Cyber attacks are very much the order of the day and they are becoming more severe and more professional. Governments, businesses and the Dutch economy are under attack and suffer a lot of damage as a result of cyber crime. The sooner a cyber threat is detected, the less damage an attack can cause, for example to computer systems, intellectual property and reputation. Prevention, monitoring and incident response alone are no longer enough – a new solution is needed. In the recently opened Cyber Threat Intelligence Lab (CTI Lab), TNO is experimenting with new technologies and developing innovative solutions.

“Many organisations are already monitoring their network closely and take action if they see anything suspicious,” says Richard Kerkdijk, cybersecurity expert at TNO. “Although this is a good approach, it is very reactive. We want to regain the initiative through cyber threat intelligence (CTI). By analysing threat information, organisations can gain insight into, for example, the methods hacker groups use and the characteristics of specific types of malware. This allows organisations to anticipate cyber threats early on and prevent damage to their systems.”

PIONEERING STAGE

CTI is a relatively new field which, according to Annemarie Zielstra, Director of Cyber Security & Resilience at TNO, is still in its infancy. ‘Organisations are doing a lot of pioneering in this field and there are still many unanswered technical and organisational questions. You have to consider the human aspect too. Given the increasing importance of cyber threat intelligence in fighting cyber attacks, TNO has decided to set up an ecosystem specially designed for this topic at the HSD campus: the CTI Lab.’ It is an ideal ecosystem for public and private parties to work in partnership on sharing existing knowledge and developing new knowledge. According to Zielstra, this joining of forces will boost further development of CTI as well as the development of cyber security products. ‘Firstly, the Netherlands will be much safer digitally if we can jointly collect, analyse and share cyber threat intelligence.

Secondly, by converting knowledge into cyber security innovations and products, we can create a strong Dutch cyber security industry. Reliable homegrown
products are good for national security and offer real economic opportunities in the global market.’

**PREVENTING ATTACKS**

ING is one of the pioneers in the field of CTI. When the major DDoS attacks on the Dutch banks started, ING set up a Cyber Crime Expertise & Response Team (CCERT).

This team collects and shares information globally within ING, alerts the organisation to cyber threats, solves problems and builds lessons learned into future practice. According to Vincent Thiele, manager of CCERT, it is important that a cyber threat intelligence team has a connection with and is aligned to the organisation and its business processes. ‘We want to pre-empt attacks with CTI. That means that everyone in the organisation has a responsibility to notify our CCERT of warning signs, and at the same time our team must be able to translate relevant information, threats and solutions to the business processes or to a specific IT system. This is the most effective strategy.’ Thiele: ‘Cyber threat intelligence impacts at the operational, tactical and strategic levels. This is why translating that information into actionable intelligence – and making proper analyses – is so important. This way you become relevant to everyone in the organisation and your judgement is trusted.’ Although ING is a frontrunner in CTI, there is still a lot to develop and improve. ‘We want to get better at “threat hunting”: actively hunting for threats worldwide and rapidly adapting our security policies accordingly. To do this, we rely on TNO’s expertise.’

**THREAT MANAGEMENT**

‘Applying cyber threat intelligence gives an organisation the ability to deploy its own resources in a targeted and focused way in a rapidly changing cyber threat landscape,’ explains Joep Gommers, CEO of EclecticIQ. His technology platform brings together information sources and helps analyse the information on threats. Like Vincent Thiele of ING, he emphasises translating CTI into actions that benefit the organisation. ‘In addition to the “red” threat narrative, the “blue” organisational narrative is also important. A CTI team must understand the business of internal stakeholders and be able to accurately assess the threats to their business. A Security Operations Centre has different needs than a Board that is focused on strategic planning and management.’ According to Gommers, CTI makes threat management within organisations possible. ‘It is an integrated process that reduces the uncertainty and risks of threats through targeted prevention, detection and security measures aimed at pre-empting cyber attacks.’

**THREAT INDEX**

In a report called ‘The economic and social necessity of more cyber security’ (‘De economische en maatschappelijke noodzaak van meer cybersecurity’) Herna Verhagen, CEO of PostNL, writes that ‘cooperation between government and industry in the field of cybersecurity needs to be strengthened and institutionalised.

We must encourage information exchange on unauthorised use, vulnerabilities in systems, and crime or espionage in the digital world.’ According to Zielstra, that is exactly what the CTI Lab does for cyber threat intelligence. As an example, she cites the Cyber Trend Watch project, where information sources are linked and analysed, and any vulnerabilities found are identified. These are then given a score, which generates a threat index. This index indicates, through a ranking of vulnerabilities, which ones have priority and have to be resolved first. ‘This process is being devised, developed and tested in the CTI Lab. We want to add machine learning to this so that we have a fast, smart and automated process with a high reliability factor.’

**CHALLENGES**

CTI gives organisations a leg up in the fight against cyber crime and in the prevention of cyber attacks. Because it is still relatively new, there are still many unanswered questions. Which sources of information are relevant to a specific organisation? How do you assess the quality of those sources? What are the criteria for labelling and prioritising threats? To what extent can the collection and analysis process be automated? What does an efficient CTI workflow consist of? How is CTI embedded in the organisational processes? How do you translate threat intelligence to all levels and departments in the organisation? What skills do CTI analysts need? How do you analyse big data? ‘These are highly relevant questions which we are researching at the CTI Lab,’ says Zielstra.

‘Partners who wish to participate in research, testing and demonstrations are invited to contact us. By working together, we can further develop cyber threat intelligence and come up with new innovations.’

**THE DIFFERENCE BETWEEN SOC, CERT AND CTI**

Security Operations Centres (SOC) are often focused on preventive detection of abnormal behaviour on their own network. Computer Emergency Response Teams (CERT) tend to focus mainly on solving problems in the event of an incident. Both are mostly reactive and have an internal focus on the organisation. The CTI team has an external focus aimed at identifying current threats that are relevant to the organisation.