Instituut
Fysieke
Veiligheid

Cyberrisico's en veiligheidsregio's

Hoe beoordelen veiligheidsregio's cyberrisico's?

De samenleving wordt geconfronteerd met nieuwe risico's. De nieuwe crises zijn moeilijk kenbaar, beperken zich niet tot één bepaalde sector en kunnen razendsnel escaleren. Ook veiligheidsregio's krijgen of hebben al te maken met nieuwe crisistypen, waaronder digitale ontwrichting. De Wetenschappelijke Raad voor het Regeringsbeleid pleit voor meer investeringen in digitale weerbaarheid.

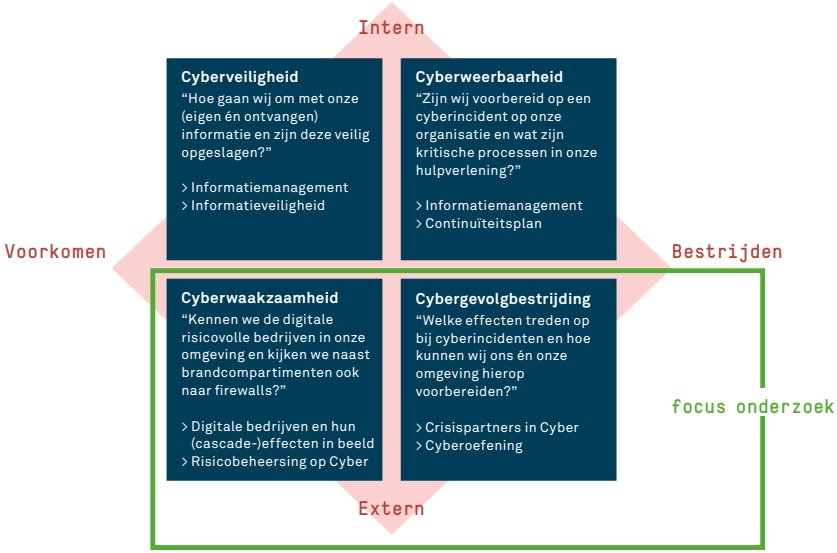
Voorbereiden op nieuw risico: digitale ontwrichting

Het lectoraat Crisisbeheersing van het IFV onderzocht in opdracht van de RDVR-portefeuillehouder Digitale Ontwrichting en Cyber de wijze waarop veiligheidsregio's cyberrisico's inventariseren en beoordelen en hoe veiligheidsregio's zich op cyberrisico's voorbereiden.

Definitie cyberrisico's
"Een risico waarvan de oorzaak en/of het gevolg in het digitale domein liggen en dat impact heeft op de samenleving, de (fysieke) veiligheid en/of openbare orde in een veiligheidsregio." - Whitepaper digitale ontwrichting en cyber (IFV, 2019)

Focus onderzoek op cyberwaakzaamheid en -gevolgbestrijding

Het onderzoek bestaat uit een scan van regionale risicoprofielen, een enquête onder veiligheidsregio's en bijeenkomsten met de werkgroep Digitale ontwrichting en cyber. Centraal staan de thema's cyberwaakzaamheid en cybergevolgbestrijding, de twee externe componenten in het onderstaande cyberkwadrant.



Hoe beoordelen veiligheidsregio's cyberrisico's?

Voor het inventariseren en beoordelen van cyberrisico's gebruiken de veiligheidsregio's de Handreiking Regionaal Risicoprofiel (83%), het Cybersecuritybeeld Nederland (57%) en het Nationaal Veiligheidsprofiel (29%). Het Cybersecuritybeeld (CSBN) wordt door bijna alle gebruikers als belangrijke informatiebron voor cyberrisico's beschouwd. Veiligheidsregio's hebben wel moeite om landelijke risico's te vertalen naar regionale risico's. Bij de inventarisatie van cyberrisico's werkt minder dan de helft van de veiligheidsregio's samen met partners. Uit de analyse van de regionale risicoprofielen van de veiligheidsregio's blijkt dat de beoordelingen van waarschijnlijkheid en impact uiteenlopen.

Belangrijkste cyberrisico's

De veiligheidsregio's zien als belangrijkste cyberrisico's:

- uitval van vitale voorzieningen, zoals drinkwater, energie, ICT en telecom
- verstoring van de eigen crisisorganisatie of hulpverlening
- verstoring van Brzo-bedrijven met veiligheids- en gezondheidsrisico's als gevolg
- hack/uitval datacentra (datalek).

Over digitale risico-objecten zoals datacentra of ICT-knooppunten lijkt nog weinig bekend te zijn binnen de regio's.

Zijn veiligheidsregio's voorbereid op cyberwaakzaamheid en -gevolgbestrijding?

Veiligheidsregio's beoordelen hun eigen preparatie op cyberwaakzaamheid en cybergevolgbestrijding met respectievelijk een 5 en 6. Door de veiligheidsregio's worden diverse activiteiten genomen om zich voor te bereiden. Als belangrijkste activiteiten worden genoemd: het opbouwen en onderhouden van regionale/landelijke netwerken (86%), het opbouwen van cyberkennis en -expertise (81%) en het oefenen met cyberscenario's (67%). Voor veel veiligheidsregio's is het nog zoeken hoe zich adequaat te prepareren op digitale verstoringen.

Wat zijn behoeften van veiligheidsregio's?

Om goed te kunnen anticiperen op cyberrisico's willen veiligheidsregio's:

- cyberrisico's in de omgeving in beeld brengen samen met partners
- ontwikkelingen van het Cybersecuritybeeld Nederland vertalen naar de eigen regio
- duidelijkheid krijgen over de rollen, taken en bevoegdheden van alle betrokken actoren (landelijk, regionaal, lokaal), inclusief hun eigen rol en de benodigde expertise

- procedures rond alarmering, opschaling en besluitvorming verhelderen (bijvoorbeeld door middel van een specifieke cybercrisisfunctionaris)
- de eigen expertise van cyberbronbestrijding en cybergevolgbestrijding vergroten
- cyberscenario's uitwerken en (samen met partners) oefenen
- een landelijk aanspreekpunt inrichten voor cyberrisico's (koud) en bij cyberincidenten (warm).

Aanbevelingen

Om beter voorbereid te zijn op cyberincidenten kunnen veiligheidsregio's een aantal acties ondernemen.

Aanbevelingen cyberwaakzaamheid

1. Ontwikkel een methodiek om cyberrisico's systematisch te inventariseren en beoordelen. Denk bijvoorbeeld aan een opleidingsmodule of systematiek voor het vertalen van het Cybersecuritybeeld Nederland naar de veiligheidsregio's en het voeren van een gedegen risicodialoog. Hierbij hoort ook een verkenning van de meerwaarde van een 'cybercrisisfunctionaris'.
2. Betrek bij de risicobeoordeling een regionaal netwerk van belanghebbenden, zoals vitale sectoren, maatschappelijke organisaties en Brzo-bedrijven. Ga met dit netwerk een dialoog aan over cyberrisico's, waarbij diverse disciplines en perspectieven worden benut.

Aanbevelingen cybergevolgbestrijding

1. Gebruik vaste vragen in gesprekken met regionale partners, bijvoorbeeld:
   - Wat zijn de belangrijkste cyberrisico's in de regio? Hoe bereidt iedereen zich daarop voor?
   - Wat verwachten we van elkaar? Wat kúnnen we verwachten?
   - Wat kunnen we voor elkaar betekenen in de koude en warme fase?
2. Gebruik naar analogie van terrorismegevolgbestrijding enkele basisscenario's voor planvorming en oefenen. Maak met de partners afspraken over alarmering, opschaling en onderlinge coördinatie bij digitale verstoringen.
3. Neem als veiligheidsregio deel aan en organiseer (boven-)regionale cyberoefeningen. Faciliteer als werkgroep Digitale ontwrichting en cyber een 'netwerk observatoren cyberoefeningen', dat opgedane ervaringen bundelt en beschikbaar stelt aan de veiligheidsregio's.

Deze factsheet is gebaseerd op de publicatie *Cyberrisico's en veiligheidsregio's. Hoe beoordelen veiligheidsrisico's cyberrisico's?* (IFV, 2020). Deze is te downloaden op www.ifv.nl.

Voor meer onderzoeken van het lectoraat Crisisbeheersing zie www.ifv.nl/lectoraatcrisisbeheersing.

Instituut Fysieke Veiligheid, februari 2020