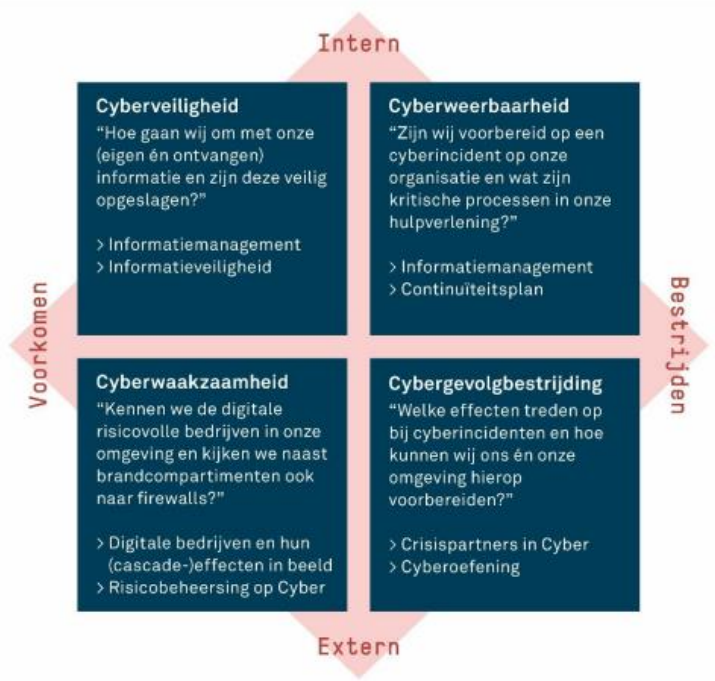
Three-pager digitale veiligheid, cyberwaakzaamheid en cybergevolgbestrijding

Kwadranten: wat omvat cyber allemaal?

'cyber' is een containerbegrip voor alles wat met informatie- en communicatietechnologie (ICT) samenhangt. Een cybercrisis is iedere (opzettelijke) verstoring, uitval of misbruik van een gedigitaliseerd proces, (informatie)systeem of informatiedienst die de maatschappelijke continuïteit, openbare orde en veiligheid bedreigt of verstoort[1].



In het cyberkwadrant wordt een onderscheid gemaakt tussen intern én extern. Enerzijds draait het om de interne organisatie ('eigen huis op orde') – waarbij het belangrijk is dat elke organisatie verantwoordelijk is voor de continuïteit van zijn eigen processen. Tevens gaat het om de externe kant, ofwel de kant van de samenleving. Digitale verstoringen kunnen leiden tot – fysieke - effecten in de samenleving, waarbij het doel is dergelijke effecten te voorkomen en ze te bestrijden. Indien er sprake is van – fysieke – effecten die impact hebben op de samenleving waarbij het maatschappelijk leven – ernstig – ontregeld raakt spreken we van een digitaal maatschappelijke ontwrichting. Het bestrijden van de fysieke effecten in de samenleving, ofwel cybergevolgbestrijding, is een taak van de regionale crisisorganisatie. De regionale crisisorganisatie doet in dit geval niet aan bronbestrijding en is derhalve geen digitale brandweer.

Cyberveiligheid en Cyberweerbaarheid m.b.t. interne organisatie VRU

De interne organisatie van de VRU is zelf verantwoordelijk voor de cyberveiligheid van haar eigen digitale processen en ICT hulpmiddelen. Zowel intern als in samenwerking met andere veiligheidsregio's binnen het VR-ISAC[2] wordt daar actief invulling aan gegeven. Het Nationaal Cyber Security Centrum (NCSC) waarschuwt met regelmaat voor actoren die op zoek zijn naar kwetsbaarheden. Deze cyber criminele activiteiten zijn respectievelijk gericht op ontwrichting van de samenleving en op financieel gewin.

Daarmee is cyberveiligheid een onderwerp geworden dat continu aandacht vraagt. Vanwege de rol van de veiligheidsregio in de samenleving is het belangrijk dat de dienstverlening en daarmee de onderliggende informatievoorziening en -systemen beschikbaar blijven voor het uitvoeren van de operationele taken van de VRU. Het borgen en versterken van de cyberveiligheid staat daarmee hoog op de agenda. De VRU moeten voldoen aan de eisen zoals die gesteld worden in de Baseline Informatiebeveiliging Overheid (BIO). Omdat de eisen van de BIO verder gaan dan alleen de IT technische inrichting van de cyberveiligheid is bij de VRU het programma 'Cyberveiligheid' opgestart. De versterking van de cyberveiligheid middels dit programma vindt plaats over drie sporen:

1. Het eerste spoor gaat over de beheersing van de processen. Na de inventarisatie van de beveiligingsrisico's per proces worden, samen met de proceseigenaar, mitigerende maatregelen voorgesteld. Het inregelen van eventuele maatregelen is een risicoafweging die samen met de proceseigenaar wordt genomen. Uiteraard dient er altijd een minimaal basisniveau voor beveiliging ingericht te worden. Deze procesgerichte benadering leidt tot een verdere professionalisering van de VRU.
2. Het tweede spoor gaat over het vergroten van de cyberweerbaarheid. Alle medewerkers van de VRU moeten zich bewust zijn van de cyberrisico's en in de organisatie moet alertheid worden gekweekt ten aanzien van dit onderwerp. Alle medewerkers worden hiervoor gericht getraind en met regelmaat worden cyber gerelateerde cases besproken. Tevens wordt er samen met de directie Crisisbeheersing geoefend op een situatie dat de VRU getroffen wordt door een cyberverstoring.

[1] Handreiking cybergevolgbestrijding, 2019
[2] Veiligheidsregio Information Sharing Analysis Centre

3. Het derde spoor betreft intensief technisch-en functioneel beheer. Het uitvoeren van dagelijkse controles & monitoring van het systeemlandschap, het actueel houden van de systemen en beveiligingsschillen (Firewalls, two-factor authentication) en het gepland veilig stellen van informatie. Om de effectiviteit vast te stellen worden met regelmaat 'ethical hack opdrachten' uitgevoerd. Naar aanleiding van de recente Apache Log4j casus zijn er binnen de VRU extra maatregelen getroffen om de continuïteit van de operationele processen te kunnen garanderen.

Binnen de VRU staat een crisisteam paraat voor het geval onze organisatie wordt getroffen door een cybercrisis. Hierin spelen onder meer de Chief Information Security Officer (CISO), de Chief Information Officer (CIO) en Functionaris Gegevensbescherming (FG) een belangrijke rol. Het verschilt per scenario welke aanvullende expertise nodig is. Zo kan een sectorale Computer Emergency Response Team (CERT), bijvoorbeeld de IBD, een organisatie adviseren en ondersteunen bij de afhandeling van de digitale verstoring of kan forensische expertise worden ingeschakeld.

Cyberwaakzaamheid
Vanuit de directie Risicobeheersing wordt een taak onderkend als het gaat om het identificeren van 'nieuwe' risico's. Het gaat hierbij om risico's in de fysieke leefomgeving in onze regio die kunnen ontstaan door verstoringen ten gevolge van een cybercrisis. In veel gevallen kunnen veiligheidsrisico's ontstaan op een voor ons bekend terrein. Bijvoorbeeld het ontstaan van een overstroming door toedoen van een cybercrisis, dit betreft geen nieuw risico. Verstoringen van vitale processen, zoals uitval van elektriciteit of betalingsverkeer, zijn inzichtelijk gemaakt en worden beschreven door landelijk ontwikkelde risicobeschrijvingen. Echter kan een cybercrisis wel leiden tot nieuwe risico's, waar de veiligheidsregio nog onvoldoende inzicht in heeft. Bijvoorbeeld het ontregelen van verkeerslichtinstallaties. De VRU wil zich richten op mogelijk lokaal optredende nieuwe risico's.

Een andere taak is het vergroten van het risicobewustzijn. Daar waar de VRU zich nu vooral richt op brandveiligheid, is het de bedoeling om steeds meer op het gehele terrein van de fysieke veiligheid te richten. Dus ook bewustwording op de veiligheidsrisico's ten gevolge van een cybercrisis. Dit door met bedrijven, organisaties en instellingen te praten over dit onderwerp. Op dit moment beschikt de VRU nog niet over de juiste expertise. Er wordt op dit moment nagedacht over het verbreden van de kennis op dit onderdeel. Maar altijd vanuit de gedachte over de fysieke gevolgen van een cybercrisis, niet over digitale veiligheid. Dat is het werkterrein van andere professionals.

Cybergevolgbestrijding
Een cybercrisis kan leiden tot maatschappelijke ontwrichting doordat er discontinuïteit plaatsvindt bij organisaties, bedrijven en instanties. Elke organisatie is zelf verantwoordelijk voor de continuïteit van zijn eigen processen, inclusief de mogelijke dienstverlening. Op dit moment heeft (verlengd) lokaal bestuur geen wettelijke bevoegdheid om in te grijpen bij derden indien er sprake is van discontinuïteit door toedoen van een cybercrisis. Eventueel ingrijpen bij (vitale) instanties is voorbehouden aan de vakminister. De burgemeester of voorzitter veiligheidsregio heeft het opperbevel indien er sprake is van een (cyber)crisis. Het is wel mogelijk om een verzoek te doen aan de vakminister om in te grijpen in de functionele keten.

Speelveld
- *Voorkomen:* Er zijn in Nederland verschillende partijen die zich bezighouden met preventie op het gebied van informatiebeveiliging. De Rijksoverheid voorziet hier bijvoorbeeld in middels het Nationaal Cyber Security Centrum, voor vitale belangen, en het Digital Trust Center, voor bedrijven. Tevens spelen gemeenten en politie een grote rol in preventie van cybercrime, maar ook private partijen dragen hier aan bij.
- *Repressie:* Tijdens een digitale verstoring is de getroffen organisatie in eerste instantie zelf verantwoordelijk om zorg te dragen voor de afhandeling van het incident. In veel sectoren zijn er Computer Emergency Response Teams (CERT) opgericht, die bedrijven/organisaties ondersteunen bij de afhandeling van incidenten. Zo bestaat er de Informatiebeveiligingsdienst (IBD) voor gemeenten, de Z-CERT voor de zorgsector en SURFCERT voor het onderwijs. Deze CERTS zijn via het Landelijk Dekkend Stelsel (LDS) aangesloten bij het NCSC, welke samen met NCC, zorg draagt voor coördinatie en informatie-uitwisseling in het geval van een bovenregionale cybercrisis met bovenregionale effecten. De regionale crisisorganisatie van de VRU staat in direct contact met het NCC.

Wie zitten er aan tafel bij een externe cybercrisis?
In het geval van een – dreigende – maatschappelijke ontwrichting zal de regionale crisisorganisatie (flexibel) opschalen om de effecten in de samenleving te beheersen en/of te bestrijden. In dat opzicht is een cybercrisis ook een gewone crisis, waar we werken volgende de normale procedures en werkwijzen van het Regionale Crisisplan. In ieder geval zullen bij de VRU de functionarissen Regionaal Operationeel Leider, Informatiemanager en (crisis)communicatieadviseur in een kernteam bijeenkomen. Vanuit dit kernteam wordt gekeken hoe de crisisorganisatie verder ingericht dient te worden. In

geval van een flitsramp, door toedoen van een digitale oorzaak, wordt opgeschaald in GRIP. Tevens is het gebruikelijk om getroffen crisispartners uit te nodigen om als liaison aan te sluiten bij de regionale crisisorganisatie (ROT, GBT of RBT).

Wat doet de regionale crisisorganisatie van de VRU bij cybergevolgbestrijding ?
De regionale crisisorganisatie van de VRU heeft in geval van een – dreigende – digitale ontwrichting enkele taken[3]:

- Gevolgbestrijder: De veiligheidsregio ondersteunt het bevoegd gezag bij het bestrijden van de (fysieke) gevolgen van externe cyberverstoringen.
- Netwerkregisseur: De veiligheidsregio als netwerkregisseur op het gebied van crisisbeheersing en cyber. De regionale crisisorganisatie heeft nauw contact met haar crisispartners. Bij – dreigende – uitval/verstoring door toedoen van digitale verstoringen is de regionale crisisorganisatie bekend met relevante partners, zowel in de regio als bij het Rijk.

[3] Cyberscenario's voor veiligheidsregio's (2021), IFV