PERSBERICHT | *Den Haag, 21 december 2016*

“Cyberdreigingsinformatie nieuw antwoord op cyberaanvallen”

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. Preventie, monitoring en incident respons alleen zijn niet meer genoeg. Een nieuw antwoord is nodig. TNO laat vandaag tijdens de opening van het Cyber Threat Intelligence Lab zien hoe organisaties met slimme innovaties vroegtijdig kunnen anticiperen op cyberdreigingen en cyberaanvallen.

Hoe eerder een cyberdreiging wordt ontdekt, des te minder schade een aanval kan toebrengen aan computersystemen. TNO experimenteert in het Cyber Threat Intelligence Lab (CTI Lab) met nieuwe technologie. Zo onderzoekt TNO samen met partners bijvoorbeeld hoe cyberaanvallen in een vroeg stadium ontdekt en afgeweerd kunnen worden. Hierbij wordt gebruik gemaakt van een technologisch platform van EclecticIQ, dat cyberdreigingsinformatie uit allerlei open en gesloten online bronnen verzamelt. De big data-analyse die daarop volgt, levert inzicht in relevante cyberdreigingen op. Dat stelt organisaties in staat om daarop te anticiperen en extra veiligheidsmaatregelen te nemen. “Door het slim verzamelen en analyseren van dreigingsinformatie ben je de aanvaller een slag voor”, aldus Annemarie Zielstra, directeur Cyber Security & Resilience bij TNO. “En als je de dreigingsinformatie ook nog eens deelt, word je met elkaar een stuk weerbaarder. Onderzoek naar vertrouwelijke gegevensuitwisseling wordt een belangrijk onderdeel van het CTI Lab”.

Schade voorkomen

“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 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.” CTI is volgens Kerkdijk nog wel een relatief nieuw werkveld waarin veel wordt gepionierd. Daarom doet TNO onderzoek op het vlak van mens, proces en technologie, omdat deze alle drie onmisbaar zijn voor het effectief gebruikmaken van cyberdreigingsinformatie. “Het CTI Lab helpt ons om samen met andere partijen te innoveren en CTI verder door te ontwikkelen.”

Digitaal veilig

Het nieuwe CTI Lab helpt TNO vergaande automatiseringsoplossingen te vinden voor het verzamelen, analyseren en delen van cyberdreigingsinformatie. En het helpt bij het ontwikkelen van een effectief werkproces binnen organisaties. Daarnaast doet TNO onder andere onderzoek naar relevantie en kwaliteit van informatiebronnen, big data-analyse, visualisatie van cyberdreigingen en benodigde competenties van te werven CTI-experts. Tijdens de opening spreekt Ingrid van Engelshoven, wethouder gemeente Den Haag, de verwachting uit dat het CTI Lab een broedplaats zal zijn van veel innovaties. “Vernieuwing is nodig om digitale veiligheid te realiseren. Dat vraagt om een plek om te pionieren en samenwerking aan te gaan. Alleen dan boeken we succes. Dat TNO kiest voor The Hague Security Delta als locatie voor het CTI Lab, maakt de kans van slagen groot. Het is de toegangspoort tot de beste kennis op het gebied van cybersecurity en TNO voegt daar de eigen kwaliteit aan toe."