Instituut
Fysieke
Veiligheid

Gijzelsoftware Veiligheidsregio Noord- en Oost-Gelderland

Evaluatie van de crisisrespons

Instituut Fysieke Veiligheid
Afdeling Onderzoek &
Kennisdocumenten
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Colofon

Instituut Fysieke Veiligheid (2021). *Gijzelsoftware VNOG. Evaluatie van de crisisrespons*. Arnhem: IFV.

Opdrachtgever:	Programma Overleg Informatievoorziening (POI)
Contactpersoon:	Guus Zijlstra
Titel:	Gijzelsoftware VNOG. Evaluatie van de crisisrespons
Datum:	18-05-2021
Status:	Definitief
Auteurs:	Laurens van der Varst, Marije Bakker, Emily Berger en Daan Heijmen
Projectleider:	Laurens van der Varst
Review:	Menno van Duin
Eindverantwoordelijk:	Menno van Duin

Voorwoord

Zaterdag 12 september 2020 viel een deel van de computersystemen in onze Veiligheidsregio Noord- en Oost-Gelderland (VNOG) uit. Diezelfde avond bleek dat wij als eerste Veiligheidsregio in Nederland gehackt waren. Wat volgde was een periode van onzekerheden. En bovendien betrof het een crisis waarbij we zelf slachtoffer waren. Er speelde veel tegelijkertijd: wat is de toedracht van de aanval, hoe groot is de schade aan onze eigen organisatie, hoe bouwen we zo snel mogelijk onze systemen weer op, en op welke wijze communiceren we zowel intern als extern?

We zijn direct vanuit de bestaande crisisstructuur te werk gegaan. Hierdoor konden we snel opschalen en de juiste kennis in huis halen. Deze structuur heeft ons geholpen om te komen tot een goede beeldvorming in onzekere tijden. Ook eindbeslissers waren direct opgenomen in de crisisorganisatie, hierdoor konden besluiten snel genomen worden. Dit bleek van vitaal belang tijdens dit cyberincident.

Tijdens deze weken heb ik een enorme betrokkenheid en inzet gezien van de eigen medewerkers, van collega's van andere Veiligheidsregio's en vele externe partners. Als Veiligheidsregio is het onmogelijk om alle kennis en capaciteit in huis te hebben om dit type incident alleen te bestrijden. Gezamenlijk optreden op dit onderwerp is daarom cruciaal. De VR-ISAC heeft hier een belangrijke rol. Daarnaast vind ik het belangrijk dat er ook een publiekprivaat platform komt, met veiligheidsorganisaties en commerciële organisaties. Het helpt niet als we allemaal op een eiland blijven zitten.

De aanval met gijzelsoftware bij onze Veiligheidsregio heeft ons nog meer bewust gemaakt van het belang van goede informatiebeveiliging. De lessen die wij geleerd hebben tijdens dit incident delen wij graag met onze collega's van de andere Veiligheidsregio's en met ketenpartners. Ik waardeer daarom het initiatief van het POI om opdracht te geven voor dit onderzoek. De medewerking aan het onderzoek heeft goede en bruikbare inzichten opgeleverd.

In april hebben we een afsluitende bijeenkomst georganiseerd voor alle medewerkers van de VNOG. Hiermee is intern het einde van de hack gemarkeerd. Onze nieuwe systemen zijn inmiddels volledig opgebouwd en alles werkt weer naar behoren. Tijdens dit moment hebben de betrokken collega's hun ervaringen over deze aanval gedeeld met de rest van de organisatie. Een waardevol moment. Tevens het startsein voor een interne awareness campagne. Dit onderzoek kan dezelfde rol vervullen: de start voor een awareness campagne over informatieveiligheid voor alle Veiligheidsregio's.

Diemer Kransen
Directeur en regionaal commandant Veiligheidsregio Noord- en Oost-Gelderland

Voorwoord

Veiligheidsregio's maken steeds meer gebruik van collectieve voorzieningen om met informatievoorziening de bedrijfsvoering en risico- en crisisbeheersing goed en efficiënt te ondersteunen. Dit maakt wel dat alle regio's afhankelijk worden van elkaars niveau van informatieveiligheid. In opdracht van het Veiligheidsberaad gaan we vanuit het POI daarom de komende jaren sturen op de uitvoering van het versnellingsplan van de 25 veiligheidsregio's om aan de BIO te gaan voldoen. De gebeurtenis waar dit rapport over gaat onderschrijft nogmaals de noodzaak daartoe en geeft richting aan de landelijke activiteiten die we voor dit versnellingsplan gaan uitvoeren.

Sinds de start van het vorige programma informatievoorziening voor de veiligheidsregio's, in 2015, staat informatieveiligheid hoog op de agenda van het Programma Overleg Informatievoorziening (POI). De inrichting van de vakgroep informatieveiligheid, advisering over gegevensveiligheid in project, kwetsbaarheidsanalyse op het ICT-Verkeersplein, toetsing van de regio's op de BIG normen en de instelling van de VR-ISAC; het zijn de eerste stappen van de veiligheidsregio's geweest om zichzelf te beschermen tegen wat de VNOG in september 2020 is overkomen. Het POI beseft zich dat de noodzaak bestaat om blijvend te investeren in informatieveiligheid. Niet alleen in de techniek, zoals incidenten zoals in Hof van Twente laten zien, ook in procedures en bewustwording, zoals een recent incident bij Bol.com aantoont.

Het POI heeft opdracht gegeven aan dit onderzoek omdat cyberincidenten als deze niet meer weg gaan en omdat we het belangrijk vinden dat alle andere regio's kunnen leren van wat de VNOG is overkomen. Het doel van het onderzoek is om uiteindelijk en bovenal, te leren hoe je als regio je hier op zult moeten voorbereiden. We zijn blij met het resultaat van het onderzoek, met de bevindingen en aanbevelingen in dit rapport kunnen alle regio's lessen trekken voor hun eigen voorbereiding op cyberincidenten.

De VNOG is deze cybercrisis overkomen, het heeft veel problemen opgeleverd, maar de regio is er tegen wil en dank ook door gegroeid. Wij hopen dat alle andere veiligheidsregio's dankbaar lessen trekken uit dit rapport, om hun eigen groeistappen te kunnen zetten, zonder er zelf zo'n cybercrisis voor te moeten doorstaan.

Arjan Mengerink
Directeur Veiligheidsregio IJsselland

Voorzitter POI

Krishna Taneja
Directeur Veiligheidsregio Noord-Holland-Noord
POI Portefeuillehouder Informatieveiligheid

Samenvatting

De Veiligheidsregio Noord- en Oost-Gelderland (VNOG) werd op zaterdag 12 september 2020 getroffen door gijzelsoftware. Deze software zorgde voor een verstoring van interne computersystemen. Het is de eerste keer dat een veiligheidsregio te maken kreeg met een dergelijke cyberverstoring. Dat onderstreept de behoefte om van het incident te leren; leerervaringen kunnen bijdragen aan het verder versterken van de incidentrespons en gevolgbestrijding bij cyberverstoringen, zowel van de VNOG zelf, als van andere veiligheidsregio's. De VNOG was in deze casus tevens zelf slachtoffer, in plaats van bijstand- of hulpverlener bij andermans crises. Het doel van dit onderzoek is dan ook het identificeren van goede praktijken en leerpunten uit deze incidentrespons en gevolgbestrijding. Daarnaast wordt advies gegeven over manieren waarop veiligheidsregio's hun incidentrespons en gevolgbestrijding kunnen bevorderen.

Er wordt gewerkt vanuit drie thema's. Het eerste is de vraag of en zo ja: in welke mate cyberverstoringen anders zijn dan klassieke flitsrampen. En als dit het geval is, hoe kunnen veiligheidsregio's zich dan op dit soort cybercrises voorbereiden? In het hoofdstuk waarin dit thema aan bod komt, wordt stilgestaan bij de bijzondere kenmerken van de gijzelsoftware bij de VNOG en de context waarbinnen de verstoring plaatsvond. Het tweede thema is de crisisorganisatie. Veiligheidsregio's dienen te beschikken over een flexibele crisisorganisatie en over relevante crisisnetwerken. Deze casus leent zich bij uitstek voor onderzoek naar de wijze waarop de regio hiermee is omgegaan. Het is interessant te bezien in welke mate reguliere crisisstructuren toepasbaar zijn geweest bij deze cyberverstoring, hoe externe expertise is gemobiliseerd en hoe relatief nieuwe cybergremia zoals het VR-ISAC hebben gefunctioneerd. Het derde thema is de crisiscommunicatie. De vraag is of de communicatie over een cybercrisis anders is dan communicatie over 'reguliere' crises. Er is onderzocht of er factoren zijn waarmee men bij een cyberverstoring (extra) rekening moet houden in de communicatie, welke uitgangspunten zijn gebruikt in de interne en externe communicatie over een cyberverstoring en of er in alle openheid kan worden gecommuniceerd of dat er juist een zekere mate van geslotenheid gewenst is.

Onze hoofdbevinding is dat de VNOG deze cyberverstoring adequaat heeft bestreden. Zij heeft de gijzelsoftware vanaf het allereerste begin uitermate serieus genomen, heeft snel opgeschaald en direct externe hulp ingeschakeld. Duidelijk is geworden dat cyberverstoringen de hele organisatie en alle medewerkers raken. Veiligheidsregio's zullen rekening moeten houden met die sociaal-emotionele impact van gijzelsoftware. In de crisisrespons was de VNOG sterk afhankelijk van externe specialistische ondersteuning en expertise. De VNOG slaagde erin om die technische expertise snel te mobiliseren in de vorm van bijstand van het NCSC, Fox-IT en KPN. Naast het feit dat de VNOG ontzettend veel goed heeft gedaan, heeft de regio ook geluk gehad. Wanneer de benodigde expertise niet tijdig kan worden georganiseerd, er sprake is van zeer geavanceerde of aanhoudende aanvallen en technisch handelingsperspectief ontbreekt, kan het verloop van een dergelijk incident er heel anders uitzien. Onze oproep aan veiligheidsregio's is dan ook om dit soort cyberverstoringen (en de voorbereiding erop) uiterst serieus te nemen. Cyberdreigingen zoals gijzelsoftware zijn per slot van rekening 'here to stay'.

Inhoud

Afkortingen

AC	Algemeen Commandant
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatieveiligheid Overheid
CISO	Chief Information Security Officer
CoPI	Commando Plaats Incident
GGD	Gemeentelijke gezondheidsdienst
GHOR	Geneeskundige Hulporganisatie in de Regio
GRIP	Gecoördineerde Regionale Incidentbestrijdingsprocedure
GZ	Geneeskundige zorg
FG	Functionaris Gegevensbescherming
HRM	Human resource management
ICT	Informatie- en communicatietechnologie
IFV	Instituut Fysieke Veiligheid
ISAC	Information Sharing and Analysis Center
IT	Informatietechnologie
IV	Informatievoorziening
Min JenV	Ministerie van Justitie en Veiligheid
LCMS	Landelijk Crisismanagement Systeem
MON	Meldkamer Oost Nederland
MT	Management Team
NCSC	Nationaal Cyber Security Centrum
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
OvD	Officier van Dienst
POI	Programma Overleg Informatievoorziening
RBT	Regionaal beleidsteam
VM	Virtual machine
VNOG	Veiligheidsregio Noord- en Oost-Gelderland
VR	Veiligheidsregio
Wbni	Wet beveiliging netwerk- en informatiesystemen
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Inleiding

Aanleiding

De Veiligheidsregio Noord- en Oost-Gelderland (VNOG) werd op zaterdag 12 september 2020 getroffen door gijzelsoftware. Deze software zorgde voor een verstoring van interne computersystemen, waardoor het interne bedrijfsnetwerk, specifieke applicaties en de e-mail niet meer functioneerden. Medewerkers van de veiligheidsregio konden niet gebruikmaken van hun werkcomputer. De verstoring vond plaats te midden van de coronapandemie, maar de werkzaamheden rondom de bestrijding van het coronavirus konden – na enige inspanningen om dit mogelijk te maken – doorgang blijven vinden.

Het is de eerste keer dat een veiligheidsregio te maken kreeg met een dergelijke cyberverstoring. Dat onderstreept de noodzaak om van het incident te leren. De leerervaringen kunnen namelijk bijdragen aan het verder versterken van de cyber incidentrespons en -gevolgbestrijding, zowel van de VNOG zelf, als van andere veiligheidsregio's. Het Programma Overleg Informatievoorziening (POI) heeft het lectoraat Crisisbeheersing van het Instituut Fysieke Veiligheid (IFV) gevraagd een evaluatie van de cyberverstoring bij de VNOG uit te voeren en leerarena's te organiseren. De opzet van het onderzoek is afgestemd met de Programmamanager Informatievoorziening, medewerkers van de VNOG en de Vakgroep Informatieveiligheid / het VR-ISAC.

Cyberverstoringen

De samenleving krijgt door ontwikkelingen op het gebied van technologie, demografie en klimaat te maken met nieuwe risico's (IFV, 2019). Eén van die nieuwe risico's is cyber – een risico dat volgens instanties zoals de Cyber Security Raad (CSR) en de Wetenschappelijke Raad voor het regeringsbeleid (WRR) hoger op de bestuurlijke agenda moet komen. Cyberverstoringen bestaan in tal van soorten en maten. Een aanval met gijzelsoftware (of ransomware) is een van de vele mogelijkheden die een cyberverstoring kan veroorzaken. Bij een aanval met gijzelsoftware worden computers of bestanden 'gegijzeld' met meestal als doel losgeld te eisen voor het ontgrendelen van de vergrendelde systemen of data. Tal van Nederlandse organisaties zijn inmiddels slachtoffer geworden van deze cybercriminaliteit, waaronder de gemeente Lochem in juni 2019. In december 2019 werd de Universiteit Maastricht gehackt. Als gevolg van de aanwezige gijzelsoftware betaalde de universiteit omgerekend 200.000 euro om weer toegang te krijgen tot haar data. Ook de gemeente Hof van Twente werd in december 2020 slachtoffer van gijzelsoftware. Een aanval met gijzelsoftware kent verschillende gradaties. Een aantal zaken zijn van invloed op de zwaarte van aanval met gijzelsoftware, waaronder:

> Achter de aanval kunnen tal van actoren schuilgaan, van solistische (amateur)hackers, criminele organisaties tot zeer professionele, statelijk gefinancierde hackerscollectieven.
> Een aanval kan relatief eenvoudig van aard zijn, maar ook (zeer) geavanceerd. Daarnaast kan een aanval zijn gericht op een branche of sector óf specifiek op één enkel bedrijf of organisatie.[1]
> Niet elke aanval is even succesvol in het onomkeerbaar versleutelen (encryptie) van de data van een bedrijf of organisatie. In enkele gevallen is het mogelijk om de versleutelde bestanden zelf (en dus zonder betaling van losgeld) te ontgrendelen (decryptie).
> De aanwezigheid en het al dan niet versleuteld zijn van (recente) back-ups is van grote invloed op de snelheid waarmee een aanval met gijzelsoftware kan worden hersteld.

[1] Zie ook: https://www.digitaltrustcenter.nl/3-soorten-cyberaanvallen

Doelstelling

Het doel van dit onderzoek is het identificeren van goede praktijken en leerpunten uit de incidentrespons en -gevolgbestrijding. Daarbij werken we vanuit drie thema's. Ook geven we advies over manieren waarop veiligheidsregio's hun incidentrespons en gevolgbestrijding kunnen bevorderen. Het feitenrelaas is opgebouwd langs crisisprocessen uit de handreiking Cybergevolgbestrijding (zie ook: Berenschot, 2020).[2]

De evaluatie richt zich op de crisisrespons door de VNOG, van de eerste detectie op 12 september tot de afschaling van de crisisorganisatie. De evaluatie richt zich niet op opsporing en forensisch onderzoek naar de achterliggende oorzaken en modus operandi. In overleg met de opdrachtgever is besloten geen informatie over de toedracht van de hack op te nemen.

Daarbij wenden we ons perspectief naar 'goede praktijken' in de crisisrespons: wat functioneerde goed (en welke lessen zijn ook bruikbaar voor andere veiligheidsregio's)? We plaatsen ons hiermee in de bestuurskundige stroming die de aandacht verlegt van het bestuderen van beleidsfalen, naar de studie en dialoog over datgene wat goed gaat en wat werkt in de specifieke context (Compton & 't Hart, 2019). We doen dit vanuit de overtuiging dat we – door de aandacht op goede praktijken en werkwijzen te richten – meer en effectiever bijdragen aan een eventueel noodzakelijke verandering van werkwijzen, crisisorganisaties en -professie. De rapportage bevat voor veiligheidsregio's grotere en kleinere leerpunten. In de aanbevelingen hebben we enkele overkoepelende aanbevelingen opgenomen.

Gebaseerd op eigen onderzoek naar cybergevolgbestrijding (IFV, 2020a) en de handreiking Cybergevolgbestrijding (Berenschot, 2020) zijn we tot de volgende drie thema's gekomen.

Thema 1: Een ander soort crisis?

Cyber is een van de risico's waar veiligheidsregio's zich op moeten voorbereiden (IFV, 2020b). Terugkerende vraag binnen veiligheidsregio's is of en zo ja: in welke mate cyberverstoringen anders zijn dan meer klassieke flitsrampen zoals branden (IFV, 2020a). En als dit het geval is, hoe kunnen veiligheidsregio's zich dan op dit soort cybercrises voorbereiden? In het hoofdstuk staan we stil bij de bijzondere kenmerken van de gijzelsoftware bij de VNOG en de context waarbinnen de verstoring plaatsvond: middenin de grootste en langdurigste crisis sinds jaren, de coronacrisis.

Thema 2: Reguliere of specifieke crisisorganisatie?

Met de Evaluatiecommissie Wet op de veiligheidsregio's (2020) staan flexibele responsorganisatie en -netwerken hoog op de agenda. Veiligheidsregio's dienen te beschikken over een flexibele crisisorganisatie en over relevante crisisnetwerken: netwerken waaruit, afhankelijk van het soort crisis, de juiste expertise kan worden gemobiliseerd. Deze discussie sluit aan bij de flexibele toepassing van de GRIP-procedure, waar eerder Van Duin en Wijkhuijs (2015) al diverse mogelijkheden voor signaleerden. Deze casus leent zich bij uitstek voor onderzoek naar de wijze waarmee de regio hiermee is omgegaan. Het is bijvoorbeeld interessant te bezien in welke mate reguliere crisisstructuren toepasbaar zijn

[2] Deze crisisprocessen betreffen detectie, impact en duiding, melding en alarmering, leiding en coördinatie, besluiten en maatregelen, crisiscommunicatie.

geweest bij deze cyberverstoring, hoe externe expertise is gemobiliseerd en hoe relatief nieuwe cybergremia zoals het VR-ISAC hebben gefunctioneerd.

Thema 3: Crisiscommunicatie: openheid of geslotenheid?

Crisiscommunicatie is cruciaal voor effectieve crisisbeheersing. In veel crisisevaluaties wordt de focus gelegd op crisiscommunicatie als succesfactor van crisisbeheersing (Evaluatiecommissie Wet veiligheidsregio's, 2020). Goede crisiscommunicatie staat voor het verspreiden van juiste, tijdige en begrijpelijke informatie over de gebeurtenis en het bieden van handelingsperspectieven tijdens en na een crisis, ramp of incident. De vraag die hierbij speelt, is of de communicatie over een cybercrisis anders is dan communicatie over 'reguliere' crises. Zijn er factoren waarmee men bij een cyberverstoring (extra) rekening moet houden in de communicatie? Welke uitgangspunten worden gebruikt in de interne en externe communicatie over een cyberverstoring? Kan er in alle openheid worden gecommuniceerd of is een zekere mate van geslotenheid gewenst?

Aanpak

In het kader van de evaluatie zijn vijftien interviews afgenomen met direct betrokken sleutelfunctionarissen.[3] Tevens zijn op locatie relevante documenten ingezien, waaronder CoPI-verslagen. De documenten en interviews vormden de basis voor het feitenrelaas en uitwerking van de drie thema's. De bevindingen zijn besproken en gevalideerd tijdens een interne lessenbijeenkomst op 11 maart 2021. Het evaluatierapport is ter review voorgelegd en besproken met de opdrachtgever. De rapportage bevat zoals gezegd geen informatie over de toedracht van de hack. De rapportage wordt gebruikt voor het organiseren van leerarena's voor andere veiligheidsregio's.

Leeswijzer

In hoofdstuk 1 wordt een uitgebreide beschrijving van de gebeurtenissen gegeven. In dit feitenrelaas wordt ingegaan op de detectie van het incident, melding en alarmering, de crisisorganisatie, de opbouw van systemen, communicatie en afschaling. In de hoofdstukken 2 tot en met 4 worden de gebeurtenissen beschouwd aan de hand van de eerder genoemde thema's. Hoofdstuk 5 bevat de bevindingen en aanbevelingen uit dit onderzoek.

[3] Respondenten: CISO & aanspreekpunt Netwerkbeheer, Informatiecoördinator CoPI & adviseur Informatie, Operationeel leider ROT Corona & Afdelingshoofd Risico- Crisisbeheersing, Leider CoPI & teamleider Informatie, NCSC, Aanspreekpunt opschoningen & uitgifte schone laptops & systeembeheerder, AC Brandweer CoPI, Leider CoPI & Afdelingshoofd Bedrijfsvoering, Directeur VNOG, Voorzitter VNOG, Voorzitter VR-ISAC, Informatiemanager CoPI, Communicatieadviseur, Functionaris Gegevensbescherming, Aanspreekpunt operationele systemen & medewerker OIV.

1 Feitenrelaas

1.1 Detectie van het incident

Het is zaterdag 12 september 2020 rond 14.30 uur als medewerkers Operationele Informatievoorziening en Kantoorautomatisering opmerken dat ze geen verbinding kunnen krijgen met de operationele systemen van de VNOG. Ook krijgen ze geen toegang tot hun e-mail. Vlak erna wordt via een Whatsapp-groep voor ICT-calamiteiten door zowel de operationele als de beheersmatige organisatie melding gemaakt van problemen met het netwerk. Een medewerker van ICT netwerkbeheer besluit vanuit huis een aantal controles op de systemen van de VNOG uit te voeren. Dit blijkt op afstand niet te lukken, waarop hij naar de werklocatie van de VNOG in Apeldoorn vertrekt. Rond 16.30 uur wordt na controles op kantoor duidelijk dat de servers die de data beheren niet kunnen worden bereikt via het wifi-netwerk. Ook via een LAN-verbinding lukt dit niet. De Chief Information Security Officer (CISO) wordt geïnformeerd over de situatie. De CISO wil weten of de back-up nog wel bereikbaar is. Dit blijkt het geval te zijn. Op advies van de CISO wordt deze volledig uitgezet uit voorzorg. Mocht er sprake zijn van een virus, dan kan de back-up (mits deze niet is besmet) worden gebruikt voor het terugzetten van gegevens. De Meldkamer Oost Nederland (MON) wordt geïnformeerd over de problemen met het versturen van informatie naar de navigatiesystemen van hulpdiensten. MON meldt vervolgens op haar beurt dat Citrix niet werkt. Meldingssystemen P2000 en C2000 werken wel.

Alarmerings- en communicatienetwerk C2000 en P2000
C2000 is een gesloten communicatienetwerk voor Nederlandse hulp- en veiligheidsdiensten, zoals politie, brandweer en ambulancediensten en maakt onderdeel uit van de vitale infrastructuur. Het netwerk is in beheer van het Ministerie van Justitie en Veiligheid. In Nederland zijn circa 600 masten voor C2000 gebouwd die onderling verbonden zijn. De masten en schakelcentrales zorgen ervoor dat hulpverleners elk moment overal in Nederland en enkele kilometers daarbuiten via hun portofoon en mobilofoon kunnen communiceren met de meldkamer. Elke C2000-mast is voorzien van een noodstroomvoorziening in de vorm van accu's die gedurende ongeveer vier uur voldoende energie leveren voor gebruik van de mast. Voor langere stroomstoringen heeft de brandweer aggregaten beschikbaar om de masten van elektriciteit te voorzien.

P2000 is een van de onderdelen van het Nederlandse C2000-alarmeringsnetwerk. Het netwerk is opgezet om personeel van hulpdiensten op te roepen in geval van een incident. P2000 is in tegenstelling tot C2000 niet versleuteld, waardoor de berichten door iedereen ontvangen en gelezen worden.

Netwerkbeheer besluit de gecombineerde virtualisatie en storageomgeving te controleren. Daar blijkt het niet mogelijk om in te loggen op een server met het normale domeinaccount. Er verschijnt een foutmelding in beeld: ‘server of diensten zijn niet beschikbaar die het aanmelden kunnen faciliteren’. Nadat er kan worden ingelogd met een lokaal account, ontstaat het vermoeden dat er sprake is van een storing op de lokale schijven. De ICT-afdeling constateert dat extra expertise nodig is en neemt contact op met de leverancier. Er wordt gedacht aan problemen in de gecombineerde virtualisatie- en storagelaag of aan de

mogelijkheid dat het een virus is. De leverancier besluit een medewerker naar de werklocatie Apeldoorn te sturen ter ondersteuning. De teamleider Informatie is inmiddels ook ter plaatse.

In afwachting van de komst van de leverancier wordt rond 18.00 uur Veiligheidsregio IJsselland ingelicht over de problemen met het versturen van informatie naar de navigatiesystemen. MON is namelijk ook de meldkamer van deze regio. Tevens wordt de AC-Brandweer geïnformeerd, omdat de problemen mogelijk iets kunnen betekenen voor het operationele optreden. Netwerkbeheer lijkt het verstandig om ook de CISO ter plaatse te laten komen; deze arriveert rond 22.00 uur. Ten slotte wordt ook het afdelingshoofd bedrijfsvoering gevraagd naar de werklocatie Apeldoorn te komen.

Netwerkbeheer voert ondertussen diverse controles uit op de systemen. Na controle van de harde schijf blijkt rond 22.00 uur dat hierop cryptolock-bestanden[4] aanwezig zijn. De aanwezigheid van gijzelsoftware op de server wordt bevestigd door de leverancier en netwerkbeheer. Op aanraden van de leverancier worden alle servers in de status 'as is'[5] gezet, kabels worden uit de apparatuur gehaald en externe verbindingen (waaronder de verbinding met het internet) worden uitgezet. Hiermee wordt getracht verder verspreiding van het virus te voorkomen, schade te reduceren en mogelijk verlies van gegevens te voorkomen.

1.2 Melding en alarmering

Na het aantreffen van de gijzelsoftware begint direct het proces van informeren en hulp vragen. Als eerste wordt de directeur van de VNOG op de hoogte gesteld door het hoofd Bedrijfsvoering. Even na middernacht wordt het Nationaal Cyber Security Centrum (NCSC) gebeld om melding te doen van de verstoring. Ook wordt door de VNOG gevraagd om ondersteuning. Na een uitleg dat ook brandweerprocessen en het coronateam zijn getroffen[6] door de verstoring, besluit het NCSC om de VNOG te ondersteunen.[7] Er wordt afgesproken dat twee medewerkers de volgende ochtend ter plaatse komen. Ook wordt de meldkamer geïnformeerd dat de eerder gemelde problemen zijn ontstaan door gijzelsoftware.

Op zondagochtend 13 september wordt de politie ingelicht over de aangetroffen gijzelsoftware op de systemen van de VNOG. Om 09.00 uur arriveren twee medewerkers van het NCSC bij de VNOG. Het afhandelen van een cyberverstoring vraagt om andere processen dan bij een meer reguliere crisis zoals een brand. Het NCSC kan daar goed in ondersteunen. Deze organisatie zorgt met name voor het aanbrengen van structuur in wat men moet doen en hoe de getroffen organisatie weer kan herstellen van een cyberverstoring. Na een overleg tussen de VNOG en advies van het NCSC om een incident-respons-partij te betrekken, besluit de VNOG om het cybersecuritybedrijf Fox-IT erbij te betrekken. In de middag arriveren twee experts van Fox-IT.

[4] Cryptolocker is een gijzelsoftware (ransomware). Deze vorm van malware zorgt ervoor dat bestanden worden versleuteld, waardoor het niet meer mogelijk is om ze te gebruiken.
[5] De status 'as is' betekent dat je niets meer doet met de systemen om eventuele sporen niet te vernietigen.
[6] Brandweerprocessen en het coronateam werken via/met de ICT-systemen van de VNOG.
[7] Het NCSC heeft een wettelijke taak om de rijksoverheid en vitale aanbieders te adviseren en te ondersteunen bij digitale dreigingen en incidenten m.b.t. hun netwerk- en informatiesystemen (Wbni, art. 3). Op grond van een vrijwillige melding kan het NCSC ook andere organisaties ondersteunen (Wbni, art. 16).

Diezelfde ochtend licht de directeur van de VNOG de andere directeuren veiligheidsregio's, de voorzitter van de VNOG en alle burgemeesters van de VNOG in via Whatsapp. Daarnaast wordt contact opgenomen met de directeur veiligheidsregio's, crisisbeheersing en meldkamer van het ministerie van Justitie en Veiligheid, die op zijn beurt onmiddellijk de minister van Justitie en Veiligheid informeert. Tevens worden die zondagmiddag de eigen medewerkers en partners van de veiligheidsregio geïnformeerd. Middels WhatsApp wordt via teamleiders en afdelingshoofden de centrale boodschap verstuurd dat de VNOG getroffen is door gijzelsoftware. Het dringend advies luidt dat medewerkers hun VNOG-laptop niet mogen aanzetten. Tevens wordt gecommuniceerd dat het gebruik van het VNOG-account niet mogelijk is. Gevraagd wordt om verdacht gedrag te melden bij de teamleider. Communicatie is alleen mogelijk via WhatsApp of Signal.

Cyberdreigingen (NCTV, 2020b)
De digitale dreiging heeft tegenwoordig een permanent karakter. Criminele cyberaanvallen tonen de grote gevolgen voor organisaties, medewerkers en burgers. Cyberincidenten kunnen zelfs tot maatschappij ontwrichtende schade leiden, zo waarschuwt het NCSC. De dreiging is in belangrijke mate afkomstig van staten en criminele groeperingen. Doelstellingen en modus operandi van deze actoren variëren. Daarbij geldt dat cyberaanvallen een aantrekkelijk verdienmodel zijn voor criminelen: 'ransomware as a service'. Dergelijke aanvallen worden gebruikt voor afpersing, diefstal van informatie en CEO-fraude. Daarbij richt de aandacht zich veelal op organisaties die in staat zijn grote geldbedragen te betalen, die beschikken over waardevolle data of waarbij de bedrijfscontinuïteit een essentieel goed is.

Gedurende de dag wordt het Veiligheidsberaad (via een WhatsApp-bericht van de voorzitter VNOG) geïnformeerd. Later volgen het VR-ISAC en het IFV. Aan het einde van de middag wordt een eerste persbericht op de website geplaatst. Aan het begin van de avond doet de functionaris gegevensbescherming melding bij de Autoriteit Persoonsgegevens. Tevens wordt het CERT (Computer Emergency Response Team) van KPN-Security om assistentie gevraagd, vanwege een urgente behoefte aan diepgaande specialistische kennis met betrekking tot de infrastructuur. Op maandag 14 september wordt er aangifte gedaan bij de politie en worden aanvullende partijen ingelicht over de cyberverstoring, namelijk de gemeenteraden van de verschillende gemeenten binnen de regio via een raadsinformatiebrief (VNOG, 2020a) en de SaaS-leveranciers[8], de archief-inspecteur[9] en de Inspectie JenV.

Effecten van de cyberverstoring
Door de cyberverstoring op de VNOG zijn de interne systemen geraakt. E-mail, agenda, MS Teams en (on premise) ondersteunende applicaties (die niet kritiek zijn voor de directe hulpverlening) werken niet meer. De meldingssystemen P2000 en C2000 werken wel en benodigde informatie voor brandweeruitrukken is beschikbaar, waardoor de veiligheid niet in het geding is. SaaS-applicaties zijn ook benaderbaar. Voor het gebruik van de SaaS-applicaties is wel een wachtwoord reset en twee factor authenticatie vereist. Dit als voorzorgsmaatregel in het geval de wachtwoorden gekraakt zijn door de hackers.
De cyberverstoring vindt plaats tijdens de coronacrisis. De door het kabinet afgekondigde coronamaatregelen worden door veiligheidsregio's vastgelegd in regionale noodverordeningen,

[8] SaaS staat voor: Software as a Service. SaaS-leveranciers leveren een softwareservice via een portal. Software draait vaak niet op het eigen systeem van een organisatie, maar op het internet en is alleen via het internet te benaderen.
[9] Er geldt een zevenjarige bewaarplicht van gegevens. Op 14 september was nog niet duidelijk wat de impact van de hack was op het archief van de VNOG. Hierover moest de archief-inspecteur geïnformeerd worden.

waarvoor juridische expertise nodig is. De veiligheidsregio informeert de gemeenten in de regio hierover. Door de cyberverstoring wordt dit bemoeilijkt, doordat informatie van de 22 gemeenten niet centraal op één plaats is. Er wordt hard gewerkt om de werkzaamheden rondom de bestrijding van het coronavirus te kunnen continueren: alternatieve emailadressen worden aangemaakt, er worden tijdelijke (opgeschoonde) laptops verstrekt, een nieuwe bereikbaarheidsomgeving wordt opgezet. Het Landelijk Crisis Management Systeem (LCMS) in beheer bij het IFV is de hele tijd bereikbaar. Geplande bijeenkomsten van het regionaal beleidsteam (RBT) in het kader van de coronacrisis gaan door. Het vastleggen van de besluitvorming gebeurt later. Genomen besluiten worden in eerste instantie via bestaande appgroepen kenbaar gemaakt aan het bestuur. Het Actiecentrum Medisch blijft actief en is telefonisch bereikbaar op het nummer van de dienstdoende AC geneeskundige zorg (GZ). Ook blijft LCMS-GZ actief, waarmee de informatievoorziening aan de acute zorgpartners gewaarborgd is. Het Regionaal Actiecentrum Communicatie Corona blijft tevens actief; updates worden via appgroepen verstuurd. Geconcludeerd kan worden dat er wel sprake is geweest van enig ongemak, maar ook niet meer dan dat.

1.3 De crisisorganisatie

Zondagochtend rond 10.00 uur wordt besloten om in de CoPI-structuur te gaan werken. Er wordt even opgeschaald naar GRIP-1, maar al snel wordt dit aangepast naar GRIP-0. Bij GRIP-1 zouden de OvD's uit de verschillende kolommen aanschuiven in het CoPI-overleg, maar die zouden in deze crisis niet allemaal van toegevoegde waarde zijn. Ook wordt er kort gesproken over GRIP-3 in verband met de mogelijke bestuurlijke effecten. Bestuurlijke effecten zijn wel aanwezig, maar een RBT is niet nodig: de cyberverstoring zorgt met name voor een interne crisis binnen de VNOG.

Zondagmiddag om 13.00 uur komt het CoPI voor het eerst bij elkaar onder voorzitterschap van het hoofd Bedrijfsvoering (die als Operationeel Leider optreedt), met de directeur van de VNOG én met de Operationeel Leider Corona (tevens hoofd Crisisbeheersing). Er wordt zo breed mogelijk gekeken wie er in het CoPI plaats moeten nemen.[10] In het eerste overleg wordt met elkaar gesproken over de gijzelsoftware, de continuïteit van de eigen organisatie en de interne en externe communicatie. Ook wordt geïnventariseerd welke systemen nog wel werken en welke niet. Het blijkt dat door de cyberverstoring interne systemen zijn geraakt en dat met name kantoorprocessen ernstig zijn verstoord. Direct zijn er 10-15 nieuwe laptops ingezet ter ondersteuning van kritieke personen/processen. Met deze laptops werd een tijdelijk en afgesloten beheernetwerk opgezet voor het uitvoeren van werkzaamheden, zoals het installeren van de schaduwomgeving én voor monitoring van de bestaande omgeving via dit geïsoleerde segment. Bovendien zijn er een aantal tijdelijke e-mailadressen aangemaakt. Hierdoor had de crisisorganisatie in ieder geval toegang tot LCMS en waren zij in staat om mail te versturen door gebruik te maken van tijdelijke emailadressen.

Later op de dag volgen nog twee CoPI-overleggen waarin voornamelijk wordt gesproken over de eerste stappen die worden gezet in de opbouw van het schaduwsysteem, het forensisch onderzoek, de communicatie en de inventarisatie van de schade die nodig is voor het herstelplan. Er wordt een prioriteitenlijst opgesteld met daarop de volgorde waarin de

[10] Vrijwel gedurende het hele incident zijn dezelfde functionarissen aanwezig in het CoPI: de leider CoPI, OvD-Brandweer, informatiemanager, communicatie, NCSC en de directeur veiligheidsregio. Op maandag 14 september vindt er een uitbreiding plaats met een tweede informatiemanager, logger, medewerker operationele informatie, afdeling ICT en Fox-IT.

informatiesystemen weer moeten worden opgestart en wanneer de schaduwinfrastructuur gereed is. Het uitgangspunt hierbij is dat alles wat impact heeft op operationele processen voorrang heeft. Daarnaast wordt een werkwijze gehanteerd waar zorgvuldigheid boven snelheid gaat.

Impact van de cyberverstoring op de brandweerorganisatie
De AC-Brandweer heeft geïnventariseerd welke digitale processen van de brandweer door de cyberverstoring werden verstoord of uit te lucht waren. Ook heeft hij aangegeven wat dat zou betekenen voor het operationele optreden van de brandweer. Samen met de afdeling communicatie is hierover een notitie opgesteld die gedeeld is met alle postcommandanten in de regio. In de notitie is aandacht voor thema's als:

Wat betekent de hack voor de brandweerorganisatie?
> P2000/C2000 is operationeel.
> Mobiele dataterminals op de voertuigen mogen gebruikt worden, maar er wordt geen nieuwe, actuele informatie naar de voertuigen gestuurd. Zowel de mobiele dataterminals als de navigatie moeten handmatig worden bediend.
> LCMS en LCMS-plot werken. Bij een groot incident zal er een mobiele commando-unit met schone laptops naar het incident worden gebracht. Zo kan er verbinding met LCMS worden gemaakt.
> Het alarmsysteem (tegen inbrekers) van bepaalde kazernes werkt niet meer. Er moet gecontroleerd worden of het systeem nog werkt. Is dit niet het geval, dan wordt politie-surveillance geregeld.

Wat is er geregeld?
> Extra ondersteuning in de meldkamer, zodat de centralist eventueel een extra voertuig kan begeleiden door handmatig de navigatie en relevante gegevens in te voeren.
> Er zal sneller een waterwagen meegestuurd worden als blijkt dat water lastiger te vinden is.
> Een extra piketcentralist wordt achter de hand gehouden.

Wat moeten de lezers van deze notitie doen?
> Brandweerpersoneel informeren via Whatsapp.
> Communiceren gaat het beste via telefonie / Whatsapp, omdat de andere systemen eruit liggen.

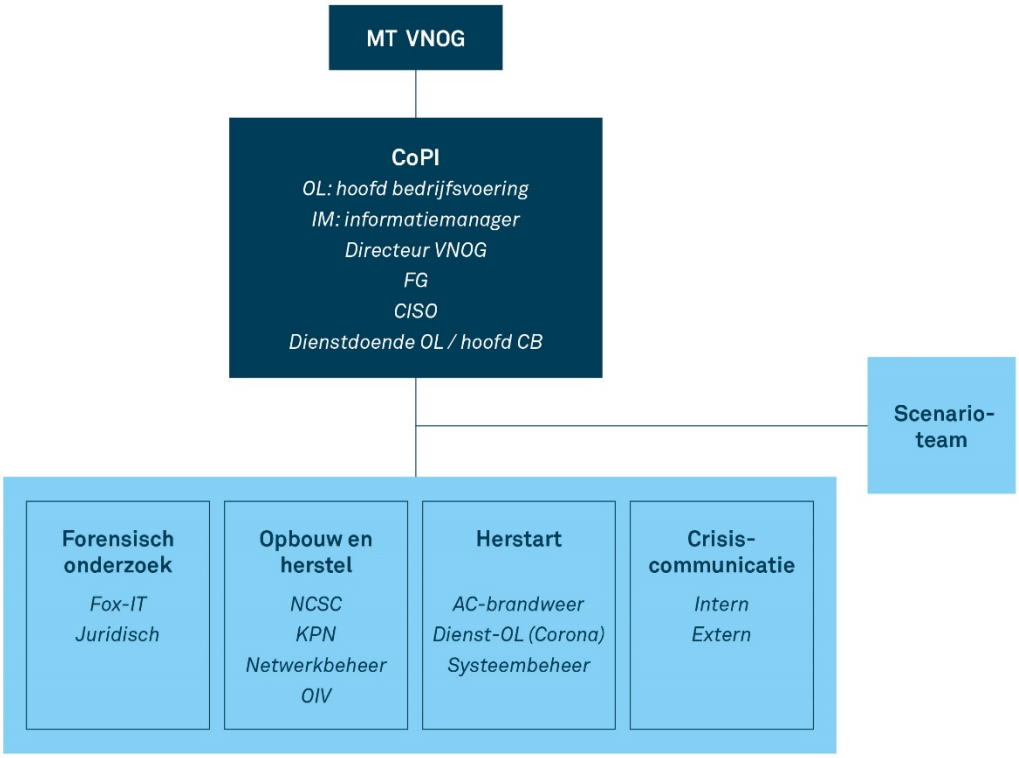
In het CoPI-overleg wordt geconstateerd dat het omwisselen en schoonmaken van de laptops een uitgebreide logistieke operatie wordt, die nu al kan worden voorbereid. Hiervoor wordt een plan van aanpak opgesteld. Naar verwachting is hierbij hulp van andere veiligheidsregio's welkom. Er wordt besloten om geen technische details over de cyberverstoring naar buiten te brengen.

In de dagen die volgen, komt het CoPI gemiddeld twee keer per dag bijeen om ervoor te zorgen dat er korte lijnen zijn en er snel afstemming kan plaatsvinden. Na ongeveer een week wordt de frequentie teruggebracht naar één vergadering per dag. Langzaam vindt een verschuiving plaats in de thema's die besproken worden in het CoPI. In het begin ligt de focus vooral op het forensisch onderzoek, het inventariseren van de impact op de organisatie en de communicatie. Naarmate de tijd vordert, komt de focus steeds meer te liggen op het herstellen van de systemen en de inname / uitrol van laptops van medewerkers.

1.3.1 Actiecentrum en scenarioteam

Maandag 14 september wordt besloten om aanpassingen te doen in de crisisstructuur. Onder het CoPI wordt een actiecentrum ingericht voor de uitvoering van besluiten. In het actiecentrum wordt gewerkt aan vier thema's: forensisch onderzoek, opbouw en herstel, herstart en crisiscommunicatie (zie figuur 1.1).

Naast het CoPI wordt ook een scenarioteam opgestart. Dit is een staf met een adviserende rol aan het MT, in afstemming met het CoPI. Het scenarioteam houdt zich bezig met onder andere de volgende vraagstukken: wat speelt er in de organisatie? Wat is de impact? Wat zijn de prioriteiten? Waar geef je voorrang aan? Aan de hand van een brainstormsessie identificeert het scenarioteam 22 thema's die geclusterd worden in een aantal hoofdgroepen: operationeel optreden, ondersteuning, communicatie, personeel en bestuur. Op basis van een bestcase- en een worstcasescenario wordt prioritering aangebracht in de werkzaamheden.



Figuur 1.1 Crisisstructuur (bron: VNOG)

1.4 Opbouw van systemen

Voor de opbouw van de systemen moet nieuwe hardware (servers, netwerk) aangeschaft worden.[11] Dit proces wordt bemoeilijkt door het feit dat het incident in het weekend plaatsvindt. Uiteindelijk lukt het om op zondagavond de benodigde hardware door hardware leverancier Ynvolve te krijgen geleverd. Ook worden op zondag de bestaande servers

[11] De hardware wordt gebruikt om de schaduwomgeving op te bouwen. Die omgeving wordt gebruikt om schone systemen op te herstellen, terwijl de oude/ geïnfecteerde omgeving afgesloten blijft.

vervangen door nieuwe servers. De oude servers worden in een nieuwe geïsoleerde en bewaakte omgeving geplaatst en, na het maken van forensische kopieën, voor onderzoek naar Fox-IT gestuurd.

Op maandag 14 september wordt, op aanraden van het NCSC en Fox-IT, gestart met de opbouw van het schaduwsysteem. Op dit schaduwsysteem mogen alleen schone laptops worden aangemeld, zodat mogelijke herinfectie voorkomen wordt.[12] Bovendien wordt op deze manier voorkomen dat de hackers mogelijkerwijs ook toegang krijgen tot deze schaduwomgeving. In deze ICT-operatie werken de VNOG en het NCSC samen met specialisten van KPN. Er wordt ingeschat dat op dit moment geen enkele ICT-dienst beschikbaar is (door onder andere geen internet en geen e-mail) en dat via drie lijnen de oplossing moet worden bereikt:

1. Een nieuwe (schone) schaduwomgeving die moet worden gebouwd.
2. Het analyseren van de oude omgeving (bruikbare geteste onderdelen kunnen mogelijk in de schone omgeving worden gebruikt).
3. Het terughalen van de back-up (als er zaken kunnen worden teruggezet, kunnen deze in de schone omgeving worden gezet).

Op dinsdag 15 september gaat de opbouw van het schaduwsysteem verder. Voor de opbouw van de tijdelijke omgeving is de vaste leverancier van de VNOG nodig. Na contact met de desbetreffende leverancier blijkt dat er een verschil in inzicht is over de dienstverlening. De VNOG besluit hierop de keuze te maken om over te gaan op een andere leverancier. Deze leverancier heeft vervolgens de benodigde ondersteuning geleverd en daarnaast ook aanpassingen en verbeteringen waar mogelijk direct ingevoerd.

De volgende dag is het schaduwsysteem zo ver klaar dat er data naar toe kunnen worden getransporteerd. Voor de herstart moet wel eerst een nieuw back-upsysteem werkzaam zijn, waar de ICT-afdeling samen met de leverancier zorg voor draagt. Als strategie voor herstel wordt gekozen voor het terughalen van gegevens uit de back-up. De VNOG ontwikkelt samen met het NCSC en Fox-IT een instructie voor het moment dat medewerkers hun laptop inleveren om schoon te maken. De instructie omvat de volgende stappen:

> Op het inleverpunt zetten medewerkers zelf hun lokale bestanden op een door de VNOG verstrekte usb-stick.
> Medewerkers leveren de laptop en usb-stick in. De usb-stick wordt door de organisatie met meerdere soorten Anti-Virus en Anti-Malware software gecontroleerd, voordat deze samen met de nieuw ingespoelde (schoongemaakte) laptop wordt teruggegeven.

Donderdag 17 september wordt, na een test vooraf en het opstellen van een proces, onder begeleiding van het NCSC en Fox-IT gestart met het daadwerkelijk opstarten van de systemen, dat langer dan verwacht duurt en niet foutloos verloopt. Omdat de VNOG de opgebouwde herstelprocessen verder zelf kon uitvoeren, doet de NCSC op vrijdag na een goede overdracht naar de medewerkers ICT van de VNOG een stap terug uit de directe ondersteuning. Het NCSC blijft betrokken en 24/7 telefonisch bereikbaar. Ook wordt er aangevangen met de inname van laptops. Rond 17.00 uur zijn ongeveer 500 laptops ingenomen.

[12] Herinfectie kan optreden zodra geïnfecteerde systemen worden aangemeld op een schone omgeving.

In de weken die volgen, wordt er hard gewerkt aan de opbouw van de tijdelijke omgeving en met het inspoelen van alle laptops.[13] Op 14 september worden 'schone laptops en tijdelijke email adressen uitgegeven aan het kernteam inzake de coronabestrijding. Op 21 september worden schone laptops uitgereikt aan een groep van vijftien medewerkers. Het gaat hierbij om de leden van het coronateam, GHOR-medewerkers, een HRM-medewerker en een medewerker van de financiële afdeling. Deze groep fungeert als pilot-groep en wordt maximaal gefaciliteerd. Op 24 september is de wifi technisch gereed. Ook is het technisch weer mogelijk om vanuit huis te werken (alleen niet via Citrix) en is er een netwerk op de werklocaties, waardoor er weer geprint kan worden. De netwerkmonitoring is voldoende op orde en ook niet-operationele systemen mogen opgestart worden. Vanaf eind september worden schone laptops aan medewerkers in de hele regio uitgereikt. Op dat moment kan er gebruik worden gemaakt van onder andere de e-mail en Microsoft Office-applicaties. SaaS-applicaties mogen in eerste instantie niet gebruikt worden. Na een inventarisatie welke SaaS-applicaties een twee factor authenticatie hebben, wordt toegestaan de applicaties met authenticatie te gebruiken na een wachtwoord reset. Applicaties zijn gefaseerd ter beschikking gekomen; in november is zo'n 95% van de functionaliteit beschikbaar voor alle medewerkers. Het duurt nog tot februari voordat alle systemen volledig op peil zijn. In totaal worden rond de 500 systemen schoongemaakt,[14] waarvan 80 procent uit laptops bestaat en het overige deel uit vaste computers.

1.5 Communicatie

Gedurende de eerste dagen wordt op een aantal momenten intern en extern gecommuniceerd over de cyberverstoring en de gevolgen voor de organisatie. Voor het informeren van medewerkers worden via afdelingshoofden en teamleiders reeds bestaande WhatsApp-groepen gebruikt of extra aangemaakt, omdat e-mail niet beschikbaar is. Na het verstrekken van de eerste informatie over de cyberverstoring aan medewerkers op zondag 13 september, volgt de dag erna een verdere toelichting. Medewerkers krijgen informatie over de cyberverstoring, wat die verstoring betekent voor hun werk en hoe ze op de hoogte worden gehouden. Ook wordt een eerste bericht op de website van de VNOG geplaatst. In het bericht wordt gedeeld dat de VNOG is getroffen door gijzelsoftware, dat interne systemen zijn geraakt en beperkt werken en dat de e-mail niet kan worden gebruikt. De veiligheid is niet in het geding en ook de rol van de veiligheidsregio bij de bestrijding van het coronavirus gaat gewoon door. Ten slotte wordt gedeeld dat de VNOG samen met landelijke autoriteiten en de politie onderzoek doen of de aanvallers toegang hebben gekregen tot data en wat de eventuele gevolgen hiervan zijn. Hoe lang het gaat duren, is op dat moment nog niet bekend. Ook is nog niet bekend uit welke hoek de aanval komt. Over losgeld wordt niet gesproken door de VNOG. De media pakken het nieuwsbericht op.

Op 14 september wordt een tweede bericht op de website geplaatst. Hierin wordt benadrukt dat het nog te vroeg is om te kunnen zeggen welke partij achter de aanval zit en hoe de aanval heeft kunnen gebeuren. Deskundigen zijn bezig met het uitvoeren van onderzoek om bewijs veilig te stellen voor forensisch onderzoek. Er wordt hard gewerkt om gecontroleerd en veilig de dienstverlening weer op te starten. Zorgvuldigheid en veiligheid gaan daarbij

[13] Inspoelen is het geautomatiseerd installeren van systemen, maar dan met een image (een vooraf geconfigureerde versie van Windows, inclusief applicaties specifiek voor VNOG).
[14] Niet alle systemen zijn overigens geïnfecteerd, maar het controleren ervan kost meer tijd en geeft geen 100% zekerheid, terwijl een herinstallatie van het systeem die zekerheid wel geeft.

boven snelheid. Ook wordt gedeeld dat in de operationele organisatie hinder wordt ondervonden van de verstoring, maar dat er kan worden teruggevallen op alternatieven. Op 15 september ontvangen medewerkers richtlijnen die gelden tot en met zondag 20 september. Daarin wordt aangegeven wat nog wel kan (bijvoorbeeld bellen en appen) en wat niet kan (bijvoorbeeld inloggen op de VNOG-laptop). Ook vindt er een aankondiging plaats voor het opschonen van laptops en desktops. Hoewel in de communicatie is aangegeven dat medewerkers niet mogen inloggen in VNOG-systemen, blijken sommige toch gebruik te maken van verschillende SaaS-applicaties. Daarnaast bestaat het vermoeden dat medewerkers zich druk maken om lokaal opgeslagen bestanden op de laptops. Zijn ze die straks kwijt? Een tussentijds bericht wordt verstuurd naar medewerkers met informatie over de oplossing voor lokale bestanden en de inname van laptops. Ook wordt opnieuw benadrukt dat SaaS-applicaties niet mogen worden gebruikt. De communicatie over de SaaS-applicaties wordt ook naar de vrijwilligers gestuurd.

Op 17 september wordt zowel intern als extern gecommuniceerd. In de interne communicatie staat een voorwoord van de directeur en wordt aan de hand van een aantal vragen informatie verstrekt over onder andere de kans dat eigen systemen thuis zijn besmet, het moment dat ingeleverde apparatuur weer wordt teruggegeven en wat medewerkers mogen doen op een privécomputer. Via de website wordt gedeeld dat de VNOG aangifte heeft gedaan bij de politie van de gijzelsoftware-aanval en dat tijd nodig is voor het veilig herstel en op orde krijgen van de systemen. Het is op dat moment nog onbekend wanneer (delen van) systemen weer beschikbaar zijn. In de dagen die volgen, krijgen medewerkers regelmatig een update over met name de voortgang van de herstelwerkzaamheden en de uitreiking van laptops.

Op 8 oktober wordt een laatste update op de website geplaatst. Daarin staat beschreven dat alle systemen na de cyberverstoring weer veilig hersteld en op orde zijn. De VNOG is weer bereikbaar per e-mail en medewerkers hebben weer toegang tot hun werkomgeving zoals lap- en desktops. Ook wordt gedeeld dat er geen data zijn gestolen en dat bij de verstoring vooral interne systemen van de VNOG zijn geraakt. De aanvallers hebben geen toegang gekregen tot gegevens. Minister Grapperhaus van JenV informeert de Tweede Kamer hierover. Ten slotte wordt nogmaals benadrukt dat de veiligheid van medewerkers, inwoners en bezoekers in de veiligheidsregio niet in het geding is geweest. Doordat het strafrechtelijk onderzoek nog loopt, kan er geen informatie naar buiten worden gebracht over welke partij achter de aanval zit en hoe deze heeft kunnen plaatsvinden.

Gijzelsoftware

Onafhankelijk onderzoek onder 5000 IT-managers verspreid over 26 landen toont aan dat bij organisaties die worden getroffen door gijzelsoftware, het de desbetreffende hackers in 73 procent van de gevallen lukt ook daadwerkelijk data te gijzelen (Sophos, 2020). Het terugkrijgen van versleutelde data (via back-ups of betaling van losgeld) kost veel tijd en geld en vergt de nodige expertise. In het onderzoek wordt gesteld dat de directe kosten van het corrigeren van de gevolgen van gijzelsoftware gemiddeld 600.000 euro bedragen voor organisaties die het geëiste losgeld niet betalen. Dit bedrag kan zelfs oplopen tot 1,2 miljoen euro als organisaties ervoor kiezen om wel losgeld te betalen (Sophos, 2020). Gijzelsoftware kan dus flinke kosten met zich meebrengen, zelfs als hackers er niet in slagen data te gijzelen.

1.6 Afschaling

In de loop van de dagen krijgt de VNOG de situatie beter in de hand. CoPI-overleggen vinden minder frequent plaats, systemen komen weer online en medewerkers krijgen weer toegang tot de systemen. Bij de VNOG ontstaat zo'n drie tot vier weken na de start van de cyberverstoring het gevoel 'dat ze er bijna zijn': de tijdelijke omgeving is ingericht, (bijna) alle applicaties staan in de omgeving, alle verbindingen werken weer en waren alle laptops volgens plan opgeschoond en omgewisseld. Er moet nog wel een slag worden gemaakt naar de eindomgeving en er zijn nog een aantal laatste problemen, maar die kunnen in de reguliere organisatie worden opgelost. ICT en systeembeheer hebben een plan van aanpak gemaakt voor de rest van het jaar om de beheeromgeving weer helemaal op orde te krijgen. Het laatste CoPI-overleg vindt hierdoor plaats op maandag 5 oktober. Uiteindelijk duurt het tot februari voordat alle systemen weer volledig werken. Er heeft in april een markeringsmoment in de vorm van een webinar voor alle medewerkers plaatsgevonden om de cyberverstoring gezamenlijk af te sluiten. Dit vormde de start van interne bewustwordingscampagne gericht op informatieveiligheid.

2 Gijzelsoftware: ander soort crisis?

Cyber is een van de risico's waar veiligheidsregio's zich op moeten voorbereiden (IFV, 2020b). Terugkerende vraag binnen veiligheidsregio's is die over de mate waarin cyberverstoringen anders zijn dan de meer klassieke flitsrampen: wat zijn bijzondere kenmerken van cyberverstoringen (IFV, 2020a)? Hieraan gerelateerd rijzen de volgende vragen: hoe kunnen veiligheidsregio's zich op cybercrises voorbereiden? Dienen zij vooral te vertrouwen op hun reguliere voorbereiding en planvorming (en bij cyberverstoringen op veerkracht en improvisatievermogen) of vragen dit soort crises specifieke voorbereidingen? Veiligheidsregio Noord- en Oost-Gelderland is de eerste veiligheidsregio die werd geconfronteerd met gijzelsoftware. In dit hoofdstuk wordt stilgestaan bij de vraag of de cyberverstoring voor de veiligheidsregio een ander soort crisis was en zo ja, wat een dergelijke crisis van de veiligheidsregio vraagt in de voorbereiding en uitvoering.

2.1 Gijzelsoftware en zelf slachtoffer: een voor de veiligheidsregio atypisch incident

Veiligheidsregio's zijn van nature extern georiënteerd en erop gericht bijstand en hulp te verlenen bij 'andermans' incidenten en crises. Dat is ook hun wettelijke taak. Tijdens de cyberverstoring door gijzelsoftware was dat ook het geval. Sterker nog: de VNOG bevond zich -met de coronacrisis- in de grootste en langdurigste crisis sinds jaren. De 25 veiligheidsregio's zaten in september 2020 al ruim zes maanden in GRIP-4. De regio's vervulden in deze crisis, naast een intermediaire rol tussen gemeenten en het Rijk, een rol in het faciliteren van de zorgsector, ondersteunen van de besluitvormingsstructuur en het informeren van gemeenten en bestuurders (IFV, 2020d). Naast de bijdrage die de VNOG leverde aan de regionale coronabestrijding in een ongekende maatschappelijke crisis, werd de regio nu zelf slachtoffer. Dat 'zelf slachtoffer zijn' is wel een bijzonder kenmerk van deze casus. De VNOG werd dus zelf getroffen en moest haar eigen interne crisis gaan oplossen. Dat was voor de veiligheidsregio en medewerkers schakelen tussen verschillende rollen. Zoals een respondent treffend opmerkte:

> "We waren als veiligheidsregio nu zelf slachtoffer, bezig onze eigen crisis op te lossen én hadden ook nog een rol in de coronabestrijding. We vervulden drie rollen tegelijkertijd…" (respondent VNOG)

Dit geeft een andere dynamiek dan wanneer hulpverleners of crisisbeheersers vanuit een professionele rol betrokken zijn bij de crisisbeheersing, zo blijkt uit de gevoerde gesprekken.

> "Persoonlijk typeer ik de gijzelsoftware voor de veiligheidsregio als een 'slow crisis', tussen flitsramp en corona in." (respondent VNOG)

> “Een cyberaanval komt wel echt binnen in je organisatie. Persoonlijk staat de gijzelsoftware met stip op één op de lijst van heftige bedrijfsongevallen. Dit gun ik m’n ergste vijand niet. Het was heftiger dan verwacht.” (respondent VNOG)

Daarnaast zijn de incidenten en crises waarin veiligheidsregio’s optreden doorgaans zogenaamde flitsrampen: betrekkelijk overzichtelijk, voorspelbaar en kortstondig. Alhoewel het primair een interne crisis betrof, was deze cyberverstoring van een andere aard: langdurig, ongrijpbaar en onzichtbaar. Er staan geen gebouwen in brand, er zijn geen sirenes hoorbaar en de samenleving ervaart vaak (nog) geen fysieke gevolgen van de verstoring. Dat kan zorgen voor een andere perceptie van gevaar en een geringer besef van urgentie.

Daarnaast voelden medewerkers van de VNOG een grote verantwoordelijkheid om de crisis snel en effectief te beheersen; de eigen organisatie werd immers aangevallen. Werknemers wilden dag en nacht werken aan het herstel. Dit toont de grote betrokkenheid en hulpvaardigheid van het personeel van de VNOG, maar kan ook een valkuil zijn bij langdurige crises. Het betekent dat dient te worden nagedacht over voldoende rustmomenten en aflossing van collega’s. Hier was in de VNOG aandacht voor, mede dankzij de ervaring van adviseurs van het NCSC en Fox-IT. Deze waarschuwden vanaf het begin voor een langdurige crisis: “houd in elk geval rekening met minimaal twee weken, mogelijk zelfs maanden”. Zodoende kon hierop tijdig worden ingespeeld, bijvoorbeeld door vast te houden aan geplande (korte) crisisoverleggen. Enerzijds is dit een kenmerk van een cybercrisis, anderzijds is het een gevolg van een crisis die de organisatie zelf raakt.

Het feit dat de veiligheidsregio zelf slachtoffer was van gijzelsoftware, is ongekend. Dat is in de geschiedenis van de veiligheidsregio’s niet eerder voorgekomen. Optreden in dergelijke *nieuwe* situaties is altijd lastig. De schok en verontwaardiging kunnen groot zijn. Daarnaast ontbreken handelingsperspectieven, waardoor het de organisatie en medewerkers tijd kost om tot handelen over te gaan en er een groter beroep op hun improvisatietalent wordt gedaan. Die handelingsverlegenheid speelde in deze casus met name in relatie tot het forensisch onderzoek (waarbij de VNOG een beroep op externen moest doen) en de hersteloperatie (waarmee de VNOG geen ervaring had). Tegelijkertijd valt op dat de VNOG snel tot actie overging om juist op deze onderwerpen extern handelingsperspectief te organiseren.

2.2 Bijzondere kenmerken van de gijzelsoftware bij VNOG

Cybercrises hebben een aantal bijzondere kenmerken, waarin zij verschillen van meer traditionele crises als branden, overstromingen of ordeverstoringen (Berenschot, 2020). Zo kan sprake zijn van moedwillige en goed georkestreerde cyberverstoringen, spionage, betrekkelijk eenvoudige verstoringen en technische defecten. Ook het spectrum aan mogelijke gevolgen van cyberverstoringen is groot, zoals het optreden van langdurige (ontwrichtende) effecten, een verstoring van diensten en producten, hoge kosten, aantasting van vertrouwen, beïnvloeding van de publieke opinie, een snelle verspreiding en cascade-effecten. Welke van deze kenmerken en effecten deden zich in deze casus voor?

Bestuurlijk-maatschappelijke impact: moedwillig karakter en gevolgen voor regionale coronabestrijding

De melding van problemen met operationele systemen en de vondst van de gijzelsoftware waren voor de VNOG het begin van een langdurige cyberverstoring. Hoewel de vondst van gijzelsoftware nog weinig duidelijkheid gaf, was door de cryptolocker-bestanden wel duidelijk dat er sprake was van opzet. Dat leidde tot veel vragen en onzekerheid. Vragen die volgens medewerkers van de VNOG speelden, waren: wie gingen achter de aanval schuil? Was de VNOG slachtoffer geworden van een gerichte aanval of min of meer toevallig? Was er sprake van een 'state sponsored' hackerscollectief, van criminele hackers of van amateurs? Werd alleen de VNOG aangevallen of betrof het een brede aanval die ook andere veiligheidsregio's trof? Het waren voor veel van de betrokken bestuurders en medewerkers van de VNOG vragen waarmee zij voor het eerst in hun leven werden geconfronteerd.

Bijzondere context: gijzelsoftware midden in de coronapandemie

De 25 veiligheidsregio's, waaronder VNOG, zitten in september 2020 al ruim zes maanden onafgebroken in GRIP-4. Het Algemeen Bestuur van de VNOG kiest op 11 maart 2020 voor GRIP-4, gelet op de verwachte lange duur van het virus, de noodzaak van centrale regie en afstemming en de mogelijkheid tot snel handelen. Net als in de meeste andere regio's monitort het speciaal ingerichte Regionaal Operationeel Team (ROT) Corona de ontwikkelingen in de virusbestrijding. Onder het ROT zijn drie actiecentra actief:

1. Actiecentrum GHOR/GGD Medisch
2. Actiecentrum Maatschappelijke Effecten
3. Regionaal Actiecentrum Communicatie Corona.

Ook komt wekelijks het Regionaal Beleidsteam (RBT) bijeen. De corona-aanpak heeft in Noord- en Oost-Gelderland, ook bestuurlijk, de hoogste prioriteit. Speciaal voor corona is er een burgemeestersoverleg ingericht, het 'AB corona', om tweewekelijks bestuurlijk af te stemmen en elkaar bij te praten over de ontwikkelingen (VNOG, z.d.-1). De gevolgen van het virus blijven niet beperkt tot de volksgezondheid. Op tal van terreinen (economisch, sociaal) zijn de effecten merkbaar. In september blijkt sprake van een toename van het aantal coronabesmettingen in Noord- en Oost-Gelderland (Rijksoverheid, z.d.). Op exact 12 september, de dag waarop de gijzelsoftware wordt aangetroffen, schieten de besmettingscijfers in de VNOG omhoog (VNOG, z.d.-2). Niemand had verwacht dat de VNOG zou worden geconfronteerd met een andere crisis die de organisatie tijdelijk tot stilstand zou brengen en die de regionale bestrijding van de coronacrisis mogelijk zelfs in gevaar zou brengen.

De gevreesde gevolgen van de gijzelsoftware op de coronabestrijding treden niet op (Grapperhaus, 2020). De regionale crisisorganisatie voor corona met de opgetuigde structuren (RBT, ROT, taskforces) draait gewoon door. De gijzelsoftware heeft geen impact op LCMS. Geplande vergaderingen gaan door. Wel wordt hinder ondervonden, doordat gebruikelijke procedures niet gevolgd kunnen worden. Daarop worden tijdelijke 'work arounds' gevonden. Zo is het digitaal vastleggen en (intern) communiceren van besluiten lastig; besluiten worden om die reden via bestaande appgroepen bekendgemaakt aan het bestuur van de VNOG. Ook wordt de procedure van de voorzitter VNOG voor het verkrijgen van corona-gerelateerde besluiten (GRIP-4), zoals het aanwijzen van een verboden gebied, tijdelijk aangepast. Als een besluit en handtekening van de voorzitter nodig zijn, kan telefonisch contact opgenomen worden met speciaal daarvoor aangewezen contactpersonen van de VNOG (VNOG, 2020a).

Het moedwillige karakter van de cyberverstoring door gijzelsoftware zorgde voor dreiging: iemand heeft het op jouw organisatie en medewerkers gemunt. Het incident kreeg daardoor meteen een andere beleving en lading. Die eerste uren en dagen waren de onzekerheid en angst onder het bestuur en alle medewerkers dan ook groot. Moedwil betekent ook een mogelijk crimineel of politiek motief, en dus aangifte doen, een opsporingsonderzoek en

hiermee samenhangende dilemma's voor onder meer communicatie. Een cyberverstoring door gijzelsoftware betekent ook: een potentiële verstoring van vitale diensten, en daarmee mogelijk effecten op de regionale virusbestrijding (zie het kader op de vorige pagina). Dat was voor de veiligheidsregio een grote bestuurlijke zorg. De cyberverstoring door gijzelsoftware voldeed dan ook aan de drie klassieke kenmerken van een crisis: er was sprake van dreiging, onzekerheid en grote urgentie (Rosenthal, 1984). Die urgentie bleek niet alleen uit de snelheid waarmee besloten werd alle servers in de 'as is' status te zetten, het verkeersplein en externe netwerkverbindingen en toegang tot het internet los te koppelen, maar ook uit de keuze direct externe expertise in te schakelen, ongeacht de kosten.

Technologie: verstoring bedrijfsvoering veiligheidsregio en ontbreken technisch handelingsperspectief

Hoewel al vrij snel bleek dat de communicatie tussen de meldkamer en de hulpverleningsvoertuigen niet was verstoord, was er toch sprake van een enorme impact op de bedrijfsvoering. Alle 350 medewerkers hadden als gevolg van de verstoring géén toegang tot e-mail, elektronische agenda's, Microsoft Teams et cetera, waardoor de gehele interne communicatie werd verstoord. Medewerkers konden tot nader order niet gebruikmaken van laptops en hadden zodoende géén toegang tot bestanden en gegevens. Hoewel P2000, C2000 en de website niet getroffen werden en bleven functioneren, was feitelijk de gehele bedrijfsvoering lange tijd verstoord.

Uit onderzoek weten we dat cybercrises zich kenmerken door grenzeloosheid en mogelijk optredende cascade-effecten (Wetenschappelijke Raad voor het Regeringsbeleid, 2019). Problemen met of uitschakelen van ICT-systemen kan tot onvoorziene effecten leiden. Hiervan lijkt in deze casus nauwelijks sprake.[15] De effecten bleven met name beperkt tot de eigen organisatie, onder andere doordat de VNOG externe verbindingen inclusief het verkeersplein (de beveiligde digitale weg tussen veiligheidsregio's) uitzette. Het was echter niet direct duidelijk of dergelijke keteneffecten optraden. Zodoende waren andere veiligheidsregio's op zoek naar duidelijkheid: zijn wij mogelijk ook geraakt? Is de kwetsbaarheid waar gebruik van is gemaakt door de hackers ook bij ons aanwezig? Wat kunnen of moeten we doen om eventuele risico's te verkleinen? Dit waren vragen waar veiligheidsregio's snel antwoord op wilden. Het nieuw opgerichte netwerk voor informatiedeling op het gebied van informatiebeveiliging (VR-ISAC, zie hoofdstuk 3) voorzag de veiligheidsregio's van informatie over (de specificaties van) de verstoring.

Bij vrijwel alle cyberverstoringen vormt het verkrijgen van meer inzicht in de gehanteerde gijzelsoftware (type, complexiteit) en de aard, omvang en ernst van het probleem een uitdaging. Hiervoor is specialistisch forensisch onderzoek nodig. Waar veiligheidsregio's normaliter "in de actiemodus" staan, zo merkte een respondent op, waren in dit geval een "diepere diagnose en onderzoek" vereist. Dat kostte tijd. Dergelijk onderzoek is van groot belang voor het bepalen van de strategie en technische maatregelen: mogelijkheden om data terug te halen en systemen te herstellen en het behoud van sporen voor opsporing. Na het aantreffen van de gijzelsoftware beseften medewerkers al snel dat zij dit probleem mogelijk niet (volledig) zelf konden oplossen, maar dat de hulp van anderen nodig was: van organisaties die over meer ervaring, kennis en kunde beschikken om dit soort crises het hoofd te bieden.

[15] Wel bleek het tijdens de inventarisatie van kritische bedrijfsprocessen en onderliggende ICT-systemen 'puzzelen' met de onderlinge verwevenheid van systemen. Zie thema 2.

Data: mogelijk verlies en aantasting van data

Naast de gevolgen voor de bedrijfsvoering gaat deze crisis ook over mogelijk verloren, aangetaste of geblokkeerde data. Welke gegevens zitten er in de systemen van de veiligheidsregio, zijn er gegevens gelekt, hebben de hackers toegang tot (vertrouwelijke) gegevens gehad en is de betrouwbaarheid van gegevens aangetast? Deze 'data-dimensie' zorgde voor de veiligheidsregio voor geheel eigen uitdagingen, waaronder het doen van onderzoek naar verlies van data, melding doen bij de Autoriteit Persoonsgegevens, het informeren van de Functionaris Gegevensbescherming en het onderzoeken van de noodzaak om gedupeerden te informeren.

Kosten

De inzet van hulpdiensten bij incidenten en crises gaat per definitie gepaard met kosten. De kosten voor een dergelijke inzet zijn voorzien in reguliere budgetten. Als organisatie had de VNOG echter geen voorziene kosten voor een cyberverstoring opgenomen in de begroting.[16] De beheersing van deze verstoring bracht echter wel degelijk kosten met zich mee. Zo werd een uitvoerig en langdurig beroep gedaan op de inzet van de functionarissen in de crisisorganisatie. Daarnaast spelen bij cyberverstoringen andersoortige kosten een rol: de kosten voor externe inhuur, aankoop (extra) hardware, mogelijk losgeld, kosten door vertraging van reguliere werkzaamheden én (bij private ondernemingen) financieel verlies in verband met inkomstenderving. Uit onderzoek blijkt dat de directe kosten om de gevolgen van gijzelsoftware op te lossen gemiddeld €600.000 zijn (voor organisaties die geen losgeld betalen) tot gemiddeld €1.200.000 (voor organisaties die besluiten losgeld te betalen) (Sophos, 2020).

Eén van de uitdagingen die bij de VNOG speelde, betrof het snel beslissen over financiële uitgaven over onder meer externe inhuur, de aanschaf van hard- en software, en forensisch onderzoek om zicht op de modus operandi van de hackers te krijgen. Lastig was dat soms niet op voorhand te zeggen was of daarmee problemen ook daadwerkelijk sneller opgelost zouden worden. Het was daadwerkelijk beslissen in onzekerheid. De regio is daarbij telkens uitgegaan van een worstcasescenario.

Uitdagingen voor de preparatie op cyberverstoringen

Wat volgens medewerkers van de VNOG atypisch was in deze crisis, was het feit dat men amper was voorbereid op een interne cyberverstoring. Er lag geen plan klaar en er was niet geoefend op een dergelijke verstoring – dat terwijl veiligheidsregio's zich normaliter middels planvorming en oefeningen voorbereiden op tal van scenario's, variërend van branden en ongevallen tot incidenten met gevaarlijke stoffen. Uit een grondige analyse van risicoprofielen blijken andersoortige, vaak nieuwe en grensoverschrijdende, crises echter geen standaard onderdeel uit te maken van regionale risicoprofielen en planvorming (IFV, 2018). Dit gold ook voor de VNOG. Een cyberverstoring is in de vorm van een verstoring van telecommunicatie en informatietechnologie genoemd in het regionale risicoprofiel van de VNOG (en als hoog ingeschat). Er heeft echter geen specifieke preparatie op plaatsgevonden, bijvoorbeeld in de vorm van oefeningen of een draaiboek. Wel heeft de regio zich gericht op het verhogen van de eigen weerbaarheid, de continuïteit van de eigen kritische processen bij (dreigende) verstoring van ICT en het inventariseren van de

[16] Naar aanleiding van de cyberverstoring bij de VNOG worden dergelijke kosten nu wel gewogen in de risicoparagraaf en op welke manier er reserves moeten worden gealloceerd indien nodig.

kwetsbaarheden in deze kritische processen. Verder heeft de VNOG de landelijke ontwikkelingen gevolgd (VNOG, 2020b). Ook zijn bepaalde onderdelen van een cyberverstoring geoefend (denk aan een oefening met betrekking tot vitale infrastructuur en een stresstest waarbij derden naar systemen kijken). Toch concludeerden respondenten dat er onvoldoende voorbereiding heeft plaatsgevonden in de vorm van een interne, generieke cyberoefening en te weinig aandacht is geweest voor interne kritieke bedrijfsvoeringsprocessen zoals salarisadministratie.

Volgens respondenten was voorafgaand aan de crisis onvoldoende nagedacht over de impact en beheersing van cyberverstoringen. Daarnaast waren investeringen in als kwetsbaar geïdentificeerde, interne systemen (nog) niet doorgevoerd. Hierdoor moest de veiligheidsregio tijdens de verstoring noodgedwongen een beroep doen op haar improvisatievermogen en veerkracht. Zo moest de VNOG, zeker voor invulling voor de langere termijn, actief op zoek naar een nieuwe ICT leverancier, doordat tijdens de verstoring een dispuut optrad met de bestaande leverancier over de dienstverlening. In de tussentijd werd door het NCSC, Fox-IT en in een later stadium KPN kennis en expertise geboden als tijdelijke oplossing, terwijl de VNOG op zoek kon naar leveranciers die deze taken voor zowel de korte als een langere termijn konden invullen. Zo werd het mogelijk om in de nacht van zondag hardware geleverd te krijgen van Ynvolve en te starten met het opbouwen van een schaduwomgeving. De snelle levering van servers en netwerkapparauur door Ynvolve is volgens betrokkenen een belangrijke factor geweest in het snel kunnen herstellen. Normaal duurt het leveren van dergelijke hardware 10 tot 14 dagen. Daarnaast werden prioriteitenlijsten ontwikkeld door een bestaand scenarioteam (vanuit de coronacrisis) en werden externe deskundigen benaderd op basis van persoonlijke relaties. Dat beroep op improvisatievermogen pakte voor de VNOG, mede door enkele meevallers, goed uit. Maar had bij minder gelukkige omstandigheden ook anders kunnen aflopen.

Mensen: impact en gevolgen voor medewerkers

De cyberverstoring had tevens veel impact op het personeel van de veiligheidsregio. De verstoring leidde tot onzekerheid, aantasting van gevoelens van veiligheid en tot veel vragen, zeker de eerste dagen toen er nog veel onduidelijk was. Een respondent omschreef dat gevoel als volgt:

> “Het voelt alsof er in je eigen woning is ingebroken; dat je weet dat er iemand in jouw woning is geweest.” (respondent VNOG)

Daarbij kwam dat de verstoring gevolgen had voor alle 350 medewerkers van de veiligheidsregio[17], door alle lagen van de organisatie heen. Van de directie tot de brandweervrijwilligers, van Winterswijk tot Harderwijk, van het kantoorpersoneel in Apeldoorn tot de uitrukdiensten in de regio: iedereen ervoer de gevolgen in het dagelijks functioneren.

De verstoring, de onzekerheid en de daaruit voortkomende vragen leiden onder medewerkers tot bezorgdheid en irritatie: mensen wilden ‘gewoon’ hun werk doen en het was hinderlijk dat dat niet mogelijk was. Het reguliere werk ging tenslotte door. Daarnaast zong de ‘individuele schuldvraag’ rond onder sommige medewerkers. Heb ik een fout gemaakt in de beveiliging of in het niet tijdig installeren van software-updates? Heb ik iets

[17] De VNOG heeft circa 350 (beroeps-)medewerkers. Daarnaast zijn er ook 1500 vrijwilligers. Deze hebben echter geen VNOG-account.

gedaan waardoor dit heeft kunnen gebeuren? Is het mijn schuld? Hoe moet ik nu omgaan met de veiligheid van mijn eigen bestanden en programma's? Het MT speelde hier adequaat op in door snelle communicatie dat alle inspanningen gericht waren op het oplossen van de problemen en niet op de schuldvraag.

Hoewel er nauwelijks onderzoek is gedaan naar de gevolgen van cybercrises voor mensen en organisaties (Leukfeldt, 2017), lijkt de emotionele impact van dergelijke crises op medewerkers een belangrijk facet om in de gevolgbestrijding rekening mee te houden, ook voor andere veiligheidsregio's. De gevolgbestrijding is, met andere woorden, niet puur een technische operatie.

3 Reguliere of specifieke crisisorganisatie?

Met de Evaluatiecommissie Wet op de veiligheidsregio's staan de flexibele responsorganisatie en -netwerken hoog op de agenda. Veiligheidsregio's dienen te beschikken over een flexibele crisisorganisatie en over relevante crisisnetwerken: netwerken waaruit, afhankelijk van het soort crisis, de juiste expertise kan worden gemobiliseerd (zie ook: Treurniet, Boersma & Groenewegen, 2019). Deze discussie sluit aan bij de flexibele toepassing van de GRIP-procedure, waar eerder al Van Duin en Wijkhuijs (2015) diverse mogelijkheden voor signaleerden. Denk hierbij aan het flexibeler oproepen van partners voor crisisoverleggen en beter te hoog of te vaak opschalen dan te laag.

De casus waarin de VNOG als veiligheidsregio voor het eerst werd geconfronteerd met een cyberverstoring door gijzelsoftware, leent zich bij uitstek voor onderzoek naar de wijze waarop een veiligheidsregio met een dergelijke crisis omgaat. Voor welke GRIP-opschaling is gekozen, welke overwegingen speelden daarbij een rol, in welke crisisorganisatie is men gaan werken en in hoeverre is gebruikgemaakt van de reguliere organisatie en procedures? Daarnaast is het interessant te bezien in welke mate reguliere crisisstructuren toepasbaar waren bij deze cyberverstoring. Die reguliere crisisstructuren blijken namelijk ook bij cyberverstoringen een goede basis voor de respons te bieden (IFV, 2020a). Tot slot is het interessant te bekijken hoe externe, voor cybercrises specifieke, expertise is gemobiliseerd en hoe relatief nieuwe cybergremia zoals VR-ISAC hebben gefunctioneerd.

3.1 Uitdagingen in de aanpak van de cyberverstoring

Zoals we in het vorige hoofdstuk beschreven, was de gijzelsoftware voor de veiligheidsregio geen traditionele crisis, ten eerste omdat de veiligheidsregio zelf slachtoffer was en ten tweede omdat de aanpak van cybercrises zijn eigen uitdagingen kent. Zo noemt het COT (2017) het gevaar van het onderschatten van het probleem (en van te optimistische verwachtingen ten aanzien van het probleemoplossend vermogen), het risico van vertraagde opschaling en de noodzaak te komen tot een integrale aanpak van de crisis. In deze casus valt op dat van onderschatting en late opschaling geen sprake was. Medewerkers handelden vrijwel direct op meldingen van verstoring; de vondst van gijzelsoftware was direct aanleiding om de hulp van leveranciers te zoeken en medewerkers alarmeerden diezelfde nacht de leiding. Het MT aarzelde niet en besloot meteen externe bijstand van het NCSC (en later van Fox-IT en het CERT van KPN-Security) te mobiliseren. Ook valt op dat door middel van de gekozen structuur werd gewerkt aan een samenhangende aanpak van problemen, waarmee gelijktijdig bron én effecten werden bestreden. Daarover later meer.

GRIP-0

Op zondagochtend vond op de werklocatie in Apeldoorn een eerste crisisvergadering plaats. Tijdens dat overleg werd besloten met een CoPI te werken en uiteindelijk resulteerde dit in de keuze om in GRIP-0 te gaan werken. Zo'n GRIP-0 had de VNOG al eerder gebruikt,

onder meer tijdens gezondheidsklachten van medewerkers van Friesland Campina (2017), een grote brand in een welnessresort en de winterstorm in 2018.[18] Wel werd overwogen om naar een hoger GRIP-niveau op te schalen.[19] De inschatting was echter dat het vooral een interne crisis binnen de veiligheidsregio betrof, een crisisteam gewenst was en dat daarmee GRIP-0 passend was. Opschaling naar GRIP-3 vanwege mogelijke bestuurlijke effecten kwam eveneens ter sprake. Achteraf kun je discussiëren of een andere GRIP (bijvoorbeeld GRIP-2 of zelfs GRIP-4) niet logischer geweest was, gelet op de mogelijke regionale effecten. Voor VNOG bleek GRIP-0 in deze omstandigheden adequaat. Ook bij de benaming CoPI kun je kanttekeningen plaatsen; feitelijk werd er een 'gelegenheidscrisisteam' samengesteld waarin ook de directeur zitting had. Relevant en belangrijk zijn dan eerder het doen 'wat werkt' om de crisis te bestrijden, dan specifieke benaming van het team.

De leider van het crisisteam en directeur wilden met GRIP-3 niet het verkeerde signaal afgeven en paniek uitstralen. De toegevoegde waarde van een klassiek beleidsteam (BT) werd daarnaast niet gevoeld. Qua bezetting wilde de VNOG voorkomen dat 'de standaard bezetting' voor een operationeel crisisoverleg werd gealarmeerd – dus met de officier van dienst GHOR en bevolkingszorg. Men was, mede door extern advies, doordrongen van de noodzaak om externe deskundigheid in te schakelen. Tevens werd besloten een zogeheten 'gesloten incident' aan te maken in LCMS, waarin slechts specifieke functionarissen toegang hadden tot de informatie in LCMS. Ook achteraf geven betrokkenen aan dat de keuze voor GRIP-0 goed heeft uitgepakt.

GRIP-procedure
Veiligheidsregio's beschikken over een gestandaardiseerde opschalingsprocedure voor incidenten en crises. Die procedure is bedoeld om bij crises hulpdiensten op basis van hun reguliere werkzaamheden om te vormen naar één multidisciplinaire crisisorganisatie voor het bestrijden van bron en effecten (IFV, 2017). Dat is geen wettelijke regeling, maar een procedure die de regio's zelf kunnen invullen. Daarbij wordt wel een landelijke richtlijn gehanteerd met vijf opschalingsniveaus (GRIP-1 t/m -5). Al naar gelang de omvang en complexiteit van de crisis én de behoefte aan onderlinge afstemming, kan besloten worden tot een bepaalde GRIP-opschaling en daarbij passende crisisorganisatie. Voor regio's is het mogelijk om van de vaste crisisorganisatie en bezetting af te wijken als de situatie daarom vraagt.

Het feit dat het gekozen GRIP-niveau en de crisisorganisatie voor de VNOG in deze casus adequaat functioneerden, betekent niet automatisch dat dit het toekomstig responsmodel voor andere regio's zou moeten zijn bij cyberverstoringen door gijzelsoftware. Per casus dient het benodigde responsmodel te worden gekozen. Daarnaast moeten organisaties de flexibiliteit inbouwen om de crisisstructuur tijdig te kunnen aanpassen als de situatie daarom vraagt (Treurniet, Boersma & Groenewegen, 2019).

Samenstelling crisisteam

Nadat de opschaling was bepaald, werd in het zondagochtendoverleg bekeken hoe het CoPI samengesteld moest worden. Daarbij werd gekozen voor maatwerk. Vanuit de eigen organisatie sloten onder meer de directeur, teamleider Informatie, netwerk- en systeembeheer, medewerker Operationele Informatievoorziening en CISO aan. Medewerkers van het NCSC waren al ter plaatse en namen vanaf het begin deel aan de overleg. Op hun aanraden werd een beroep gedaan op een externe incident respons

[18] GRIP-0 is ook voor gemeenten vrij gangbaar, met name zodra zij worden geconfronteerd met een interne crisis en/of situatie waarbij geen inzet van hulpdiensten nodig is.
[19] Bij de cyberverstoring bij gemeente Hof van Twente werd uiteindelijk wel opgeschaald naar GRIP-3.

specialist, waarna de VNOG de gespecialiseerde diensten van Fox-IT heeft ingezet. Tevens werd op basis van persoonlijke contacten KPN-Security benaderd. Deze 'pick & choose' benadering sluit volledig aan bij de filosofie van de flexibele crisisorganisatie, zoals voorgestaan door de Evaluatiecommissie Wet op de veiligheidsregio's. Deze aanpak nam de situatie als uitgangspunt voor het organiseren en samenstellen van de crisisorganisatie (in plaats van de bestaande organisatie als vertrekpunt te nemen). Een slimme en doelgerichte aanpak, die we onderschrijven.

> "Er waren veel andere partijen dan normaal in het CoPI. Dat ging soms wat moeizaam, omdat men toch het beeld tot in detail wilde delen. Toen is de Informatiemanager gaan sturen op bondigheid: diepere technische informatie hoeft in het CoPI niet op tafel te komen." (respondent VNOG)

Een dergelijke flexibele aanpak kent ook een aantal nadelen. Een dergelijk flexibele aanpak vereist wel enig inzicht in eigen kwetsbaarheiden en onvolkomenheden[20] en het vermogen om snel ontbrekende kennis en kunde te mobiliseren. Verder kunnen formele lijnen en besluitvormingsprocessen niet voor iedereen even duidelijk zijn. Hoewel de directeur zitting had in het CoPI (en er daarmee een eindbeslisser in het CoPI vertegenwoordigd was), was er ook een rol voor het bredere MT in de besluitvorming over de prioriteitstelling en afstemming met de politie en het Openbaar Ministerie. Dat zou in praktijk kunnen leiden tot onduidelijkheid, hoewel we daar in de gesprekken weinig over hebben gehoord. Daarnaast zouden specifieke functionarissen / kolommen zich gepasseerd kunnen voelen doordat er geen beroep op hun inzet werd gedaan. Uitdaging bij zo'n 'gelegenheidscoalitie' kon bovendien zijn dat teamleden minder goed op elkaar waren ingespeeld en dat onderlinge taken en rollen niet helder waren.

Dat een interne cybercrisis nieuw was voor de VNOG, bleek ook uit het feit dat de Functionaris Gegevensbescherming (FG) niet meteen werd aangesloten bij het CoPI. De FG is een betrekkelijk nieuwe functie; een uitvloeisel van de Algemene Verordening Gegevensbescherming (AVG). De FG vervult een toezichthoudende rol en adviseert over privacy en gegevensbescherming. De persoon die deze functie pas twee weken vervulde, hoorde op de radio van de verstoring en nam zelf contact met het Hoofd Bedrijfsvoering. De FG kreeg van het MT 'carte blanche' om zich aan te sluiten en te adviseren waar nodig. Nadat hij zich een beeld had gevormd over de omvang en ernst van het verstoring, deed de FG een voorlopige melding van de cyberverstoring door gijzelsoftware bij de Autoriteit Persoonsgegevens. Voor hem was het belangrijk het risico op het lekken van (bijzondere) persoonsgegevens in te schatten. In dat geval was het namelijk verplicht de gedupeerden op de hoogte te stellen. Daarvan bleek echter geen sprake.

Strategie en aanpak

De directeur stond gedurende het incident voortdurend in verbinding met de voorzitter van de veiligheidsregio. Met elkaar bespraken zij de situatie, mogelijke dilemma's en benodigde acties, zoals het informeren van het Veiligheidsberaad en de burgemeesters in de regio.

Het MT van de VNOG gaf in de aanpak van de cyberaanval twee uitgangspunten mee voor de operatie, namelijk: 'zorgvuldigheid voor snelheid' en 'operationele systemen eerst'. Binnen deze kaders waren de crisisteams en functionarissen vervolgens behoorlijk zelfsturend, wat de snelheid van handelen ten goede kwam. Dergelijke algemene kaders

[20] Dat houdt in: als veiligheidsregio weten welke kennis en kunde je zelf in huis hebt.

gaven medewerkers veel ruimte en vertrouwen om op basis van hun ervaring, kennis en vaardigheden naar eigen inzicht beslissingen te nemen. Juist bij nieuwe crises waarin minder routinematig en volgens vaste procedures kan worden gewerkt, is een dergelijke aanpak vaak uitermate geschikt.

> “Er werd snel verteld dat we vier weken niet de IT-systemen zouden hebben. Sommige mensen zeiden: ‘maar dat weten we niet zeker’. Toch was het goed om die boodschap te verkondigen; het verandert hoe je erin staat: ervan uitgaan dat er niks is tot die datum.” (respondent VNOG)

> “Snelheid versus zorgvuldigheid is ook een dilemma. Er is gekozen voor zorgvuldigheid. Je wilt absoluut voorkomen dat je de geïnfecteerde omgeving weer terugzet. Zorgvuldigheid is daarom een heel belangrijke. Er is gekozen om het proces zo op te zetten dat er een extern specialisme bij betrokken was, die kon bevestigen: ja, dat is veilig.” (respondent VNOG)

Ondanks het feit dat de VNOG in haar strategie zorgvuldigheid voor snelheid verkoos, moesten er regelmatig beslissingen worden genomen over financiële gevolgen. Denk aan het inschakelen van adviesbureaus en het aanschaffen van nieuwe hardware. Voor een effectieve crisisrespons is mandaat nodig om verreikende beslissingen te nemen. De VNOG voorzag in die beslisbevoegdheid door de nauwe betrokkenheid van de directeur van de VNOG in het CoPI. Op deze manier waren de mensen met beslisbevoegdheid op de hoogte van de keuzes waar de organisatie voor stond, was snelle afstemming mogelijk en konden besluiten effectief worden genomen.

Sleutelbesluiten
In de respons zijn tal van beslissingen genomen. Enkele sleutelbesluiten – dat wil zeggen: besluiten die een beslissende wending aan het verloop van het incident gaven – waren:
> Afsluiten van alle systemen en voorzieningen
> Vervangen van alle servers
> Snel inschakelen van hulp
> Informeren van stakeholders
> Prioriteren aan coronabestrijding en herstel van operationele systemen tijdens hersteloperatie
> Besluit om geen risico’s te nemen: ‘better safe, than sorry’
> Instellen crisisteam Gijzelsoftware met externe adviseurs
> Besluit om geen losgeld te betalen (principe)

Externe expertise mobiliseren

Het vermogen van organisaties om de juiste (technische) expertise en vaardigheden te mobiliseren, wordt gezien als een van de factoren van een effectieve respons op cybercrises (Backman, 2020).[21] Die expertise werd door de VNOG actief gezocht en al snel gevonden in de vorm van het NCSC. Medewerkers van het NCSC dachten mee en adviseerden over de aanpak. Daarnaast adviseerde het NCSC, zoals genoemd, om een gespecialiseerd bureau in te schakelen voor forensisch onderzoek (onderzoek naar toedracht, type dader en inventarisatie van de schade). De betrokkenheid van het NCSC en Fox-IT voor forensisch onderzoek bij dit soort incidenten is niet uniek, maar juist een vrij gangbare praktijk (IFV, 2020a). Daarbij kan het bij dit soort ‘spontane samenwerkingen’ zoeken zijn naar onderlinge verwachtingen en verantwoordelijkheden en taakverdeling.

[21] Andere factoren die de auteur noemt: creativiteit, improvisatievermogen en pragmatisme en de aanwezigheid van bruggenbouwers / ‘liaison officers’.

> “De ondersteuning door het NCSC was hard nodig. Hun uitgebreide ervaring met zulke verstoringen en expertise heeft ons als veiligheidsregio erg geholpen. Ook hun relaties met (externe) deskundigen, waardoor we benodigde expertise snel konden inschakelen, bleken goud waard Zij hebben veel werk verricht in de afhandeling van het cyberincident.” (respondent VNOG)

De formele taakstelling van het NCSC richt zich op de rijksoverheid en vitale aanbieders. Veiligheidsregio’s zijn wettelijk gezien (nog) niet aangemerkt als aanbieders van vitale diensten, noch zijn ze rijksoverheid. De bijstand in deze specifieke casus was daarmee geen automatisme. Wel maakt het NCSC, bij dergelijke verzoeken bij ernstige incidenten, telkens, per casus, een afweging. In die afweging worden factoren meegewogen als: wat is de specifieke context? Welke impact is er op ICT systemen? Is er een risico op maatschappelijke ontwrichting? Wat kunnen we als NCSC bijdragen aan het oplossen van problemen?

Het NCSC besloot in dit geval, na de melding en verzoek tot hulp van de VNOG, ter plaatse te gaan om bijstand te verlenen. In die afweging woog de mogelijke maatschappelijke impact van de verstoring zeker mee, ook gelet op de rol van veiligheidsregio’s in de virusbestrijding tijdens de coronapandemie. Tevens was er die zaterdag nog veel onbekend over (mogelijk cascade-effecten van) de gijzelsoftware; een andere reden voor het NCSC om ter plaatse te gaan. De inzet van het NCSC tijdens de cyberverstoring betrof: algemene coördinatie van de incident response, vinden en dichten van de ‘point of origin’, verzamelen van informatie ten behoeve van het delen met doelgroepen, veiligstellen van mogelijk forensisch materiaal en assisteren bij het herstellen van processen. Regelmatig ondersteunen het NCSC en Fox-IT getroffen organisaties ook bij het optuigen van een crisisorganisatie. Dit was in dit geval echter niet nodig doordat de VNOG hierin zelf kon voorzien.

Nationaal Cyber Security Centrum (NCSC)
Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland en het nationale contactpunt voor digitale dreigingen en incidenten. Het NCSC verricht als het Computer Security Incident Response Team (CSIRT) voor de rijksoverheid en vitale aanbieders, de operationele coördinatie bij een grote uitval of verstoring. Het NCSC is onderdeel van het ministerie van JenV en verricht zijn activiteiten binnen de in de Wet beveiliging netwerk- en informatiesystemen (Wbni) genoemde taken ook namens de minister.

Wettelijke kerntaken zijn onder meer het bijstaan van de rijksoverheid en vitale aanbieders bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen en het informeren en adviseren van deze en andere aanbieders in en buiten Nederland over dreigingen en incidenten met betrekking tot informatiesystemen van de rijksoverheid en vitale aanbieders. Deze taken worden door het NCSC verricht met het oog op het voorkomen en beperken van maatschappelijke ontwrichting door cyberdreigingen en -incidenten en het versterken van de digitale weerbaarheid in de samenleving. Daarnaast heeft het NCSC tot taak het mogelijk in behandeling nemen van een vrijwillige melding van een incident door een organisatie die niet behoort tot vitale aanbieders of onderdelen van het Rijk.[22]

[22] Zie ook: https://www.ncsc.nl/over-ncsc/wettelijke-taak

Organisaties zijn bij cyberverstoringen sterk afhankelijk van externe hulp en specialistische expertise. Dat bleek ook in deze casus. Enerzijds betekent dit dat organisaties zoals veiligheidsregio's dit soort crises niet zelfstandig kunnen oplossen en kwetsbaar zijn. Anderzijds is het niet meer dan logisch dat veiligheidsregio's niet over deze kennis en kunde beschikken. Het betreft namelijk zulke specialistische kennis, dat het ondoenlijk is die expertise als organisatie zelf in huis te hebben (te duur, te specialistisch). Voor veiligheidsregio's is het wel belangrijk na te gaan hoe enige vorm van bijstand – door het NCSC en/of anderszins – collectief kan worden georganiseerd.

Opsporing

Door het moedwillige karakter en de vraag om losgeld was afstemming met de politie en het Openbaar Ministerie vereist. Na het doen van aangifte op maandag 14 september, vond afstemming plaats in het kader van opsporingsonderzoek en over de communicatie. Een MT-lid van de VNOG werd aangewezen om contact te onderhouden met het cybercrime-team van de politie. Dit MT-lid stond in directe verbinding met de directeur van de VNOG. Respondenten gaven aan dat dergelijke contactpersonen praktisch dag en nacht beschikbaar moesten zijn en om moesten kunnen gaan met vertrouwelijke informatie. Met betrekking tot het al dan niet betalen van losgeld is er regelmatig overleg geweest tussen de Politie, de directeur en de voorzitter van de veiligheidsregio en het ministerie van JenV en is besloten uit principe geen losgeld te betalen. Op advies van betrokken partijen is hier niet over gecommuniceerd.

Reguliere procedures, leiding en coördinatie

In het CoPI werd gewerkt volgens de BOB-methodiek,[23] een gebruikelijke methode voor crisisbesluitvorming. Dat beviel de externe partners goed: het is een gestructureerde manier van werken die zij herkennen en zelf ook gebruiken. De deelnemers aan het overleg vormden zich telkens een beeld van de situatie. Hierbij werd feitelijk gewerkt conform de Cyber-Crisis-Cirkel uit de *Handreiking Cybergevolgbestrijding G4-gemeenten* (Berenschot, 2020). Die Cyber-Crisis-Cirkel is een hulpmiddel voor beeldvorming en maatregelen in het kader van bron- en effectbestrijding. In het operationele beeld staan vier thema's centraal:

1. Forensisch onderzoek
2. Herstart: inventarisatie van problemen en effecten op interne systemen en voorzieningen
3. Communicatie
4. Opbouw & Herstel.

Op basis van de thema's kwamen de crisispartners tot een onderlinge taakverdeling. Onder het CoPI functioneerde een actiecentrum waarin vier teams werkten aan de vier zojuist genoemde thema's (zie figuur 1.1 in hoofdstuk 1). Daarnaast was er een scenarioteam. Fox-IT richtte zich op het forensisch onderzoek naar de cyberverstoring door gijzelsoftware en het NCSC nam de leiding in de opbouw- en hersteloperatie en ondersteunde waar nodig de communicatie en inventarisatie. De VNOG pakte de overkoepelende leiding op zich en was verantwoordelijk voor de herstart van de organisatie en de crisiscommunicatie. Ook bestond het scenarioteam uit werknemers van de VNOG. Twee functionarissen (die elkaar afwisselen) gaven leiding aan het CoPI: de teamleider Informatie en het hoofd Bedrijfsvoering van de VNOG. Gelet op de impact op de bedrijfsvoering was dat een logische keuze. Deze twee functionarissen werden ondersteund door een

[23] Beeld- Oordeels- en Besluitvorming.

informatiemanager en informatiecoördinator. Deze rollen werden ingevuld door het team Informatiemanagement.

Deze thematische aanpak doet denken aan het zogeheten ‘knoppenmodel’. De gedachte achter dat model is het activeren van specifieke, monodisciplinaire teams / processen die nodig zijn voor het bestrijden van problemen. Afhankelijk van de situatie kunnen meer of minder processen worden geactiveerd. Bij de VNOG werd gekozen voor vier processen, waaronder forensisch onderzoek en opbouw & herstel. Ook voor cybergevolgbestrijding kan een dergelijk model in de toekomst bruikbaar zijn.

Naast het CoPI werd gewerkt met een scenarioteam. Dit team had als taak de gevolgen van de cyberverstoring door gijzelsoftware te inventariseren. Daarbij werd gebruikgemaakt van de scenario-aanpak die binnen de coronacrisis door de regio was ontwikkeld en toegepast. Er vond met teamleiders van verschillende afdelingen een brainstorm plaats, waarbij 22 belangrijke processen in beeld werden gebracht en werden gegroepeerd rond 5 clusters (operationeel optreden, ondersteuning, communicatie, personeel en bestuur). Deze exercitie vormde de basis voor de prioriteitstelling: welke onderlinge systemen en processen dienden prioriteit te krijgen in de hersteloperatie? Het scenarioteam bereidde dit advies – in afstemming met het CoPI – voor en legde het voor aan het MT. Het MT besloot vervolgens over de prioriteiten. Eén van de adviezen die op 28 september werd gegeven, was het met voorrang teruggeven van ‘devices’ aan medewerkers met een rol in de coronacrisis, zoals medewerkers van de GHOR, adviseurs Crisisbeheersing en Informatiemanagers. Op 14 september waren er al ‘schone laptops en tijdelijke email adressen uitgegeven aan het kernteam inzake de coronabestrijding. Bij het uiteindelijke herstel heeft (de rest van) het team voorrang gekregen. Dit was duidelijk een advies ingegeven door de toenemende coronadreiging.

Het bestaande corona scenarioteam dat werd ingezet voor de gijzelsoftware lijkt een positieve bijdrage te hebben gehad aan de crisisrespons van de VNOG. Wel kan men zich afvragen of veel van de activiteiten die het team heeft ondernomen, zoals het opstellen van de prioriteitenlijsten, niet al grotendeels in de koude fase hadden moeten worden uitgevoerd.

> “Er is een scenarioteam gecreëerd met een linking pin in CoPI-overleg. Daardoor laat je business de prioriteiten bepalen en in het CoPI-overleg bekijk je wat technisch kan en verantwoord is. Daarmee krijg je een redelijk gebalanceerde weg naar herstel, waarbij wel oog en oor is voor de businessprioriteiten, maar de IT-capaciteit niet voortdurend van hoog naar laag wordt gestuurd.” (respondent VNOG)

> “Het is beter om zo spoedig mogelijk een scenarioteam te hebben. Kan een organisatie enorm helpen. Meerwaarde: onzekerheden van de toekomst in beeld krijgen. Gezamenlijke taal ontwikkelen; de crisis duurt nog lang. Hoe lang dan, en wat gebeurt er na twee weken, vier weken, zes weken? Wat heb je dan al staan of niet? De aansturing van normale bedrijfsvoering gaat er anders uitzien. Dan denk je er al over na.” (respondent VNOG)

Die onderlinge taakverdeling, het onderlinge vertrouwen in elkaars expertise, de vrijheid om naar bevind van zaken te handelen, in combinatie met een duidelijke beslissingsstructuur, werden door respondenten unaniem als goede praktijken genoemd.

> “De Informatiemanager maakte standaard een uur voor het CoPI een rondje langs de velden: langs Fox-IT, NCSC, CISO, netwerkbeheer, operationele informatievoorziening, systeembeheer en communicatie in verband met omgevingsanalyse en sentiment. Het was een complexe rol: normaal is een crisis minder vakinhoudelijk.” (respondent VNOG)

> “Ik vind de aanpak van dit incident een schoolvoorbeeld. VNOG is meteen de crisisorganisatie ingegaan en met BOB gaan werken. De VNOG bleek geoefend om dat proces strak te organiseren. Het heeft ook geholpen dat de VNOG in een vroeg stadium betrokkenen hebben geïnformeerd en hebben gekeken waar ze experts en advies konden inwinnen, in plaats van eerst zelf problemen op te lossen.” (respondent NCSC)

VR-ISAC en onderlinge bijstand

Veiligheidsregio’s beschikken sinds juni 2020 over een zogeheten ‘Information Sharing & Analysis Center’. Dit VR-ISAC is een platform waarin veiligheidsregio’s en het NCSC – onder voorwaarde van vertrouwelijkheid – informatie uitwisselen over cyberdreigingen, maatregelen en best practices (IFV, 2020c). Ook de VNOG is aangesloten bij het VR-ISAC (VNOG, 2020c).[24] Op het moment van de cyberverstoring was het VR-ISAC pas drie maanden actief. Het VR-ISAC werd door de VNOG de eerste dagen niet gebruikt om informatie te delen met de CISO’s van de aangesloten veiligheidsregio’s. Dat zou echter handig zijn geweest om relevante functionarissen, bottom-up, van informatie te voorzien. Maar het is logisch te verklaren dat dit proces niet vlekkeloos verliep. Ten tijden van crisis kan er immers druk komen te staan op informatiedeling (IFV, 2020a). Bij de VNOG heerste in het begin veel onduidelijkheid en onzekerheid; men wist onvoldoende wat er aan de hand was en achtte zichzelf dan ook niet in staat om de gevraagde antwoorden te geven. Daarnaast bestonden er binnen het VR-ISAC (nog) geen afspraken over het delen van informatie bij daadwerkelijke verstoringen en was de cyberverstoring bij de VNOG de eerste keer dat een dergelijke verstoring op deze manier plaatsvond. Maar ook met gemaakte afspraken kan informatiedeling in een kleine, besloten groep onder druk komen te staan bij cyberverstoringen, vaak omringd door vertrouwelijkheid (IFV, 2020a)

> “Het contact met het VR-ISAC verliep informeel. Er zijn geen goede afspraken gemaakt over wat wel of niet gedeeld kon worden. Wel waren er afspraken over dat het een veilige omgeving moet zijn. Er kon wel gedeeld worden dat andere veiligheidsregio’s niet in gevaar waren. Het zou goed zijn om duidelijke afspraken te maken met het VR-ISAC; in dergelijke situaties is er wel behoefte aan één vertrouwenspersoon vanuit het VR-ISAC.” (respondent VNOG).

Gaandeweg kwam het proces echter goed op gang, nadat de voorzitter van het VR-ISAC naar voren trad als contactpersoon met de CISO van de VNOG. Maar in het begin is het over en weer nog zoeken naar een passende vorm van afstemming en wat het VR ISAC voor de VNOG kon betekenen (en andersom). Daarbij komt dat de CISO van de VNOG geen tijd had om updates op te stellen, maar wel om de voorzitter van het VR ISAC bij te praten.

Tijdens de cyberverstoring leefde er onder andere regio’s wel degelijk een informatiebehoefte, zo constateerde de voorzitter van het VR-ISAC. Andere regio’s wilden

[24] https://www.vnog.nl/actueel/nieuws/2235-vnog-sluit-zich-aan-bij-samenwerkingsverband-tegen-cyberincidenten.

namelijk weten wat er speelde en wat dit voor hen zou kunnen betekenen. De voorzitter nam daarom zelf contact op met de CISO van de VNOG met het verzoek om kerninformatie over het incident voor de andere regio's. Zij spraken onderling af een communicatiebericht (informatie, duiding en handelingsperspectief) op te stellen, dat vervolgens in het VR-ISAC kon worden verspreid. Zo vonden ze met elkaar, heel pragmatisch, een voor beide partijen werkbare oplossing.

Omdat nog niet alle 25 regio's bij het VR-ISAC waren (en zijn) aangesloten,[25] werd besloten ook te communiceren naar de vakgroep Informatieveiligheid. Hierbij vond wel een scheiding plaats: gevoelige informatie werd alleen via VR-ISAC verspreid, de rest ook via de vakgroep. Tijdens het verdere verloop van de cyberverstoring voerde het VR-ISAC meerdere taken uit. Zo vervulde het een vraagbaakfunctie en het verrichtte hand-en-spandiensten (zoals het helpen bij het inrichten van reservelaptops). Daarnaast fungeerde het als een soort uitzendbureau, waarbij mensen uit enkele andere veiligheidsregio's werden ingezet bij de crisisrespons. De VNOG kreeg vanuit verschillende regio's namelijk hulp en bijstand aangeboden. Dat werd, zo geven respondenten aan, erg gewaardeerd. Een dilemma dat hierbij wel speelde, was hoe die externe collega's een volwaardige plek kon worden geboden in de responsorganisatie. Vaak is dergelijke aangeboden bijstand immers van korte duur, voor slechts één of meerdere dagen. Om echt goed mee te draaien in de crisisorganisatie was echter een langdurige betrokkenheid wenselijk. Die langdurige inzet was voor de collega's van andere regio's ook een uitgelezen kans geweest voor het opdoen van ervaring, kennis en kunde met dit soort verstoringen. Kennis en kunde die zij op hun beurt weer mee terug hadden kunnen nemen naar de eigen regio. Het leveren van onderlinge bijstand en hulp bij beveiligingsincidenten is overigens eerder een taak van een toekomstig Computer Emergency Respons Team (CERT) voor veiligheidsregio's. Over zo'n CERT beschikken veiligheidsregio's op het moment van evalueren echter niet.

Afschalen

Afschalen is bij praktisch elke crisis een punt van aandacht (zie ook: COT, 2010). Wanneer schalen we de crisisorganisatie af? Hoe houden we zicht op de verdere nasleep? Welke nafasethema's spelen er? Over de nafase van cyberverstoringen weten we overigens nog vrij weinig. Wel weten we dat het lastig kan zijn om vast te stellen dat systemen en data weer veilig zijn (IFV, 2020a), dat het verhalen van schade ingewikkeld kan blijken en de impact op organisatie en personeel aandacht vraagt (Berenschot, 2020).

> "Opschalen kan iedereen, maar afschalen is veel moeilijker. Een incident is nooit klaar. Je bent er voor 80 procent doorheen, maar je hebt ook nog 20 procent onzekerheden waar je mee te maken hebt. Voor een volgende keer: wel eindpunt markeren, maar daarbij aangeven wat nog niet is afgerond." (respondent VNOG)

> "Er is niet een punt gezet achter de interne crisisstructuur. Er waren steeds nieuwe winstpuntjes te melden, het werd steeds mooier en volledliger, dus ga je niet zeggen: het is nu brand meester en het incident klaar. Dit ging geleidelijk." (respondent VNOG)

In deze casus was afschalen eveneens een aandachtspunt. Weliswaar was het laatste CoPI-overleg duidelijk gemarkeerd en was de overgang van 'crisisorganisatie' naar 'lijnorganisatie' volgens respondenten helder. Ook is een nafaseplan gemaakt, waarmee feitelijk een einde kwam aan de continuïteitscrisis. Voor de functionarissen in de

[25] In maart 2020 zijn 18 veiligheidsregio's aangesloten.

crisisorganisatie was die afschaling helder, maar voor de bredere organisatie ontbrak het aan een dergelijk gemarkeerd eindmoment. Ook in het MT heeft nog geen formele afsluiting plaatsgevonden.

Hoewel de continuïteitscrisis op 5 oktober werd afgerond, liep de IT-nasleep nog langer door. Waar de meeste functionaliteiten na 3 tot 4 weken weer beschikbaar waren (mede door gebruik van een tijdelijk uitwijkapparaat), werd achter de schermen door de IT-afdeling gewerkt aan het opbouwen van een nieuwe operationele omgeving. Dit opbouwen duurde tot circa februari 2021, vijf maanden na de start van het incident. Met name dit aspect van de hersteloperatie is niet gemarkeerd en sluimerde lange tijd voort. Inmiddels is er op 20 april 2021 een afsluitende bijeenkomst geweest van alle medewerkers van de VNOG.

4 Crisiscommunicatie: openheid of geslotenheid?

Crisiscommunicatie is cruciaal voor een effectieve crisisbeheersing. In veel crisisevaluaties wordt de focus gelegd op crisiscommunicatie als succesfactor voor crisisbeheersing (Evaluatiecommissie Wet veiligheidsregio's, 2020). Goede crisiscommunicatie staat voor het verspreiden van juiste, tijdige en begrijpelijke informatie over de gebeurtenis en het bieden van handelingsperspectieven tijdens en na een crisis, ramp of incident. De vraag die hierbij speelt, is of de communicatie over een cybercrisis anders is dan communicatie over 'reguliere' crises. Zijn er factoren waar men bij een cyberverstoring (extra) rekening mee moet houden in de communicatie? Welke uitgangspunten worden gebruikt in de interne en externe communicatie over een cyberverstoring? Kan er in alle openheid worden gecommuniceerd of is een zekere mate van geslotenheid gewenst?

Tijdens de cyberverstoring bij de VNOG werd op verschillende momenten zowel intern als extern gecommuniceerd. Het uitgangspunt was dat interne communicatie vóór externe communicatie ging. Bij de interne communicatie stond vooral het informeren van de eigen medewerkers centraal over wat de cyberverstoring voor hun werkzaamheden betekende en hoe ze zouden worden geïnformeerd over de afwikkeling van de verstoring. Deze informatie verliep met name via Whatsappgroepen, omdat de e-mail niet werkte. Wat betreft externe communicatie werden in totaal vier berichten geplaatst op de eigen website, die nog wel werkte. Er werden korte updates geplaatst met feitelijke informatie over het getroffen zijn door gijzelsoftware en over de gevolgen voor de organisatie; ook werd een beknopte uitleg over de aanpak gegeven. Onder andere de Stentor en de NOS pakten deze berichtgeving op, maar de cyberverstoring werd niet breed uitgemeten in de media. Naast de communicatie via de website werd informatie gedeeld met andere veiligheidsregio's, het VR-ISAC en werden de verschillende gemeenteraden binnen de veiligheidsregio geïnformeerd. Ook is er contact geweest tussen de directeur en voorzitter van de VNOG, en minister Grapperhaus. Vervolgens heeft minister Grapperhaus de Tweede Kamer geïnformeerd over de cyberverstoring door middel van een brief (Grapperhaus, 2020).

4.1 Uitdagingen in de communicatie over cyberincidenten

De essentie van crisiscommunicatie bij een cybercrisis is niet per definitie afwijkend van de communicatie bij reguliere crises. Zo zijn er een aantal algemene uitgangspunten voor crisiscommunicatie die gelden voor alle type crises:

> Richt je in de communicatie eerst op schadebeperking en vervolgens op het beantwoorden van de maatschappelijke informatiebehoefte en het duiden van de gebeurtenis.
> Communiceer omgevingsbewust, open, tijdig, consistent en proactief.
> Communiceer over het proces (wat er al wel en niet bekend is, welke stappen er worden gezet en hoe de burger moet handelen).

> Communiceer over zichtbare maatregelen en indien wenselijk / mogelijk ook over onzichtbare maatregelen.
> Bevestig wat zichtbaar is, vertel wat je wel en niet weet, ontkracht geruchten of laat weten dat je de geruchten kent en onderzoekt.
> Communiceer zonder afstemming niet over SISOS: slachtoffers, identiteiten, scenario's, oorzaken en schade (Eenheid Communicatie NCTV, 2021).

Toch vraagt de crisiscommunicatie bij cybercrises op een aantal vlakken een andere aanpak dan bij meer reguliere crises. Kenmerkend voor een cybercrisis is dat het soms lang kan duren voordat duidelijk is wat er precies aan de hand is.[26] Bij de VNOG duurde het zo'n acht uur na de eerste detectie van de verstoring van processen voordat men wist dat er sprake was van een cyberverstoring door gijzelsoftware. Pas daarna werd gestart met communiceren. Bij meer reguliere crises wordt de communicatie vaak al binnen een uur opgestart. De VNOG had dit ook kunnen doen door procesinformatie te geven over de detectie van processen die verstoord waren en over de te nemen stappen om de oorzaak van de verstoring te achterhalen. De vraag is dan wel of dit niet juist tot onrust had geleid onder bijvoorbeeld het personeel van de VNOG. Medewerkers hadden waarschijnlijk op dat moment nog helemaal niet in de gaten dat er iets aan de hand was. Het was een voordeel dat de aanval in het weekend plaatsvond en niet op een doordeweekse dag binnen kantooruren. De meeste werknemers waren tijdens de start van het incident niet aan het werk en ondervonden daardoor niet direct hinder van de verstoring. Dit leverde tijdwinst op om de communicatie zorgvuldig op te starten en zorgde ervoor dat het geven van procesinformatie in een vroeg stadium niet direct nodig was.

Dat de eigen systemen waren geraakt, leverde op het vlak van communicatie direct een uitdaging op: hoe zorg je er als organisatie dan voor dat de interne en externe communicatieboodschappen de wereld in komen? Reguliere communicatiekanalen zoals e-mail, waren door de verstoring immers niet meer beschikbaar. Persberichten konden niet worden verstuurd. De website van de VNOG was echter niet getroffen door de cyberverstoring en was daardoor online gebleven. Zodoende heeft de VNOG de website kunnen inzetten als communicatiekanaal voor de buitenwereld. Intern is gekozen om het eigen personeel te informeren via WhatsApp en Signal (en later toen dat weer mogelijk was via de e-mail). Via teamleiders en afdelingshoofden werden appgroepen aangemaakt om zo de interne communicatie te kunnen verspreiden. Toch was het onzeker of iedereen hiermee zou worden bereikt. De VNOG was juist voor dergelijke gevallen bezig met de implementatie van een sms-service om bij calamiteiten alle medewerkers te kunnen bereiken, maar dit systeem was op het moment van de cyberverstoring nog niet operationeel.

Een ander aspect dat de crisiscommunicatie anders maakte dan bij een reguliere crisis, was dat de VNOG zelf was geraakt door de cyberverstoring. Er was dus sprake van een interne crisis. Waar de crisiscommunicatie zich normaal richt op (onbekende) betrokkenen van een incident, waren het nu de eigen collega's die moesten worden geïnformeerd. De impact van de verstoring concentreerde zich juist op medewerkers van de VNOG. Zij kregen te maken met de nodige onzekerheid: heb ik iets verkeerd gedaan waardoor dit kon gebeuren? Kan ik mijn privécomputer nog veilig gebruiken? Ben ik straks al mijn bestanden kwijt? Opvallend aan de interne communicatie was, dat er goed werd ingespeeld op de vragen die leefden onder het personeel. Diverse keren werd een update verstuurd in de vorm van een Q&A.

[26] Dit geldt niet uitsluitend voor cybercrises. Bijvoorbeeld tijdens de aanslag in Brussel (2016) was er een periode van onduidelijkheid over de vraag of de explosie 'gewoon' een explosie was of het gevolg van een aanslag.

Een uitgangspunt dat werd gehanteerd, was: bij vragen van medewerkers geven we antwoord. Hierdoor kon een groot deel van de onrust worden weggenomen.

Om een duidelijk handelingsperspectief op te kunnen stellen, moet er voldoende zicht zijn op wat er precies speelt. Bij een cyberverstoring is deze informatie behoorlijk technisch en zijn communicatieadviseurs afhankelijk van de informatie die wordt gedeeld door ICT-medewerkers die bovendien gewend zijn om in vaktaal te communiceren. Bij de VNOG lag er dus een uitdaging om die vaktaal te vertalen naar begrijpelijke lekentaal. Dat vergt van communicatie met name goed doorvragen, om zo technische termen te kunnen vertalen en processen uit te kunnen leggen. Ook moet er aandacht zijn voor de woordkeuze in de berichtgeving. Kies je voor het woord cyberaanval of is gijzelsoftware neutraler? Soms kan het verstandig zijn om hiervoor een inhoudelijke sparringpartner te zoeken, zoals door de VNOG is gedaan. In dit geval werd gekozen voor de term ‘gijzelsoftware’ vanwege het gevoel van angst dat het woord ‘aanval’ op kan roepen.

Tips voor communicatie bij incidenten in het digitale domein
In de koepelnotitie *Communicatie bij digitale incidenten* (Eenheid Communicatie NCTV, 2021) wordt een aantal tips gegeven die uitermate relevant zijn voor de crisiscommunicatie bij cyberincidenten, zoals de cyberaanval op de VNOG:

> Zo lang niet zeker is of er sprake is van opzettelijk handelen, dienen verwijzingen naar mogelijke oorzaken, duur en omvang vermeden te worden.
> Het kan soms lang duren voordat duidelijk is wat er precies aan de hand is. Geef waar mogelijk wel alvast procesinformatie.
> Wanneer vanuit veiligheidsoverwegingen communicatie over het incident, de impact en/of maatregelen niet mogelijk is, wordt dat gemeld.
> Communicatie van bestuurders verbindt de samenleving (maar zorgt ook voor verbinding binnen de eigen organisatie) en doet een beroep op de veerkracht van de samenleving (of organisatie).

Voor de voorbereiding van de crisiscommunicatie worden ook een aantal tips gegeven, waaronder:

> Maak een overzicht van de communicatiepartners. Deze zijn bij een cybercrisis vaak anders dan bij een fysieke crisis.
> Zorg voor aansluiting bij operationele collega’s die zich met digitale incidenten bezighouden.
> Bereid een lijstje met (in- en externe) experts voor die technische informatie kunnen duiden tijdens een incident.
> Maak een plan voor het geval de gebruikelijke digitale communicatiemiddelen niet beschikbaar zijn.
> Denk na over de manier waarop beeld (infographics, visuals et cetera) kan helpen om technische materie begrijpelijk te communiceren.

4.2 Interne en externe communicatie

Interne communicatie

Het is een gouden regel bij crisiscommunicatie, maar een die – ondanks de beste bedoelingen – nog wel eens wordt vergeten: in het geval van een crisis informeer je als eerste de eigen medewerkers. Deze gouden regel is tijdens de cyberverstoring bij de VNOG en het herstel ervan goed gevolgd, wat gezien de aard van de crisis ook wel logisch te noemen is: de VNOG was immers vooral intern geraakt. Er is veelvuldig gecommuniceerd

met medewerkers. De inzet van de interne communicatie was erop gericht om medewerkers voortdurend zo uitgebreid mogelijk te informeren om hen zo snel mogelijk weer aan het werk te kunnen krijgen. De manier van communiceren droeg hierdoor bij aan het creëren van rust in het herstelproces en begrip en draagvlak bij de medewerkers die niet op hun computer of laptop konden werken. De VNOG formuleerde een aantal uitgangspunten voor de interne communicatie:

> Communicatie is een vast thema binnen het CoPI / crisisteam.
> Zorg voor alternatieve communicatiekanalen naast e-mail (WhatsApp, Signal).
> Informeer medewerkers op hetzelfde niveau als externen. Geef mee wat de kernboodschap naar buiten is en blijf deze regelmatig herhalen. Zo wordt de kans dat het juiste verhaal wordt verteld groter.
> Neem medewerkers consequent en goed mee in het proces:
  – Schets tijdlijnen (doe aan verwachtingsmanagement)
  – Wees concreet in wat de cyberaanval betekent voor medewerkers: wat zijn de impact en het handelingsperspectief?
> Gebruik begrijpelijke taal.

Het hanteren van deze uitgangspunten lukte over het algemeen goed tijdens de gehele afhandeling van de cyberverstoring. Op sommige momenten ontstond er wel wat onrust onder het personeel of rezen er vragen, maar hier werd goed op gereageerd door de VNOG. Toen er vragen ontstonden over het gebruik van SaaS-applicaties, het inleveren van laptops of het veiligstellen van bestanden op de lokale schijf, werd dit direct opgepakt en volgden de antwoorden in een nieuwbrief of een Q&A. In de Q&A van 17 september werd een voorwoord van de directeur toegevoegd om tegemoet te komen aan het sentiment in de organisatie: men was ongerust. De directeur toonde empathie door een compliment te geven over de flexibele en veerkrachtige organisatie, door aan te geven hoe vervelend de situatie voor iedereen was en door het uitspreken van zijn vertrouwen. Dit was meteen een belangrijk verschil met de externe communicatie. Waar intern werd gecommuniceerd vanuit empathie, was de toon extern veel zakelijker.
Ten slotte heeft de VNOG goed voor ogen gehouden dat interne communicatie gelijk moet zijn aan externe communicatie. Een andere gouden regel voor crisiscommunicatie is namelijk dat intern geen zaken worden gedeeld die niet extern mogen gaan, en dat extern geen dingen worden verteld waarvan eigen medewerkers niet op de hoogte zijn.

Externe communicatie

In de externe communicatie wilde de VNOG graag zelf de regie houden op het informatieproces. Dat deed zij door periodieke updates te geven via de eigen website. Tot en met 8 oktober werden vier updates gegeven die compact waren – zeker in vergelijking met de uitgebreide berichtgeving na de cyberincidenten bij de gemeente Lochem en de Universiteit Maastricht. De VNOG heeft er bewust voor gekozen om geen lange stukken te schrijven, maar korte en duidelijke boodschappen. Nu waren er in dit geval ook wel een stuk minder externe effecten dan bij de hiervoor genoemde twee casus. Het uitgangspunt was om terughoudend te zijn in de communicatie. Een risico van inhoudelijk weinig delen is wel dat er verhalen van journalisten kunnen komen met speculaties, waardoor je je als organisatie moet gaan verdedigen. De VNOG heeft hier geen last van gehad. De nieuwsberichten werden opgepakt door de media, maar hebben tot weinig vragen van journalisten geleid. Ongetwijfeld hielp het mee dat het coronavirus weer oplaaide ten tijde van de cyberverstoring, naast het feit dat er weinig externe effecten waren. Ook uit de

omgevingsbeelden kwam een rustig beeld naar voren: vooral tech-redacteuren volgden de casus op de voet.

Naast de communicatie via de website heeft de VNOG ook informatie gedeeld met onder andere burgemeesters uit de regio, directeuren veiligheidsregio's, het VR-ISAC en het ministerie van JenV. De informatie was voor een groot deel hetzelfde als wat via de website werd gedeeld, maar werd waar mogelijk (of nodig) aangevuld met wat relevant was voor de betreffende partner.

Ondanks het feit dat er weinig vragen binnen kwamen bij de afdeling communicatie op basis van de berichtgeving op de website, kwamen op twee andere plaatsen wel vragen binnen over de cyberverstoring. Het scenarioteam kreeg vragen van partners, zoals de meldkamer en de waterschappen. Ook organisaties die regelmatig e-mailcontact hebben met de VNOG vroegen zich af of zij zelf risico zouden lopen. Vanuit het CoPI werd aangegeven welk antwoord kon worden gegeven. Bij de voorzitter van het VR-ISAC kwamen vragen binnen van andere veiligheidsregio's, waar sprake was van wat onrust: wat is er aan de hand? Wat betekent dit voor ons? Er was behoefte aan duiding. De voorzitter van het VR-ISAC heeft dit aangegeven bij de VNOG en heeft afgestemd met de CISO en informatiemanager hoe hiermee omgegaan moest worden. Het VR-ISAC heeft vervolgens gefungeerd als vangnet en de informatievoorziening naar de veiligheidsregio's op gang gebracht. Deze acties zijn buitenom de afdeling communicatie gegaan.

4.3 Openheid in communicatie

Een terugkerend thema bij cybercrises is het afwegen in hoeverre de organisatie open moet communiceren. Over het algemeen heeft open communicatie in crisiscommunicatie de voorkeur, maar ál te openlijk communiceren kan ook een risico vormen. Organisaties leggen daarmee namelijk hun eigen kwetsbaarheden bloot. Daarnaast kan het openlijk delen van gegevens over incidenten lastig blijken in de hectiek van de crisis, bijvoorbeeld omdat andere belangen dan gaan meespelen (zoals opsporing en vervolg, reputatie en herstel van de interne bedrijfsvoering). Zodra fysieke gevolgen optreden en mensen hinder ondervinden door het incident, is het in principe onvermijdelijk om over het incident te communiceren (IFV, 2020a).

Communiceren over het betalen van losgeld wordt bij cyberaanvallen gezien als een duivels dilemma. Het bedrag benoemen kan het risico met zich meebrengen dat een norm wordt gezet, waar criminelen in het vervolg rekening mee zouden kunnen houden. Ook zouden de reacties op de hoogte van het bedrag in de media effect kunnen hebben (Van Duin & Wijkhuijs, 2020). De VNOG heeft de keuze gemaakt om beperkt te communiceren over de oorzaak van de cyberverstoring en het al dan niet betalen van losgeld. Dit is ook wat de politie adviseerde. Over het bedrag dat gevraagd werd, is niets gedeeld. Kwaadwillenden zouden die informatie kunnen gebruiken bij een cyberaanval gericht op andere veiligheidsregio's en dat moest natuurlijk niet gefaciliteerd worden. Daarnaast was het strafrechtelijk onderzoek nog in volle gang. Bij de afweging om iets al dan niet te communiceren, werd door de VNOG het onderscheid gemaakt tussen 'nice to know' en 'need to know' – heeft het meerwaarde om over iets te communiceren?

Het valt op dat andere (overheids)instanties die werden getroffen door een cyberaanval zoals de gemeente Lochem, de gemeente Hof van Twente, de Universiteit Maastricht en recentelijk de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) openlijker communiceerden dan de VNOG heeft gedaan. Zo maakte de NWO zelf bekend door welke groep criminelen zij was gehackt en dat niet werd meegewerkt aan de eis om losgeld te betalen, omdat zij “als onderdeel van de Nederlandse Rijksoverheid op principiële gronden niet in[gaat] op de eisen van criminelen” (NOS, 2021). De VNOG deelde dit soort informatie niet in persberichten. Ook de Universiteit Maastricht was een stuk opener dan de VNOG en koos voor een open, eerlijke en transparante manier van communiceren vanwege haar overtuigingen en waarden, waaronder het stimuleren van een open en transparante cultuur. De universiteit nam het publiek mee in het proces, omdat er “geen onzekerheid [was] over het feit dat de digitale systemen plat lagen en geen onzekerheid over wie dat allemaal trof en in welke mate”. Zowel de Universiteit Maastricht als de gemeente Lochem deelden onderzoeksbevindingen en gaven regelmatig statusupdates, en daarnaast organiseerde de universiteit een symposium om lessen te delen (IFV, 2020). Om een einde te maken aan geruchten over het betalen van losgeld, maakte de Universiteit Maastricht zelfs het exact betaalde bedrag aan losgeld bekend tijdens dit symposium (Van Duin & Wijkhuijs, 2020). Ze gaf aan het taboe in de publieke discussie over het belonen van criminelen te willen doorbreken en een debat te willen starten over dilemma’s rond cyberveiligheid in het hoger onderwijs (IFV, 2020).

In de koepelnotitie ‘Communicatie bij incidenten in het digitale domein’ (Eenheid Communicatie, NCTV, 2021) wordt aangegeven dat wanneer communicatie over (technische en operationele) kwetsbaarheden en/of maatregelen niet mogelijk is vanuit veiligheidsoverwegingen, het goed is om dat te melden (dus dat er om die reden geen nadere mededelingen gedaan worden). Daarbij wordt gesteld dat waar mogelijk wel procesinformatie kan worden gegeven. Bij de VNOG wilde men vanwege veiligheidsoverwegingen niet communiceren over de oorzaak van de cyberverstoring. In lijn met de koepelnotitie werd wel procesinformatie gegeven: er werd ingegaan op het verloop van het onderzoek naar de aanval en de gevolgen voor de organisatie, en vermeld dat nog niet duidelijk was hoe lang een en ander nog zou gaan duren.

In de vierde en laatste update (8 oktober) werd gemeld dat alle systemen weer veilig hersteld en op orde waren. Hierbij werd aangegeven dat er geen data waren gestolen bij de aanval en dat vooral interne systemen van de VNOG waren geraakt. Dit impliceert dus dat het betalen van losgeld niet nodig was, omdat het de VNOG zelf (met hulp van experts) is gelukt om de systemen te herstellen en dat communiceren over losgeld daarom niet nodig was. In de interne communicatie aan de medewerkers werd ook niet gesproken over losgeld, maar in de raadsinformatiebrief aan de gemeenten binnen de regio werd dit wel behandeld (VNOG, 2020a). Hierover werd door de VNOG aangegeven: “We hebben tot nu toe alleen een waarschuwing gekregen, we hebben op aanraden van de autoriteiten nog geen contact gehad met de criminelen”.

De VNOG heeft in vergelijking met andere organisaties die werden getroffen door een cyberverstoring relatief summier gecommuniceerd. Het is de vraag of dit, hierop terugkijkend, een probleem was of dat meer openheid in de communicatie niet nodig was. Daarbij speelt natuurlijk ook de hoeveelheid informatie waarover gecommuniceerd zou kunnen worden mee. Een overweging van de VNOG om niet te veel te communiceren, was dat dit tot meer vragen zou kunnen leiden en juist tot minder in plaats van meer vertrouwen

in de afhandeling van de verstoring. Bovendien werden er weinig vragen gesteld. Werd er toch een vraag gesteld over bijvoorbeeld het losgeld, dan werd als antwoord gegeven dat het onderzoek nog in volle gang was en dat de politie voor dat deel aan zet was. Dat antwoord was dan afdoende.

Ook nadat de verstoring vrijwel was afgerond voor de VNOG, werd er geen afsluitend communicatiebericht op de website geplaatst. Er was niemand meer die vragen stelde, dus had het dan toegevoegde waarde om te communiceren? Zou het goed zijn geweest om te communiceren dat er geen losgeld is betaald? Wellicht zouden er alleen maar slapende honden mee wakker zijn gemaakt, en zou dergelijke informatie alleen maar zorgen voor nieuwe vragen waar de organisatie eigenlijk niet op zit te wachten. Voor de eigen medewerkers van de VNOG is het echter wel wenselijk om meer openheid te geven over de cyberverstoring. Veel medewerkers weten niet wat er precies is gebeurd en zitten met vragen. Terughoudendheid in het delen van informatie is in eerste instantie begrijpelijk, maar het is goed om in een later stadium meer te delen.

De VNOG heeft ervoor gekozen om meer open te zijn naar de eigen medewerkers over wat er is gebeurd, op het moment dat de laatste werkzaamheden zijn afgerond door de ict-medewerkers. In een bijeenkomst voor alle medewerkers is aandacht voor wat de VNOG precies is overkomen. Daarnaast is het een officieel moment waarmee de hack gezamenlijk wordt afgesloten.

5 Bevindingen en adviezen

5.1 Overkoepelende bevindingen

> De VNOG heeft deze cyberverstoring naar ons oordeel adequaat bestreden. Zij heeft de gijzelsoftware vanaf het allereerste begin uitermate serieus genomen, heeft snel opgeschaald en direct externe hulp ingeschakeld. Dat bleek ook nodig, gelet op de mogelijke risico's voor de regionale corona- en incidentbestrijding. Die bijzondere context, midden in de coronapandemie, zorgde voor een groot besef van urgentie.

> De respons op cyberverstoringen is méér dan alleen een technische operatie. Dit soort incidenten raakt de hele organisatie en alle medewerkers, in het bijzonder IT medewerkers die een grote verantwoordelijkheid voelen. De sociaal-emotionele impact van cyberverstoringen op medewerkers is voor alle veiligheidsregio's een belangrijk onderwerp om zich bewust van te zijn. Biedt steun, blijf communiceren en met elkaar in verbinding, voorkom 'blame games' en richt je op datgene wat medewerkers nodig hebben.

> De VNOG was in de crisisrespons sterk afhankelijk van externe specialistische ondersteuning en expertise. De VNOG slaagde erin om die technische expertise snel te mobiliseren in de vorm van bijstand van het NCSC, Fox-IT en KPN. De afhankelijkheid van deze expertise betekent dat veiligheidsregio's in hun respons op cyberverstoringen kwetsbaar zijn. Hoewel veiligheidsregio's niet zelf over deze specialistische kennis en kunde hoeven (en kunnen) beschikken, is het voor veiligheidsregio's wel noodzakelijk om dergelijke expertise snel te kunnen mobiliseren, bijvoorbeeld door het investeren in publiek-private partnerschappen.

> Hoewel we als onderzoekers onder de indruk zijn van het voortvarende optreden van de VNOG bij deze cyberverstoring (de snelheid van handelen, inschakelen van externe hulp, het organisatie- en improvisatievermogen) heeft de VNOG ook geluk gehad. Als back-ups onbruikbaar zijn, als benodigde expertise niet tijdig georganiseerd kan worden, als sprake is van zeer geavanceerde of aanhoudende aanvallen, als een technisch handelingsperspectief ontbreekt, als de aanval doordeweeks had plaatsgevonden, kan het verloop van zo'n incident er ineens heel anders uitzien. De oproep aan veiligheidsregio's is dan ook om dit soort cyberverstoringen (en de voorbereiding erop) uiterst serieus te nemen. Cyberdreigingen zoals gijzelsoftware zijn per slot van rekening 'here to stay'.

5.2 Specifieke bevindingen

Ander soort crisis

> Deze casus was voor de veiligheidsregio anders dan de traditionele flitsrampen die zij gewend is. De VNOG was in deze casus zelf slachtoffer in plaats van hulpverlener en crisisbestrijder bij externe calamiteiten. Dat maakte deze verstoring voor de

veiligheidsregio atypisch. Zo waren er gevolgen voor de interne bedrijfsvoering, was er impact op de eigen medewerkers, waaronder IT medewerkers en er waren hoge kosten. Daarnaast betrof het een wat afwijkend soort crisis waar nog weinig ervaring mee was opgedaan. Het moedwillige karakter, risico's wat betreft de veiligheid van gegevens en het benodigde handelingsperspectief voor forensisch onderzoek en herstel waren bijzondere kenmerken.

> Naast de gevolgen voor de bedrijfsvoering ging dit incident ook over mogelijk verloren, aangetaste of geblokkeerde data. De 'data-dimensie' zorgde voor allerlei extra stappen die genomen moesten worden: informeren van de Functionaris Gegevensbescherming onderzoek naar verlies van data, melding doen bij de Autoriteit Persoonsgegevens en onderzoeken hoe gedupeerden geïnformeerd moesten worden.

> Getroffen worden door een cyberverstoring is kostbaar voor een organisatie. Er zijn natuurlijk ook andere incidenten denkbaar die de eigen organisatie veel geld kunnen kosten zoals een brand, maar een aantal elementen waren uniek voor een cyberverstoring. Zo zijn de beslissingen die snel genomen moeten worden over financiële uitgaven voor onder meer de aanschaf van hard- en software en de externe inhuur extra uitdagend.

> De VNOG was in feite niet voorbereid op een cyberverstoring die haarzelf zou treffen. Er had geen interne, generieke cyberoefening plaatsgevonden, er lag geen plan klaar en er was weinig aandacht voor de continuïteit van bedrijfsvoeringsprocessen. De focus in planvorming en oefening lag op preparatie voor *externe* calamiteiten.

Crisisorganisatie

> De VNOG heeft de GRIP-procedure flexibel toegepast en een specifieke responsorganisatie ingericht die toegerust was voor bron- en effectbestrijding. De algehele leiding, prioriteitstelling en communicatie lagen bij de VNOG. Fox-IT richtte zich op het forensisch onderzoek, KPN op de inrichting van de nieuwe virtualisatieomgeving en het NCSC op incidentrespons en de hersteloperatie. Onder leiding van de VNOG werd een goede onderlinge taakverdeling en coördinatie tot stand gebracht.

> De door de VNOG gehanteerde thematische aanpak doet denken aan flexibele GRIP / 'knoppenmodel'. De gedachte achter dat model is het activeren van specifieke, monodisciplinaire teams / processen die nodig zijn voor het bestrijden van problemen. Bij de VNOG werd gekozen voor vier processen, waaronder forensisch onderzoek en opbouw & herstel. Voor veiligheidsregio's kan een dergelijk model bruikbaar zijn in het kader van cybergevolgbestrijding.

> Belangrijke 'lessons learned' voor veiligheidsregio's zijn het gebruik van generieke procedures en een generieke crisisstructuur, bestuurlijke betrokkenheid, gebruikmaken van eerdere ervaringen (scenario's) en de inzet van functionarissen (zoals het hoofd Bedrijfsvoering en FG) met ervaring in de warme fase van een crisis. Ook het werken met bestuurlijke uitgangspunten gaf de operatie richting. Op basis van de uitgangspunten 'zorgvuldigheid voor snelheid' en 'operationele systemen eerst' waren de crisisteams behoorlijk zelfsturend, wat de snelheid van handelen ten goede kwam.

> Een cyberverstoring en andere informatie gerelateerde risico's vragen tijdige alarmering van de Functionaris Gegevensbescherming. Tevens bleek het nodig om in de operatie snel verreikende beslissingen te kunnen nemen over inhuur van externen en aanschaf van nieuwe soft- en hardware.

> Informatiedeling kan tijdens een crisis onder druk komen te staan, maar is essentieel. De samenwerking tussen de VNOG en het VR-ISAC kon mede hierdoor beter. Daarnaast werd een VR-CERT gemist.

Crisiscommunicatie

> Hoewel de essentie van crisiscommunicatie bij een cyberverstoring niet per definitie afwijkend is van de communicatie bij reguliere crises, vroeg de cyberverstoring bij de VNOG op een aantal aspecten om een andere aanpak.
  - Doordat de reguliere communicatiekanalen zoals e-mail door de verstoring niet meer beschikbaar waren, moest nagedacht worden over alternatieve manieren voor de interne en externe communicatie. Al snel werd een oplossing gevonden door de externe communicatie te plaatsen op de website en de interne communicatie plaats te laten vinden via Whatsapp en/of Signal.
  - Deze cyberverstoring betrof een crisis binnen de eigen organisatie. Waar de crisiscommunicatie van de VNOG zich normaal richt op (onbekende) betrokkenen van een incident, waren het nu de eigen collega's die betrokken waren en geïnformeerd moesten worden.
  - Een cyberverstoring is een vrij technische aangelegenheid. Voor communicatieadviseurs is het een uitdaging om technische informatie over een cybercrisis te vertalen naar een duidelijke en begrijpelijke communicatieboodschap. De VNOG is hier goed in geslaagd.

> Bij de VNOG is veel aandacht geweest voor de interne communicatie. Gezien de aard van de crisis was dit logisch: de VNOG was vooral intern geraakt. De manier van communiceren heeft bijgedragen aan het creëren van rust. Er heeft inmiddels een markeringsmoment geweest om de cyberverstoring samen met alle medewerkers af te sluiten. Deze bijeenkomst werd door medewerkers gewaardeerd en was het startpunt voor een interne bewustwordingscampagne over informatieveiligheid..

> Het is de VNOG gelukt om zelf de regie te houden over het externe informatieproces. Er is bewust gekozen voor korte en duidelijke boodschappen. De boodschappen werden opgepakt door de media, maar hebben tot weinig vragen van journalisten geleid. Ongetwijfeld hebben het oplaaien van het coronavirus en de beperkte externe effecten van de verstoring hierin een rol gespeeld.

> Hoewel de afdeling communicatie weinig vragen kreeg, kwamen op twee andere plaatsen wel vragen binnen over de cyberverstoring. Het scenarioteam kreeg vragen van (crisis)partners, zoals de waterschappen en de meldkamer. Het VR-ISAC kreeg vragen van andere veiligheidsregio's. Over dat laatste was de afdeling communicatie van de VNOG (op dat moment) niet op de hoogte.

> Een terugkerend thema bij cyberverstoringen is de vraag in hoeverre er open gecommuniceerd kan worden. Geconcludeerd kan worden dat de VNOG in vergelijking met andere casus terughoudend was in de communicatie. De VNOG deelde enkel dat

de organisatie getroffen was door gijzelsoftware. Op advies van de politie is er geen informatie gedeeld over de (mogelijke) daders, de oorzaak en het al dan niet betalen van losgeld. In zowel de interne als externe communicatie is door de VNOG terecht steeds onderscheid gemaakt tussen ‘nice to know’ en ‘need to know’.

5.3 Aanbevelingen voor veiligheidsregio’s

Deze rapportage bevat voor veiligheidsregio’s grotere en kleinere leerpunten. In de onderstaande paragraaf geven we enkele overkoepelende aanbevelingen.

Bereid je als veiligheidsregio voor op het onvermijdelijke: je zult een keer worden gehackt. Zorg als veiligheidsregio dat je daarvoor een plan/draaiboek klaar hebt liggen. Als vooraf duidelijk is wat je als regio zelf kunt en waarvoor externe expertise of hulp bij nodig hebt, kun je die expertise en ondersteuning vooraf organiseren. Vertrouwen op improvisatietalent en reguliere voorbereidingen zijn voor veiligheidsregio’s belangrijk, maar volstaan bij dit soort cyberverstoringen niet. Voor dit soort crises is door veiligheidsregio’s een specifieke preparatie nodig. Zorg voor:

- een overzicht van kritieke bedrijfsprocessen/ opstellen van een continuïteitsplan draaiboek voor cyberverstoringen, waaronder besluitvorming over het ontkoppelen van servers (‘stekkermandaat’) door netwerkbeheer.
- ruimte in je begroting, rekening houdend met een dergelijke cyberverstoring of een manier waarop reserves kunnen worden gealloceerd indien nodig.
- het op orde en up-to-date zijn van de ICT-omgeving, bijvoorbeeld door een jaarlijkse review van de ICT-infrastructuur. Zorg ervoor dat je voldoet aan de BIO (Baseline Informatieveiligheid Overheid) en investeer hier blijvend in.
- inzicht in de manier waarop de ICT-omgeving van je organisatie eruitziet, waar afhankelijkheden zitten en waar cascade-effecten kunnen optreden.
- het maken van goede afspraken met leveranciers (hardware, software, cybersecurity) over acute bijstand tijdens een cyberverstoring en snelle levering van diensten.
- verbetering van de samenwerking tussen veiligheidsregio’s en het VR-ISAC (en een mogelijk toekomstig VR-CERT). Betrek tijdens een cyberverstoring naast CISO’s ook communicatieadviseurs bij het contact met deze partij(en)
- inzicht in communicatiepartners die relevant zijn specifiek voor cyberverstoringen, zoek uit welke (externe) deskundigen kunnen helpen met de vertaling van technische termen en denk na over communicatiekanalen die onafhankelijk zijn van interne IT systemen en dus kunnen worden gebruikt bij uitval van de reguliere communicatiekanalen.
- Inzicht in een mogelijke responsorganisatie, bijvoorbeeld gebaseerd op het ‘knoppenmodel’ (met specifieke, monodisciplinaire teams / processen die nodig zijn voor bron- en gevolgbestrijding).
- oefeningen met cyberscenario’s.

Verken als veiligheidsregio’s hoe collectieve bijstand aan elkaar te organiseren bij langdurige cyberverstoringen. Denk hierbij aan:

- specialistische expertise en ondersteuning voor forensisch onderzoek, incident respons en herstel. Hierbij kan gedacht worden aan het NCSC, VR-ISAC / CERT en/of branche brede contracten met specialistische IT dienstverleners.

- standaardisering op gebied van IT infrastructuur (hardware, software en data); door meer gezamenlijke aanbestedingen te doen op het gebied van hardware, door gezamenlijke inkoop en door gebruik te gaan maken van de softwarecatalogus en door het invoeren en gebruiken van de kernregistraties en het uitwerken van de BIV classificaties.
- meer langdurige, praktische ondersteuning in de hersteloperatie op het gebied van IT (capaciteit, kennis en kunde), bijvoorbeeld vanuit het VR ISAC.

Vertrouw tijdens een cyberverstoring door gijzelsoftware naast specifieke plannen en draaiboeken op reguliere voorbereidingen en de veerkracht en het improvisatietalent van de organisatie en zijn medewerkers. Houd hierbij rekening met:

- de snelle alarmering van de Functionaris Gegevensbescherming bij een cyberverstoring en andere informatie gerelateerde dreigingen en verstoringen.
- een flexibele crisisstructuur met voldoende bestuurlijke beslisbevoegdheid in de crisisorganisatie, bijvoorbeeld door de directeur of een ander MT-lid op te nemen in het crisisteam.
- de inzet van ervaren crisisfunctionarissen en functionarissen uit bedrijfsvoering met ervaring in de warme fase van een crisis. Deze ervaring in de warme fase van een crisis wordt als zeer waardevol beschouwd.
- het inbouwen van voldoende rustmomenten voor medewerkers in de crisisorganisatie. Een cyberverstoring is een marathon, geen sprint.
- wees je bewust van de sociaal-emotionele impact van gijzelsoftware op medewerkers. Biedt steun, blijf communiceren en met elkaar in verbinding, voorkom ‘blame games’ en richt je op datgene wat medewerkers nodig hebben.
- de afschaling van de crisis(organisatie) en overgang naar de nafase. Een cyberverstoring heeft de neiging lang voort te sluimeren. Maak duidelijke afspraken over de nafasethema’s.
- organiseer een moment waarop de cyberverstoring met de medewerkers van de VNOG afgesloten kan worden (*closure*). Niet alle medewerkers weten wat er precies gebeurd is en zitten (mogelijk) nog met vragen, waar inmiddels wel antwoord op gegeven kan worden.

Literatuurlijst

- Backman, S. (2020). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*. Ontleend aan https://onlinelibrary.wiley.com/doi/full/10.1111/1468-5973.12347.
- Berenschot (2020). *Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten. Deel 1: Warme fase.* Utrecht: Berenschot Groep B.V.
- Compton, M. & Hart, P. 't (2019). *Great policy successes*. Oxford: Oxford University.
- COT (2010). *En nu…? Handboek voor de nafase van incidenten, rampen en crises.* Den Haag: Boom Juridische Uitgevers.
- COT (2017). *10 bijzonderheden van cybercrises en het belang van cyber crisismanagement.* Ontleend aan: https://www.linkedin.com/pulse/10-bijzonderheden-van-een-cybercrisis-abderrahman-kaouass/?originalSubdomain=nl.
- Duin, M. van & Wijkhuijs, V. (2015). *De flexibiliteit van GRIP*. Arnhem: Instituut Fysieke Veiligheid.
- Duin, M. van & Wijkhuijs, V. (2020). Cyberaanval op de Universiteit Maastricht. In: V. Wijkhuijs & M. van Duin (Red.), *Lessen uit crises en mini-crises 2019* (pp. 266-279). Den Haag: Boom bestuurskunde.
- Eenheid Communicatie NCTV (2021). *Communicatie bij incidenten in het digitale domein*. Ontleend aan https://www.nctv.nl/onderwerpen/crisiscommunicatie/documenten/publicaties/2021/02/23/koepelnotitie-communicatie-bij-digitale-incidenten.
- Evaluatiecommissie Wet veiligheidsregio's (2020). *Evaluatie Wet veiligheidsregio's: naar toekomstbestendige crisisbeheersing en brandweerzorg*. Ontleend aan https://www.evaluatiewvr.nl/wpcontent/uploads/2020/12/Rapport_evaluatie_Wet_veiligheidsregios_dec_2020.pdf.
- Grapperhaus, F. (2020, 7 oktober). Gijzelsoftware-aanval op Veiligheidsregio Noord- en Oost-Gelderland [Kamerbrief]. Ontleend aan https://www.rijksoverheid.nl/documenten/kamerstukken/2020/10/07/tk-gijzelsoftware-aanval-op-veiligheidsregio-noord-en-oost-gelderland-vnog.
- IFV (2017). *Basisinformatie regionale Crisisbeheersing.* Arnhem: Instituut Fysieke Veiligheid.
- IFV (2018). *Risico's in samenhang. Een verkennende studie naar de aansluiting tussen regio's en Rijk*. Arnhem: Instituut Fysieke Veiligheid.
- IFV (2020a). *Cybergevolgbestrijding: lessen uit recente Nederlandse casus*. Arnhem: Instituut Fysieke Veiligheid.
- IFV (2020b). *Cyberrisico's en veiligheidsregio's*. Arnhem: Instituut Fysieke Veiligheid.
- IFV (2020c). *Nieuw cyber-inlichtingencentrum voor veiligheidsregio's*. Ontleend aan https://www.ifv.nl/nieuws/Paginas/Nieuw-cyber-inlichtingencentrum-voor-veiligheidsregios.aspx.
- IFV (2020d). *De veiligheidsregio's in de eerste weken van de coronacrisis*. Arnhem: Instituut Fysieke Veiligheid.
- Leukfeldt, E.R. (2017). *Research agenda. The human factor in cybercrime and cybersecurity.* Eleven.

- NCTV (2020a). *Nationaal Crisisplan Digitaal.* Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
- NCTV (2020b). *Nationaal Cybersecuritybeeld Nederland CSBN 2020*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
- NOS (2021, 24 februari). *Wetenschapsorganisatie NWO afgeperst door bekende cybercriminelen, gaat niet in op eisen*. Ontleend aan https://nos.nl/artikel/2370178-wetenschapsorganisatie-nwo-afgeperst-door-bekende-cybercriminelen-gaat-niet-in-op-eisen.html.
- Rijksoverheid (z.d.). *Positief geteste mensen in Noord- en Oost-Gelderland*. Op 20 maart 2021 ontleend aan https://coronadashboard.rijksoverheid.nl/veiligheidsregio/VR06/positief-geteste-mensen.
- Rosenthal, U. (1984). *Rampen, rellen en gijzelingen. Crisisbesluitvorming in Nederland.* Amsterdam: De Bataafsche Leeuw.
- Sophos (2020). *The state of ransomware 2020. Results of an independent study of 5,000 IT managers across 26 countries.* Ontleend aan https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx.
- Treurniet, W., Boersma, F.K. & Groenewegen, P. (2019). Configuring emergency response networks. *International Journal of Emergency Management*, *15*(4), 316-333.
- Veiligheidsberaad (2019). *Bestuurlijk routeboek digitale ontwrichting*. Ontleend aan https://veiligheidscoalitie.nl/action/?action=download&id=2358.
- VNOG (2020a). *Raadsinformatie brief VNOG n.a.v. cyberaanval VNOG. 14-09-2020*. Apeldoorn: Veiligheidsregio Noord- en Oost-Gelderland. Ontleend aan https://raad.oude-ijsselstreek.nl/documenten/ingekomen-stukken/20-340-VNOG-Raadsinformatiebrief-n-a-v-cyberaanval-VNOG.pdf.
- VNOG (2020b). *Regionaal risicoprofiel 2021-2024.* Apeldoorn: Veiligheidsregio Noord- en Oost-Gelderland.
- VNOG (2020c). *VNOG sluit zich aan bij samenwerkingsverband tegen cyberincidenten.* Ontleend aan https://www.vnog.nl/actueel/nieuws/2235-vnog-sluit-zich-aan-bij-samenwerkingsverband-tegen-cyberincidenten.
- VNOG (z.d.-1). *Toelichting Crisisstructuur voor eindverantwoording.* Apeldoorn: Veiligheidsregio Noord- en Oost-Gelderland. Op 20 maart 2021 ontleend aan https://publicaties.vnog.nl/verantwoordingsverslag-voorzitter/crisisorganisatie.
- VNOG (z.d.-2). *Toename coronabesmettingen in Noord- en Oost-Gelderland*. Op 20 maart 2021 ontleend aan https://www.vnog.nl/coronavirus/nieuws-over-corona/2292-toename-coronabesmettingen-in-noord-en-oost-gelderland.
- Wetenschappelijke Raad voor het Regeringsbeleid (WRR) (2019). *Voorbereiden op digitale ontwrichting.* Den Haag: WRR.