# GEBRUIK VAN DREIGINGSINFORMATIE VOORKOMT SUCCESVOLLE CYBERAANVALLEN


*Visualisatie van Cyber Threat Intelligence in het TNO CTI Lab op de HSD campus*

TNO innovation for life

Cyberaanvallen zijn aan de orde van de dag en ze worden steeds heviger en professioneler. Overheden, bedrijven en de Nederlandse economie liggen onder vuur en lijden veel schade. Hoe eerder een cyberdreiging wordt ontdekt, des te minder schade een aanval kan toebrengen, bijvoorbeeld aan computersystemen, intellectueel eigendom en imago. Preventie, monitoring en incident respons alleen zijn niet meer genoeg. Een nieuw antwoord is nodig. In het recent geopende Cyber Threat Intelligence Lab (CTI Lab) experimenteert TNO met nieuwe technologieën en het ontwikkelen van innovatieve oplossingen.

“Veel organisaties houden hun netwerk al nauwlettend in de gaten en ondernemen actie als ze iets verdachts zien”, vertelt Richard Kerkdijk, cybersecurity expert bij TNO. “Dit is een goede maar erg reactieve aanpak. Met cyber threat intelligence (CTI) willen we een stuk van het initiatief herwinnen. Door dreigingsinformatie te analyseren krijgen organisaties bijvoorbeeld inzicht in de werkwijze van hackergroepen en in de kenmerken van specifieke soorten malware. Dit stelt hen in staat om in een vroeg stadium te anticiperen op cyberdreigingen en schade aan hun systemen te voorkomen.”

## PIONIEREN

CTI is een relatief nieuw werkveld, dat volgens Annemarie Zielstra, directeur Cyber Security & Resilience bij TNO, nog in de kinderschoenen staat. “Er wordt door organisaties veel gepionierd en er zijn nog veel onbeantwoorde technische en organisatorische vragen, en ook de menskant heeft aandacht nodig. Aangezien het belang van cyber threat intelligence steeds groter wordt in het bestrijden van cyberaanvallen, heeft TNO besloten om speciaal voor dit onderwerp een ecosysteem in te richten op de HSD campus: het CTI Lab.” In dit ecosysteem komen publieke en private partijen bij elkaar om als partners bestaande kennis uit te wisselen en nieuwe kennis te ontwikkelen. Deze krachtenbundeling geeft volgens Zielstra een boost aan de doorontwikkeling van CTI én aan de ontwikkeling van cybersecurityproducten. “Enerzijds wordt Nederland digitaal een stuk veiliger als gezamenlijk cyber threat intelligence wordt verzameld, geanalyseerd en gedeeld. Anderzijds ontstaat door het omzetten van kennis naar cybersecurity-innovaties en -producten een sterke Nederlandse cybersecurity-industrie. Betrouwbare producten van

eigen bodem zijn goed voor de nationale veiligheid en het biedt enorme economische kansen op de wereldmarkt."

## AANVALLEN VÓÓR ZIJN

ING is een van de pioniers op het gebied van CTI. Toen de grote DDoS-aanvallen op de Nederlandse banken begonnen, heeft ING een Cyber Crime Expertise & Response Team (CCERT) opgericht. Dit team verzamelt en deelt informatie wereldwijd binnen ING, alarmeert de organisatie bij dreigingen, lost problemen op en borgt geleerde lessen. Volgens Vincent Thiele, manager CCERT, is het belangrijk dat een cyber threat intelligence-team een verbinding heeft met en nauw aansluit bij de bedrijfsprocessen en business. "Met CTI willen we aanvallen vóór zijn. Dat betekent dat iedereen binnen onze organisatie een verantwoordelijkheid heeft om signalen door te geven aan ons CCERT, maar andersom moet ons team relevantie informatie, dreigingen en oplossingen weten te vertalen naar de businessprocessen of naar een specifiek IT-systeem. Dan ben je het meest effectief." Cyber threat intelligence heeft betrekking op operationeel, tactisch en strategisch niveau, zegt Thiele. "Daarom is die vertaling zo belangrijk. En dat er goede analyses worden gemaakt. Dan ben je relevant voor iedereen in de organisatie en word je oordeel vertrouwd." Hoewel ING voorloper is op CTI, valt er nog genoeg te ontwikkelen. "We willen beter worden in 'threat hunting', actief jagen op dreigingen, wereldwijd: en dan snel ons beveiligingsbeleid daarop aanpassen. Hiervoor maken we gebruik van de expertise van TNO."

## THREAT MANAGEMENT

"Het gebruik van dreigingsinformatie – cyber threat intelligence – biedt een organisatie de mogelijkheid om de eigen resources gericht en gefocust in te zetten in een snel veranderend dreigingslandschap." Dat zegt Joep Gommers, CEO EclecticIQ. Zijn technologisch platform brengt informatiebronnen bij elkaar en helpt de dreigingsinformatie te analyseren. Net als Vincent Thiele van ING legt hij de nadruk op de vertaalslag van CTI naar de organisatie. "Naast het rode – dreigings – verhaal, is ook het blauwe – organisatie – verhaal belangrijk. Een CTI-team moet de business van interne stakeholders begrijpen en in dat licht dreigingen op waarde kunnen schatten. Een Security Operations Center heeft een andere behoefte dan de board die strategisch wil sturen." CTI maakt volgens Gommers threat management binnen organisaties mogelijk. "Het is een geïntegreerd proces, dat de onzekerheid en risico's van dreigingen vermindert door gerichte preventie, detectie en beveiligingsmaatregelen, om zo cyberaanvallen voor te zijn."

## THREAT INDEX

In het rapport 'De economische en maatschappelijke noodzaak van meer cybersecurity' schrijft Herna Verhagen, CEO PostNL, dat "de samenwerking tussen overheid en bedrijfsleven op het gebied van cybersecurity moet worden verstevigd en geïnstitutionaliseerd. Informatie-uitwisseling op het gebied van ongeoorloofd gebruik, kwetsbaarheden in systemen, criminaliteit of spionage in de digitale wereld moet worden bevorderd." Dat is volgens Zielstra precies wat het CTI Lab doet voor cyber threat intelligence. Als voorbeeld noemt zij het project 'Cyber Trend Watch'. In dit project worden informatiebronnen gekoppeld en geanalyseerd, en vervolgens worden daar kwetsbaarheden uitgehaald. Die krijgen een score mee, waardoor er een threat index ontstaat. Deze index geeft via een rangschikking aan welke kwetsbaarheden prioriteit hebben en als eerste opgelost moeten worden. "Dit proces wordt in het CTI Lab uitgedacht, ontwikkeld en getest. We willen machine learning hier nog aan toe gaan voegen, zodat het proces sneller, geautomatiseerd en slim verloopt met een hoge betrouwbaarheidsfactor."

## UITDAGINGEN

CTI is een instrument om aan de voorkant te komen van het cybercrime-bestrijdingsproces en cyberaanvallen te voorkomen. Omdat het nog relatief nieuw is, zijn er nog veel onbeantwoorde vragen. Want welke informatiebronnen zijn relevant voor een specifieke organisatie? Hoe beoordeel je de kwaliteit van die bronnen? Wat zijn de criteria om dreigingen te labelen en te prioriteren? In hoeverre valt het verzamel- en analyseproces te automatiseren? Waar bestaat een efficiënte CTI-workflow uit? Hoe wordt CTI ingebed in de organisatieprocessen? Hoe vertaal je dreigingsinformatie naar alle niveaus en afdelingen in de organisatie? Welke vaardigheden hebben CTI-analisten nodig? Hoe analyseer je big data? "Zeer relevante vragen, waarnaar we onderzoek doen in het CTI Lab", vertelt Zielstra. "Partners die deel willen nemen aan onderzoeken, testen en demonstraties nodigen we uit om contact met ons op te nemen. Als we de handen ineenslaan, kunnen we cyber threat intelligence doorontwikkelen en tot nieuwe innovaties komen."

### VERSCHIL TUSSEN CTI, SOC EN CERT

Security Operations Centers zijn vaak preventief gericht op detectie van afwijkend gedrag op het eigen netwerk. Computer Emergency Response Teams richten zich vooral op het oplossen van problemen als zich een incident voordoet. Beiden zijn veelal reactief en gericht op de eigen organisatie. Het CTI-team is naar buiten gericht en kijkt welke actuele dreigingen relevant zijn voor de organisatie.

**TNO.NL**

CONTACT
TNO Cyber Security & Resilience zet kennis en technologie in om innovaties te creëren op het gebied van cyber die de veiligheid van de samenleving versterken.

Tjarda Krabbendam
E tjarda.krabbendam@tno.nl
T 088 866 09 12
I www.tno.nl/cybersecurity