whitepaper

CYBER CRISIS MANAGEMENT

De volgende crisis die uw organisatie kan bedreigen is op dit moment al in ontwikkeling!

Vereniging
Beveiligingsprofessionals
Nederland

Changing Crisis Challenges: Cyber Crisis Management

De volgende crisis die uw organisatie kan bedreigen is op dit moment al in ontwikkeling.

Beroepscriminelen en staat gesponsorde hackers voeren dagelijks duizenden cyberaanvallen uit en richten hiermee in toenemende mate schade aan. Deze cyberaanvallen worden steeds geavanceerder, om hierop een antwoord te kunnen hebben, moeten organisaties mee met deze ontwikkeling.[1]

De normen en waarden die in de fysieke wereld gelden, lijken niet van toepassing te zijn in cyber space. Wanneer Rusland 10.000 troepen aan de grens heeft staan om ons land binnen te vallen noemen we dat in de fysieke wereld oorlog. Maar wanneer één hacker 10.000 maal door een firewall van een Nederlandse gemeente probeert te prikken, lijken daar weinig gevolgen aan te zitten. Recente incidenten als WannaCry en Not-Peyta laten zien dat het niet meer de vraag is of we getroffen worden door een cyber crisis, maar wanneer.

Informatie en communicatietechnologie (ICT) is tegenwoordig een belangrijk onderdeel van onze maatschappij en de trend van digitalisering zet nog altijd voort. Dit heeft de manier veranderd waarop we werken, communiceren en onszelf voorzien van informatie. ICT is geïntegreerd in onze maatschappij en we zijn in sterke mate afhankelijk geworden van deze technologie.

Ook cybercriminelen volgen deze trend. Het Nationaal Cyber Security Centrum (NCSC) ziet dat criminelen in toenemende mate acteren in het cyberdomein. Zij worden beter in het inzetten van de middelen die zij tot hun beschikking hebben en opsporing en vervolging vormen een grote uitdaging, mede doordat cyber criminelen vaak over de landsgrenzen heen opereren. De schade voor de Nederlandse maatschappij, veroorzaakt door cyber crime, wordt geschat op 10 miljard euro per jaar[2]. Wereldwijde aanvallen als WannaCry en Not-Peyta laten zien dat overheden en het bedrijfsleven zich dienen voor te bereiden op een mogelijke cyber crisis. Hierbij horen nieuwe, strategische vraagstukken, zoals het betalen van ransomeware, het ontkoppelen van ICT-infrastructuren en communicatie naar interne en externe stakeholders. Omdat een cyber crisis elke organisatie kan treffen, is voorbereiding van immens belang.

[1] Cyber Security Beeld Nederland 2017
[2] Cyber Value at Risk (2016)

Allereerst is het van belang om als organisatie een heldere definitie van het begrip ‘cybercrisis’ te hebben. Een gangbare, traditionele definitie van ‘crisis’ is vastgesteld door experts binnen het vakgebied, zoals Uri Rosenthal en Arjan Boin. Zij stellen: *“Een crisis is een situatie waarin beleidsmakers een druk ervaren jegens de basisstructuren of fundamentele normen van een (organisatie) systeem.”*

Deze definitie is van toepassing op elk crisistype, ongeacht de oorzaak of de omgeving waarin deze zich afspeelt. Tijdens een crisis moeten er onder tijdsdruk en bij een hoge mate van onzekerheid vitale beslissingen worden genomen.

Echter zijn er een aantal kritieke succesfactoren te onderkennen welke wezenlijk anders zijn in het geval van een cyber crisis.

1. **Overtuig het topmanagement van het belang van een adequate cyber crisis management organisatie.**

Een crisis, ongeacht diens aard, brengt strategische vraagstukken met zich mee, waar een strategisch antwoord op nodig is. Voor een traditionele crisis hebben veel organisaties hier dan ook een antwoord op, bestuurders zijn tenslotte verantwoordelijk voor het managen van een crisis. Bij gemeenten ligt deze verantwoordelijkheid bij de burgemeester, met een heldere onderliggende organisatiestructuur. In het geval van een cyber crisis lijkt deze organisatiestructuur nog niet zo goed ingericht. Een goede vertaalslag van een ICT-incident, naar een strategisch vraagstuk, moet nog gemaakt worden.

2. **Inrichting van de cyber crisis management organisatie**

Om een crisis effectief te kunnen managen is het van belang dat deze zo snel mogelijk onderkend en bestreden wordt. Bij een brand of grote hoeveelheden media aandacht, is het als snel duidelijk dat de organisatie te maken heeft met een crisis. Echter, wanneer cybercriminelen de systemen van een organisatie binnen zijn gedrongen, bestaat de kans dat zij langere tijd onopgemerkt te werk kunnen gaan. In tegenstelling tot een traditionele crisis is de kans groot dat een potentiele cyber crisis langdurig onzichtbaar blijft, totdat het te laat is.

De capaciteit om cyberaanvallen te kunnen detecteren en hier adequaat op te kunnen reageren, wordt in sterke mate bepaald door de volwassenheid van de cyber security en cyber incident management organisatie. Een organisatie met een goede mix van technische, organisatorische en fysieke beveiligingsmaatregelen, heeft daarom een grotere kans om een cyber crisis effectief te managen.

3. **Aanhaken van cyberspecialisten bij het crisis management team**

De huidige crisis management functies binnen gemeentelijke organisaties zijn veelal ingericht op traditionele crisistypen. De functionarissen zijn getraind op deze soorten crises en crisis management plannen zijn eveneens hierop afgestemd. De kans is echter groot, dat een cyber crisis nog niet op een vergelijkbare wijze is voorbereid. Het is daarom van belang dat cyberspecialisten, bij de crisis management organisatie worden betrokken. Deze

betrokkenheid zou zich moeten uiten in het mede voorbereiden van cyber crisis scenario's, evenals het trainen en oefenen met deze scenario's. Dit maakt het mogelijk dat cyberspecialisten mee kunnen draaien in de bestaande crisis management organisatie.

4. Besluitvorming bij cyber crises

Een gedegen besluit wordt genomen door de verantwoordelijke voor dat onderwerp, op basis van relevante en geverifieerde informatie. Dit geeft ook direct aan waarom het tijdens een crisis moeilijk is om tot een gedegen besluit te komen. Verantwoordelijkheden zijn niet altijd even helder vastgelegd noch gecommuniceerd, teams worden overspoeld met informatie en hebben door tijdsdruk moeite met filteren en verifiëren van sturings-informatie. Een groot gedeelte van crisis besluitvorming berust dan ook op informatiemanagement en mandaatregeling. Dit is bij een crisis met een cyber scenario niet anders. Het is van essentieel belang dat de uiteindelijke besluitvormer zich laat informeren en adviseren door de inhoudsdeskundigen, de cyber security organisatie en hen hierin vrijheid geeft om creatieve oplossingen te bedenken voor het probleem. Echter is het onverantwoord teveel mandaat neer te leggen bij de operationele laag. Enerzijds omdat deze operationele organisatie niet of in mindere mate in staat is om een holistische/strategische aanpak te hanteren voor het probleem. Anderzijds omdat een IT-manager simpelweg niet verantwoordelijk zou moeten zijn voor het nemen van vitale beslissingen voor de organisatie. Crisis besluitvorming, ook bij cyber crisis is een 'balancing act' en bedrijven doen er goed aan om na te denken over uitdagingen als informatiemanagement onder tijdsdruk en het verstrekken van mandaten.

5. Neem als organisatie het initiatief met betrekking tot de crisisberichtgeving, met speciale aandacht voor de samenwerking tussen de cyberspecialisten en het crisiscommunicatieteam

Een brand is een brand, een aanslag is een aanslag. Fysieke crises bieden minder ruimte voor interpretatie dan cyber crises, veelal omdat een cyber crisis minder tastbaar is.
Om de geruchtenvorming te beperken, is het van belang om als organisatie zelf naar buiten te communiceren. Hiervoor is de samenwerking tussen cyberspecialisten en communicatiemedewerkers zeer belangrijk. Zij dienen samen een correcte, maar ook eenvoudig te begrijpen bericht naar buiten te brengen.

6. Test, train en oefen met cyberscenario's

Het moet te allen tijde worden voorkomen dat een cybercrisis een probleem wordt van de IT-afdeling. Crisis management is een strategische verantwoordelijkheid, welke op het hoogste niveau binnen de organisatie belegt dient te zijn. Het is daarom zaak om vanaf het eerste moment integraal en op strategisch niveau te trainen en te oefenen op cyber scenario's, bij voorkeur in samenwerking met de ondersteunende teams. Op deze wijze kunnen processen op elkaar afgestemd worden en wordt het duidelijk hoe communicatie

lijnen lopen, zodat deze procesgericht en afgestemd op elkaar kunnen werken en weten waar de informatiebehoefte ligt en hoe communicatielijnen lopen.

Daarnaast is het aan te raden te oefenen met de IT-keten, zodat SLA's en third party assurance getest kan worden. Het rendement van trainen en oefenen is het grootst wanneer er actief geëvalueerd wordt. Om de cirkel rond te maken: maak personen verantwoordelijk voor de implementatie van lessons learned, inclusief tijdlijnen.

Geef het beestje een naam

Dit artikel begon met de vraag hoe een cyber crisis geplaats moet worden binnen crisis management; een cyber crisis, of een crisis met een cyber scenario. In de praktijk ligt het antwoord hierop ergens in het midden. Het managen van een cyber crisis heeft veel raakvlakken met traditioneel crisis management. In de praktijk zal bij veel organisaties er ook geen aparte cyber crisis management organisatie bestaan.

Echter, wanneer we kijken naar de uitdagingen van een cyber crisis, zijn er ook significante verschillen:

- Een cyber crisis is over het algemeen minder zichtbaar;
- De reguliere crisismanagement organisatie heeft vaak weinig tot geen ervaring met cyber crises;
- Cyber incidenten worden vaak nog als IT-probleem gezien;
- Crisis communicatie tijdens een cyber crisis vraagt om een andere aanpak.

Doordat een cyber crisis andere vraagstukken met zich meebrengt, dient een organisatie te overwegen, indien een cyber crisis als een scenario wordt beschouwd, of dit scenario dan voldoende is voorbereid. Het kan een passende oplossing zijn om cyber crises met de staande organisatie te managen. Veel organisaties zullen een vorm van cyber incident management hebben, in de vorm van een incidentmanagementteam of een IT-calamiteitenteam. Eveneens zal er veelal een crisismanagement organisatie zijn ingericht, om traditionele crises te kunnen managen. Deze structuur brengt als nadeel met zich mee, dat er sprake is van een 'gat' tussen de incidentfunctie en crisis management. Wanneer een cyber incident de capaciteiten en mandaten van de incidentfunctie ontstijgt, is er dan een overdracht mogelijk naar het strategische niveau, of wordt het gezien als een IT-probleem?

Ongeacht de definitie of de aanpak die je als organisatie hanteert, zijn er een aantal aandachtspunten waar rekening mee moet worden gehouden voor het bestrijden van een cyber crisis:

- Cyber crisis management is een strategische activiteit, zorg ervoor dat dit belegd is op het juiste niveau;
- De maturiteit van de cyber security kan een belangrijke bijdrage leveren aan het tijdig onderkennen en bestrijden van een cyber crisis, heb je dit als organisatie op orde?;

- Bepaal of de cyber crisis management of -incidentfunctie kan integreren in de bestaande crisismanagement organisatie, of dat er een aparte organisatie voor moet worden opgetuigd;
- Zorg ervoor dat mechanismen van escalatie en besluitvorming ook voor een cyber crisis zijn ingericht, hierbij is extra aandacht nodig voor de rollen en verantwoordelijkheden van de IT-afdeling;
- Bepaal je crisiscommunicatie strategie voor een cyber crisis, deze kan wezenlijk verschillen ten opzichte van een traditionele crisis, met name wanneer de cyber criminelen nog actief zijn binnen de systemen;
- Oefen als organisatie ook met cyber crisis scenario's, hierbij is speciale aandacht nodig voor mogelijke IT'ers die aanhaken bij een regulier crisis management team.

Cyber crisis of crisis met een cyber scenario? Geef het beestje een naam. Veel relevanter is de vraag of een organisatie klaar is om een cyber crisis te bestrijden. Het is slechts een kwestie van tijd, voordat de volgende organisatie wordt getroffen.

Over de schrijvers van dit artikel

Thijs Maters, werkzaam bij Deloitte Risk Services en volgt een master opleiding aan de Radboud Universiteit.

Lodewijk Leunk, werkzaam bij Capgemini als Cyber Security Consultant met een focus op Governance, Risk en Compliance.

Thijs Maters en Lodewijk Leunk zijn in juli 2017 afgestudeerd voor de opleiding Security Management aan Hogeschool Saxion te Apeldoorn. Ze hebben in het kader van hun afstudeeropdracht onderzoek gedaan naar de maturiteit van cyber crisis management binnen de Nederlandse decentrale overheid. Om dit in kaart te brengen hebben zij een volwassenheidsmodel ontwikkeld waarmee zij binnen twee overheidsinstanties onderzoek gedaan hebben. Daarnaast hebben zij een baseline ontwikkeld voor organisaties als minimaal level voor cyber crisis management capaciteit.

Tijdens dit onderzoek zijn zij vraagstukken tegengekomen waar andere organisaties mogelijk ook mee worstelen. Deze vraagstukken, eveneens als de mogelijke oplossingen, wilden zij delen met een breder publiek. Dankzij Rien van der Linden en Ben Nagel hebben zij de mogelijkheid gekregen om een artikel te schrijven over hun afstudeeronderwerp.