Press release
English

March, 17th 2014

To secure the Industrial Control Systems SCADA
Conclusion of an international workshop in Luxembourg

Within the EU project CockpitCI: "Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructure", itrust consulting and CREOS, under the patronage of Étienne Schneider from the Ministry of Economy and Foreign Trade, organised the 3rd CockpitCI Workshop on "SCADA Cybersecurity" at Creos' national dispatching centre on March 10th.

This workshop enabled the European Agency for cyber security, Luxembourgish authorities (Ministry of Economy, GOVCERT.LU, HCPN), the national electricity and gas provider CREOS and other Luxembourgish industrial attendees as well as the project partners including the security consultancy and research company itrust consulting, the CRP Henri Tudor from Luxembourg, the project coordinator Selex ES from Italy, Romanian operators, and researchers from Italy, Portugal, Great Britain, Israel, Norway and Belgium to discuss the problems and solutions concerning the security of critical infrastructures.

The workshop also gave itrust consulting the chance to present two pieces of new software that were developed by the organization during the project: AVCaesar and Software Checker.

Nowadays, Critical Infrastructures (CI) like electricity, gas or water distribution systems have become a target of cyber-attacks. The European research project CockpitCI which started two years ago, aims to create a framework and tools enabling the detection, analysis, and real time information sharing of cyber-attacks in order to assess risks and avoid disastrous cascading effects. The research experiment (Aurora) and recent attacks (Stuxnet, Duqu, Red October) have shown that all these networks and underlying industrial systems are potentially under real and critical threats and that only an improved and global awareness and supervision approach will keep these infrastructures, which are vital for the functioning of European organisations and industrial sectors, in a secure state or at least partially operational in the event of an attack. It is imperative to design systems which allow operators to assess the operational risks of QoS (Quality of Service) degradation and to implement the suitable containment and treatment strategies.

In his introduction, Dr Carlo Harpes, Managing Director of itrust consulting, referred to the famous novel "Blackout" by Mark Elsberg, which describes the consequences of a cyber-attack shutting down the entire electrical supply of Europe: This fictitious novel is based upon solid investigations on the functioning of the European electrical grid and its present vulnerabilities. The book describes the impossibility of detecting the causes and sources of the problem quick enough and shows that the measures to prepare the population for the coming disaster have been insufficient. Dr Harpes underlined the importance of the new security standards in this domain (the IEC 62442 standard family) and also of the importance of communicating risks between CI professionals and being prepared in order to react effectively in case of an attack.

Mr François Thill of the Ministry of Economy guaranteed the Ministry's support to all Luxembourgish initiatives focused on acquiring the necessary competencies in order to protect the electricity, gas and water supply against malicious attacks.

Carlo Bartocci, responsible of Creos' dispatching, spoke about technical problems encountered during the migration of their current controlling system. The improved performance of supervision systems makes them increasingly more complex and thus it is more difficult to find errors (whether a simple technical incompatibility, or even worse; a malware). This presentation highlighted why it is extremely important to protect SCADA networks from the open telecom network and the retracement of flux, by functional and security tests before changing and high level monitoring.

Adrian PAUNA, NIS expert at ENISA, presented several European initiatives: ERNCIP aimed at sharing knowledge to harmonise test protocols, the recommendations to use security certified products, and the recent project for cybersecurity skills certification of SCADA experts. He invited all experts to participate in their ICS SCADA Expert Group.

Paul Rhein, Haut-Commissariat à la Protection National (HCPN), presented Luxembourg's governmental actors in cybersecurity, like the CERTs, and their coordination bodies. A new law should increase the importance of cybersecurity and crisis preparedness, as a reaction to the fear expressed by the EU commissioner Neelie Kroes that "self-regulation does not work here".

In the second part of the workshop, Antonio Graziano from Selex ES, Italy, presented the CockpitCI project. He compared the cyber threats on control systems with an F16 jet attacking a WW1 battlefield. The CockpitCI system under construction should be a decision making system in passive mode; detecting, analysing and managing cybersecurity risk in real time. Prof Paulo Simões, University of Coimbra (Portugal), explained the detection architecture: In a distributed network, probes bring information from IT networks, Operator networks, and Field networks through correlators to the Security Management Platform. These probes or detection agents consist of intrusion detection systems, fieldbus honeypots, software and configuration checkers, etc. Prof. Stefano Panzieri, University of Roma Tre, illustrated the On-Line Risk Prediction System. He discussed interdependency models, knowledge bases with countermeasures, risk assessments, etc., to process the detected information. If needed, his system alerts and proposes counter-measures to the control centre through a so-called Cockpit. Prof. Michele Minichino, ENEA Italy, illustrated the underlying models established in CockpitCI for an electrical grid. Prof Leandros Malgaras from the University of Surrey (UK) presented a tool for the consolidation of detection information based on "One Class Support Vector Machines".

Finally, itrust consulting demonstrated for the first time two tools it has developed under CockpitCI: **AVCaesar**, a meta-antivirus that combines several antivirus programs that perform an in-depth scan of any document exchange between a SCADA network and the local IT network (often linked to the internet). This tool can also be used by security incident analysis teams in order to scan and pre-analyse suspicious files.

The second tool is called **Software Checker**. After installation on several machines that are connected to the same network, Software Checker informs the server integrated in the CockpitCI of the installed software and key elements of the configuration. This is an essential element for defining the vulnerability level and even for the detection of installed malware.

In the after-workshop-discussion, the participants discussed the importance of developing complementary competencies which enable the detailed analysis of sophisticated cyber-attacks. itrust consulting, which is operating the first private CSIRT (Computer Incidence Response Team) in Luxembourg, "malware.lu CERT" and which is in partnership with CIRCL and GOVCERT.LU is motivated to assist control system operators in this challenge.

For more information about the MICIE project or the results of the workshop, please visit the website www.cockpitci.eu or directly contact Carlo Harpes, harpes@itrust.lu.