Checklist Cybercrisis

Samen slimmer met data

Een cybercrisis wordt gekenmerkt door complexiteit, onzekerheid en een onvoorspelbare ontwikkeling. Om enig overzicht en grip te krijgen op de situatie kan worden gewerkt met scenario's. Onderstaand schema kan worden gebruikt om, samen met de CISO, een crisisdiagnose te stellen en een eerste inschatting van het scenario te maken. Daarnaast kunnen een aantal eerste acties worden geïdentificeerd aan de hand van het scenario.

Voorbereide plannen kunnen helpen om in control te komen, zoals een bedrijfscontinuïteitsplan, de handreiking cybergevolgbestrijding G4 (te openen via de QR-code hiernaast), het Nationaal Crisisplan Digitaal en de GRIP-procedure (ingeval van bedreiging van vitale belangen in de samenleving).

In welke fase zit de cybercrisis?

Tijdsindicatie per crisisfase

Ontdekking (24 uur – "paniek")
Respons (1 week – "chaos")
Wederopbouw (3+ maanden – "stress")
Nazorg en evaluatie (1 jaar – "normaal")

Welke eerste acties zijn uitgevoerd?

- □ Activeren continuïteitsplan
- □ Formeren intern crisisteam
- □ Inschakelen externe deskundigen
- □ Afkoppelen systemen/netwerken
- □ Veiligstellen Back-Ups
- □ Interne communicatie opstarten
- □ **Activeren crisisorganisatie** □ **GRIP3 structuur**

Wat is het vermoedelijke scenario?

Scenariovraag	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Hoe lang gaat de verstoring (verwacht) duren?	Minder dan 8 uur	8-24 uur	Meer dan 24 uur	Weken
Zijn er keteneffecten of is het systeem bedrijfskritisch?	Geïsoleerd en niet bedrijfskritisch	Ketengevoelig (keten nog niet geraakt) en/of bedrijfskritisch	Meerder systemen in de keten geraakt en bedrijfskritisch	
Wie is probleem eigenaar?	Eigen systeem/er zijn alternatieven beschikbaar	Leverancier herstelt op basis van contract/SLA	Geen SLA/probleem te complex voor snel herstel	Wereldwijd systeem, geen invloed op herstel
Is er sprake van opzet?	Nee	Niet uit te sluiten	Ja	Ja + statelijke actor
Is er technisch oplossings-perspectief?	Ja	Onduidelijk	Nee	
Welk geografisch gebied is geraakt?	1 specifieke organisatie	Meerdere organisaties in een veiligheidsregio	Meerdere veiligheidsregio's	Internationaal
Hoe lang gaan de *effecten* (verwacht) duren?	Minder dan 8 uur	8-24 uur	Meer dan 24 uur	Weken
Welk domein is verstoord?	Alleen ICT-domein	Alleen bedrijfsvoering van de eigen organisatie	Operationele/bedrijfs-kritische systemen	Vitale processen zijn verstoord
Kunnen effecten worden gereduceerd of is er kans op escalatie?	Reductie mogelijk, effect blijft beperkt	Enige reductie mogelijk, effecten blijven aanwezig	Reductie onmogelijk, escalatie dreigt	Escalatie van effecten onafwendbaar
Wat is de maatschappelijke impact?	Klein (mensen merken er weinig van/er zijn back-ups)	Gemiddeld (hinder in dagelijks leven/niet direct een alternatief aanwezig)	Groot (vitale voor-zieningen of dagelijkse levensbehoeften geraakt)	
>>dit scenario is een	**S1: Klein scenario, beperkte impact**	**S2: Gemiddeld scenario, langere termijn, enige impact op maatschappelijk leven**	**S3: Groot scenario, lange verstoring, grote impact, onduidelijke oplossing**	**S4: Zeer groot scenario (inter)nationale crisis**

Checklist Cybercrisis

Samen slimmer met data

Welke actoren kunnen betrokken zijn bij dit scenario?

Betrokken actoren bij scenario	S1	S2	S3	S4
Interne ICT afdeling, CISO, FG	●	●	●	●
Intern crisisteam	●	●	●	●
Autoriteit Persoonsgegevens	●	●	●	●
Digitale dienstverleners (ICT-leveranciers) getroffen partijen	●	●	●	●
Eventueel derde (commerciële) partijen voor ondersteuning, expertise of kennis	●	●	●	●
Getroffen partijen	●	●	●	●
NCSC en NCTV	●	●	●	●
CERT's (IBD, Z-Cert, Surfcert), Digital Trust Center, Landelijk Dekkend Stelsel		●	●	●
Aanbieders getroffen vitale processen			●	●
Politie			●	●
Openbaar Ministerie			●	●
KMar			●	●
Forensische/onderzoekende en commerciële partijen			●	●
Ministeries, verantwoordelijk voor getroffen domeinen of partijen			●	●
Veiligheidsregio's, LOCC c.q. LOCC-B			●	●
Ministeries verantwoordelijk voor getroffen vitale processen (beleidsdirecties en DCC's)			●	●
ICT Response Board			●	●
AIVD, MIVD				●
Internationaal netwerk via NCSC en NCC				●
Ministerie van Buitenlandse Zaken				●
Ministeries van AZ, BZ, BZK, DEF, JenV				●

Bron: Nationaal Crisisplan Digitaal

Welke bestuurlijke dilemma's zijn er?

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.

Bron: handreiking cybergevolgbestrijding G4

Wat zijn mogelijk sleutelbesluiten?

Inhoudelijk:
- 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.

Proces:
- 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.

Bron: handreiking cybergevolgbestrijding G4