Instituut Fysieke Veiligheid

Cyberscenario's voor veiligheidsregio's

#1 Cyberdreiging bij BRZO-bedrijf

#2 Gijzelsoftware bij veiligheidsregio

#3 Verstoring ICT bij regionale zorginstelling

#4 Grote cyberverstoring bij drinkwaterbedrijf

#5 Landelijke stroomuitval door cyberverstoring

De cyberscenario's zijn opgesteld als hulpmiddel voor veiligheidsregio's om op een gestructureerde wijze na te denken over hun voorbereiding op en wijze van optreden bij cyberverstoringen. Veiligheidsregio's kunnen de scenario's gebruiken voor (bestuurlijke) table tops, oefeningen en planvorming.

DE HAAGSE HOGESCHOOL

Instituut Fysieke Veiligheid

16 juni 2021

Inhoud

Opdrachtgever:
Steven van de Looij, portefeuillehouder Digitale ontwrichting en cyber namens de Raad van Commandanten en Directeuren Veiligheidsregio (RCDV)

Contactpersoon:
Laurens van der Varst (IFV)

Auteurs:
Daan Heijmen, Laurens van der Varst (IFV) en
Jelle Groenendaal (De Haagse Hogeschool).

Voorwoord

De digitalisering van de wereld om ons heen gaat steeds sneller. Dit biedt ons een hoop kansen, maar stelt ons ook voor (nieuwe) uitdagingen. De afhankelijkheden nemen toe en digitale incidenten kunnen vergaande gevolgen hebben. Het is zaak dat veiligheidsregio's en crisispartners zich goed voorbereiden om de impact van digitale ontwrichting zo klein mogelijk te houden.

Hoewel het vakgebied cybergevolgbestrijding niet meer volledig nieuw is, blijft het volop in ontwikkeling. Er zijn al verschillende crisisplannen ontwikkeld en het Nationaal Crisisplan Digitaal heeft de bouwstenen-methodiek geïntroduceerd. Deze bouwstenen bieden houvast bij de duiding van een digitale verstoring. We merkten echter dat in aanvulling hierop behoefte was aan wat meer concrete scenario's.

Daarom heb ik het lectoraat Crisisbeheersing van het IFV gevraagd om vijf concrete cyberscenario's te ontwikkelen. De scenario's zijn verschillend van schaal en scope, maar voorzien alle vijf een bepaalde rol voor de veiligheidsregio. Ze kunnen de basis zijn voor regionale cyberoefeningen of table-tops en bieden houvast bij het gesprek over rollen, netwerken en relevante crisispartners. Ik nodig veiligheidsregio's en crisispartners van harte uit de scenario's ter hand te nemen en aan de slag te gaan!

Ik wens jullie veel succes met het voorkomen van en voorbereiden op de volgende cybercrises!

Steven van de Looij
Portefeuillehouder Digitale ontwrichting
en cyber, namens de RCDV

Aanleiding

Cyberdreigingen vormen een actueel risico. Veiligheidsregio's bereiden zich op verschillende manieren voor op cyberrisico's. Door investeren in informatieveiligheid, door plan- en netwerkvorming voor cybergevolgbestrijding en door oefenen. De portefeuillehouder Digitale ontwrichting en cyber van de RCDV heeft het lectoraat Crisisbeheersing van het Instituut Fysieke Veiligheid gevraagd maatgevende cyberscenario's voor veiligheidsregio's uit te werken. Deze cyberscenario's moeten veiligheidsregio's helpen om zich voor te bereiden op cyberverstoringen.

Doel

Veiligheidsregio's kunnen met tal van cyberverstoringen te maken krijgen. Weinig realistisch is dat regio's voorbereidingen treffen op alle type verstoringen: de capaciteit is schaars en regio's moeten ook geprepareerd zijn op risico's als ongevallen en natuurbranden. Daarom zijn er vijf voorstelbare, maar nadrukkelijk fictieve scenario's geselecteerd.

De cyberscenario's dienen voor veiligheidsregio's als hulpmiddel om op een gestructureerde manier na te denken over hun wijze van optreden. Het doel is dat veiligheidsregio's hun eigen antwoorden formuleren op vragen als:

1. Hoe ziet de veiligheidsregio haar eigen rol in de verschillende scenario's?
2. Hoe is de regio op deze scenario's voorbereid?
3. Hoe verlopen processen als opschaling en alarmering, leiding en coördinatie, en crisiscommunicatie?
4. Welke kennis en kunde zijn er nodig voor cybergevolgbestrijding?

Veiligheidsregio's kunnen de scenario's gebruiken als materiaal voor trainingen, oefeningen en bestuurlijke table-tops. Daarnaast kunnen de scanario's als input dienen voor vervolgonderzoek, opleiding en onderwijs. We hopen dat de scenario's bijdragen aan het vergroten van bewustwording en aan een open houding en vernieuwende manier van denken en doen: hoe zijn we als veiligheidsregio voorbereid, welke rol kunnen we vervullen bij cyberverstoringen en welke partners hebben we daarbij nodig?

Aanpak

De vijf uitgewerkte scenario's zijn het resultaat van een verkennend onderzoek bestaande uit drie stappen:

1 Het opstellen van een groslijst aan mogelijke cyberscenario's

Hiervoor hebben we een beknopt bronnenonderzoek gedaan en tien experts geïnterviewd, werkzaam binnen de cybersecurity, veiligheidsregio's of als aanbieder van een vitale dienst. Voor het bronnenonderzoek hebben we gekeken naar eerdere relevante publicaties, zoals

- de Handreiking Cybergevolgbestrijding G4-gemeenten (Berenschot, 2020)
- het Nationaal Crisisplan Digitaal (NCTV, 2020)
- de Toekomstverkenning van het Cyberdomein in 2022 (RIVM, 2015) en
- het Cybersecuritybeeld van Nederland (NCSC, 2020).

De tien geïnterviewde experts waren werkzaam voor Berenschot, COT, Hunt & Hackett, NCC, NCSC, Politie, Saxion Hogeschool, TNO, Vodafone Ziggo en een veiligheidsregio.

Op basis van het bronnenonderzoek en de interviews hebben we een groslijst opgesteld met twintig cyberscenario's die volgens de experts waarschijnlijk of mogelijk kunnen plaatsvinden. Het merendeel van de scenario's had betrekking op een aanval op of verstoring van de (vitale) infrastructuur. Ook veel benoemd waren scenario's die de hulpverlening/veiligheidsregio's zelf raken.

2 Selectie van vijf maatgevende scenario's uit de groslijst

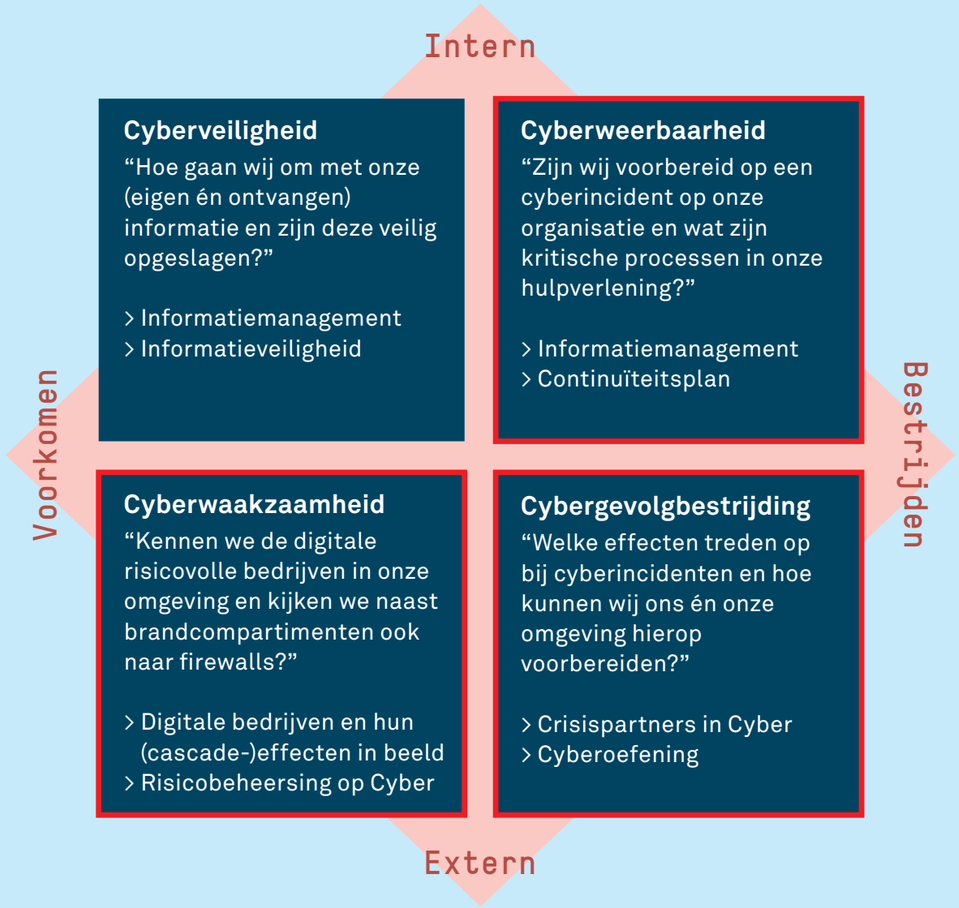
Hiervoor hebben we enerzijds bepaald welke scenario's het vaakst door de experts zijn benoemd, en anderzijds de bouwstenen uit het Nationaal Crisisplan Digitaal bekeken. Ons doel was vooral om te zorgen voor een diversiteit aan scenario's (alle bouwstenen moeten in verschillende configuraties terugkomen in de scenario's) en verschillende zwaarteniveaus (van een dreiging via impact in slechts één veiligheidsregio tot een nationale cybercrisis die alle burgers raakt). De vijf geselecteerde scenario's en de voorgestelde aanpak voor het uitwerken ervan zijn gevalideerd door de Werkgroep Digitale ontwrichting en cyber.

3 Het uitwerken van de vijf geselecteerde scenario's

Hiervoor zijn eerst de scenario's verder vormgegeven op basis van bronnenonderzoek (van bronnen over bijvoorbeeld incidenten die eerder hebben plaatsgevonden) en de input van experts. Tijdens een ontwerpsessie hebben we een aantal van de eerdergenoemde experts gevraagd om de scenario's verder in te kleuren. Hierbij is aandacht besteed aan inhoud en tijdsverloop van het scenario, overwegingen (voortkomend uit enkele kerndilemma's en -besluiten), vragen die in het scenario kunnen spelen en de (bestuurlijke) aandachtspunten. Bij de ontwikkeling hebben we gestreefd naar scenario's die voor veiligheidsregio's plausibel, relevant en verrassend zijn.

Veiligheidsregio en cyberverstoringen: cyberkwadrant

Een bruikbaar ordeningskader is het zogeheten cyber-kwadrant zoals opgesteld door Veiligheidsregio IJsselland. Dat kwadrant ordent op twee assen: voorkomen - bestrijden, en intern - extern. De cyberscenario's raken aan alle kwadranten. De focus ligt op weerbaarheid, waakzaamheid en cybergevolgbestrijding.



Cyberkwadrant
(Veiligheidsregio IJsselland, 2019)

Rollen veiligheidsregio bij cyberverstoringen

We onderscheiden zes mogelijke rollen voor veiligheidsregio's bij cyberverstoringen.

Risicoadviseur:
De veiligheidsregio als risicoadviseur op het gebied van cyber, hoofdzakelijk in de koude fase. De risicoadviseur voert met instellingen en bedrijven een risicodialoog en draagt zodoende bij aan bewustwording.

Netwerkregisseur:
De veiligheidsregio als netwerkregisseur op het gebied van cyber, zowel in de koude als warme fase. De netwerkregisseur brengt partijen bij elkaar, bijvoorbeeld voor risico- en scenarioanalyse en gemeenschappelijke oefeningen.

Bijstandsverlener:
De veiligheidsregio als bijstandsverlener bij cyberverstoringen, zoals het faciliteren van een crisisstructuur en/of helpen bij crisiscommunicatie.

Probleemeigenaar:
De veiligheidsregio als verantwoordelijke voor bron- en effectbestrijding als gevolg van een verstoring die de regio zelf raakt.

Gevolgbestrijder:
De veiligheidsregio als verantwoordelijke voor het bestrijden van de (fysieke) gevolgen van externe cyberverstoringen.

Digitale brandweer:
De veiligheidsregio als digitale brandweer betrokken bij de bron- en effectbestrijding van een externe cyberverstoring.

Let op! Dit zijn *mogelijke rollen* die een veiligheidsregio zou kunnen vervullen op het gebied van cyber. Een rol voor de veiligheidsregio als digitale brandweer ligt bijvoorbeeld niet voor de hand en is momenteel weinig realistisch[1]. De rollen dienen vooral als hulpmiddel en als herinnering om per casus pragmatisch te kijken naar de toegevoegde waarde die een veiligheidsregio kan hebben, los van haar wettelijke taken.

[1] De WRR (2019) stelt dat grote bedrijven een eigen digitale brandweer moeten hebben, bijvoorbeeld in de vorm van de eigen cybersecurityafdeling, een sectoraal CERT of particulier cybersecuritybedrijf.

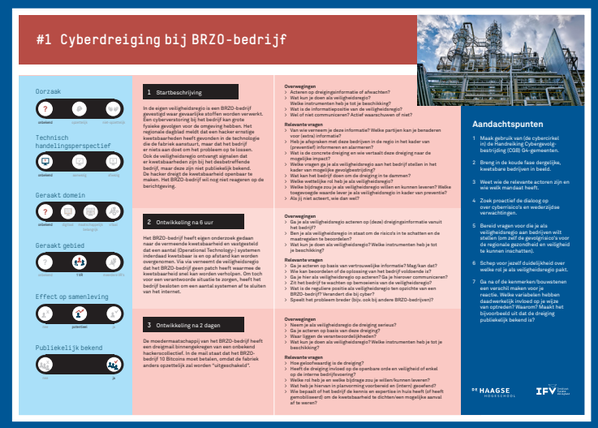
Gebruiksinstructie cyberscenario's

Zoals gezegd zijn er vijf scenario's:
#1 Cyberdreiging bij BRZO-bedrijf
#2 Gijzelsoftware bij veiligheidsregio
#3 Verstoring ICT bij regionale zorginstelling
#4 Grote cyberverstoring bij drinkwaterbedrijf
#5 Landelijke stroomuitval door cyberverstoring

Dit zijn fictieve scenario's. Scenario's voltrekken zich nooit volgens plan; géén crisis is hetzelfde. Wees alert op tunnelvisie en blinde vlekken, en houd, in de voorbereiding en acute crisis, altijd oog voor het bijzondere. Het staat iedereen vrij de scenario's op eigen wijze te gebruiken. Ons advies zou zijn om één of twee scenario's te kiezen en deze uitvoerig te doorleven. Daarbij geldt: bij voorkeur klein beginnen (met scenario 1, 2 of 3).

Elk scenario begint met een startbeschrijving en twee vervolgbeschrijvingen. Links van deze beschrijvingen worden aan de hand van schuifjes de kenmerken (of: bouwstenen) van het geschetste scenario weergegeven. Rechts van de beschrijvingen staan de mogelijke rollen voor een veiligheidsregio bij een cyberverstoring.
Ga op basis van dit eerste beeld in gesprek. Wat betekent dit scenario voor de veiligheidsregio? Welke rollen zou de regio kunnen pakken? Welke vragen roept het geschetste scenario op?

Op de tweede pagina van het geschetste scenario zijn enkele overwegingen en relevante vragen toegevoegd. Daarnaast worden enkele algemene aandachtspunten benoemd. Ga de overwegingen en de relevante vragen af. Welke antwoorden kunnen worden gegeven? Welke vragen roept het scenario op?



Overzicht scenario's

#1 Cyberdreiging bij BRZO-bedrijf

#2 Gijzelsoftware bij veiligheidsregio

#3 Verstoring ICT bij regionale zorginstelling

#4 Grote cyberverstoring bij drinkwaterbedrijf

#5 Landelijke stroomuitval door cyberverstoring

#1 Cyberdreiging bij BRZO-bedrijf

1 Startbeschrijving

In de eigen veiligheidsregio is een BRZO-bedrijf gevestigd waar gevaarlijke stoffen worden verwerkt. Een cyberverstoring bij het bedrijf kan grote fysieke gevolgen voor de omgeving hebben. Het regionale dagblad meldt dat een hacker ernstige kwetsbaarheden heeft gevonden in de technologie die de fabriek aanstuurt, maar dat het bedrijf er niets aan doet om het probleem op te lossen. Ook de veiligheidsregio ontvangt signalen dat er kwetsbaarheden zijn bij het desbetreffende bedrijf, maar deze zijn niet publiekelijk bekend. De hacker dreigt de kwetsbaarheid openbaar te maken. Het BRZO-bedrijf wil nog niet reageren op de berichtgeving.

Oorzaak

onbekend | opzettelijk | niet-opzettelijk

Technisch handelingsperspectief

onbekend | aanwezig | afwezig

Geraakt domein

onbekend | digitaal | maatschappelijk belangrijk | vitaal

Geraakt gebied

onbekend | één veiligheidsregio | meerdere veiligheidsregio's

Effect op samenleving

nee | potentieel | ja

Publiekelijk bekend

nee | ja

2 Ontwikkeling na 6 uur

Het BRZO-bedrijf heeft eigen onderzoek gedaan naar de vermeende kwetsbaarheid en vastgesteld dat een aantal (Operational Technology-) systemen inderdaad kwetsbaar is en op afstand kan worden overgenomen. Via via verneemt de veiligheidsregio dat het BRZO-bedrijf geen patch heeft waarmee de kwetsbaarheid snel kan worden verholpen. Om toch voor een verantwoorde situatie te zorgen, heeft het bedrijf besloten om een aantal systemen af te sluiten van het internet.

3 Ontwikkeling na 2 dagen

De moedermaatschappij van het BRZO-bedrijf heeft een dreigmail binnengekregen van een onbekend hackerscollectief. In de mail staat dat het BRZO-bedrijf 10 Bitcoins moet betalen, omdat de fabriek anders opzettelijk zal worden "uitgeschakeld".

Mogelijke rollen veiligheidsregio's

- Risicoadviseur
- Netwerkregisseur
- Bijstandsverlener
- Probleemeigenaar
- Gevolgbestrijder
- Digitale brandweer

DE HAAGSE HOGESCHOOL

IFV Instituut Fysieke Veiligheid

#1 Cyberdreiging bij BRZO-bedrijf

Oorzaak

Technisch handelingsperspectief

Geraakt domein

Geraakt gebied

Effect op samenleving

Publiekelijk bekend

1 Startbeschrijving

In de eigen veiligheidsregio is een BRZO-bedrijf gevestigd waar gevaarlijke stoffen worden verwerkt. Een cyberverstoring bij het bedrijf kan grote fysieke gevolgen voor de omgeving hebben. Het regionale dagblad meldt dat een hacker ernstige kwetsbaarheden heeft gevonden in de technologie die de fabriek aanstuurt, maar dat het bedrijf er niets aan doet om het probleem op te lossen. Ook de veiligheidsregio ontvangt signalen dat er kwetsbaarheden zijn bij het desbetreffende bedrijf, maar deze zijn niet publiekelijk bekend. De hacker dreigt de kwetsbaarheid openbaar te maken. Het BRZO-bedrijf wil nog niet reageren op de berichtgeving.

Overwegingen
- Acteren op dreigingsinformatie of afwachten?
- Wat kun je doen als veiligheidsregio? Welke instrumenten heb je tot je beschikking?
- Wat is de informatiepositie van de veiligheidsregio?
- Wel of niet communiceren? Actief waarschuwen of niet?

Relevante vragen
- Van wie verneem je deze informatie? Welke partijen kan je benaderen voor (extra) informatie?
- Heb je afspraken met deze bedrijven in de regio in het kader van (preventief) informeren en alarmeren?
- Wat is de concrete dreiging en wie vertaalt deze dreiging naar de mogelijke impact?
- Welke vragen ga je als veiligheidsregio aan het bedrijf stellen in het kader van mogelijke gevolgbestrijding?
- Wat kan het bedrijf doen om de dreiging in te dammen?
- Welke wettelijke rol heb je als veiligheidsregio?
- Welke bijdrage zou je als veiligheidsregio willen en kunnen leveren? Welke toegevoegde waarde lever je als veiligheidsregio in kader van preventie?
- Als jij niet acteert, wie dan wel?

2 Ontwikkeling na 6 uur

Het BRZO-bedrijf heeft eigen onderzoek gedaan naar de vermeende kwetsbaarheid en vastgesteld dat een aantal (Operational Technology-) systemen inderdaad kwetsbaar is en op afstand kan worden overgenomen. Via via verneemt de veiligheidsregio dat het BRZO-bedrijf geen patch heeft waarmee de kwetsbaarheid snel kan worden verholpen. Om toch voor een verantwoorde situatie te zorgen, heeft het bedrijf besloten om een aantal systemen af te sluiten van het internet.

Overwegingen
- Ga je als veiligheidsregio acteren op (deze) dreigingsinformatie vanuit het bedrijf?
- Ben je als veiligheidsregio in staat om de risico's in te schatten en de maatregelen te beoordelen?
- Wat kun je doen als veiligheidsregio? Welke instrumenten heb je tot je beschikking?

Relevante vragen
- Ga je acteren op basis van vertrouwelijke informatie? Mag/kan dat?
- Wie kan beoordelen of de oplossing van het bedrijf voldoende is?
- Ga je hier als veiligheidsregio op acteren? Ga je hierover communiceren?
- Zit het bedrijf te wachten op bemoeienis van de veiligheidsregio?
- Wat is de reguliere positie als veiligheidsregio ten opzichte van een BRZO-bedrijf? Verandert die bij cyber?
- Speelt het probleem breder (bijv. ook bij andere BRZO-bedrijven)?

3 Ontwikkeling na 2 dagen

De moedermaatschappij van het BRZO-bedrijf heeft een dreigmail binnengekregen van een onbekend hackerscollectief. In de mail staat dat het BRZO-bedrijf 10 Bitcoins moet betalen, omdat de fabriek anders opzettelijk zal worden "uitgeschakeld".

Overwegingen
- Neem je als veiligheidsregio de dreiging serieus?
- Ga je acteren op basis van deze dreiging?
- Waar liggen de verantwoordelijkheden?
- Wat kun je doen als veiligheidsregio? Welke instrumenten heb je tot je beschikking?

Relevante vragen
- Hoe geloofwaardig is de dreiging?
- Heeft de dreiging invloed op de openbare orde en veiligheid of enkel op de interne bedrijfsvoering?
- Welke rol heb je en welke bijdrage zou je willen/kunnen leveren?
- Wat heb je hiervan in planvorming voorbereid en (intern) geoefend?
- Wie bepaalt of het bedrijf de kennis en expertise in huis heeft (of heeft gemobiliseerd) om de kwetsbaarheid te dichten/een mogelijke aanval af te weren?

Aandachtspunten

1. Maak gebruik van (de cybercirkel in) de Handreiking Cybergevolg-bestrijding (CGB) G4-gemeenten.
2. Breng in de koude fase dergelijke, kwetsbare bedrijven in beeld.
3. Weet wie de relevante actoren zijn en wie welk mandaat heeft.
4. Zoek proactief de dialoog op over cyberrisico's en wederzijdse verwachtingen.
5. Bereid vragen voor die je als veiligheidsregio aan bedrijven wilt stellen (om zelf de gevolgrisico's voor de regionale gezondheid en veiligheid te kunnen inschatten).
6. Schep voor jezelf duidelijkheid over welke rol je als veiligheidsregio pakt.
7. Ga na of de kenmerken/bouwstenen een verschil maken voor je reactie. Welke variabelen hebben daadwerkelijk invloed op je wijze van optreden? Waarom? Maakt het bijvoorbeeld uit dat de dreiging publiekelijk bekend is?

DE HAAGSE HOGESCHOOL
IFV Instituut Fysieke Veiligheid

#2 Gijzelsoftware bij veiligheidsregio

Oorzaak

Technisch handelingsperspectief

Geraakt domein

Geraakt gebied

Effect op samenleving

Publiekelijk bekend

1 Startbeschrijving

Een medewerker Operationele Systemen van de veiligheidsregio krijgt op zaterdagochtend meldingen van verstoringen van systemen. Samen met zijn collega's van IT onderzoekt de medewerker de aanleiding van de verstoringen. Na 2 uur blijkt uit de eerste bevindingen dat er vermoedelijk sprake is van ransomware. Ze willen zeker zijn van hun zaak en proberen eerst zelf het probleem te verhelpen. Ze besluiten dan ook door te gaan met hun onderzoek.

2 Ontwikkeling na 8 uur

Acht uur na het eerste onderzoek, doen de medewerkers melding bij hun leidinggevende. Er blijkt inderdaad sprake van ransomware; in een hackersnote eisen de hackers €200.000 losgeld. De hackers hebben een deel van de systemen versleuteld. De leidinggevende informeert direct het MT, waarop dit besluit meteen alle systemen volledig offline te halen.
De reguliere communicatiekanalen (zoals de website en Outlook) functioneren niet en de impact op personeel en bedrijfsvoering zijn enorm. Er is veel onrust onder het personeel: medewerkers zitten met praktische vragen. De emotionele impact is groot. De meldkamer en C2000/P2000 zijn wel gewoon beschikbaar en de operationele inzet is niet direct in gevaar.
De veiligheidsregio besluit het NCSC direct te informeren, evenals het VR-ISAC. De veiligheidsregio neemt contact op met commerciële incidentresponsebedrijven en bedrijven die zich richten op forensisch onderzoek; die hebben echter weinig capaciteit beschikbaar vanwege een zeer urgente cyberdreiging.

3 Ontwikkeling na 2 dagen

Back-ups zijn niet beschikbaar. Daarnaast kunnen de salaris-betalingen van vrijwilligers en leveranciers niet plaatsvinden, doordat de salarisadministratie is geraakt. Tevens speelt er een urgent risico dat acute inzet vergt, namelijk extreem weer. Dit risico gaat op korte termijn grootschalige inzet van de veiligheidsregio vergen. Uit een analyse blijkt dat tenminste 500 MB aan data het bedrijfsnetwerk verlaten heeft. Het is onduidelijk wat voor data het betreft. Het Team High Tech Crime van de nationale politie is gestart met onderzoek. De Inspectie Justitie en Veiligheid besluit landelijk onderzoek te doen naar de informatiebeveiliging bij veiligheidsregio's.

Mogelijke rollen veiligheidsregio's

- Risicoadviseur
- Netwerkregisseur
- Bijstandsverlener
- Probleemeigenaar
- Gevolgbestrijder
- Digitale brandweer

DE HAAGSE HOGESCHOOL

IFV Instituut Fysieke Veiligheid

#2 Gijzelsoftware bij veiligheidsregio

Oorzaak

Technisch handelingsperspectief

Geraakt domein

Geraakt gebied

Effect op samenleving

Publiekelijk bekend

1 Startbeschrijving

Een medewerker Operationele Systemen van de veiligheidsregio krijgt op zaterdagochtend meldingen van verstoringen van systemen. Samen met zijn collega's van IT onderzoekt de medewerker de aanleiding van de verstoringen. Na 2 uur blijkt uit de eerste bevindingen dat er vermoedelijk sprake is van ransomware. Ze willen zeker zijn van hun zaak en proberen eerst zelf het probleem te verhelpen. Ze besluiten dan ook door te gaan met hun onderzoek.

Overwegingen
- Wat is het detectievermogen van de organisatie?
- Ga je preventief informeren?
- Wanneer ga je over tot alarmeren?

Relevante vragen
- Welke interne afspraken zijn er over opschaling en alarmering bij verstoringen?
- Welke werknemers zijn in het weekend beschikbaar?
- Hoe is de veiligheidsregio voorbereid op gijzelsoftware?
- Heb je inzicht in het ICT-landschap?
- Is er geoefend met cyberverstoringen?

2 Ontwikkeling na 8 uur

Acht uur na het eerste onderzoek, doen de medewerkers melding bij hun leidinggevende. Er blijkt inderdaad sprake van ransomware; in een hackersnote eisen de hackers €200.000 losgeld. De hackers hebben een deel van de systemen versleuteld. De leidinggevende informeert direct het MT, waarop dit besluit meteen alle systemen volledig offline te halen.
De reguliere communicatiekanalen (zoals de website en Outlook) functioneren niet en de impact op personeel en bedrijfsvoering zijn enorm. Er is veel onrust onder het personeel: medewerkers zitten met praktische vragen. De emotionele impact is groot. De meldkamer en C2000/P2000 zijn wel gewoon beschikbaar en de operationele inzet is niet direct in gevaar.
De veiligheidsregio besluit het NCSC direct te informeren, evenals het VR-ISAC. De veiligheidsregio neemt contact op met commerciële incidentresponsebedrijven en bedrijven die zich richten op forensisch onderzoek; die hebben echter weinig capaciteit beschikbaar vanwege een zeer urgente cyberdreiging.

Overwegingen
- Crisiscommunicatie: hoe open/gesloten ben je?
- Hoe mobiliseer je externe expertise?
- Hoe richt je de interne crisisorganisatie/opschaling in (GRIP)?
- Voor welke crisisstructuur kies je: reguliere of flexibele crisisorganisatie?

Relevante vragen
- Wat ga je intern en extern communiceren? Via welke kanalen?
- Wie zijn belangrijke stakeholders die je moet informeren?
- Hoe mobiliseer je externe expertise? Wie ga je bellen?
- Is er contact met het VR-ISAC?
- Welke afspraken zijn er met leveranciers?
- Welke interne collega's moet je betrekken?
- Wat is de samenstelling van de interne crisisorganisatie?
- Welke hulpmiddelen (plannen, draaiboeken) kan je benutten?
- Is er aangifte gedaan?
- Hoe organiseer je beslisbevoegdheid? Wie is bevoegd tot bijvoorbeeld het besluit inzake losgeld?

3 Ontwikkeling na 2 dagen

Back-ups zijn niet beschikbaar. Daarnaast kunnen de salaris-betalingen van vrijwilligers en leveranciers niet plaatsvinden, doordat de salarisadministratie is geraakt. Tevens speelt er een urgent risico dat acute inzet vergt, namelijk extreem weer. Dit risico gaat op korte termijn grootschalige inzet van de veiligheidsregio vergen. Uit een analyse blijkt dat tenminste 500 MB aan data het bedrijfsnetwerk verlaten heeft. Het is onduidelijk wat voor data het betreft. Het Team High Tech Crime van de nationale politie is gestart met onderzoek.
De Inspectie Justitie en Veiligheid besluit landelijk onderzoek te doen naar de informatiebeveiliging bij veiligheidsregio's.

Overwegingen
- Geef je prioriteit aan forensisch onderzoek of herstelwerkzaamheden?
- Kies je voor snelheid of zorgvuldigheid?
- Betaal je losgeld of niet?

Relevante vragen
- Ga je het losgeld betalen omdat je geen back-ups hebt?
- Wat zijn je prioriteiten in herstel? Heb je een Business Continuity Plan klaarliggen?
- Welke strategie kies je (snelheid of zorgvuldigheid)?
- Wie voert forensisch onderzoek uit?
- Wie werkt aan recovery?
- Om welke data (500 MB) gaat het? Wat betekent dat?
- Wat betekent dit voor de reguliere crisisorganisatie? Wat doe je met de aankomende, acute crisis?

Aandachtspunten

1. Zorg dat je als veiligheidsregio bent voorbereid op een cyberverstoring met gijzelsoftware.
   Maak afspraken over o.a.:
   - Alarmering en opschaling
   - Leiding en coördinatie
   - Interne kennis en kunde: welke interne functionarissen betrekken? Denk aan: CISO, Functionaris Gegevens-bescherming
   - Externe kennis en kunde: afspraken met externe leveranciers, NCSC en andere relevante stakeholders. Ben je in staat snel expertise te mobiliseren?
   - Bijstand: afspraken over bijstand vanuit andere regio's
   - Hulpmiddelen: plannen, draaiboeken
   - Communicatie
2. Maak in de koude fase inzichtelijk welke kritische processen, systemen en gegevens er zijn. Waar bevinden deze zich, hoe liggen afhankelijkheden en wat moet altijd beschikbaar zijn (Business Continuity Management)?
3. Geef duidelijk aan of je als veiligheids-regio in staat bent tot bronbestrijding of dat je daarbij de hulp van anderen nodig hebt.
4. Heb aandacht voor de (emotionele) impact van dergelijke verstoringen op het eigen personeel. Wees daarop voorbereid.

DE HAAGSE HOGESCHOOL
IFV Instituut Fysieke Veiligheid

#3 Verstoring ICT bij regionale zorginstelling

1 Startbeschrijving

Bij het regionale ziekenhuis liggen op donderdagmiddag de ICT-voorzieningen plat. Mogelijke oorzaak is een lekkage tijdens grootschalige renovatiewerkzaamheden. Hierdoor zijn patiëntendossiers niet beschikbaar en functioneren systemen niet (o.a. administratie en planning). Niet noodzakelijke operaties en visitaties moeten noodgedwongen worden uitgesteld en patiënten kunnen via reguliere communicatiekanalen zoals e-mail en (digitale) telefoon niet worden bereikt. Via Twitter laat het ziekenhuis weten dat er problemen spelen en dat wordt gewerkt aan een oplossing. Het is onduidelijk of er als gevolg van de storing vergelijkbare ICT-problemen spelen bij dependances van het ziekenhuis op andere locaties.

2 Ontwikkeling na 6 uur

Er komen via diverse kanalen steeds meer signalen binnen bij de veiligheidsregio dat het ziekenhuis de problemen niet onder controle krijgt. Er zou intern sprake zijn van chaos en een heldere crisisstructuur zou ontbreken. Patiënten zouden in veel gevallen niet goed worden geïnformeerd over de verstoring. Men vreest voor uitstel van spoedeisende zorg. Op sociale media neemt de onrust over het incident toe. De voorzitter van de veiligheidsregio krijgt vragen van raadsleden.

3 Ontwikkeling na 4 maanden

Na 2 dagen is de verstoring verholpen en er wordt een onafhankelijk onderzoek ingesteld. Na 4 maanden verschijnt het onderzoeksrapport. Het kritische onderzoeksrapport concludeert dat het ziekenhuis onvoldoende was voorbereid op een cyberverstoring. De crisisrespons van het ziekenhuis was daardoor ondermaats. Er zou met name behoefte zijn geweest aan een heldere crisisstructuur en crisiscommunicatie (met handelingsperspectieven) richting de patiënten en de samenleving.

Oorzaak

onbekend | opzettelijk | niet-opzettelijk

Technisch handelingsperspectief

onbekend | aanwezig | afwezig

Geraakt domein

onbekend | digitaal | maatschappelijk belangrijk | vitaal

Geraakt gebied

onbekend | één veiligheidsregio | meerdere veiligheidsregio's

Effect op samenleving

nee | potentieel | ja

Publiekelijk bekend

nee | ja

Mogelijke rollen veiligheidsregio's

- Risicoadviseur
- Netwerkregisseur
- Bijstandsverlener
- Probleemeigenaar
- Gevolgbestrijder
- Digitale brandweer

DE HAAGSE HOGESCHOOL

IFV Instituut Fysieke Veiligheid

#3 Verstoring ICT bij regionale zorginstelling

Oorzaak

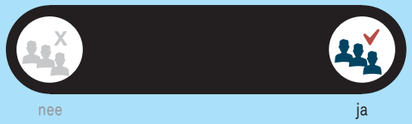
Technisch handelingsperspectief

Geraakt domein

Geraakt gebied

Effect op samenleving

Publiekelijk bekend



1 Startbeschrijving

Bij het regionale ziekenhuis liggen op donderdagmiddag de ICT-voorzieningen plat. Mogelijke oorzaak is een lekkage tijdens grootschalige renovatiewerkzaamheden. Hierdoor zijn patiëntendossiers niet beschikbaar en functioneren systemen niet (o.a. administratie en planning). Niet noodzakelijke operaties en visitaties moeten noodgedwongen worden uitgesteld en patiënten kunnen via reguliere communicatiekanalen zoals e-mail en (digitale) telefoon niet worden bereikt. Via Twitter laat het ziekenhuis weten dat er problemen spelen en dat wordt gewerkt aan een oplossing. Het is onduidelijk of er als gevolg van de storing vergelijkbare ICT-problemen spelen bij dependances van het ziekenhuis op andere locaties.

Overwegingen
- Wat is de informatiepositie van de veiligheidsregio?
- Welke rol pak je als veiligheidsregio?

Relevante vragen
- Hoe bereikt deze info de veiligheidsregio?
- Zie je een mogelijke rol voor de regio? Ga je bijstand verlenen?
- Ga je preparatief opschalen?
- Maakt het voor de veiligheidsregio uit wat de oorzaak van de verstoring is?

2 Ontwikkeling na 6 uur

Er komen via diverse kanalen steeds meer signalen binnen bij de veiligheidsregio dat het ziekenhuis de problemen niet onder controle krijgt. Er zou intern sprake zijn van chaos en een heldere crisisstructuur zou ontbreken. Patiënten zouden in veel gevallen niet goed worden geïnformeerd over de verstoring. Men vreest voor uitstel van spoedeisende zorg. Op sociale media neemt de onrust over het incident toe. De voorzitter van de veiligheidsregio krijgt vragen van raadsleden.

Overwegingen
- Wat is de informatiepositie van de veiligheidsregio?
- Waar kan je van toegevoegde waarde zijn?
- Welke bijstand kan je verlenen?

Relevante vragen
- Zie je een rol voor de regio? Welke? Wat ga je doen?
- Ga je opschalen?
- Weet je welke relevante CERT's (zoals Z-CERT) actief zijn en wie je kunt benaderen voor informatie over de duur van de verstoring?

3 Ontwikkeling na 4 maanden

Na 2 dagen is de verstoring verholpen en er wordt een onafhankelijk onderzoek ingesteld. Na 4 maanden verschijnt het onderzoeksrapport. Het kritische onderzoeksrapport concludeert dat het ziekenhuis onvoldoende was voorbereid op een cyberverstoring. De crisisrespons van het ziekenhuis was daardoor ondermaats. Er zou met name behoefte zijn geweest aan een heldere crisisstructuur en crisiscommunicatie (met handelingsperspectieven) richting de patiënten en de samenleving.

Overwegingen
- Wat is je wettelijke versus niet-wettelijk taak?

Relevante vragen
- Welke rol zie je voor de regio op het gebied van cyberwaakzaamheid?
- Ken je de digitale risicovolle bedrijven in je verzorgingsgebied?
- Ga je als regio proactief de dialoog aan met regionale (maatschappelijke) organisaties over cybersecurity en onderlinge samenwerking?

Aandachtspunten

1 Ga na wat je informatiepositie als veiligheidsregio is bij dit soort verstoringen. Hoe bereikt relevante informatie de regio?

2 Denk na over de rol die je als veiligheidsregio mogelijk zou kunnen pakken bij een dergelijke cyber-verstoring. Waar kun je van toegevoegde waarde zijn? Waar liggen je wettelijke en niet-wettelijke taken? Welke bijstand zou je kunnen verlenen? Ben hierin pragmatisch en denk bijvoorbeeld aan (crisis) communicatie of het inbrengen van een crisisstructuur.

3 Denk na over je niet-wettelijke taak op het gebied van cyberwaakzaamheid. Ken je de digitale risicovolle bedrijven in je verzorgingsgebied en ben je daarmee in gesprek over cyberrisico's?

4 Welke afspraken over alarmering & opschaling en leiding & coördinatie bij cyberverstoringen zijn er gemaakt met maatschappelijk relevante bedrijven en organisaties in je verzorgings-gebied?

DE HAAGSE HOGESCHOOL
IFV Instituut Fysieke Veiligheid

#4 Grote cyberverstoring bij drinkwaterbedrijf

Oorzaak

onbekend | opzettelijk | niet-opzettelijk

Technisch handelingsperspectief

onbekend | aanwezig | afwezig

Geraakt domein

onbekend | digitaal | maatschappelijk belangrijk | vitaal

Geraakt gebied

onbekend | één veiligheidsregio | meerdere veiligheidsregio's

Effect op samenleving

nee | potentieel | ja

Publiekelijk bekend

nee | ja

1 Startbeschrijving

Bij een drinkwaterbedrijf wordt een storing geconstateerd in de installatie die zorgdraagt voor de waterzuivering. De installatie reageert slecht op bepaalde commando's en de verschillende sensoren geven vreemde signalen af. Via verschillende kanalen (sociale media, klantenservice, meldkamer) komen er klachten binnen dat het drinkwater een (sterke) zoutachtige smaak heeft. Er is nog geen informatie bekend over een mogelijke oorzaak.

2 Ontwikkeling na 6 uur

Het drinkwaterbedrijf heeft de waterzuivering handmatig stilgezet, omdat het niet meer de controle leek te hebben over de installatie en sensoren. Het gevolg is dat de drinkwaterlevering stil is komen te liggen. Inwoners van drie veiligheidsregio's hebben nu geen drinkwater meer en mensen proberen massaal drinkwater in te slaan bij de supermarkten. Supermarkten kunnen deze vraag logistiek niet bijbenen en er ontstaat schaarste. Het drinkwaterbedrijf geeft aan dat het nog minstens 24 uur gaat duren om de installatie weer stabiel en draaiend te krijgen. Hierbij zegt het bedrijf onderzoek te doen naar de mogelijkheid dat een derde toegang gekregen heeft tot de installatie en de integriteit van de technologie heeft aangetast.

3 Ontwikkeling na 2 dagen

De drinkwaterlevering is na 24 uur weer hervat, maar de systemen moeten nog wel handmatig worden gecontroleerd. Uit het eerste onderzoek blijkt inderdaad dat de storing ontstaan is door een aanval. Verschillende deskundigen melden via Twitter dat zij aanvallen op andere (vitale) organisaties op zeer korte termijn niet uitsluiten. Daarnaast zegt de politie aanwijzingen te hebben dat een deel van de klachten via sociale media over het drinkwater nep zijn.

Mogelijke rollen veiligheidsregio's

- Risicoadviseur
- Netwerkregisseur
- Bijstandsverlener
- Probleemeigenaar
- Gevolgbestrijder
- Digitale brandweer

DE HAAGSE HOGESCHOOL

IFV Instituut Fysieke Veiligheid

#4 Grote cyberverstoring bij drinkwaterbedrijf

Oorzaak

Technisch handelingsperspectief

Geraakt domein

Geraakt gebied

Effect op samenleving

Publiekelijk bekend

1 Startbeschrijving

Bij een drinkwaterbedrijf wordt een storing geconstateerd in de installatie die zorgdraagt voor de waterzuivering. De installatie reageert slecht op bepaalde commando's en de verschillende sensoren geven vreemde signalen af. Via verschillende kanalen (sociale media, klantenservice, meldkamer) komen er klachten binnen dat het drinkwater een (sterke) zoutachtige smaak heeft. Er is nog geen informatie bekend over een mogelijke oorzaak.

Overwegingen
- Wat is je informatiepositie?
- Welke rol voorzie je voor de veiligheidsregio?

Relevante vragen
- Hoe raak je als veiligheidsregio betrokken?
- Hoe verloopt het contact tussen veiligheidsregio's en waterzuiveringsbedrijf?
- Is er contact tussen veiligheidsregio's?

2 Ontwikkeling na 6 uur

Het drinkwaterbedrijf heeft de waterzuivering handmatig stilgezet, omdat het niet meer de controle leek te hebben over de installatie en sensoren. Het gevolg is dat de drinkwaterlevering stil is komen te liggen. Inwoners van drie veiligheidsregio's hebben nu geen drinkwater meer en mensen proberen massaal drinkwater in te slaan bij de supermarkten. Supermarkten kunnen deze vraag logistiek niet bijbenen en er ontstaat schaarste. Het drinkwaterbedrijf geeft aan dat het nog minstens 24 uur gaat duren om de installatie weer stabiel en draaiend te krijgen. Hierbij zegt het bedrijf onderzoek te doen naar de mogelijkheid dat een derde toegang gekregen heeft tot de installatie en de integriteit van de technologie heeft aangetast.

Overwegingen
- Ga je ervan uit dat het probleem binnen 24 uur wordt opgelost of anticipeer je op uitloop?
- Hoe verloopt de samenwerking tussen meerdere veiligheidsregio's? Wie pakt de regie?

Relevante vragen
- Wat zijn worst case en best case scenario?
- Hoe ga je als betrokken veiligheidsregio's samenwerken?
- Voor welke GRIP-procedure kies je? Welke veiligheidsregio neemt de leiding?
- Neem je als veiligheidsregio extra maatregelen nu blijkt dat er mogelijkerwijs een cybercomponent bij is betrokken?

3 Ontwikkeling na 2 dagen

De drinkwaterlevering is na 24 uur weer hervat, maar de systemen moeten nog wel handmatig worden gecontroleerd. Uit het eerste onderzoek blijkt inderdaad dat de storing ontstaan is door een aanval. Verschillende deskundigen melden via Twitter dat zij aanvallen op andere (vitale) organisaties op zeer korte termijn niet uitsluiten. Daarnaast zegt de politie aanwijzingen te hebben dat een deel van de klachten via sociale media over het drinkwater nep zijn.

Overwegingen
- Wanneer ga je afschalen?

Relevante vragen
- Wat ga je als veiligheidsregio's doen wanneer er verhoogde kans is dat ook andere vitale organisaties worden aangevallen?

Aandachtspunten

1 Schep duidelijkheid over je informatiepositie bij dit soort verstoringen. Hoe bereikt relevante informatie de regio?

2 Zorg voor planvorming voor dit scenario. Wees voorbereid!

3 Bepaal kernvragen die je als veiligheidsregio aan de drinkwaterbedrijven stelt voor het inschatten van verwachte (fysieke) effecten: duur, eigen prognoses, benodigde bijstand.

4 Ga na wat je als regio zou kunnen toevoegen in dergelijke casus. Welke bijstand zou je kunnen verlenen? Op welke thema's ga je je als veiligheidsregio richten?

5 Inventariseer in de koude fase welke (vitale en niet-vitale, maatschappelijke) organisaties er zijn in jouw verzorgingsgebied. Welke afspraken over alarmering & opschaling, leiding & coördinatie bij cyberverstoringen zijn er gemaakt?

DE HAAGSE HOGESCHOOL
IFV Instituut Fysieke Veiligheid

#5 Landelijke stroomuitval door cyberverstoring

Oorzaak

onbekend | opzettelijk | niet-opzettelijk

Technisch handelingsperspectief

onbekend | aanwezig | afwezig

Geraakt domein

onbekend | digitaal | maatschappelijk belangrijk | vitaal

Geraakt gebied

onbekend | één veiligheidsregio | meerdere veiligheidsregio's

Effect op samenleving

nee | potentieel | ja

Publiekelijk bekend

nee | ja

1 Startbeschrijving

Het is een warme zomerdag net voor de avondspits in juli wanneer in grote delen van Nederland het stroom uitvalt. Uit de website www.allestoringen.nl blijkt dat vrijwel alle stroomleveranciers zijn geraakt. Door de stroomstoringen zitten miljoenen huishoudens zonder stroom en daarmee zonder wifi-verbinding. Elektronische apparaten en voertuigen kunnen niet meer worden opgeladen en treinen, trams en metro's vallen stil. Spoorbomen gaan niet meer open of dicht. Verkeerslichten en matrixborden boven de weg vallen uit en veel tankstations kunnen niet meer worden gebruikt. Airconditioning in verpleeg- en verzorgingshuizen is uitgevallen. Doordat meerdere stroomleveranciers tegelijkertijd zijn geraakt, is de verdenking groot dat er sprake is van een gecoördineerde cyberaanval.

2 Ontwikkeling na 6 uur

Verschillende stroomleveranciers melden dat het erop lijkt dat een deel van de Operational Technology (OT) intentioneel verwoest is. Verwacht wordt dat binnen 24 uur het grootste deel van het stroomnet weer operationeel is. De impact is echter enorm. Er is een verkeersinfarct ontstaan en in veel gebieden is de waterdruk weggevallen waardoor (hogere) appartementen geen water meer hebben. GSM- en 4G-masten zijn uitgevallen met als gevolg dat mensen hun mobiele telefoon niet meer kunnen gebruiken. Meldkamers zijn niet of nauwelijks bereikbaar. Er is sprake van veesterfte doordat de airconditioning in stallen is uitgevallen. In veel winkels kan niet meer elektronisch worden betaald. Ziekenhuizen blijven operationeel, omdat ze beschikken over noodaggregaten.

3 Ontwikkeling na 2 dagen

Na 30 uur is het grootste deel van Nederland weer voorzien van stroom. De stroomvoorziening is echter nog altijd niet stabiel, met als gevolg dat de stroom in sommige delen van het land weer voor kortere tijd uitvalt. Stroomleveranciers bevestigen nu dat ze zijn aangevallen. Er is veel maatschappelijke verontwaardiging over de aanval en de impact die deze heeft gehad. Media vragen zich af of Rijk en veiligheidsregio's wel in voldoende mate waren voorbereid.

Mogelijke rollen veiligheidsregio's

- Risicoadviseur
- Netwerkregisseur
- Bijstandsverlener
- Probleemeigenaar
- Gevolgbestrijder
- Digitale brandweer

DE HAAGSE HOGESCHOOL

IFV Instituut Fysieke Veiligheid

#5 Landelijke stroomuitval door cyberverstoring

Oorzaak

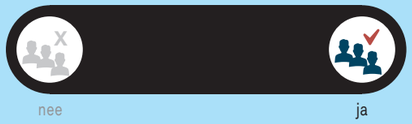
Technisch handelingsperspectief

Geraakt domein

Geraakt gebied

Effect op samenleving

Publiekelijk bekend



1 Startbeschrijving

Het is een warme zomerdag net voor de avondspits in juli wanneer in grote delen van Nederland het stroom uitvalt. Uit de website www.allestoringen.nl blijkt dat vrijwel alle stroomleveranciers zijn geraakt. Door de stroomstoringen zitten miljoenen huishoudens zonder stroom en daarmee zonder wifi-verbinding. Elektronische apparaten en voertuigen kunnen niet meer worden opgeladen en treinen, trams en metro's vallen stil. Spoorbomen gaan niet meer open of dicht. Verkeerslichten en matrixborden boven de weg vallen uit en veel tankstations kunnen niet meer worden gebruikt. Airconditioning in verpleeg- en verzorgingshuizen is uitgevallen. Doordat meerdere stroomleveranciers tegelijkertijd zijn geraakt, is de verdenking groot dat er sprake is van een gecoördineerde cyberaanval.

Overwegingen
- Hoe worden de schaarse hulpmiddelen verdeeld?
- Hoe wordt hierover gecommuniceerd?
- Leiding & coördinatie: welke partij is coördinerend? Hoe ziet de (crisis)structuur eruit?

Relevante vragen
- Prioritering: wie hebben welke hulp het hardst nodig?
- Communicatie: hoe worden deze mensen bereikt?
- Welke problemen zijn voor de veiligheidsregio's en welke voor andere partijen? Hoe kan zelfredzaamheid worden bevorderd?
- Hoe vindt afstemming tussen veiligheidsregio's plaats? En tussen veiligheidsregio's en landelijke actoren?

2 Ontwikkeling na 6 uur

Verschillende stroomleveranciers melden dat het erop lijkt dat een deel van de Operational Technology (OT) intentioneel verwoest is. Verwacht wordt dat binnen 24 uur het grootste deel van het stroomnet weer operationeel is. De impact is echter enorm. Er is een verkeersinfarct ontstaan en in veel gebieden is de waterdruk weggevallen waardoor (hogere) appartementen geen water meer hebben. GSM- en 4G-masten zijn uitgevallen met als gevolg dat mensen hun mobiele telefoon niet meer kunnen gebruiken. Meldkamers zijn niet of nauwelijks bereikbaar. Er is sprake van veesterfte doordat de airconditioning in stallen is uitgevallen. In veel winkels kan niet meer elektronisch worden betaald. Ziekenhuizen blijven operationeel, omdat ze beschikken over noodaggregaten.

Overwegingen
- Scenario's: ga je ervan uit dat het binnen 24 uur wordt opgelost of anticipeer je op uitloop?
- Welke rol pak je als veiligheidsregio?

Relevante vragen
- Wat zijn het worst case en best case scenario?
- Welke problemen zijn voor de veiligheidsregio's en welke voor andere partijen? Hoe kan zelfredzaamheid worden bevorderd?

3 Ontwikkeling na 2 dagen

Na 30 uur is het grootste deel van Nederland weer voorzien van stroom. De stroomvoorziening is echter nog altijd niet stabiel, met als gevolg dat de stroom in sommige delen van het land weer voor kortere tijd uitvalt. Stroomleveranciers bevestigen nu dat ze zijn aangevallen. Er is veel maatschappelijke verontwaardiging over de aanval en de impact die deze heeft gehad. Media vragen zich af of Rijk en veiligheidsregio's wel in voldoende mate waren voorbereid.

Overwegingen
- Wanneer ga je afschalen?

Relevante vragen
- Hoe ga je om met de kritiek op o.a. de veiligheidsregio's?

Aandachtspunten

1 Ga als veiligheidsregio na wat je nodig hebt van andere partijen zoals het NCSC en vitale partners bij dit soort verstoringen. Denk aan:
- dreiging-/duidingsinformatie
- prognoses (duur, omvang)
- handelingsperspectief/maat-regelen/advies.

2 Ga na wat je als regio zou kunnen toevoegen in dergelijke casus. Welke bijdrage kun je concreet leveren aan het beperken van de fysieke en maatschappelijke gevolgen?

3 Ga als veiligheidsregio na hoe je de veerkracht van de samenleving bij langdurige verstoringen kunt ondersteunen.

4 Beoefen als veiligheidsregio's de bovenregionale/landelijke afstemming en coördinatie bij dit soort landelijke verstoringen.

DE HAAGSE HOGESCHOOL
IFV Instituut Fysieke Veiligheid

Algemene aandachtspunten bij cyberscenario's

Op basis van eerdere publicaties (o.a. IFV, 2020) en de gevoerde interviews zijn enkele algemene aandachtspunten geformuleerd en toegevoegd aan elk scenario. Deze aandachtspunten geven een veiligheidsregio houvast bij het doorleven van de scenario's én van andere cyberverstoringen.

1 Eigen informatiepositie

Denk als veiligheidsregio na over het opbouwen van een informatiepositie bij cyberverstoringen. Welke informatie heeft de regio nodig? Hoe bereikt dergelijke informatie de regio?

2 Mogelijke rollen als veiligheidsregio

Bespreek welke mogelijke rollen de veiligheidsregio in debetreffende situatie kan spelen. Welke toevoegde waarde kan de veiligheidsregio hebben? Welke bijdrage kan de regio leveren aan de bron- en effectbestrijding van de cyberverstoring?

3 Responsorganisatie

Bepaal hoe de eventuele responsorganisatie van de veiligheidsregio er uitziet. Hoe is het team samengesteld? Welke expertise moet in het team zijn vertegenwoordigd? Welk mandaat heeft dit team namens de veiligheidsregio?

4 Benodigde kennis en kunde

Denk na over de benodigde expertise bij cyber-verstoringen. Welke expertise heeft de veiligheidsregio zelf in huis en welke kennis en kunde moeten extern worden gemobiliseerd? Bestaan er aan de voorkant afspraken tussen de veiligheidsregio en dergelijke partijen?

5 Beschikbare tools

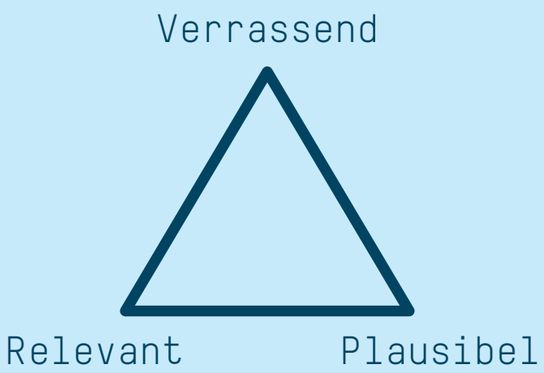
Zorg dat de veiligheidsregio zicht heeft op beschikbare instrumenten. Waar liggen haar bevoegdheden? Wat zijn haar wettelijke kaders? Welke hulpmiddelen heeft de veiligheidsregio daarbij tot haar beschikking (denk aan het Nationaal Crisisplan Digitaal en de Handreiking Cybergevolgbestrijding G4-gemeenten)?

6 Preparatie (planvorming, opleiding, oefening)

Zorg dat de veiligheidsregio is voorbereid op cyber-verstoringen. Bestaat er planvorming? Is er geoefend?

Toelichting scenario's

Een scenario is een chronologische beschrijving van een bepaalde gebeurtenis (of reeks gebeurtenissen) die heeft plaatsgevonden of nog moet plaatsvinden. Het is als het ware een draaiboek of script. Een scenario schetst dus een reeks gebeurtenissen waar organisaties mee te maken kunnen krijgen.
Zo'n scenario stelt organisaties in staat om op gestructureerde wijze na te denken over toekomstige ontwikkelingen en zodoende de risico's, kansen en interventiemogelijkheden te identificeren en prioriteren. De scenario's helpen veiligheidsregio's om bij zichzelf na te gaan wat de door hen gewenste wijze van optreden is als het betreffende scenario zich daadwerkelijk voordoet.



Criteria aan scenario's

Uit onderzoek weten we dat een goed scenario voldoet aan de volgende criteria:

1. Plausibel: de geschetste ontwikkelingen en gebeurtenissen moeten op logische wijze verband houden met elkaar en logischerwijs leiden tot het geschetste eindbeeld.
2. Relevant: het scenario moet daadwerkelijk ingangen en aanknopingspunten bieden voor de praktijk.
3. Verrassend: het scenario moet leiden tot nieuwe, originele inzichten, uitdagend zijn en impliciete veronderstellingen expliciet maken.

Scenariokeuze

We hebben er bewust voor gekozen om in dit document niet alleen 'gitzwarte scenario's' op te nemen, waarin maatschappelijke ontwrichting dreigt. Wij zijn er namelijk van overtuigd dat veiligheidsregio's ook veel kunnen leren van uitdagende, maar wat lichtere scenario's.

Literatuur

Berenschot (2020). *Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten. Deel 1: Warme fase. Praktische handvatten tijdens een cybercrisis.* Utrecht: Berenschot Groep B.V.

Instituut Fysieke Veiligheid (2019). *Whitepaper digitale ontwrichting en cyber.* Arnhem: IFV.

Instituut Fysieke Veiligheid (2020). *Cybergevolgbestrijding: lessen uit recente Nederlandse casus.* Arnhem: IFV.

Janssen, A.N.G, Gramberger, M.R., Ruijter. P.A. de & Heijningen, J. van (2004). *Regeren is vooruitzien! Scenario's maken en gebruiken voor beleidsontwikkeling, wetgeving en handhaving.* Den Haag: Expertisecentrum Rechtshandhaving.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020). *Cybersecuritybeeld 2020.* Den Haag: NCTV.

Nationaal Cyber Security Centrum (2020). *Nationaal Crisisplan Digitaal.* Den Haag: Ministerie van Justitie en Veiligheid.

Notten, P. van (2006). Scenario development: a typology of approaches. In: OECD (red.), *Think Scenarios, Rethink Education.* Parijs: OECD.

RIVM (2015). *Toekomstverkenning: het cyberdomein in 2022.* Bilthoven: RIVM.

Veiligheidsberaad (2019). *Bestuurlijk routeboek digitale ontwrichting.* Arnhem: Veiligheidsberaad.

Wetenschappelijke Raad voor het Regeringsbeleid (2019). *Voorbereiden op digitale ontwrichting.* Den Haag: 2019.

Meer weten over cyberverstoringen?

Bekijk dan deze links:

- Kennisdossier Digitale weerbaarheid (IFV, z.d.)
- Gijzelsoftware Veiligheidsregio Noord- en Oost- Gelderland. Evaluatie van de crisisrespons (IFV, 2021)
- Cybergevolgbestrijding: lessen uit recente Nederlandse casus (IFV, 2020)
- Cyberrisico's en veiligheidsregio's (IFV, 2020)

IFV Instituut Fysieke Veiligheid

Instituut Fysieke Veiligheid
Postbus 7010
6801 HA Arnhem

026 355 24 00

www.ifv.nl | info@ifv.nl