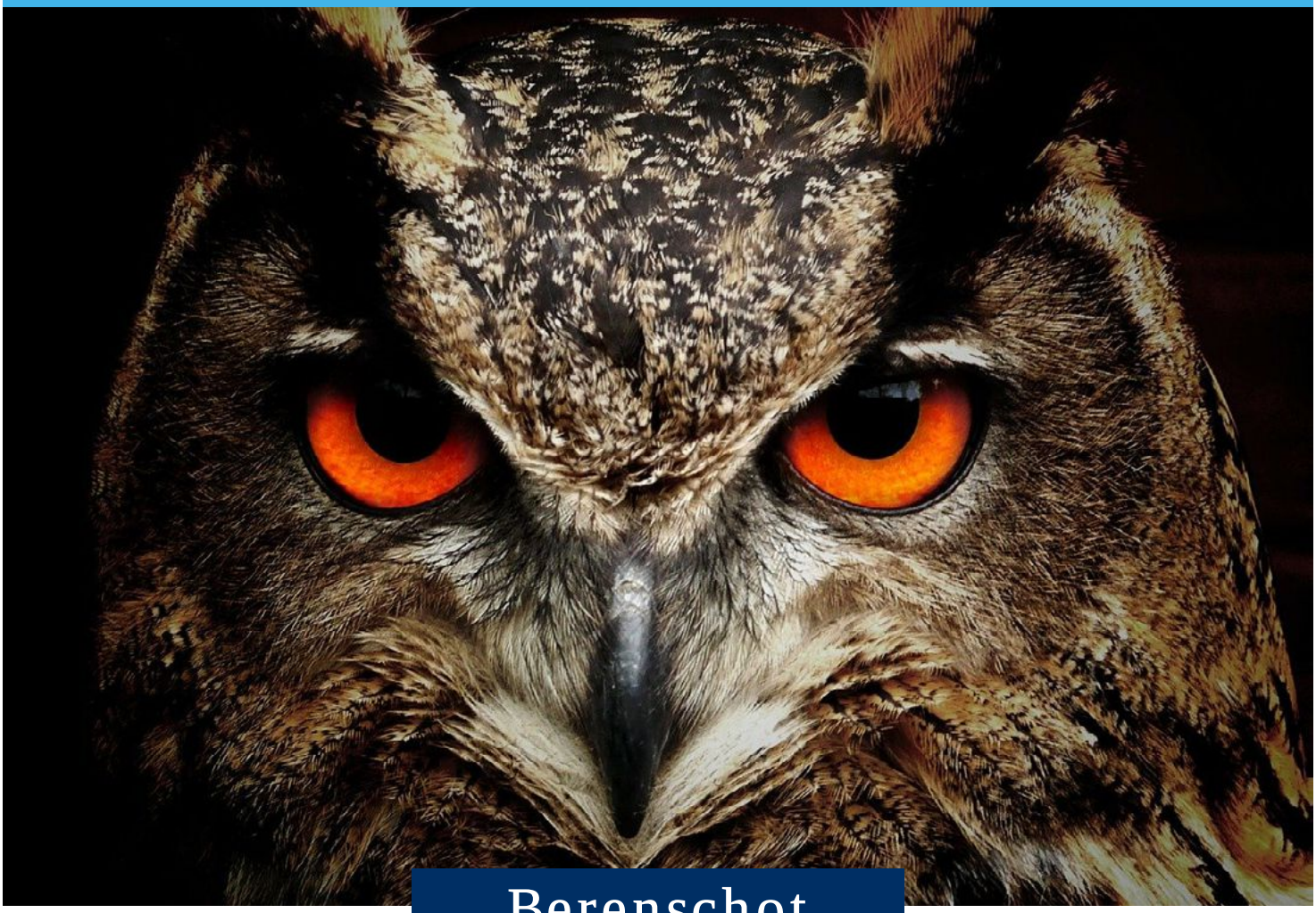
- Bij ransomware: wel of niet betalen van het losgeld (kan onder andere effect en effectduur beïnvloeden).
- Inhuur: inschakelen forensische experts en digitale experts van buiten (kostenpost, capaciteit beperkt).
- Vrijgeven systeem: duur van monitoring van het systeem na infectie ten opzichte van het vrijgeven van het systeem. Dit speelt niet als de organisatie 24-uurs monitoring al heeft ingeregeld via SOC-SIEM.
- Uitschakelen (nog niet getroffen) systemen: uitschakelen van systemen en/of applicaties waardoor bepaalde bedrijfsprocessen stilvallen met als doel isolatie, maar met als gevolg onduidelijke keteneffecten (het uitschakelen van bijvoorbeeld al het mailverkeer van een organisatie kan consequenties hebben voor lopende onderhandelingen met leveranciers of afnemers binnen het normale bedrijfsproces).
- Voortgang dienstverlening: dienstverlening vanuit nog niet getroffen systemen stilleggen.
- Crisiscommunicatie: communiceren over (dreiging van) aanval of escalatie.

Mogelijke proces besluiten:

- Op- en afschaling: wordt de crisis door het meest effectieve team met de juiste bevoegdheid bestreden?
- Aflossing: zorg dat bij langer durende crises het team wordt afgelost en draag zorg voor een goede overdracht.
- Liaisons: naar welke partijen of teams gaat een liaison/ van welke partijen of teams vragen we liaisons.
- Informeren stakeholders: welke bestuurders en ketenpartners willen/moeten dit weten en wie informeert ze.

Extra: afkortingenlijst

ACM	Autoriteit Consument & Markt
AC-Pol	Algemeen Commandant Politie
AED	Aanbieder van een essentiële dienst
AIVD	Algemene Inlichtingen en Veiligheidsdienst
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BT	Beleidsteam
BZ	Ministerie van Buitenlandse Zaken
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CERT	Computer Emergency Response Team
CGB	Cybergevolgbestrijding
CISO	Chief Information Security Officer
CoPI	Commando Plaats Incident
CSBN	Cybersecuritybeeld Nederland
CSIRT	Computer Security Incident Response Team
CSR	Cyber Security Raad
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DEF	Ministerie van Defensie
DTC	Digital Trust Center
ECO	Eenheid Communicatie
ECR	Eenheid Crisiscoördinatie
ENISA	European Union Agency for Cybersecurity
EZK	Ministerie van Economische Zaken en Klimaat
G4	De vier grootste gemeenten (Amsterdam, Den Haag, Rotterdam en Utrecht)
GBT	Gemeentelijk Beleidsteam
GMS	Geïntegreerd Meldkamer Systeem
GRIP	Gecoördineerde Regionale Incidentbestrijdings Procedure
GSM	Global system for mobile communications
HIN	Hoofd Informatie Politie
HOPEX	Hoofd Opsporingsexpertise Politie
HOPS	Hoofd Opsporing Politie
IBD	Informatiebeveiligingsdienst
IDC	Intern Dienstencentrum
ICT	Informatie- en communicatietechnologie
IenW	Ministerie van Infrastructuur en Waterstaat
IFV	Instituut Fysieke Veiligheid
IoT	Internet of Things
IRB	ICT Response Board
ISAC	Information Sharing and Analysis Center
IWWN	International Watch and Warning Network
JenV	Ministerie van Justitie en Veiligheid
JSCU	Joint Sigint Cyber Unit
LCMS	Landelijk Crisis Management Systeem
LOCC	Landelijk Operationeel Coördinatiecentrum
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NCC	Nationaal Crisiscentrum
NCP-Digitaal	Nationaal Crisisplan Digitaal
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDN	Nationaal Detectie Netwerk
NRN	Nationaal Respons Netwerk
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap
OKTT	Organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren.
OM	Openbaar Ministerie
OOV	Openbare Orde en Veiligheid
OT	Operationeel Team
RBT	Regionaal Beleidsteam
ROT	Regionaal Operationeel Team
SIEM	Security Information & Event Management
(N)SGBO	(Nationale) Staf Grootschalig en Bijzonder Optreden
SLA	Service Level Agreement
SOC	Security Operations Center
TDO	Team Digitale Opsporing Politie
THTC	Team High Tech Crime Politie
Wbni	Wet Beveiliging Netwerk- en Informatiesystemen
Wiv	Wet op inlichtingen en veiligheidsdiensten
WRR	Wetenschappelijke Raad voor het Regeringsbeleid
VNG	Vereniging Nederlandse Gemeenten



Berenschot

Berenschot is een onafhankelijk organisatieadviesbureau met 350 medewerkers wereldwijd. Al 80 jaar verrassen wij onze opdrachtgevers in de publieke sector en het bedrijfsleven met slimme en nieuwe inzichten. We verwerven ze en maken ze toepasbaar. Dit door innovatie te koppelen aan creativiteit. Steeds opnieuw. Klanten kiezen voor Berenschot omdat onze adviezen hen op een voorsprong zetten.

Ons bureau zit vol inspirerende en eigenwijze individuen die allen dezelfde passie delen: organiseren. Ingewikkelde vraagstukken omzetten in werkbare constructies. Door ons brede werkterrein en onze brede expertise kunnen opdrachtgevers ons inschakelen voor uiteenlopende opdrachten. En zijn we in staat om met multidisciplinaire teams alle aspecten van een vraagstuk aan te pakken.

Berenschot Groep B.V.

Europalaan 40, 3526 KS Utrecht
Postbus 8039, 3503 RA Utrecht
030 2 916 916
www.berenschot.nl
/berenschot