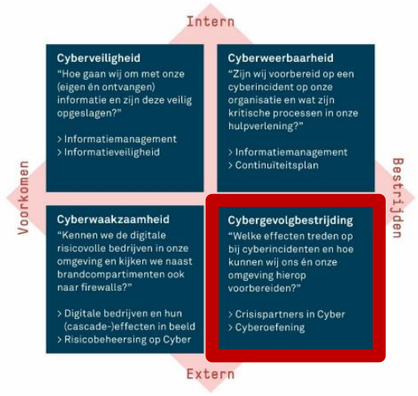
Coördinatiekaart Digitale ontwrichting en Cybergevolgbestrijding

Versie 0.8 / 7 januari 2022

Duiding

Deze coördinatiekaart richt zich primair op het bestrijden van de gevolgen van een cyberincident in de warme fase.
Dit cyberincident kan zowel intern bij de VRBZO voor de interne crisisorganisatie of als extern incident voor de regionale crisisorganisatie een vraagstuk worden. Met uitzondering van het thema “Interne crisisorganisatie en continuïteit” richt deze kaart zich hoofdzakelijk op de gevolgbestrijding van externe cyberincidenten binnen de VRBZO.



Het digitale domein in relatie tot veiligheidsregio’s kent meerdere aspecten en is hiernaast weergegeven in een cyberkwadrant. De fase ‘cybergevolgbestrijding’ waar deze coördinatiekaart over gaat, is rood omkaderd.

Onder cybergevolgbestrijding worden alle activiteiten verstaan die worden ontplooid om de situatie te normaliseren, nadat een cyberincident met digitale ontwrichting heeft plaatsgevonden. De focus voor de VRBZO ligt daarbij op het beperken en bestrijden van de gevolgen van een cybercrisis. De aanpak van de oorzaak bij een extern cyberincident ligt bij de organisatie waar het incident plaatsvindt.

Een cyberincident kan zich op onder meer de volgende manieren openbaren:

- Meerdere of opvallende meldingen van ICT-verstoringen bij de meldkamer;
- Melding(en) van een ICT-verstoring door (vitale) partner(s) binnen de VRBZO;
- Melding(en) door landelijke partner(s), zoals het LOCC, NCSC of NCC;
- Melding(en) door andere veiligheidsregio(‘s);
- Melding(en) door een van de kolommen binnen de VRBZO.

Kwetsbare objecten

Wanneer de effecten van een cyberaanval op een object regionale maatschappelijke ontwrichting teweegbrengt of grote maatschappelijke risico’s ontstaan, noemen we deze objecten kwetsbaar.
Voorbeelden van kwetsbare objecten en sectoren in geval zij getroffen worden door een cyberincident zijn:

- BRZO-bedrijven;
- Vitale infrastructuur (denk aan drinkwater, gas, elektriciteit);
- Overheids- en hulpdiensten;
- Ziekenhuizen en zorginstellingen;
- Productie of distributie levensmiddelen;
- Banken / het betalingsverkeer;
- Openbare vervoersbedrijven;
- Luchthaven Eindhoven en Kempen Airport;
- Defensieterreinen.

Melding, alarmering en opschaling

Melding - alarmering

- Zorg dat de CaCo wordt gealarmeerd/geïnformeerd!

Contactgegevens	
Afdeling crisisbeheersing	040 – 22 03 426 (piketnummer)
CISO VRBZO (= tevens vertegenwoordiger VR-ISAC)	Telefoonnummer ?
NCC	070 – 751 54 00

Opschaling

- Bij een verstoring met grote maatschappelijke gevolgen, gevolgen voor de openbare orde of rechtsorde, overweeg opschaling naar minimaal GRIP 2.
- **Acuut:**
  Beoordeling van aanpak door CaCo in afstemming met ROL. Gebruik hiervoor de “bouwstenen voor scenariobepaling” verderop in deze coördinatiekaart.
- **Niet acuut:**
  CaCo en ROL beoordelen de aanpak in overleg met afdelingshoofd Crisisbeheersing en CISO VRBZO.

Informatiemanagement

Afhankelijk van de situatie kunnen verschillende informatiepartners betrokken worden.
Mogelijke informatiepartners zijn:

- **Getroffen (vitale) organisatie(s);**
- **De CISO van de VRBZO;**
  Naast het leveren van cyberexpertise vertegenwoordigt de CISO het VR-ISAC dat tevens de schakel vormt naar het landelijk dekkend cyberstelsel. De CISO speelt daarmee een cruciale rol in cybergevolgbestrijding.
- **NCC;**
  Het NCC is voor veiligheidsregio’s het 24/7 informatieloket en contactpunt van het rijk.
- **De driehoek;**
- **Aangrenzende veiligheidsregio’s;**
- **Media;**
- **Bij intern VRBZO incident: interne crisisorganisatie (CRT : Crisis Response Team)**.
  Zie daarvoor de *Coördinatiekaart voor het Crisis Response Team (CRT) van de VRBZO bij een intern cyber incident* (in ontwikkeling).

Een landelijk document met uitgebreide informatie over cyberincidenten is het “Nationaal Crisisplan Digitaal”.

Crisiscommunicatie

Uitgangspunt is 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. Daarnaast zijn de volgende zaken van belang:

- Zolang niet zeker is of een incident opzettelijk handelen is, vermijden we verwijzingen naar mogelijke oorzaken, duur en omvang;
- Communiceer dat bij een extern cyberincident de regionale crisisorganisatie zich enkel richt op het beperken van de gevolgen;
- Geef waar mogelijk procesinformatie;
- Wanneer vanuit veiligheidsoverwegingen communicatie over kwetsbaarheden en/of maatregelen niet mogelijk is, melden we dat;
- Communicatie van bestuurders verbindt de samenleving en doet een beroep op de veerkracht van individuele burgers en van de Nederlandse samenleving als geheel.

Interne crisisorganisatie en continuïteit

De opvolging van een intern cyberincident bij de VRBZO is afwijkend van andere type incidenten waar we ons als VRBZO op voorbereiden. Bij een intern cyberincident dient een interne crisisorganisatie opgestart te worden. Overige (externe) expertise kan naar behoefte worden aangehaakt.
Zie hiervoor de *Coördinatiekaart voor het Crisis Response Team (CRT) van de VRBZO bij een intern cyber incident* (in ontwikkeling).

VeiligheidsRegio Brabant • Zuidoost

Leiding en coördinatie

Een cyberincident kan leiden tot maatschappelijke onrust of verstoring van de openbare orde. Om de gevolgen van zo'n crisis te kunnen beheersen dient de crisisorganisatie daarom een goed beeld te vormen van de gebeurtenissen en informatie uit te wisselen met betrokken crisispartners. Voor de beeldvorming van het incident en de effecten daarvan, kan onderstaand stappenplan gebruikt worden. De bouwstenen waar naar verwezen wordt staan beschreven in het thema 'Bouwstenen voor scenariobepaling'. Het stappenplan ziet er als volgt uit:

- **Stap 1:** Bepaal of en in welke mate een bouwsteen geraakt is. Het kan zijn dat bouwstenen meerdere scenario's weergeven.
- **Stap 2:** Beantwoord per scenario de volgende drie vragen:
  - Wat zijn de belangrijkste mogelijke (in)directe gevolgen en effecten van het incident?
  - Welke mitigerende maatregelen zijn nodig om de gevolgen en effecten (slachtoffers, schade) te voorkomen of te beheersen?
  - Welke partijen zijn betrokken c.q. nodig voor een adequate aanpak?

NB: bij verstoring van vitale processen dient de planvorming die is opgesteld voor verstoring van het desbetreffende vitale proces in werking te treden.

De effecten van een cyberincident kunnen gedurende het incident veranderen. In dat geval kunnen bovenstaande stappen opnieuw doorlopen worden.

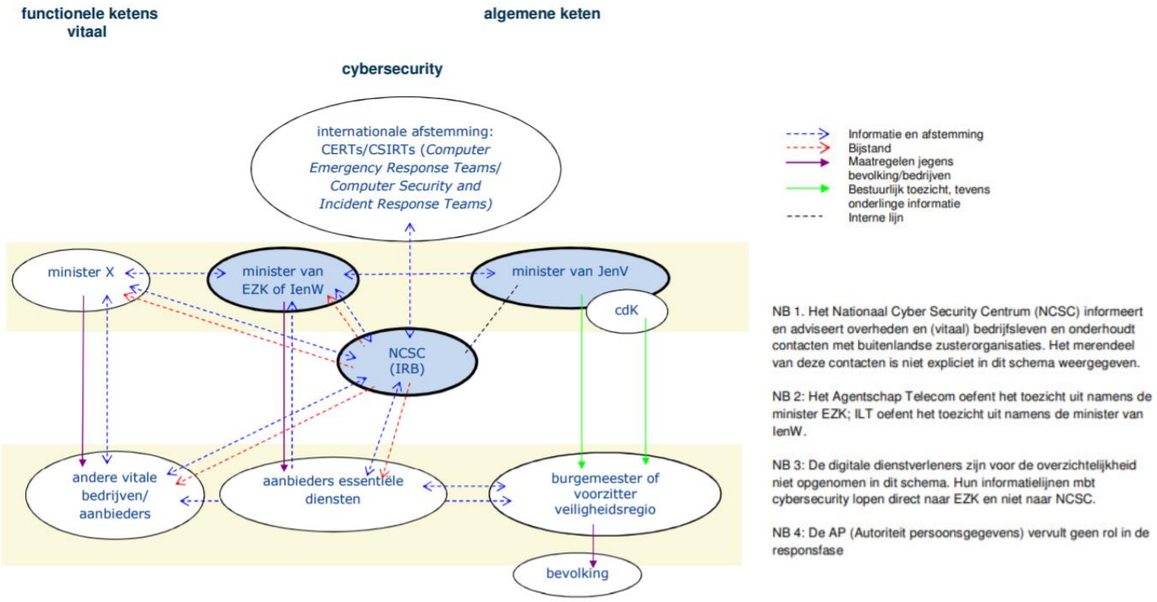
Bouwstenen voor scenariobepaling

Het doel van onderstaande bouwstenen is het vormen van een beeld van de situatie en het krijgen van inzicht in de ernst van het incident wat kan helpen om een passende interventie te plegen. Zoals in stap 1 van het stappenplan onder 'Leiding en coördinatie' genoemd, kan het zijn dat een cyberincident bouwstenen bevat die meerdere scenario's opleveren. In dat geval zal een weging gegeven moeten worden aan de bouwstenen afhankelijk van de situatie en de taakstelling van de VRBZO. Vanuit dat laatste bekeken zullen in elk geval de bouwstenen 'maatschappelijke impact' en 'het verstoorde domein' voor een groot deel bepalen in hoeverre de regionale crisisorganisatie in actie dient te komen.

Bouwstenen	**Incidentscenario's**			
De (verwachte) duur van de verstoring	< 8 uur	8 – 24 uur	> 24 uur	Weken
Aantal betrokken digitale systemen	1, geïsoleerd	Ketengevoelig (maar nog geen andere systemen geraakt)	>1 systeem geraakt	>1 systeem geraakt
Bedrijfskritisch	Nee	Ja	Ja	Ja
Herstelmogelijkheden	Alternatieven zijn beschikbaar	SLA* beschikbaar, snel herstel verwacht	Geen duidelijke SLA[1] afspraken, geen snel herstel mogelijk	Wereldwijd systeem, geen invloed op herstel
Opzettelijke verstoring	Nee	Misschien	Ja	Ja
Maatschappelijke impact	Klein	Middel	Groot	Zeer groot
Reductie effect	Reductie mogelijk, beperkte effecten	Beperkte reductie mogelijk	Geen reductie mogelijk, kans op escalatie	Escalatie is gegarandeerd
Het verstoorde domein	Alleen ICT-domein	Alleen dienstverlening of productie van een organisatie is getroffen	Verstoring maatschappelijk belangrijke voorzieningen (niet-vitaal)	Verstoring vitale processen
Getroffen geografisch gebied	Primair binnen een of enkele gemeente(n)	(Grote delen van) de veiligheidsregio	Meerdere veiligheidsregio's betrokken	Nationaal / internationaal
	Scenario 1 Klein scenario, beperkte impact	**Scenario 2** Gemiddeld scenario, langere termijn, enige impact op maat-schappelijk leven	**Scenario 3** Groot scenario, lange verstoring, grote impact, onduidelijk-heid over oplossing	**Scenario 4** Zeer groot scenario, (inter)nationale crisis

Bestuurlijke Netwerkkaart Cybersecurity

In de "Bestuurlijke Netwerkkaart 21b Cybersecurity" is de afstemming tussen de functionele vitale ketens en de algemene keten schematisch weergegeven:



NB 1. Het Nationaal Cyber Security Centrum (NCSC) informeert en adviseert overheden en (vitaal) bedrijfsleven en onderhoudt contacten met buitenlandse zusterorganisaties. Het merendeel van deze contacten is niet expliciet in dit schema weergegeven.

NB 2: Het Agentschap Telecom oefent het toezicht uit namens de minister EZK; ILT oefent het toezicht uit namens de minister van IenW.

NB 3: De digitale dienstverleners zijn voor de overzichtelijkheid niet opgenomen in dit schema. Hun informatielijnen mbt cybersecurity lopen direct naar EZK en niet naar NCSC.

NB 4: De AP (Autoriteit persoonsgegevens) vervult geen rol in de responsfase

Afkortingen

CISO	= Chief Information Security Officer
NCC	= Nationaal Crisis Centrum
VR-ISAC	= Information Sharing and Analysis Center voor veiligheidsregio's
NCSC	= Nationaal Cyber Security Centrum
SLA	= Service Level Agreement. Een contract met een leverancier die in dit geval digitale systemen bij verstoringen kan proberen te verhelpen.

Bronvermelding

Bij het opstellen van deze coördinatiekaart is gebruik gemaakt van de volgende bronnen:

- Berenschot Groep B.V. (2020). *Handreiking cybergevolgbestrijding (CGB) G4-gemeenten.* https://www.berenschot.nl/media/mhwhexbk/ handreiking_cybergevolgbestrijding_g4_-_deel_2_koude_fase.pdf
- IFV. (2019). *Whitepaper digitale ontwrichting en cyber.* https://www.ifv.nl/kennisplein/digitale-weerbaarheid/publicaties/whitepaper-digitale-ontwrichting-en-cyber
- IFV. (2019). *Crisiscommunicatietips voor incidenten met een cybercomponent.* https://www.ifv.nl/kennisplein/Paginas/Crisiscommunicatietips-voor-incidenten-met-een-cybercomponent.aspx
- IFV. (2019). *Bestuurlijke netwerkkaart Cybersecurity.* https://www.ifv.nl/kennisplein/Paginas/Bestuurlijke-Netwerkkaart-21b-Cybersecurity.aspx
- NCTV. (2021). *Koepelnotitie communicatie bij digitale incidenten.* https://www.nctv.nl/documenten/publicaties/2021/02/23/koepelnotitie-communicatie-bij-digitale-incidenten#:~:text=hier%3A%20Home%20Documenten-,Koepelnotitie%20Communicatie%20bij%20digitale%20 incidenten%202021,storing%20of%20aanval%20kan%20zijn.
- NCTV. (2020). *Nationaal Crisisplan Digitaal.* https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal

Coördinatiekaart Digitale ontwrichting en Cybergevolgbestrijding **Versie 0.8 / 7 januari 2022**

[1] *SLA staat voor Service Level Agreement. Een contract met een leverancier die in dit geval digitale systemen bij verstoringen kan proberen te verhelpen.*

VeiligheidsRegio Brabant • Zuidoost

VeiligheidsRegio Brabant • Zuidoost