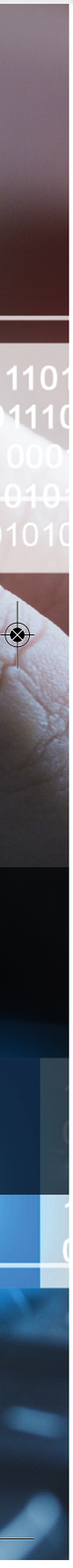
Auteur: Noortje Henrichs is teamleider van het team Cyber Threat Intelligence en Dreigingsanalyse (CTI/DA) bij het NCSC. Samen met haar team is zij verantwoordelijk voor het leveren van tijdige en relevante informatie over digitale dreigingen aan de doelgroepen van het NCSC. Het is haar missie om organisaties en bedrijven een goed inzicht te bieden in het huidige dreigingslandschap en informatie te leveren over de digitale aanvallen die er op Nederland afkomen. Noortje is bereikbaar via noortje.henrichs@ncsc.nl.

CTI en dreigingsanalyse binnen het NCSC

Omgaan met een groeiende informatiebehoefte in een divers organisatielandschap



Binnen het Nationaal Cyber Security Centrum (NCSC) is het team Cyber Threat Intelligence & Dreigingsanalyse (CTI/DA) verantwoordelijk voor het onderzoeken, duiden en inschatten van digitale dreigingen uit binnen- en buitenland. Dreigingsanalisten en specialisten van het NCSC helpen zo organisaties aan relevante informatie om zich te beschermen tegen cyberaanvallen. De vraag naar dreigingsinformatie neemt toe.

Toen in januari dit jaar de spanningen tussen Rusland en Oekraïne verder opliepen en Russische troepen zich verzamelden voor de Oekraïense grenzen, heerste er bij Nederlandse bedrijven en organisaties grote onzekerheid over wat er ging gebeuren.

Naast zorgen over een fysieke invasie, leefde er ook onrust over mogelijke cyberaanvallen die in het kader van dit conflict uitgevoerd konden worden. Al in 2017 hadden we in Nederland immers een voorproefje gezien van een digitale aanval op Oekraïense doelwitten, waarvan ook bedrijven in andere landen slachtoffer werden. De NotPetya-aanval richtte wereldwijd grote schade aan door computers te vergrendelen zonder dat dit teruggedraaid kon worden.

Deze zogenoemde wiper-aanval is een voorbeeld van een ongecontroleerd cyberwapen dat in het verleden al vaker in een conflict is ingezet. In het kader van deze bezorgdheid werd het NCSC geregeld benaderd door organisaties en bedrijven met vragen over digitale dreiging. Wat was er tot nu toe waargenomen en welk soort cyberaanvallen konden organisaties in Nederland in de toekomst verwachten?

Taak van het NCSC bij dreigingen

Het NCSC ontvangt geregeld vragen van organisaties die zich zorgen maken over hun digitale veiligheid en over de dreigingen die ze op zich af zien komen. Om hier goed antwoord op te kunnen geven, zet het NCSC de expertise in van het team Cyber Threat Intelligence & Dreigingsanalyse (CTI/DA). Dit team, met medewerkers met verschillende achtergronden, onderzoekt en duidt digitale aanvallen en schat de waarschijnlijkheid en impact van deze aanvallen in voor doelgroeporganisaties. Hiernaast maakt het team gebruik van het Nationaal Detectie Netwerk (NDN). Het team deelt eigenschappen van malafide verkeer voor detectie met doelgroeporganisaties en monitort zelf ook op deze eigenschappen binnen de rijksoverheid.

De veelzijdigheid van kennis en mensen in dit team zorgt voor een interessante en afwisselende werkomgeving waar ik met plezier deel van uitmaak. Ik vertel dan ook graag iets meer over het onderwerp dreigingsinformatie en hoe het NCSC daarmee omgaat.

Dreigingsinformatie delen

In het Cybersecuritybeeld Nederland wordt 'dreiging' gedefinieerd *als een cyberincident dat zich in de toekomst kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten die kunnen plaatsvinden*. Binnen het NCSC neemt team CTI/DA daarom een andere plaats in dan bijvoorbeeld het team Incident Response dat uitrukt bij incidenten die zich ook daadwerkelijk manifesteren.

De medewerkers van ons team zijn gespecialiseerd in digitale aanvallen en campagnes die zich misschien in Nederland nog niet hebben voorgedaan, maar die wel op ons afkomen. Ook houdt het team de digitale aanvallen bij, die we nu al veel zien in combinatie met de trends en ontwikkelingen die zich daarbij voordoen. Door de informatie over deze toekomstige dreigingen te delen, draagt het team bij aan het versterken van de weerbaarheid van organisaties. Wie weet wat er op hem/haar afkomt, ligt op veiligheidsgebied altijd een stap voor.

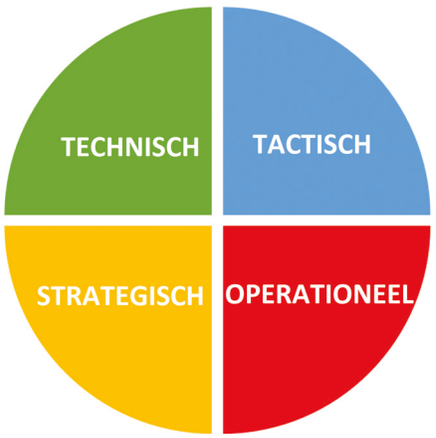
In de periode vóór de Russische invasie in Oekraïne heeft het NCSC bijvoorbeeld op de NCSC-website beschreven welk soort aanvallen in Nederland volgens het NCSC te verwachten waren en welke maatregelen organisaties kunnen treffen om zich

tegen dit soort aanvallen te beschermen (1). Tot nu toe heeft het NCSC geen aan de oorlog gerelateerde, digitale aanvallen gericht op Nederlandse belangen waargenomen.

Hoewel we altijd zoveel mogelijk informatie via onze website delen, is uiteraard niet al onze dreigingsinformatie geschikt voor openbare publicatie. Bepaalde informatie is gevoelig en wordt door het NCSC alleen gedeeld met doelgroeporganisaties voor wie dit relevant is. We hebben hier een goede reden voor: we willen digitale aanvallers niet wijzer maken dan ze al zijn.

Combineren van dreigingsinformatie op verschillende niveaus

Dreigingsinformatie over digitale aanvallen is niet eenduidig, er bestaan verschillende typen. Britse voorlopers van het huidige NCSC-UK hebben dreigingsinformatie onderverdeeld in vier niveaus: het technische, operationele, tactische en strategische niveau.



Figuur 1: Niveaus van dreigingsinformatie, bron: CPNI.gov.uk.

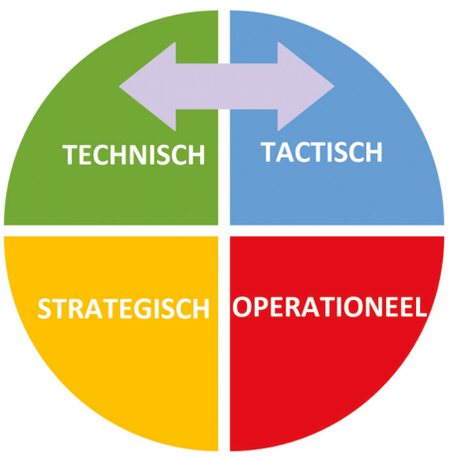
In 2018 werkten de dreigingsanalisten binnen het NCSC nog gescheiden van de meer technische CTI-specialisten. Zij concentreerden zich op dreigingsinformatie op tactisch niveau, bijvoorbeeld de werkwijze van digitale aanvallers en hoe zij hun digitale hulpmiddelen ontwikkelen. Deze analisten hebben meestal geen technische opleiding gehad, maar hebben een achtergrond in bijvoorbeeld integrale veiligheidskunde, inlichtingen of criminologie. Dit stelt ze in staat om digitale dreigingen ook in een breder verband, bijvoorbeeld op geopolitiek vlak, te kunnen duiden.

Toen ik werd aangesteld om het team van dreigingsanalisten te leiden, werd mij duidelijk dat tactische dreigingsinformatie niet erg waardevol is, als je deze niet kunt combineren met de bijbehorende informatie op technisch niveau. Want hoe zouden we organisaties goed kunnen helpen als we alleen de context en werkwijze van bijvoorbeeld een wiper-malware publiceren, zonder dat we ook de bijbehorende technische details leveren?

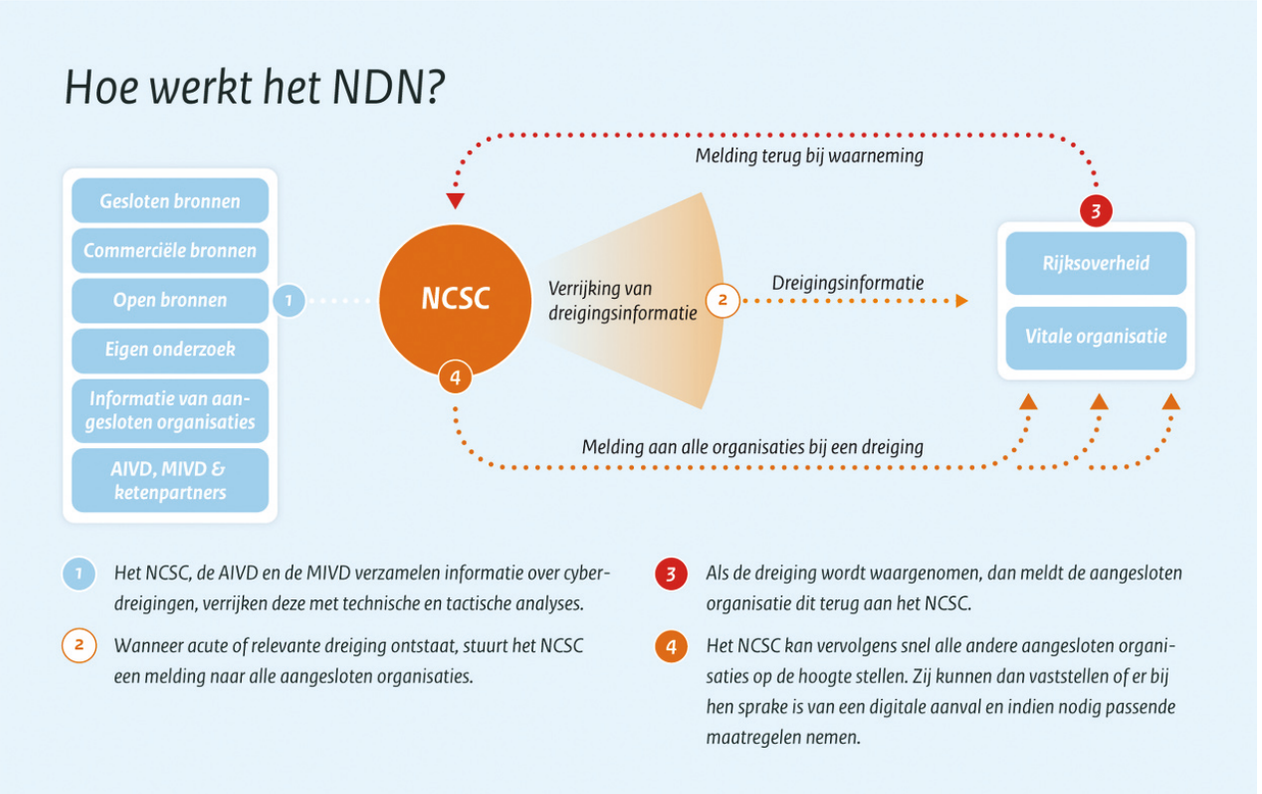
Technische dreigingsinformatie bestaat bijvoorbeeld uit herkenbare eigenschappen van malafide verkeer die organisaties vervolgens kunnen gebruiken voor detectie. Onder technische dreigingsinformatie vallen IoC's (Indicators of Compromise), zoals URL's, domeinnamen, hashes, YARA-rules en andere malware-eigenschappen. Zonder deze technische informatie kunnen organisaties de eerder genoemde wiper-malware niet binnen hun eigen netwerk detecteren of op deze malware monitoren.

Andersom geldt hetzelfde: je kunt wel technische informatie zoals IoC's hebben, maar zonder context weet je niet hoe relevant deze indicatoren zijn voor jouw organisatie. Je weet niet wat de malware precies als oogmerk heeft en wat de waarschijnlijkheid en mogelijke impact van een besmetting zal zijn.

De verschillende niveaus van dreigingsinformatie moeten samenwerken om een compleet beeld te krijgen van digitale dreigingen waar Nederland mee te maken krijgt. Dit volledige beeld wordt in jargon ook wel het 'dreigingslandschap' genoemd. Alleen met kennis van dit dreigingslandschap kan het NCSC de vraag beantwoorden welke digitale aanvallen we in Nederland kunnen verwachten. Dit is de reden waarom ik pleit voor het samenvoegen van tactische analisten en technische specialisten in hetzelfde team als het gaat om digitale dreigingsinformatie, zoals bij het NCSC nu het geval is (2). Daarnaast is dit



Figuur 2: De combinatie van technische en tactische dreigingsinformatie binnen het NCSC.



Figuur 3: De IoC-feed van het Nationaal Detectie Netwerk.

ook de reden waarom het NCSC graag informatie over digitale incidenten van organisaties en bedrijven teruggedeeld krijgt. Een incident bij de één is immers een waarschuwing voor de ander.

Diversiteit aan producten

De analisten en specialisten van ons team werken iedere dag aan informatieproducten die een beeld geven van het huidige dreigingslandschap. Maar digitale dreiging is niet voor alle organisaties hetzelfde. Het mag duidelijk zijn dat banken zich over andere cyberaanvallen zorgen maken dan bijvoorbeeld universiteiten. Het ministerie van Defensie zal doorgaans ook een ander soort aanvallers aantrekken dan een gemeente. Geen organisatie of sector is hetzelfde en 'one-size-fits-all' levert daarom zelden een goede bijdrage aan de digitale veiligheid.

Hiermee hebben we meteen de moeilijkheid te pakken. Hoewel de meeste organisaties en bedrijven goed kunnen uitleggen welk soort dreigingsinformatie voor hun netwerken en systemen relevant is, moeten CERT's (Computer Emergency Response Teams) zoals het NCSC meer dan driehonderd (!) doelgroepen kunnen bedienen met specifieke dreigingsinformatie. En als je dan bedenkt dat iedere organisatie weer een andere informatiebehoefte heeft, is dat nogal een uitdaging. Precies de reden voor ons team om verschillende informatieproducten te publiceren die de diverse dreigingsniveaus raken.

Een van de vele producten die we onze doelgroepen aanbieden, is onze IoC-feed. Deze bestaat uit indicatoren voor malafide verkeer (IoC's) die CTI-specialisten elke dag uit een hoeveelheid van bronnen verzamelen, analyseren en van labels voorzien. Deze feed wordt door middel van een platform verspreid naar organisaties die deelnemen aan het Nationaal Detectie Netwerk. Een van onze andere publicaties is de NCSC-dreigingsanalyse voor partijen in de vitale sector en de rijksoverheid. In de dreigingsanalyse kijken we elke drie maanden terug op de voor Nederland relevante dreigingen die ons team heeft waargenomen.

Daarnaast faciliteert ons team zogenoemde scenariosessies voor organisaties. Hierbij identificeren we gezamenlijk toekomstscenario's die zich richten op dreigingskans en -context. Het doel van deze sessies is om verschillende toekomstige digitale aanvallen te inventariseren, hierop te anticiperen en risico's te beoordelen (fysieke, politieke, financiële et cetera)

Ook in de aanloop naar de oorlog in Oekraïne heeft ons team, begin vorig jaar, dreigingsscenario's ontwikkeld. In deze scenario's hebben we op basis van precedentenonderzoek verschillende aanvallen geïdentificeerd die Nederland kunnen treffen in relatie tot de gespannen geopolitieke situatie. We hebben deze scenario's zo breed mogelijk binnen onze doelgroepen verspreid. En toen de oorlog uitbrak, heeft ons team de scenario's gepresenteerd aan onze doelgroepen en aan leden van het CIO Platform Nederland. In een informatiesessie mede georganiseerd door het Digital Trust Centre (DTC), zijn we vervolgens dieper ingegaan op de specifieke digitale dreigingen die een gevolg van deze oorlog kunnen zijn (een sessie die terug te kijken is op You Tube (3). Nu de oorlog al een tijd voortduurt, houdt het team de ontwikkelingen doorlopend in de gaten en worden dreigingsscenario's en handelingsperspectief voortdurend door onze analisten geactualiseerd.

Over handelingsperspectief gesproken: naast dreigingsinformatie is het zeer belangrijk dat in berichtgeving wordt benoemd wat organisaties kunnen doen om een bepaalde dreiging tegen te gaan. Binnen het NCSC werken de dreigingsanalisten daarom nauw samen met adviseurs die zijn gespecialiseerd in beveiligingsmaatregelen. Buiten het NCSC vindt op dit vlak bovendien nauwe afstemming plaats met partners binnen de overheid, zoals inlichtingendiensten en politie.

Toenemende vraag

Binnen het team merken we dat de vraag naar dreigingsinformatie toeneemt. Geopolitieke spanningen en gebeurtenissen met maatschappelijke impact zijn vaak aanleidingen voor aanvallen in het digitale domein. Daarnaast zal de nieuwe Europese richtlijn voor netwerk- en informatiebeveiliging (NIB2) tot gevolg hebben dat het aantal doelgroepen van het NCSC zal toenemen. Dat heeft voor het NCSC als gevolg dat er veel meer nieuwe doelgroepen met dreigingsinformatie bediend moeten worden dan tot nu toe het geval was.

Om aan deze vraag te kunnen voldoen, zal ons team meer gaan samenwerken met internationale en commerciële organisaties. Er zal een sterker beroep op ons worden gedaan om onze informatie met meerdere partijen te delen. Daarvoor zullen we manieren moeten vinden om op grotere schaal vertrouwelijke informatie te kunnen delen met partijen voor wie dit relevant is. En natuurlijk zullen we zo goed mogelijk inzicht moeten geven in het huidige dreigingslandschap, zonder daarbij uit het oog te verliezen welke veiligheidsmaatregelen organisaties kunnen treffen om een specifieke dreiging het hoofd te kunnen bieden. De oorlog in Oekraïne is een goed voorbeeld van een situatie waar de vraag naar actuele dreigingsinformatie zeer groot was. Een vraag die maatschappelijk veel breder leefde dan alleen binnen de rijksoverheid en vitale sectoren.

'Heeft de oorlog in Oekraïne gevolgen voor mijn digitale veiligheid?' 'Welk soort digitale aanvallers zijn actief in mijn sector en wat zijn hun werkwijzen?' 'Mijn detectiesensor neemt een indicator waar op mijn netwerk. Word ik aangevallen?' Het NCSC bereidt zich voor op een toename van dit soort vragen en bouwt aan een effectievere en efficiëntere manier om te zorgen dat dreigingsinformatie op de juiste plekken terechtkomt.

Tegelijkertijd blijven de dreigingsanalisten, CTI-specialisten en de teamleiders van mijn team zich iedere dag enthousiast inzetten om de meest actuele dreigingsinformatie te publiceren en blijven wij graag met u samenwerken aan de digitale veiligheid van Nederland.

Referenties

(1) https://www.ncsc.nl/onderwerpen/oekraine-met-welke-digitale-aanvallen-moet-u-rekening-houden

(2) Ter aanvulling mbt. de andere twee soorten informatie in de kwadranten. Dreigingsinformatie op operationeel niveau biedt doorgaans specifieke en gedetailleerde inlichtingen op zeer korte termijn, expliciet gericht op organisaties en dreigingen. Als een dreiging acuut en concreet wordt, wordt de zaak binnen het NCSC vaak overgedragen naar het incident response team en nemen we zo snel mogelijk contact op met de (mogelijk) getroffen partijen. Dreigingsinformatie op strategisch niveau omvat met name inlichtingen over ontwikkelingen in digitale veiligheid die voor een langere termijn gelden en bruikbaar zijn voor een beleids- of bestuurslaag in een organisatie. Binnen het NCSC draagt het team CTI/DA jaarlijks bij aan het Cybersecuritybeeld Nederland, een voorbeeld van een strategisch informatieproduct.

(3) https://www.youtube.com/watch?v=bZoceLpruDQ