Overheidsbrede Cyberoefening & Webinars

Scenario Overheidsbrede Cyberoefening 2021

#0.2
Datum: 23 november 2021
Auteurs: Pascaal Renckens, Luuk Rietveld, Inge van der Beijl

Rijksoverheid

NORTHWAVE
Intelligent Security Operations

ICTU

INHOUDSOPGAVE

AANLEIDING

Nederland is een van de meest gedigitaliseerde landen ter wereld. Digitalisering dringt door in alle facetten van onze maatschappij en speelt een steeds belangrijkere rol in het dagelijks leven, zo ook bij de overheid. Een kerntaak van de overheid is het voortouw nemen bij het streven naar een veilig en stabiel Nederland. De overheid heeft een grote verantwoordelijkheid ten aanzien van de beveiliging van gegevens die burgers en ondernemers aan haar toevertrouwen en de ICT –systemen waarmee zij werkt. Het op orde hebben en houden van het eigen informatieveiligheidsbeleid is dan ook randvoorwaardelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en systemen.

Burgers moeten op overheidsdienstverlening kunnen rekenen evenals dat hun grondrechten zowel online als offline gewaarborgd zijn en dat hun privacy ook in het digitale domein gegarandeerd is. Tegelijkertijd nemen kwetsbaarheden en dreigingen in het digitale domein toe. Zo heeft de overheid een verantwoordelijkheid in de digitale veiligheid van infrastructuur waarvoor ze verantwoordelijk is bijvoorbeeld bruggen, afvalwaterzuiveringen, verkeers-en tunnelinstallaties dit raakt direct de fysieke veiligheid.

Aan de basis hiervan staat veilig handelen; randvoorwaardelijk daarvoor is dat bestuurders, managers en medewerkers zich bewust zijn van digitale dreigingen en daaruit voortkomende (mogelijke) risico's. Hoewel er de afgelopen jaren veel is geïnvesteerd in de bewustwording en kennisopbouw van digitale dreigingen, is een volgende stap het transformeren van kennis naar kunde: daadwerkelijk veilig handelen om enerzijds incidenten en crises te voorkomen, en anderzijds als cyberincidenten en crises optreden deze weten te beheersen en mitigeren. Vertrekpunt daarbij is het bieden van handelingsperspectief (weten wat te doen) aan bestuurders, managers en medewerkers van de gehele overheid, om er vervolgens ook daadwerkelijk mee te oefenen in realistische incident- en crisissituaties in een veilige omgeving.
In navolging van de succesvolle editie van 2019 en 2020 heeft ICTU in 2021 de opdracht gekregen om ten tijde van de campagne Alert Online en de maand van de Europese Cybersecurity (oktober) wederom een programma op te zetten die aandacht heeft voor overheidsbrede samenwerking, kennisdelen en het oefenen met een cyberincident.

Dit document beschrijft de onderbouwing, opbouw en inhoud van het scenario zoals dit is gebruikt tijdens de Overheidsbrede Cyberoefening 2021 op 1 november 2021. U kunt dit scenario in uw eigen context hergebruiken om te trainen en oefenen. Het oorspronkelijke scenario hebben wij zoveel mogelijk intact gehouden. Hoe het scenario toepasbaar gemaakt kan worden voor uw eigen context wordt in de leeswijzer van dit document beschreven.

LEESWIJZER

Door te oefenen wil je voorbereid zijn op een uitzonderlijke dreigende situatie waarbij een effectieve afhandeling grote voordelen heeft. De overheidsbrede cyberoefening was een zogenaamde Table Top oefening. Bij een Table Top oefening wordt een gesimuleerde aanval aan de spelers gepresenteerd, bijvoorbeeld door het presenteren van mediaberichten en injects. Aan het crisisteam de taak om ervoor te zorgen dat besluitvorming en communicatie soepel verloopt in relatieve rust.

Gedurende de Table Top oefening wordt geoefend op basis van het oefenscenario. Het oefenscenario bevat een overzicht van wat wanneer waar gaat gebeuren tijdens de Table Top oefening. Het oefenscenario is daarin de algemene beschrijving van de gebeurtenis. In het oefenscenario wordt een mogelijke en realistische cyberdreiging beschreven.

Om het gebruikte oefenscenario toepasbaar te maken voor uw eigen organisatie dient u [de groen gearceerde tekst tussen haken] te wijzigen naar uw eigen context.
Een aantal bijzondere aandachtspunten daarbij:

- Op alle plekken waar [de organisatie] staat kun u uw eigen organisatie invullen.
- [Assensio] wordt in het scenario benoemd als externe IT-leverancier. Dit is een fictieve naam. Deze kunt u dus hergebruiken. U kunt hier echter ook één van uw huidige of oude externe IT-leveranciers invullen, voor een hoger realiteitsgehalte.
- In het scenario staat het [SPP-systeem] centraal. Dit is een fictief systeem. Om uw scenario op maat te maken adviseren wij om hier een kritiek systeem van uw organisatie in te vullen. Deze kunt u eenvoudig halen uit een gehouden Business Impact Analyse (BIA). Heeft u geen (recente) BIA voorhanden, bedenk dan welk systeem de grootste impact heeft op de continuïteit van de organisatie.
- In het scenario staat het kritieke proces [inkomensbetaling] centraal. Om uw scenario op maat te maken adviseren wij om hier een kritiek proces welke een relatie heeft met het gebruikte kritieke systeem in te vullen. Kijk hier weer naar de BIA of vraag u af met welke (ondersteunende) kritische processen de organisatie werkt.
- In het scenario staat een ransomware note bedrag genoemd in euro (€). Dit wordt gevraagd in cryptovaluta, meestal BTC of XMR en bedraagt 1-4% van de jaarlijkse omzet. Pas dit bedrag aan uw situatie aan.
- In het scenario wordt meermaals gesproken over [gevoelige informatie]. Maak dit organisatie specifiek door hier informatie in te vullen welke voor uw context gevoelig is.

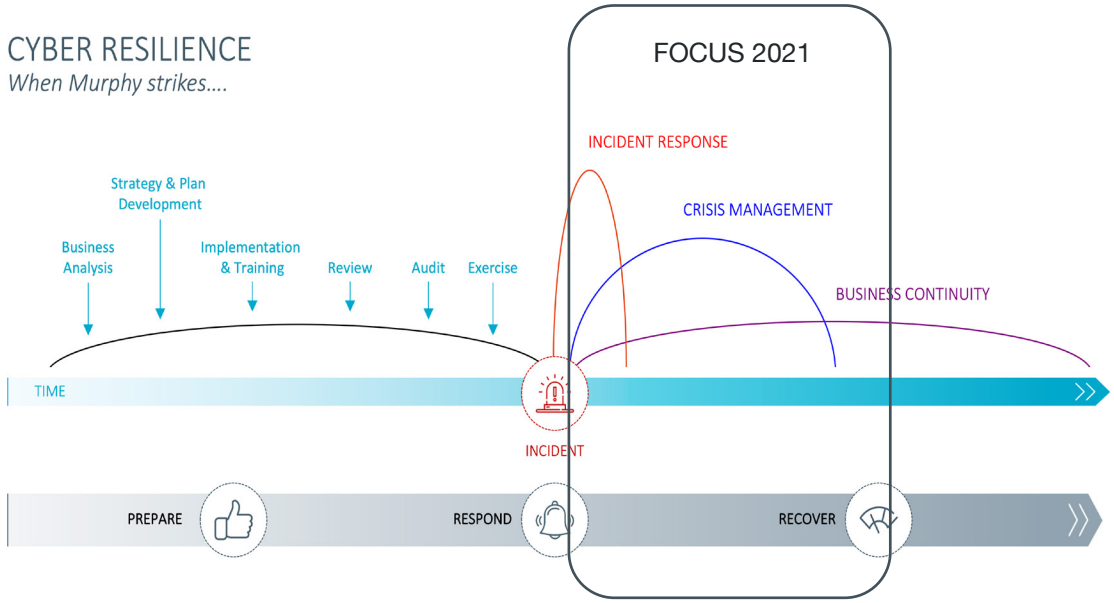
Tot slot is het goed om weten dat dit document de eerste drie stappen bevat van het ontwikkelen van een oefenscenario voor het beoefenen van een cybersecuritycrisis. De laatste twee stappen: het maken van een oefentijdlijn en het ontwikkelen van ‘injects’ staan niet in dit document beschreven. Informatie hierover en over wat er verder allemaal komt kijken bij het opzetten van een cybersecuritycrisis oefening staat in Handreiking Cyberoefenen (www.cybersecurityalliantie.nl/handreiking-cyberoefenen). Deze handreiking kan gebruikt worden als checklist en inspiratiebron bij het opzetten van een cyberoefening binnen de eigen organisatie.

1. INLEIDING

1.1. OEFENFUNCTIE OVERHEIDSBREDE OEFENING

De afgelopen twee jaar was de functie en focus van de oefening vooral ‘oriënteren’, oftewel het verkennend oefenen op het ontstaan van het incident, de opschaling en de warme fase van een cybercrisis.

Dit jaar is de oefenfunctie ‘leren’ en wordt de focus gelegd op hoe er gehandeld moet worden als de crisis een feit is. Ook is gekozen voor een focus op de interne organisatie. Met deze scope is het scenario goed herkenbaar én herbruikbaar voor gemeenten, provincies en waterschappen.



1.2. DOEL VAN DE OEFENING

Het centrale oefendoel is kennis, vaardigheden en competenties overbrengen. Deelnemers doen ervaring op met oplossen van een cyberincident (gericht op hoe er gehandeld moet worden als de crisis een feit is). Het centrale oefendoel kent een aantal subdoelstellingen, te weten:

- Het belang laten zien van processen en procedures:
  - Wat als alle systemen niet toegankelijk zijn?
  - Hoe ondersteunt een crisisteam de organisatie?
  - Wie heeft welke rol aan tafel / binnen de organisatie?
- Het belang laten zien van besluitvorming:
  - Hoe wordt de crisis op een goede manier afgehandeld?
  - Inzichtelijk maken welke informatie cruciaal is om tot goede besluitvorming te komen
  - Wat zijn cruciale beslismomenten en hoe komt de organisatie zo snel mogelijk weer op gang, zodat het haar werkzaamheden weer (enigszins) kan uitvoeren?
- Het belang laten zien van goede interne en externe communicatie:
  - Wie communiceert wanneer met wie en waarover?
  - Welke interne communicatiemiddelen zijn beschikbaar tijdens een crisis?
  - Wie zijn de belangrijkste (externe) stakeholders?

1.3. OEFENVORM

De oefenvorm van de overheidsbrede oefening was een hybride oefenvorm waarbij de nadruk op digitale deelname lag. Het publiek is betrokken tijdens de oefening door middel van vraagstelling en het gebruik van mentimeter.

Het scenario, zoals dit voor u ligt, kan worden uitgespeeld in een paper table top of een klassieke table top oefening, waarbij gebruik wordt gemaakt van de reguliere crisisstructuren in de organisatie. Of u gebruikt de hoofdvragen/dilemma's voor een interactieve discussie met uw directie of bestuur. Hierbij wordt aangeraden de oefening te laten faciliteren door iemand die buiten het incident response of crisisteam staat.

1.4. DOELGROEP VAN DE OVERHEIDSBREDE OEFENING

De doelgroep van de overheidsbrede oefening bestaat in de eerste plaats uit bestuurders en professionals van gemeenten, waterschappen en provincies. Professionals en bestuurders vanuit de Rijksoverheid, ZBO's en andere publiek en private organisaties behoren niet tot de primaire doelgroep van de oefening, maar mogen wel deelnemen.

Voor het beoefenen van het scenario in uw eigen context kunt u gebruik maken van uw incident response en crisisteam.

1.5. DEFINITIE CYBERCRISIS

Een cybercrisis is iedere (moedwillige) verstoring, uitval of misbruik van een gedigitaliseerd proces, (informatie)systeem of informatiedienst die de maatschappelijke continuïteit, openbare orde en veiligheid bedreigt of verstoort.

1.6. CRISISBEHEERSINGSSTRUCTUUR

Bij een cybercrisis is de getroffen organisatie zelf verantwoordelijk voor het oplossen van de technische verstoring en het continueren van de dienstverlening. Omdat acties ten behoeve van de bronbestrijding impact kunnen hebben op effectbestrijding is het belangrijk dat er een goede informatielijn ontstaat tussen het team dat zich bij de getroffen organisatie bezighoudt met het oplossen van de verstoring en het team dat zich bezighoudt met de effectbestrijding alsmede het team dat zich buigt over strategische beleidsvraagstukken.

Bij het scenario (hoofdstuk 2) ligt de focus op de bedrijfscontinuïteit van de organisatie en welke ketenelementen dit met zich meebrengt. Ook zijn er verschillende teams die elk met hun eigen uitdagingen en dilemma's aan de gang moeten gaan.

Tijdens de oefening kunnen meerdere teams worden aangehaald/ uitgebeeld bij het doorlopen van het scenario, maar richt zich op het Crisis Management Team (CMT):

Incident Response Team (IRT)
Het IRT bevat medewerkers van de getroffen organisatie die expert zijn op één of meerdere (technische) gebieden, aangevuld met één of meerdere externe incident onderzoeker(s). Zij stellen de omvang van het incident vast. Ook zijn zij in staat om tijdens het incident (technische) ondersteuning te bieden aan het oplossen van het incident. Zij zorgen voor een goede informatieoverdracht aan het CMT ten behoeve van de beeldvorming en oordeelsvorming en geven daarnaast ook adviezen ten behoeve van de besluitvorming aan het CMT.

Crisis Management Team (CMT)
Het CMT is de directie van de organisatie, aangevuld met (externe) experts. Zij richten zich op de bescherming van de reputatie en de interne en externe stakeholders en hebben hierbij dus de focus op de effecten van de crisis. Zij brengen de kernactiviteiten van de organisatie in kaart en bewaken de geloofwaardigheid van de organisatie. Daarnaast nemen zij besluiten over zaken die dringende maatregelen vereisen. Zij doorlopen hierbij gericht de fasen beeldvorming, oordeelsvorming en besluitvorming.

Algemeen Bestuur (AB)
Het AB van de geraakte organisatie zijn ten tijde van een crisis de zogenaamde ‘decision-making authority’ en hebben daarbij bestuursbevoegdheid. Zij buigen zich over de hogere bestuurlijke dilemma’s en laten zich hierbij adviseren door het CMT.

2. HET SCENARIO

Het scenario is opgebouwd aan de hand van een gebeurtenis (de kwetsbaarheid of het probleem) die beoefend gaat worden. Deze staat omschreven in paragraaf 2.1. Vervolgens is deze gebeurtenis verder uitgewerkt aan de hand van een aantal onderdelen/ bouwstenen, welke beschreven worden in paragraaf 2.2. Hierna wordt in 2.3 een samenhangend verhaal van de inhoud uit 2.1 en 2.2 gemaakt, het scenario, waarin staat omschreven wat er gebeurt en hoe dit kan gebeuren en wat de effecten zijn die in de oefening naar voren gaan komen.

2.1. DE HOOFDGEBEURTENIS

In het scenario staat een aanval/hoofdgebeurtenis centraal waarbij de organisatie het doelwit is. De hoofdgebeurtenis is een ransomware incident. Ransomware is een vorm van malware die de bestanden van een slachtoffer versleutelt. De aanvaller eist vervolgens losgeld van het slachtoffer om tegen betaling de toegang tot de gegevens te herstellen. Gebruikers krijgen instructies te zien voor het betalen van een bedrag in cryptovaluta (bv. Bitcoin) om de ontsleutelingssleutel te krijgen. Meer recentelijk hebben aanvallers de neiging om gevoelige gegevens te stelen en dreigen ze ook om de gegevens van het slachtoffer te publiceren als deze niet gehoorzaamt bij het betalen van het geëiste losgeld. En zeer recentelijk zien we dat medewerkers (of cliënten) van de organisatie onder druk worden gezet indien er geen losgeld wordt betaald.

De lijn vanuit de overheid is om nooit te betalen aan criminelen. Vanuit politieke partij VVD is onlangs een motie ingediend die overheden handvatten moet bieden hoe zij ransomware dienen te voorkomen. Daarnaast is er vanuit het Ministerie van Justitie en Veiligheid een taskforce ransomware opgericht.

2.2. ONDERDELEN/ BOUWSTENEN

- **Oorzaak:**
  - Het incident wordt door opzettelijk handelen veroorzaakt.
- **Bron:**
  - De oorzaak van het incident ligt (ook) in het buitenland.
- **Actor:**
  - Er is sprake van een incident veroorzaakt door een niet-statelijke actor. De actor is een criminele organisatie.
- **Geraakt domein:**
  - Maatschappelijk belangrijke voorzieningen (niet-vitaal): de vitale processen zoals gedefinieerd door de rijksoverheid worden niet geraakt. Gelijksoortige kwetsbaarheden zijn terug te vinden binnen diverse publieke organisaties zoals gemeenten, maar ook bij organisaties welke vallen onder de Wet gemeenschappelijke regelingen (WGR). Burgers en overheid binnen en buiten de getroffen organisaties ondervinden significante hinder van het incident.
- **Geraakt gebied:**
  - Het incident leidt tot effecten binnen één veiligheidsregio in Nederland.
- **Oplossingsperspectief (technisch):**
  - Het is onduidelijk hoe het incident technisch op korte termijn opgelost kan worden, waardoor er geen maatregelen met betrekking tot het incident zelf in gang gezet kunnen worden (alleen effect mitigerende maatregelen).

2.3. SCENARIO

Hieronder wordt het scenario beschreven. Allereerst worden de hoofdvragen, mogelijke gevolgen en effecten beschreven. In de laatste sub paragraaf staat een samenhangend verhaal van alle voorgaande stappen waarin staat omschreven wat er gebeurt en hoe, hoe dit kan gebeuren en wat de effecten zijn die in de oefening naar voren gaan komen.

2.3.1. HOOFDVRAGEN

De volgende hoofdvragen/ dilemma's staan centraal tijdens de dag voor de crisisteams:

- Hoe werken de cybercriminelen en verloopt de opbouw naar een cyberaanval?
- Wat als alle systemen niet toegankelijk zijn?
- Hoe ondersteunt een crisisteam de organisatie?
- Wie heeft welke rol aan tafel/ binnen de organisatie?
- Hoe wordt de crisis op een goede manier afgehandeld?
- Wat zijn cruciale beslismomenten en hoe komt de organisatie zo snel mogelijk weer op gang, zodat het haar werkzaamheden weer (enigszins) kan uitvoeren?
- Hoe wordt invulling gegeven aan in- en externe communicatie?

2.3.2. MOGELIJKE GEVOLGEN EN EFFECTEN

- Mensen en instanties worden gedupeerd (financieel, chantage, laster, imagoschade)
- Afname vertrouwen aangeboden digitale diensten
- Continuïteit van de aangeboden diensten wordt gehinderd
- Integriteit informatievoorziening aangetast
- Maatschappelijke onrust
- Gevolgen, effecten eventueel groter door mogelijkheid nieuw incident, herhaling of onbekendheid aantal betrokkenen
- Verstoring bedrijfsprocessen getroffen bedrijven, instanties en organisaties
- Aantasting integriteit systemen
- Politieke onrust/ maatschappelijke verontwaardiging
- Reputatieschade en vertrouwensverlies

2.3.3. HET VERHAAL

Hieronder wordt de verhaallijn van het scenario beschreven. De verhaallijn is lineair beschreven, wat inhoudt dat de problemen zich in chronologische volgorde opstapelen. Het is echter aan het team aan tafel en aan de deelnemers in welke snelheid dit gaat en in welke volgorde. Hierin heeft de oefenleiding de vrijheid om hier meer of minder snelheid in te maken en bepaalde informatie wel of niet te verstrekken naargelang het team en de deelnemers de diverse aandachtspunten en sleutelbesluiten goed aanpakken of niet.

2.3.4.1 Achtergrond

- Net als veel andere organisaties heeft de organisatie grote veranderingen meegemaakt op het gebied van digitalisering. Bijna alle processen zijn hierdoor tegenwoordig afhankelijk van digitale systemen en informatie.
- Die digitaliseringsslag is in hoog tempo doorgevoerd waardoor nu veel systemen in gebruik zijn, waar niet altijd even goed nagedacht is over securitymaatregelen. Hierdoor kent het netwerk van [de organisatie] weinig segmentatie en is er sprake van een aantal 'legacy systemen' die nog actief zijn.
- [de organisatie] heeft een IT-leverancier voor het beheren van hun IT-landschap, infrastructuur en software en is daarmee ook verantwoordelijk voor de digitale werkplek van alle werknemers van [de organisatie]. Deze IT-leverancier heet [Assensio].

- In samenwerking met [Assensio] is 1,5 jaar geleden een groot project gestart om alle belangrijke systemen van [de organisatie] te migreren naar de Cloud. Dit verloopt tot nu toe moeizaam, ongeveer 50% van de gebruikte systemen draaien inmiddels in de Cloud. Het project is nog niet afgerond en er wordt volop gewerkt om meer systemen binnenkort te migreren.
- Belangrijkste systeem is [SPP]: bijvoorbeeld een systeem met een database van de inwoners wat gebruikt wordt voor communicatie en registratie. Dit systeem had volgens de planning al gemigreerd moeten zijn naar de Cloud. Maar wegens een aantal 'hick-ups' vanuit [de organisatie] én problemen bij [Assensio] is dit nog niet gebeurd.
- De totale interne infrastructuur van [de organisatie] bestaat uit [251] servers. Hiervan draaien er als gevolg van de migratie ongeveer een derde extern en twee derde 'on premise'.
- Van het [SPP-systeem] worden iedere week online back-ups gemaakt. Deze worden vervolgens opgeslagen op een aparte server van [de organisatie]. De afgelopen jaren is echter niet getest hoe gemakkelijk deze ook echt kunnen worden teruggezet indien nodig.
- [De organisatie] heeft vanuit zijn eigen netwerk ook verschillende koppelingen met andere organisaties zoals bijvoorbeeld gemeentes binnen de regio en andere organisaties welke vallen onder de Wet gemeenschappelijke regelingen (WGR).
- Een van de systemen die momenteel nog draait op een lokale server is de VPN-server van [de organisatie]. De VPN die wordt afgenomen door [de organisatie] is BEAT-VPN. Deze VPN-server wordt gebruikt door alle medewerkers van [de organisatie] die thuiswerken om hiermee veilig hun werk te kunnen doen.
- In 2019 is door een relatief onbekend beveiligingsbedrijf een penetratietest uitgevoerd op het netwerk van [de organisatie]. Daarbij werd een, volgens dit beveiligingsbedrijf, 'laag risico' gedetecteerd op het gebruik van de BEAT-VPN- applicatie. Het ontbreken van MFA werd bij dat onderzoek niet aangegeven als een kwetsbaarheid. Vanuit een risicomanagement-afweging van [de organisatie] is destijds besloten om het risico te accepteren en er geen prioriteit aan te geven. In 2020 nam thuiswerken door corona echter een vlucht en werd er veel (meer dan voorheen) gebruik gemaakt van deze applicatie.
- Via het/de [NCSC/IBD/DTC) bereikte vorige maand [de organisatie] het bericht dat er een kwetsbaarheid was te vinden in de toenmalige versie van BEAT-VPN. De kwetsbaarheid gaf toegang tot de interne netwerken en systemen van organisaties. Op het darkweb werden hiervoor ook al verschillende exploits aangeboden en uitgewisseld. Op basis van de berichtgeving heeft [Assensio] op aanvraag van [de organisatie] uiteindelijk binnen 5 dagen een update kunnen uitvoeren op de BEAT-VPN server. Hierdoor kan deze nu weer als veilig worden beschouwd.

2.3.4.2 Technische oorsprong crisis

- Helaas heeft het updaten van de BEAT-VPN server een criminele organisatie (vanaf nu 'Initial access broker') er niet van weerhouden om toegang te verkrijgen tot het interne netwerk van [de organisatie].
- Het blijkt dat de kwetsbaarheid en bijbehorende exploits al een ruime week op het darkweb te vinden waren en dat hier door veel internetcriminelen volop gebruik van is gemaakt. Zo heeft de Initial access broker al voor het verhelpen van de kwetsbaarheid toegang weten te verkrijgen tot het interne netwerk van [de organisatie] en een zogenaamde 'backdoor' geplaatst.
  Deze backdoor is een aangemaakt administrator account op de VPN-server. Hiermee kunnen zij ook na het updaten van de BEAT-VPN server ongezien toegang verkrijgen tot het netwerk van [de organisatie].
- Na het plaatsen van de 'backdoor' door de initial access broker wordt de toegang tot het interne netwerk van [de organisatie] te koop aangeboden op het darkweb. Deze wordt vervolgens binnen een dag al verkocht aan een andere organisatie die vanaf nu 'ransomware affiliate' wordt genoemd.
- De ransomware affiliate gaat vervolgens aan de slag met de gekochte toegang tot [de organisatie]. Middels de verkregen backdoor (account op BEAT-VPN) weten zij administrator rechten te verkrijgen op dit systeem. Dit doen zij door het programma Mimikatz te laten lopen en hiermee inloggegevens op te vragen in het systeem. Wat zij vervolgens doen is het gehele netwerk van [de organisatie] in kaart brengen.

- Middels het vergaren van meerdere inloggegevens uit Mimikatz kunnen de ransomware affiliates zichzelf nu toegang geven tot alle systemen en gegevens van [de organisatie].
- De ransomware affiliate maakt hier gebruik van en beginnen met het onderzoeken van het interne netwerk van [de organisatie]. Hierbij zoeken ze uit welke systemen en processen het belangrijkste zijn voor [de organisatie] en op welke servers deze processen en systemen draaien.
  Ook doorzoeken zij de systemen op gevoelige informatie en exfiltreren gedeeltes van de informatie die voor hen interessant kan zijn.
- Nadat het onderzoek door de ransomware affiliate is afgerond, is het tijd om over te gaan tot de daadwerkelijke aanval. Door de ransomware affiliate wordt via het darkweb ransomware software ingekocht van een criminele organisatie die hierin is gespecialiseerd. Vervolgens wordt door de ransomware affiliate ransomware geïnstalleerd en geactiveerd op alle servers van [de organisatie]. Hieronder vallen ook de servers waar het [betalingssysteem] op draait.
- Door het onderzoek wat door de ransomware affiliate is gedaan en de toegang die zij hebben tot alle informatie over [de organisatie] weet de ransomware affiliate dat [iedere 10e van de maand de inkomensondersteuning naar inwoners van de gemeenten wordt uitbetaald]. Om die reden wordt de ransomware 1 dag voor die datum geactiveerd.
- Vervolgens wist de ransomware affliate zoveel mogelijk logbestanden en wordt er afgewacht tot [de organisatie] contact met hen zal opnemen.
- Wat [de organisatie] zich mogelijk nog niet gelijk beseft is dat de organisatie op meerdere manieren verbonden is met ketenpartners zoals bijvoorbeeld gemeenten en/of andere organisaties welke vallen onder de Wet gemeenschappelijke regelingen (WGR). Deze ketenpartners kunnen mogelijk ook hinder gaan ondervinden als [de organisatie] in de problemen komt. In het ergste geval kan het zelfs mogelijk zijn dat een probleem zich via [de organisatie] verspreidt richting één van de ketenpartners.

2.3.4.3 Startsituatie (dag 1, 09:00-10:30)

- 09:00: Voor [de organisatie] lijkt het een dag te worden als alle andere. Wel is het deze dagen extra druk voor alle medewerkers omdat [alle betalingen voor de inkomensondersteuning morgen moeten worden betaald].
- 09:10: Echter komt hier gelijk verandering in zodra de eerste werknemers die dag aan het werk gaan. Nadat de ransomware affiliate de ransomware s'nachts heeft geactiveerd zijn alle lokale servers van [de organisatie] versleuteld en heeft geen enkele medewerker van de organisatie meer toegang tot de bestanden op de fileservers van [de organisatie].
- 09:20: Aangezien de servicedesk van [de organisatie] gebruik maakt van vaste telefonielijnen (en dus nog bereikbaar is) wordt de servicedesk/IT-afdeling van [de organisatie] overspoelt met telefoontjes van de medewerkers. Hierbij hebben sommige medewerkers geen idee wat hen overkomt en beginnen andere medewerkers met meer IT-kennis al te speculeren over een ransomware aanval.
- 09:40: Na een spoedoverleg tussen de IT-afdeling van [de organisatie] en IT-leverancier [Assensio] blijkt dat het duidelijk is dat [de organisatie] geraakt is door een ransomware aanval en dat zeker de helft van de systemen momenteel niet benaderbaar is. Hieronder valt ook het [SPP-systeem] dat nog op een lokale server draait.
- 09:45 Na deze bevinding wordt het crisisteam van [de organisatie] gelijk geactiveerd. Ondertussen is door het IT-team al besloten om het gehele netwerk van [de organisatie] uit te schakelen en alle inkomende en uitgaande verbindingen via de firewall tijdelijk te blokkeren om verdere verspreiding en problemen te voorkomen. Dit betekent dat [de organisatie] nu volledig is afgesloten van de buitenwereld en geen enkele medewerker werkzaamheden kan uitvoeren waar internetverbinding voor nodig is.
- 09:50: Intussen ontstaat er veel onrust binnen de organisatie. Medewerkers proberen massaal de servicedesk van [de organisatie] te bereiken, maar deze kan momenteel nergens op reageren omdat de meeste systemen (exclusief de telefonie) via internetverbinding verlopen. Ook beginnen er al veel geruchten te ontstaan over hackers etc.

- 10:15: Ook de inwoners van de gemeenten ondervinden hinder van de aanval op [de organisatie]. Zij ontvangen geen communicatie meer over [het werk dat door [de organisatie] wordt verstrekt] en kunnen niemand bereiken. Normaliter gebeurt dit via e-mails en berichten op de website. Dit zorgt ook voor veel vragen op sociale media. Medewerkers beginnen ook op eigen houtje contact te zoeken met burgers binnen de gemeenten. Hierdoor ontstaan er nog meer geruchten en onrust op sociale media.
- 10:30: In de ransomware note van de criminele organisatie staat aangegeven dat er [€300.000,-] dient te worden betaald om de ontsleutelaar van de ransomware in handen te krijgen. [de organisatie]volgt alsnog het richtgevende standpunt vanuit de overheid om geen gehoor te geven hieraan en niet te betalen aan een criminele organisatie.

Sleutelbesluiten startfase:
- Welke mitigerende acties zijn er nodig en gaan/kunnen we deze uitvoeren.
- Hoeveel impact heeft dit op onze dienstverlening en wat wordt onze strategie (snelheid vs zorgvuldigheid).
- Hebben we de juiste expertise in huis om dit op te lossen of dienen we externe hulp in te schakelen.
- Hoe gaan we als organisatie zo snel mogelijk aan de juiste informatie komen.
- Hoe gaan we als organisatie communiceren met interne/externe stakeholders.

Dilemma's startfase:
- Wat vertellen we onze medewerkers?
- Gaan we (en indien ja: hoe?) onze klanten/partners informeren.
- Gebruiken standaard communicatiemiddel of niet zonder duidelijkheid over de veiligheid hiervan.
- Blijven we onze netwerkverbindingen blokkeren of niet?
- Hoe denken wij als organisatie over het betalen van losgeld?

2.3.4.4 Tweede fase: nadere gevolgen (Dag 1, 15:00-17:00)

Na een aantal crisis overleggen komt er steeds meer informatie beschikbaar voor het Crisisteam en ontwikkelt de situatie zich.

- 15:00: Er is inmiddels op aanraden van een specialistische partij contact geweest met de criminele organisatie. Hieruit blijkt dat de criminele organisatie aangeeft inderdaad ook gevoelige informatie van burgers in handen te hebben en dat deze informatie zal worden gepubliceerd indien [de organisatie] niet binnen 24 uur overgaat tot de betalingen van [€300.000,-] in Bitcoin.
- 15:30: Na verder onderzoek is gebleken dat er naast versleuteling inderdaad ook data is geëxfiltreerd door de criminele organisatie. Dit gaat om gevoelige informatie zoals [namen, BSN-nummers en zelfs gezondheidsgegevens en financiële informatie van burgers].
- 15:45: Uit het eerste forensische onderzoek blijkt dat alle server die momenteel nog on premise draaien zijn versleuteld.
- 16:00: [de organisatie] heeft veel moeite om met het afgesloten netwerk de burgers te bereiken. Hiervoor wordt normaliter e-mail gebruikt, maar zonder actief netwerk kan dit alleen via de vaste telefoon of sociale media. Een oplossing om dit wel beter te kunnen doen is het herstellen van de netwerkverbinding van een aantal applicaties die internet nodig hebben maar niet versleuteld zijn. Hieronder valt onder andere de e-mail omgeving die via een niet versleutelde server loopt. Dit levert echter wel een risico op verder verspreiding (ook naar andere partijen) op. Ook is het niet duidelijk of de aanvallers mogelijk toegang hebben tot de e-mail omgeving en deze dus niet onveilig kan zijn. Het crisisteam moet hierover besluiten.
- 16:15: Middels een aantal noodplannen uit het Business Continuity Plan van [de organisatie] blijken een aantal processen nog steeds handmatig uitvoerbaar. Dit haalt iets van druk weg voor [de organisatie] maar de belangrijkste processen zijn niet uitvoerbaar op het moment. Deze handmatige processen verlichten de druk dus iets.

- 16:30: Er is gekeken naar de mogelijkheid om [de betalingen van de inkomenssteun] handmatig te doen. Dit is mogelijk, maar alleen aan de hand van een schatting van de situatie 3/4 maanden geleden. Hierbij is het vrijwel zeker dat [niet alle gerechtigden hun inkomenssteun gaan krijgen en veel exacte bedragen kloppen niet]. Daardoor kan veel onrust ontstaan.
- 16:35: Het [betalingsproces] kan worden uitgevoerd, maar hier zal veel werk aan verricht moeten worden door werknemers binnen [de organisatie].
- 16:45: Het contact tussen IT-leverancier [Assensio] en [de organisatie] verloopt moeizaam. Er is sprake van discussie over het uitvoeren van acties en het zit [de organisatie] niet lekker dat het [SPP-systeem] volgens de planning al gemigreerd had moeten zijn naar de Cloud (wat nu veel problemen had gescheeld).
- 16:55: Er begint binnen belangrijke stakeholders (zoals bijvoorbeeld aangesloten gemeenten) steeds meer onrust te ontstaan door de problemen bij [de organisatie]. Meerdere burgers komen in de problemen met hun werk en melden dit inmiddels ook bij de diverse gemeentehuizen. Op basis hiervan beginnen de gemeenten ook steeds meer vragen te stellen over de situatie.
- 17:00: De situatie wordt nu ook steeds duidelijker voor de buitenwereld. Meerdere journalisten bellen richting [de organisatie] en de ketenpartners voor tekst en uitleg. Ook beginnen de eerste artikelen in de lokale nieuwsmedia te verschijnen. Wat gaat er worden verteld aan de media hierover?
- 17:00: Er blijken verbindingen te zijn met andere organisaties, deze beginnen te klagen omdat de in-en uitkomende verbindingen zijn geblokkeerd. Deze ketenpartners ondervinden mogelijk dus hinder van de situatie binnen [de organisatie]. Ook beginnen er binnen [de organisatie] geluiden te klinken over de mogelijke verspreiding van ransomware naar de ketenpartners als gevolg van verbindingen die openstaan.

Sleutelbesluiten tweede fase:

- Betalen van losgeld of niet.
- De netwerkverbinding herstellen of niet.
- Kunnen we op basis van onze kennis over de infrastructuur van [de organisatie] bepalen wat de exacte impact van de aanval is.
- Handmatig uitvoeren van processen of niet.
- Kritieke processen handmatig uitvoeren of niet.
- Hoe te communiceren over de situatie.
- Hoe om te gaan met leverancier [Assensio].
- Hoe om te gaan met andere organisaties die verbindingen hebben met [de organisatie] en hinder ondervinden van de situatie.

Dilemma's tweede fase:

- Hoe denken wij als organisatie over het betalen van losgeld?
- Vinden we als organisatie acceptabel als we onze belangrijke processen voor langere tijd niet kunnen uitvoeren?
- Wat is de data van onze burgers waard?
- Gebruiken we standaard communicatiemiddel of niet (zonder duidelijkheid over veiligheid hiervan)?
- Openheid van zaken geven of voorzichtig zijn met het duiden van de situatie naar medewerkers en externen?

2.3.4.5 Derde fase: de druk wordt opgevoerd (dag 2, 11:00-14:00)

Nadat [de organisatie] de eerste acties en communicatie heeft uitgezet wordt een tijdsprong gemaakt naar de [betaling dag] met nieuwe informatie.

- 11:00: De nationale media begint het verhaal ook op te pikken en meerdere berichten verschijnen in de nationale media. Een securitywebsite weet zelfs al te melden dat er mogelijk gevoelige gegevens van burgers zijn buitgemaakt. Dit heeft ook consequenties richting AP.
- 11:30: Er is gekeken naar de backups van de systemen binnen [de organisatie]. Deze zijn aanwezig maar blijken niet gemakkelijk terug te zetten omdat deze lopen op verouderde software die niet meer beschikbaar is. Er moet verder worden uitgezocht of dit mogelijk gaat zijn. Wel kan [de organisatie] ervan uitgaan dat het herstellen van systemen door middel van back-ups zeker 14 dagen gaat duren. Zonder de backups kan [de organisatie] zijn belangrijkste processen waarschijnlijk niet voortzetten.
- 11:45: Na verder forensisch onderzoek blijkt dat de gevoelige gegevens van zeker [1000 burgers] in het bezit is van de criminele organisatie. Deze organisatie weet van geen wijken en dreigt na meermaals onderhandelen nog steeds om de gegevens te publiceren. De verwachting is dat de criminele organisatie dit ook echt gaat doen als er niet wordt betaald. Wel is het gevraagde losgeld inmiddels gezakt naar [€200.000,-].
- 12:30: De druk op het betalen neemt toe. De criminele organisatie heeft inmiddels ook bewijs aangeleverd voor het bezitten van zeer gevoelige informatie en dreigt de gegevens van [honderden/duizenden burgers] te publiceren/door te verkopen als er niet snel betaald wordt. Hoe gaat [de organisatie] om met deze ethische vraag? Welke partijen kunnen hierbij hulp bieden?
- 13:00: Meerdere organisaties benaderen [de organisatie] met de vraag wat er precies aan de hand is en om ervoor te waken dat de criminele organisatie niet ook toegang kan/heeft kunnen verkrijgen tot het netwerk van andere organisaties. Vooral [een van de meest belangrijke keten-partners] maakt zich hier erg druk om. Uit het eerste onderzoek blijkt vervolgens dat het niet uit te sluiten valt dat via gelinkte systemen ook geprobeerd is binnen te komen bij het [deze belangrijke ketenpartner]. Hierover zijn veel zorgen.
- 13:30: Uit nieuwe informatie blijkt dat er een mogelijke oplossing is voor [het uitbetalen van de inkomenssteun] via een partner/derde partij. Echter is dit een oplossing die pas over 2 weken kan worden uitgevoerd waardoor [de betaling van de inkomenssteun deze maand niet kan worden uitgevoerd]. Dit heeft grote gevolgen. Hier moet dus een oplossing voor worden gevonden.
- 13:45: Vele burgers nemen contact op met [de organisatie] over de situatie waarbij twee onder-werpen steeds terugkomen: 1. [Krijg ik mijn inkomenssteun deze maand?] 2. Zijn mijn gegevens in handen van criminelen?
- 14:00: Inmiddels krijgt [de organisatie] vanuit de media ook veel vragen over de mogelijk geëxfiltreerde data. Kan [de organisatie] aangeven of dit het geval is en zo ja welke data van burgers er buit is gemaakt?

Sleutelbesluiten derde fase:

- Zelf actief communiceren in de media of niet.
- Hoe om te gaan met de gestolen data die momenteel zeker al in handen is van de criminelen.
- Betalen van cybercriminelen of niet.
- 14 dagen lang zonder gebruik belangrijke systemen (en dus de belangrijkste processen) werken of niet.
- Houden we de netwerkverbindingen met andere organisaties in stand (zonder deze verbindingen werkt bijna geen enkel proces binnen [de organisatie] meer).
- Gaan we [inkomenssteun uitbetalen] op basis van oude gegevens met de kans op onjuiste [betalingen].
- Gaan we de backups terugzetten of niet.

Dilemma's derde fase:

- Hoe denken wij als organisatie over het betalen van losgeld?
- Wat gaan we onze interne- en externe stakeholders vertellen?
- Is de data van onze burgers het betalen van cybercriminelen waard?
- Weten we zeker dat de backups uiteindelijk bruikbaar/veilig gaan zijn?
- Durven we het risico te nemen om andere organisaties te besmetten door onze verbindingen actief te houden?

2.3.4.6 Eerste start nafase (dag 3, 09:00)

Nadat de belangrijkste beslissingen zijn gemaakt en dilemma's zijn opgelost kan er ook al worden gekeken naar de toekomst.

- Hoe gaan we het vertrouwen van de burger terugwinnen?
- Hoe zorgen we dat we hier voortaan beter op zijn voorbereid en de situatie beter kunnen managen?
- In Nederland ontstaat een bredere discussie over de security van overheidsorganisaties en of het beschermen van de burger het betalen van criminele organisaties waard is.
- Uit het verdere forensische onderzoek blijkt dat de kwetsbaarheid in BEAT-VPN en het slechte wachtwoordbeleid ervoor hebben gezorgd dat [de organisatie] slachtoffer kon worden van deze aanval.
- Gaat [de organisatie] volledige transparantie geven over wat er gebeurd is, hoe de criminele organisatie de aanval heeft kunnen uitvoeren en welke gegevens precies zijn buitgemaakt?