Instituut
Fysieke
Veiligheid

Evaluatie veiligheidsregio's ISIDOOR 2021

Van 1 t/m 3 juni 2021 vond de landelijke cyberoefening ISIDOOR-3 plaats. De oefening werd georganiseerd door het NCSC in samenwerking met de NCTV. De oefening simuleerde een digitale 'crisis' die uit meerdere soorten cyberaanvallen bestond, met fysieke gevolgen voor de samenleving: geen of vervuild drinkwater, uitval van energie en digitaal betaalverkeer, en een verstoring van de transportsector. Uiteindelijk vormden de aanvallen een bedreiging voor de nationale veiligheid. Tijdens ISIDOOR 2021 zijn afspraken, structuren en processen uit het Nationaal Crisisplan Digitaal (NCP-Digitaal) geoefend. Aan de oefening namen meer dan 80 operationele diensten en 1500 mensen deel, waaronder de Rijksoverheid, veiligheidsregio's, uitvoeringsorganisaties, vitale partners en professionals op het gebied van cyber-security.[1] Het was de eerste keer dat veiligheidsregio's deelnamen aan ISIDOOR.

[1] Cyberoefening ISIDOOR 2021 (NCSC, 2021)

Openbaar - IFV september 2021

Ervaren uitdagingen tijdens de cyberoefening

Crisisbeheersing

1. Het ontbreken van fysieke effecten, waardoor de operationele crisisteams van de veiligheidsregio's meer dan normaal 'op hun handen moesten zitten'. En de langere aanloopfase en duur van de 'crisis' dan bij klassieke flitsrampen ('creeping crisis').
2. Het grensoverschrijdende karakter met betrokkenheid van partijen uit meerdere sectoren.
   - Informatie: het grensoverschrijdende karakter zorgde voor het ontstaan van meerdere informatiestromen (cybersecurity, sociale media, fysieke effecten).
   - Beeld- en oordeelsvorming: het bemoeilijkte de beeld- en oordeelsvorming, zowel de overkoepelende duiding als de beeld- en oordeelsvorming over de regionale impact.
   - Coördinatie: het grensoverschrijdende karakter bemoeilijkte de onderlinge coördinatie.
3. De 'cyberdimensie' van de crisis, waardoor
   - het doorgronden van risico's en potentiële dreigingen voor veiligheidsregio's lastig bleek,
   - expertise voor het duiden van risico's en dreigingen ontbrak in de crisisbeheersing en
   - het zoeken was naar de rol en wijze van optreden van de veiligheidsregio.

VR-ISAC

1. De afhankelijkheid van het NCSC voor gevalideerde informatie.
2. Koppeling en escalatieprocedure VR-ISAC-CISO / RCDV-Crisisbeheersing
3. Het leveren van een bijdrage als VR-ISAC aan beeld- en oordeelsvorming voor de crisisbeheersing door de veiligheidsregio's.
4. Actief monitoren van informatie uit verschillende (informele) kanalen, waaronder sociale media en de security community. Dergelijke informatie is mogelijk bruikbaar, maar niet gevalideerd.

Zes overkoepelende observaties

"Het spel spelen zonder de regels te kennen" (deelnemer veiligheidsregio)

1. Weinig zicht op het grotere geheel

De deelnemende crisisteams (OT's, LOCC) waren in de eerste uren erg gericht op het eigen functioneren. Daarbij hielden de teams zich aan bestaande planvorming, gebruikten specifieke cyberplannen en traden behoorlijk rolvast op. De teams hadden weinig gevoel en beeld bij de bredere dreigingssituatie en responsoperatie en hoe daaraan bij te dragen. De afwezigheid van fysieke effecten biedt veiligheidsregio's wel enige voorbereidingstijd: tijd om informatie in te winnen, contacten met vitale partijen te leggen en scenario's op te stellen.

2. Cyberexpertise ontbreekt

Operationele teams en LOCC beschikten niet over specifieke cyberexpertise. Dat was een gemis, onder meer voor het duiden van cyberrisico's en potentiële dreigingen, voor het interpreteren van informatie en het goed doorgronden van de gehele responsstructuur. Opvallend is dat dezelfde informatie door veiligheidsregio's/LOCC en VR-ISAC anders wordt geïnterpreteerd.

3. Het spel spelen zonder de regels te kennen

Voor de veiligheidsregio's, het LOCC en het VR-ISAC was het de eerste keer dat zij oefenden met een grootschalig cyberscenario. Voor crisisfunctionarissen was dat onwennig. Ook ervaarden sommige deelnemers een andere wijze van optreden: meer terughoudend en onderzoekend, dan actiegericht. De operationele crisisteams moesten het spel spelen, zonder dat zij de regels van het spel kenden. Dat was leerzaam, maar roept wel de vraag op hoe veiligheidsregio's en crisisprofessionals hierin verder te bekwamen.

4. Beperkte samenhang en kennisdeling

Doordat teams erg op zichzelf gericht waren (terugkerend patroon in de eerste crisisfase), hebben we weinig onderlinge samenhang en kennisdeling gezien. Zowel tussen de veiligheidsregio's, tussen de veiligheidsregio's en het VR-ISAC en tussen de algemene en functionele (cyber)keten. Onderlinge coördinatie en gezamenlijke oordeelsvorming kwam niet tot stand. Verzachtende omstandigheid is evident de complexe responsstructuur, met diverse sectoren, cybersecurity en crisisbeheersing; die complexiteit bemoeilijkt onderlinge coördinatie.

5. Bijdrage VR-ISAC aan cybersecurity respons niet helder

De rol, taken en verantwoordelijkheden van het VR-ISAC waren voor veiligheidsregio's en LOCC niet duidelijk. Het VR-ISAC was bovendien sterk afhankelijk van gevalideerde informatie van het NCSC. Voor veiligheidsregio's is nu nog niet duidelijk hoe het VR-ISAC tijdens cyberdreigingen en -verstoringen kan bijdragen aan incidentbestrijding en crisisbeheersing door veiligheidsregio's. Het VR-ISAC vormt de schakel tussen NCSC en CISO's van de veiligheidsregio's. Operationele teams hebben het VR-ISAC niet herkend en gebruikt als experts en vertegenwoordigers van veiligheidsregio's in het Landelijk Dekkend Stelsel.

6. Veiligheidsregio's niet actief benaderd door vitale partners

Voor veiligheidsregio's bleek het lastig informatie van en afstemming met de vitale partners te vinden, waardoor onduidelijk bleef wat de mogelijke risico's op het optreden van maatschappelijke effecten was. Dat maakte preparatie op mogelijke risico's en maatschappelijke effecten voor regio's lastig.

Specifieke observaties VR-ISAC

1. Het VR-ISAC is voor zijn optreden sterk afhankelijk van informatie van het NCSC. Zonder gevalideerde informatie kan het VR-ISAC geen invulling geven aan zijn kerntaak: informatie delen en analyseren.

2. Het VR-ISAC heeft de juiste expertise in huis om zijn taken goed te vervullen. Winst is dat het VR-ISAC tevens beschikt over ruime ervaring met crisisbeheersing. Zij heeft geen toegang tot LCMS, wat nuttig kan blijken voor de eigen informatiepositie.

3. Het VR-ISAC heeft op basis van beschikbare informatie cyberbeelden opgesteld en gedeeld binnen het eigen netwerk (CISO's/ RCDV). De cyberbeelden bevatten informatie, voorzien van duiding en handelings-perspectief, gericht op cybersecurity van veiligheidsregio's. De cyberbeelden voegen ons inziens waarde toe voor de beeldvorming in veiligheidsregio's.

4. Technische (dreigings)informatie wordt door het VR-ISAC anders geïnterpreteerd dan door operationele teams. Voor crisisteams bleek het lastig technische dreigingsinformatie te vertalen naar crisisinformatie. Het VR-ISAC kan veiligheidsregio's helpen in de duiding en analyse van technische informatie. Dat is nu onvoldoende gebeurd.

5. Formaliseer de escalatielijnen vanuit het VR-ISAC naar de regionale CISO's en RCDV.

6. Het VR-ISAC is momenteel slecht bereikbaar. Er is geen centraal nummer, geen gegarandeerde bereikbaarheid buiten kantoortijd en geen piket. Het VR-ISAC is geen lid van het Nationaal Respons Netwerk, waardoor deze geen IOC's (Indicators Of Compromise) ontvangt.

Lessen en goede praktijken

1. Deelname van de veiligheidsregio's aan deze cyberoefening had waarde op zichzelf. Het was de eerste keer dat regio's mee oefenden en gevoel konden krijgen bij het verloop van zo'n grootschalig cyberscenario.
2. De operationele crisisteams waren tevreden over het verloop van het scenariodenken en het gebruik van cyberplannen, zoals de multidisciplinaire scenariokaart Cyber.
3. De operationele crisisteams van veiligheidsregio's traden op met grote rolvastheid. Ze waren zich bewust van de eigen rol en verantwoordelijkheid, weerstonden de neiging om direct tot actie over te gaan en 'aapjes op de schouder' te nemen.
4. Het LOCC werd goed gevonden bij het opstellen van scenario's op nationaal niveau.
5. Op basis van beschikbare informatie heeft het VR-ISAC twee cyberbeelden opgesteld en gedeeld binnen het eigen netwerk (CISO's en RCDV). De cyberbeelden bevatten informatie, voorzien van duiding en handelingsperspectief, gericht op cybersecurity van veiligheidsregio's.
6. Het verloop van de informatiedeling tussen het NCSC en het VR-ISAC in de eerste uren van de oefening verliep adequaat: tijdig, gevalideerd en conform afspraak. De informatiedeling tussen sectoren binnen het Landelijk Dekkend Stelsel wordt door het VR-ISAC als goede praktijk beschouwd: laagdrempelig, intensief en gericht op zicht krijgen op de cyberdreiging en oplossingen.
7. Het VR-ISAC beschikt over de juiste expertise om zijn kerntaak uit te voeren, namelijk het delen en analyseren van informatie op het gebied van cybersecurity.

Adviezen voor bovenregionale afstemming

Gezamenlijke situatiebriefings

Organiseer periodieke gezamenlijke situatiebriefings met Rijk en regio's voor 'shared consiousness'. Breng verschillende disciplines aan één (digitale) tafel bijeen: ICT, cybersecurity, crisisbeheersing en communicatie. Betrokken organisaties en teams krijgen zo meer gevoel en begrip voor de situatie en de 'bredere crisisoperatie'.

OL calls

Organiseer gezamenlijke situatiebriefings tussen veiligheidsregio's: 'OL calls' met daarbij (leden van) VR-ISAC en communicatie. Juist bij complexere crises zorgen meerdere verschillende perspectieven voor betere beeldvorming en nieuwe oplossings-richtingen. Veiligheidsregio's kunnen zelf zo'n call organiseren, maar enige vorm van facilitering (voorbereiden, verslaglegging) door een landelijk platform is, zeker bij langdurige crises, wel handig. Zo'n platform kan tevens bijdragen aan de afstemming tussen Rijk en regio's.

Onderzoek

Onderzoek nieuwe vormen van bovenregionale coördinatie en verbindingen tussen algemene en functionele ketens die meer recht doen aan de inherente complexiteit.

Adviezen voor de veiligheidsregio’s

Cybersecurity & crisisbeheersing

Zorg voor verbinding tussen crisisfunctionarissen en ICT-professionals. Zorg bij in- en externe cyberverstoringen voor meer specialistische cyberexpertise in het operationeel team, b.v. in de vorm van de CISO of adviseur IT. Onderzoek de toegevoegde rol en taken van een ‘OvD-Cyber’. Doorloop met alle betrokkenen binnen de eigen regio enkele cyberscenario’s voor het beter begrijpen en benutten van elkaars expertise.

Vitale partners

Investeer in de relaties met vitale partners. Bespreek onderlinge informatiebehoeften bij cyberdreigingen en -verstoringen op basis van ‘need to know’. Veiligheidsregio’s zijn voor hun eigen preparatie gebaat bij informatie over prognoses en scenario’s bij vitale partners zoals drinkwater en energie (en niet bij bedrijfsgevoelige en anderszins sensitieve informatie over dreigingen en maatregelen). Een stap verder in het versterken van de onderlinge relaties (en opbouw van begrip en wederzijds vertrouwen) is het uitwisselen van liaisons.

Oefenen

Oefen kleinschalig om crisisfunctionarissen bekend te maken met cyberplannen, actoren en basis-terminologie. Nodig daarbij vertegenwoordigers van het VR-ISAC en het NCSC uit voor nadere uitleg.

Communicatie

Maak een overzicht van actoren en informatieposities voor Communicatie: wie beschikt over welke informatie?

Opleidingsadvies

Verhogen kennisniveau crisisfunctionarissen

Gebruik oefeningen en opleidingen om het kennisniveau van crisisfunctionarissen op het gebied van cyber te verhogen. Een mogelijkheid is het ontwikkelen van een ‘opleidingsmodule Cyber’ voor operationeel leiders en andere crisisfunctionarissen van de veiligheidsregio’s, die meer duidelijkheid geeft over hun taken en verantwoordelijkheden tijdens een cyberincident. Daaraan kunnen veiligheidsregio’s, landelijke netwerken (zoals de werkgroep Cyber en het VR-ISAC) en IFV bijdragen, onder andere door het uitwisselen van eigen oefenervaringen, evaluaties en kennisopbouw.

Sectorale cyberoefening voor veiligheidsregio’s

Organiseer als veiligheidsregio’s in 2023 een sectorale cyberoefening, waaraan alle 25 veiligheidsregio’s deelnemen. Hierbij kan geleerd worden van de sectorale cyberoefening in het hoger onderwijs door SURF.

Evaluatie optreden

Het IFV evalueerde het optreden van de veiligheidsregio's, het LOCC en het VR-ISAC tijdens de ISIDOOR 2021 oefening. Deze evaluatie was gericht op leren, waarbij de focus lag op drie oefendoelen:

1. Informatie-uitwisseling tussen Rijk en regio én met crisispartners.
2. Bovenregionale afstemming tussen LOCC, het VR-ISAC en regio's.
3. Nagaan in hoeverre huidige expertise van crisisfunctionarissen én ingeregelde afspraken zich voldoende lenen voor een landelijke cybercrisis.

Aanpak

Voor de evaluatie is door het IFV een evaluatie-kader opgesteld. De evaluaties hadden de vorm van tussentijdse intervisie tijdens de oefening (1 t/m 3 juni 2021) en waren gericht op leren en verbeteren. De evaluatoren begeleidden twee evaluatiemomenten per team. Daarnaast vond op 17 juni een gezamenlijke evaluatie plaats met deelnemers van de oefening. De bevindingen zijn op 23 juni 2021 besproken met de werkgroep Digitale ontwrichting en cyber.

Opdrachtgevers: Portefeuillehouder Digitale ontwrichting en cyber en POI

Contactpersonen: Jana Domrose, Laurens van der Varst

September 2021 | Instituut Fysieke Veiligheid | 026 355 24 00 | www.ifv.nl | info@ifv.nl

Instituut Fysieke Veiligheid