Fight cyberattacks to water infrastructure with STOP-IT tools

At the beginning of February 2021, a hacker attempted to elevate the amount of sodium hydroxide in the water to dangerous levels at a drinking water treatment plant in Florida, taking advantage of old software and poor password habits. And this is just one attack in the long line of cyber- or physical attacks since then.

Are our critical water infrastructures are safe and adapting to the ever-growing cyber and physical risks and threats and the growing digitalization?

The European research project STOP-IT has developed a number of tools to meet those kind of risks and threats but in particular three tools that could detect an attack such as it happened in Florida.

The Real-Time Anomaly Detector (RTAD) on cyber-physical infrastructures uses machine learning and signature-based detection of abnormal behaviours within the network. It provides an additional layer of security by detecting potential threats from the logs of the system. The tool is composed of three main components: a security Big Data platform, machine learning algorithms, and signature-based rules.

The Cross Layer Security Information and Event Management (XL-SIEM) receives events coming from different sources to generate correlated alarms that indicate the risk level, and detailed information about the event (description, IP source and destination, Port source and destination, Protocols). The tool can perform automatic countermeasures or generate tickets for further investigation. It provides enhanced capabilities to address storage limitations, correlation, performance and visualization issues, enabling a reduced reaction time

The Network Traffic Sensors and Analysers (NTSA) incorporates five categories of sensors able to identify different malicious patterns such as TTL-based attacks, brute force attacks, DNS answer attacks, time-based attacks, and domain-based attacks. The Network Traffic Sensors and Analysers go one step beyond of traditional anomaly detection systems based on pattern and regular expressions analysis, by using well-known machine learning mechanisms: One-class Support Vector Machine (One-class SVM) to identify abnormal behaviour in the traffic capture based on a multi-featured approach that restricts the analysis to a modelled IP address and extended in terms of samples (valid and invalid ones).

Find out more about the STOP-IT tools on our website.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740610.