COT | Instituut voor Veiligheids- en Crisismanagement
an Aon company

De cyberagenda voor de veiligheidsregio 2017 - 2020: voorbereid, betrokken en betrouwbaar

Abderrahman Kaouass & Marco Zannoni
18 april 2017

1. Toelichting

Er zijn tegenwoordig weinig onderwerpen zo 'hot' en tegelijkertijd zo ongrijpbaar als 'cyber' of digitale (on)veiligheid. Vele overheden en bedrijven werken aan cyber security, bijvoorbeeld gericht op het voorkomen van *hacks*, datalekken en IT-storingen en aan het beperken van de gevolgen hiervan. Maar er zijn nog veel vragen over wat nodig is als een incident een cybercrisis dreigt te worden.

Op 4 en 10 april jl. faciliteerde het COT Instituut voor Veiligheids- en Crisismanagement twee bijeenkomsten over het thema 'Veiligheidsregio en Cyber'. Meer dan 50 deelnemers hebben vragen, ervaringen, zorgen en kennis uitgewisseld. De deelnemers zijn afkomstig van 10 veiligheidsregio's, nationale veiligheidspartners en overheden en vitale bedrijven. De belangrijkste opbrengsten hebben we samengevat in deze notitie.

We benutten deze notitie vooral om een gezamenlijke agenda voor de komende paar jaar vorm te geven. Op veel plaatsen spelen immers dezelfde uitdagingen. Op basis hiervan en onze eigen cyberervaring hebben wij een basis top 5 benoemd (wat moet eerst?) en een vervolg top 5 (wat is aanvullend nodig?). Vanzelfsprekend is er meer nodig, maar focus geeft meer garantie op uitvoering.

Mede op verzoek van de deelnemers brengen wij deze agenda actief – via sessies, gesprekken en sociale media - onder de aandacht van zowel nationale veiligheidspartners als de veiligheidsregio's zelf. Wij geloven dat een goede voorbereiding en respons onmisbaar zijn voor een weerbaar Nederland. Juist nu. We moeten organisaties verbinden, onze basisstructuur voor crisis benutten en goed aansluiten op IT security. Continuïteit en betrouwbaarheid van hulpdiensten is cruciaal voor iedereen, zeker bij crises. Alleen met een gerichte agenda kunnen we dan de snelle ontwikkelingen op cybergebied volgen en de risico's voldoende mitigeren.

2. Afbakening: wat is cyber?

Er zijn veel verschillende definities en mogelijke ordeningen van cyberincidenten. Wij combineren twee invalshoeken: verschijningsvormen en reikwijdte.

A. We maken een onderscheid in **vier verschijningsvormen** waarmee je als organisatie te maken kunt krijgen: uitval van IT, verlies van persoonsgevoelige of bedrijfsgevoelige informatie en onbetrouwbaarheid van data/systemen. Dit kan moedwillig worden veroorzaakt of het gevolg zijn van een fout of anderszins onbedoeld plaatsvinden. Zo zijn er vele verschillende type incidenten. Een cyberaanval kan bijvoorbeeld resulteren in uitval van IT en gepaard gaat met het verlies van gevoelige informatie.

B. Een tweede invalshoek is **de reikwijdte**. Dit kan gaan over de continuïteit van de eigen organisatie als veiligheidsregio (bijvoorbeeld uitval van systemen, hack van een twitteraccount of ransomware), over de keten (uitval van de meldkamerfunctie of communicatie/dataverkeer, niet beschikbaar zijn van LCMS) en/of over de regionale crisisbeheersing waarin de veiligheidsregio een cruciale rol heeft (de respons op een crisis als gevolg van cyber). Het meest complex is de situatie waarin zowel de eigen organisatie als de keten en de crisisbeheersing worden geraakt. Bijv. wanneer zowel de energievoorziening als de meldkamer worden ontregeld of LCMS niet kan worden gebruikt.

3. Beeld van de huidige situatie (ervaringen, ontwikkelingen en initiatieven)

- Deelnemers geven aan dat veiligheidsregio's meerdere ervaringen hebben opgedaan met 'kleine' incidenten: van het hacken van een Twitter account tot DDoS-aanvallen, *phishing mails* en uitval van telefonie. Dit bleef vooralsnog beperkt tot de eigen organisatie en met beperkte impact.
- Cyber security (of digitale onveiligheid) krijgt bij sommige, maar lang niet alle veiligheidsregio's aandacht. Voor specifieke onderdelen van de organisatie zijn er continuïteitsplannen en -maatregelen, maar niet voor het brede functioneren van de hulpverleningsketen in Nederland.
- Verscheidene veiligheidsregio's hebben cyber op de eigen agenda gezet als onderwerp voor 2017 en 2018. Veelal nog zonder duidelijk beeld op welke manier zij hier invulling aan gaan geven.
- Een enkele veiligheidsregio heeft een cyberoefening georganiseerd. Andere voorbeelden van activiteiten zijn het uitwerken van cyber in het kader van het regionaal risicoprofiel en het starten met het inventariseren van kritische processen in de eigen organisatie. Soms is bij hoog risico evenementen nagedacht over cyber (zoals bij de Troonswisseling en de *Nuclear Security Summit*).
- Er is een sterk wisselend beeld van de bestaande samenwerking tussen veiligheidsregio's en vitale bedrijven. Soms zijn er intensieve vormen van samenwerking (uitwisselen liaisons, gezamenlijke

oefening) en soms zijn er alleen de samenwerkingsconvenanten die nooit verder zijn gekomen dan ‘het fotomoment.’
- Er is beperkt zicht op de eigen kritische processen en systemen: waar zijn we afhankelijk van digitale toepassingen? Continuïteit van de eigen organisatie is tot nu toe geen of onvoldoende speerpunt.
- Er is toenemende, ontluikende bestuurlijke en managerial interesse voor het onderwerp, vooral in termen als ‘moeten we hier niet iets mee?’.
- Beschikbare informatie over cyberdreigingen en ontwikkelingen is bij veiligheidsregio’s beperkt bekend en lijkt zelden te worden benut voor interne reflectie: ‘wat betekent het voor ons?’.

4. Terugkerende vragen en behoeften

Cyber en de eigen organisatie
- Er is behoefte aan een hulpmiddel om kritieke processen in kaart te brengen. Iedere veiligheidsregio heeft vergelijkbare processen en functies: waar zitten de voorstelbare en voorspelbare afhankelijkheden en kwetsbaarheden waar in ieder geval zicht op moet zijn en waarvan beschikbaarheid/continuïteit moet worden geborgd? Als dit in beeld is kan worden gekeken naar beschikbare/mogelijke alternatieven bij uitval (van andere systemen tot handwerk).
- Het is raadzaam om bij het vaststellen van de kritieke processen ook de preventieve aspecten in ogenschouw te nemen. Bijv. de informatiebeveiligingsplannen, ICT-onderhoudsplannen en facilitaire onderhoudsplannen. Deelnemers benoemden ook de noodzaak van aandacht voor oude systemen of toepassingen die niet of nauwelijks nog worden gebruikt maar wel kunnen worden misbruikt.
- Er is verwondering over het feit dat de hulpverleningssector geen ‘vitale sector’ is. Omdat de veiligheidsregio’s geen vitale sector zijn en ook geen onderdeel zijn van de rijksoverheid, kunnen zij geen volwaardig beroep doen op het NCSC als *Computer Emergency Response Team* (CERT). Veiligheidsregio’s zijn als vorm van verlengd bestuur ook niet zelf aangesloten op de Informatiebeveiligingsdienst (IBD). Dit is de CERT voor gemeenten. De veiligheidsregio valt daarmee tussen wal en schip en heeft ook niet zelf een vorm van samenwerking georganiseerd. Dit geldt ook voor het delen van informatie en het geven van alerts (zoals dit gebeurt in een *Information Sharing and Analysis Centre* (ISAC).

De veiligheidsregio en crisismanagement
- Er een breed gedragen behoefte aan informatie over en inzicht in bestaande voorbereidingen, rollen en verantwoordelijkheden, maar ook mogelijke bijzonderheden, maatregelen, sleutelbesluiten en doelen en uitgangspunten. Voorbeelden van genoemde bijzonderheden zijn de onzekerheid (wie zit er achter?), een mogelijke vervolgdreiging en het werken met andere partners voor de bronbestrijding. Dit kan bijvoorbeeld in de vorm van een handreiking cybergevolgbestrijding (zoals is ontwikkeld voor terrorismegevolgbestrijding) worden vormgegeven.
- Er is beperkt tot geen zicht op de verwachte/beoogde samenwerking tussen de nationale en regionale crisisstructuren: wie doet wat en hoe vindt afstemming plaats? Er is een nationaal crisisplan IT-uitval, maar de inhoud (en betekenis) hiervan is bij de meeste veiligheidsregio’s niet bekend. Ook zijn er meerdere systemen die landelijk worden beheerd (zoals C2000, LCMS): hoe verloopt afstemming en samenwerking bij cyberincidenten voor deze systemen?
- Het nadenken over cyber dwingt ook tot reflectie op de rol van de veiligheidsregio. Hoe ver gaat deze? De veiligheidsregio heeft in ieder geval te maken met de maatschappelijke effecten van een (grote) verstoring. De bronbestrijding voor cyber ligt veelal niet bij de veiligheidsregio maar elders, zoals bij een direct betrokken vitaal bedrijf terwijl het effectgebied wel altijd regionaal/bovenregionaal is. Een vraag is of de veiligheidsregio ook een rol heeft om bij een cyberaanval proactief sectoren te informeren en te betrekken om na te denken over mogelijke vervolgaanvallen/-dreigingen. Of doen de sectoren dat zelf? Of is dit juist een rol voor het Rijk?
- In het kader van flexibilisering van de crisisrespons is de vraag hoe ‘cyber’ hierin is te passen. Een voorbeeld is het realiseren van een continuïteitsteam dat zich vooral richt op een zo snel mogelijk herstel van uitgevallen diensten/processen. Dit is deel van het managen van de impact. Ook is een mogelijk om een cyberresponsteam (een vorm van CERT) te benutten en aan te sluiten op de crisisstructuur voor de bronbestrijding en het inschatten van ernst en mogelijke impact).

5. Benutten wat er is

Er zijn veel bestaande voorbereidingen en initiatieven die ook nuttig zijn bij de voorbereiding op grootschalige/impactvolle cybercrises. Voorbeelden hiervan zijn:

- Bestaande voorbereidingen vanuit de eigen IT-organisatie op cyber.
- Bestaande projecten op het gebied van de uitval van voice en data (uitval communicatiemogelijkheden).
- Bestaande voorbereidingen op uitval van IT en stroom
- Bestaande initiatieven in het kader van het project *Continuïteit van de samenleving* (onderdeel van de strategische agenda van het Veiligheidsberaad) dat zich richt op versterking van de samenwerking tussen veiligheidsregio's en vitale bedrijven. Voorbeelden hiervan zijn de vorming van (boven)regionale platforms voor onderlinge afstemming over voorbereiding en respons op continuitsverstoringen.

Meer informatie

a) Nationaal Cyber Security Centrum - https://www.ncsc.nl/
b) Informatiebeveiligingsdienst voor gemeenten - https://www.ibdgemeenten.nl/
c) Project Continuïteit van de samenleving - http://www.strategische-agenda.nl/project/continuiteit-van-de-samenleving/
d) Emergency Services Sector Cyber Security Initiative (VS) - https://www.dhs.gov/emergency-services-sector-cybersecurity-initiative

Over het COT en Aon

Het COT ondersteunt overheden en bedrijven bij de voorbereiding op mogelijke cybercrises. Voorbeelden hiervan zijn het ontwikkelen van een plan van aanpak, het begeleiden van de implementatie hiervan en het gericht opleiden, trainen en oefenen. COT maakt deel uit van het Aon-concern dat klaarstaat voor opdrachtgevers om data impact analyses op te stellen en te adviseren over verzekeringsoplossingen die de financiële gevolgen van cyberrisico's opvangen.