Greater readiness repels cyber threats to manufacturers

December 14 2016

Together with the National Emergency Supply Agency and the private sector, VTT Technical Research Centre of Finland has developed tailored solutions bringing improved cyber security and disruption-free operations to manufacturers. The results of the now ending KYBER-TEO project will make companies more able to ward off possible cyber threats.

A breach of cyber security could easily cause millions of euros of damage in terms of lost production alone. In addition, damaged equipment, environmental contamination and personal injuries could occur. At worst, the problem could affect the whole of society.

The testing and project results of the KYBER-TEO project (2014-2016), led by VTT Technical Research Centre of Finland, have improved the ability of manufacturers to e.g. purchase cyber-secure automation systems and develop their own concepts, instructions and practices for ensuring cyber security and operational continuity.

"In the case of every company, the cyber security of the tested systems was developed even further and in a better direction," says Principal Scientist, Pasi Ahonen of VTT. "Hopefully, the companies have also learned how to identify information security vulnerabilities or gaps in their systems."

For example, VTT's closed Cyber War room helped participants to develop managed, authentic cyber security testing, as well as cyber

training which they can pass onto customers. Such training includes exploring the attitudes of cyber attackers, and identifying and repulsing attacks.

The National Emergency Supply Agency, which is the main customer of the overall project, aims to develop cyber security for automation, particularly from the perspective of security of supply in Finland.

"Various types of automation are being implemented at an accelerating pace within a range of environments which are critical to security of supply, from manufacturing to transport and housing," says Sauli Savisalo, a Director at the National Emergency Supply Agency. "Broad-based development of the security of automation is critically important."

As part of the overall project, a small-scale, online cooperation forum on automation-system cyber security was developed. Such a forum would be desirable as a way of deepening confidential communication in the future.

Service companies can now provide manufacturers with more-tailored cyber security services. The results may also support the activities of the organisations covered by the security of supply principle.

The industrial pioneers and cyber security service providers participating in the overall project can seek further support, when necessary, from e.g. The National Cyber Security Centre Finland of the Finnish Communications Regulatory Authority (FICORA).

The participating companies included e.g. Nordic LAN&WAN Communication Oy, Prosys PMS Ltd, Nixu Corporation, Insta DefSec Oy, Schneider Electric Finland Oy and Neste Oyj.

Manufacturers can defend themselves against cyber

attacks as follows:

- Greater awareness and training of employees in relation to cyber security
- Clear internal guidelines and policies
- Taking account of cyber security during the automation system procurement stage, by e.g. presenting the related requirements
- Monitoring the status of the automation network
- Defining and implementing secure remote-access concepts
- Defining and implementing a secure network architecture
- Cyber security testing of automation systems (particularly system vendors)

Provided by VTT Technical Research Centre of Finland