A l'attention des rédactions / To editors

De la part de:	Claudine Weber
Téléphone:	+352 267 6212
Fax:	+352 26 710 978
E-mail:	Info@itrust.lu
Nombre de pages:	2

Communiqué de presse
Français

17 mars 2014

Cybersecurity de Système de contrôle SCADA
Bilan d'un workshop international au Luxembourg

Dans le cadre du projet Européen CockpitCI « Cybersecurity on SCADA : risk prediction, analysis and reaction tools for Critical Infrastructure », itrust consulting et CREOS, sous le patronage du Ministère de l'Économie et du Commerce extérieur, Étienne Schneider, ont organisé, ce 10 mars 2014 au centre de dispatching de CREOS, le 3e CockpitCI workshop intitulé "SCADA Cybersecurity".

Ce workshop a été l'occasion pour les participants, Agence Européenne de 'cyber-sécurité, autorités luxembourgeoises (Ministère de l'Économie, GOVCERT, HCPN), CREOS gestionnaire luxembourgeois de réseaux d'électricité et de gaz , industriels luxembourgeois invités et partenaires du projet, comme itrust consulting (société de conseil et de recherche en sécurité), le CRP Henri Tudor, le coordinateur du projet Selex ES d'Italie, l'opérateur d'électricité roumain, ainsi que des chercheurs italiens, portugais, anglais et belges, de s'échanger sur la sécurité des infrastructures critiques, tant au niveau des problématiques que des solutions envisageables.

L'événement fut aussi l'occasion pour itrust consulting de présenter pour la première fois deux logiciels développés dans ce projet : AVCaesar et Software Checker.

Aujourd'hui, les infrastructures critiques, comme les réseaux électriques, d'eau, de gaz, ne sont pas à l'abri des menaces de piratages informatiques. Le projet de recherche européen CockpitCI démarré il y a 2 ans, vise à concevoir un cadre et des outils permettant de détecter, d'analyser et d'échanger en temps réel des informations sur des cyberattaques, afin d'en évaluer les risques et d'éviter les effets redoutés de domino. Les expérimentations (Aurora experiment) et récentes attaques (Stuxnet, Duqu, Red October) ont montré que les différents réseaux et les systèmes industriels de contrôle sous-jacents (souvent appelé SCADA, acronyme pour Supervisory Control And Data Acquisition) sont potentiellement menacés et que seules une vigilance et une supervision accrue et globale permettront de mettre en sécurité ces infrastructures indispensables au bon fonctionnement des institutions et de secteurs vitaux européens. Il est donc essentiel que les opérateurs puissent rapidement identifier les risques potentiels à la qualité de service, afin de mettre en place des mesures de prévention et de confinement d'une attaque.

Dans son introduction, Dr Carlo Harpes, gérant d'itrust consulting s'est référé au fameux roman de Mark Elsberg, «Blackout», décrivant les conséquences d'une cyberattaque conduisant à l'arrêt total de l'approvisionnement en électricité dans toute l'Europe : « Ce roman fondé sur des investigations solides portant sur le fonctionnement du réseau électrique européen et sur ses vulnérabilités actuelles, raconte l'impossibilité pour les autorités de détecter rapidement les causes du problème et de mettre en place les réactions adéquates pour préparer la population au désastre qui l'attend ». Une telle histoire souligne l'importance des nouveaux standards de sécurité dans ce domaine, la famille des normes IEC 62442, et surtout la nécessité pour les professionnels du secteur de communiquer sur les risques et de mettre en place des stratégies de réaction efficaces pour réagir en cas d'attaque.

M. François Thill du Ministère de l'Économie, second orateur, a mis en exergue le soutien du ministère aux initiatives des acteurs luxembourgeois visant à acquérir les compétences nécessaires pour protéger les réseaux d'approvisionnement en électricité, en gaz, et en eau, de tout acte malveillant.

M. Carlo Bartocci, responsable du Dispatching de Creos, a dressé un tableau très réaliste sur quelques problèmes techniques vécus lors de la migration actuelle de leur système de contrôle vers les nouvelles technologies. Les

nouveaux systèmes de supervision, aux performances améliorées, deviennent de plus en plus complexes, et trouver une erreur, qu'elle émane d'un simple problème d'incompatibilités techniques ou pire, d'une origine malicieuse, devient une tâche de plus en plus ardue. D'où l'importance de mettre en place des stratégies de sécurité, comme le cloisonnement du réseau SCADA par rapport au réseau télécom ouvert, comme le traçage des flux, les tests fonctionnels et tests de sécurité avant toute modification, et in fine d'assurer un monitoring efficace et précis.

M. Adrian PAUNA, expert en sécurité des réseaux auprès de l'ENISA a présenté quant à lui les initiatives européennes en la matière : ERNCIP (European Reference Network for Critical Infrastructure Protection) visant à partager des informations pour harmoniser les protocoles de tests, les diverses actions destinées à encourager l'utilisation de systèmes certifiés, et enfin un futur projet de certification des compétences en matière de cybersécurité des experts SCADA. Il a invité tous les experts présents à participer au groupe d'experts ICS-SCADA.

M. Paul Rhein du Haut-Commissariat à la Protection National (HCPN) a présenté les acteurs luxembourgeois, comme les CERT publiques, et les organes de coordination. Une nouvelle loi devrait donner plus d'importance à la sécurisation et à la préparation aux crises, en réaction aux craintes exprimées récemment par le commissaire européen Neelie Kroes que «l'autorégulation ne fonctionne pas ici».

Lors de la seconde partie du workshop, Antonio Graziano de Selex ES (Italie), a présenté le projet CockpitCI. Il a comparé les nouvelles menaces SCADA à la menace qu'aurait fait peser une attaque d'un avion de chasse F16 sur un champ de bataille de la Première Guerre mondiale. Le système CockpitCI, encore au stade de prototype, devrait offrir, en mode passif, un système d'aide à la décision qui détecte, analyse et gère le cyber-risque en temps réel. Faisant suite à cette vision générale, le Prof Paulo Simões de l'Université de Coïmbra (Portugal), a expliqué l'architecture de détection mise en place. Cette dernière est fondée sur des sondes réparties dans les divers réseaux, réseau IT, réseau de contrôle, réseau opérationnel, qui permettent de remonter l'information via des corrélateurs à la centrale de gestion de la sécurité. Ces sondes ou agents de détection sont constitués de systèmes de détection d'intrusion, de fieldbus honeypots, de software checker, antivirus, etc. Les éléments détectés sont alors utilisés comme le Prof Stefano Panzieri de l'Université de Roma Tre a présenté. Cet outil de prédiction, «On-Line Risk Prediction System» utilise des modèles sophistiqués d'interdépendance, des bases de connaissances sur les menances, des appréciations de risques,… Le système devrait alerter ou proposer des contre-mesures. La connaissance des impacts possibles d'attaques spécifiques sur les réseaux étant une donnée essentielle, le Pr Michele Minichino, du laboratoire italien de recherche ENEA, a donné un aperçu des modèles de simulation de gestion des fautes de réseaux électriques, en fonctionnement normal ou lors d'une attaque (contamination virale). Prof Leandros Malgaras, de l'Université de Surrey (UK), a présenté un outil spécifique d'analyse des informations issues des sondes de détection et fondé sur des algorithmes de type « One Class Support Vector Machines » permettant d'obtenir des données de détection consolidées à partir d'un nombre très important de données.

Finalement, itrust consulting a montré pour la première fois deux outils développés pour CockpitCI: AVCaesar, un meta-antivirus permettant de combiner plusieurs logiciels antivirus destinés à analyser en profondeur tout fichier échangé entre un réseau SCADA et un réseau local IT, qui est souvent connecté à l'internet afin de mesurer leur dangerosité et afin de transmettre les fichiers à des organisations de veille sécuritaire comme des CERT privé ou public. Cet outil est aussi destiné aux équipes d'analyse d'incidents de sécurité pour scanner et pré-analyser un grand nombre de fichiers suspicieux. Le deuxième outil est appelé Software Checker. Une fois installé sur un grand nombre de machines d'un réseau, il informe via son serveur intégré dans CockpitCI des vulnérabilités des logiciels installés et des éléments clés de la configuration. C'est là un élément essentiel au Cockpit pour établir le niveau de vulnérabilité, voire même pour détecter des malware installés.

Lors de la discussion qui a suivi, les participants ont souligné l'importance de créer des pôles de compétences spécifiques, complémentaires aux réactions automatiques, afin d'être en mesure d'analyser en profondeur des cyberattaques complexes. itrust consulting qui opère le premier CERT privé au Luxembourg, le malware.lu CERT et qui agit en partenariat avec les CIRCL et GOVCERT.LU est motivée à prendre à son compte ce défi et à assister les opérateurs de système de contrôles.

Pour de plus amples informations sur le projet CockpitCI (www.cockpitci.eu) ou les résultats du workshop, merci de contacter Carlo Harpes, harpes@itrust.

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 the Ministry of Economy and Foreign Trade, Étienne Schneider, organised at Creos' national dispatching centre on March 10th the 3rd CockpiCI Workshop on "SCADA Cybersecurity".

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 invitees 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.

It also gave itrust consulting the opportunity to present for the first time two softwares that it has developed during this 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 allowing to detect, to analyse, and to share in real time information on cyber-attacks in order to assess risks and avoid disastrous cascading effects. The research experiment (Aurora experiment) 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 allow keeping these infrastructures, which are vital for the functioning of European organisations and industrial sectors, in a secure state or at least partially operational and prevent a total shutdown in case 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 in Europe: « This novel, thank God it's fictive, is based upon solid investigations on the present functioning and the present vulnerabilities. It describes the impossibility to detect the causes and sources of the problem quick enough and shows that the reactions in order 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 first of all the importance of the communication concerning risks between CI professionals and the importance to be prepared in order to react effectively in case of an attack.

Mr François Thill of the Minsitry of Economy guaranteed his support to the initiative of Luxembourgish actors acquiring the necessary competencies in order to protect the electricity, gas and water supply against any malicious attack.

Carlo Bartocci, responsible of Creos' dispatching, informed on technical problems encountered during the migration of their current controlling system. The supervision systems, in addition to improved performances, becomes more and more complex and it becomes difficult to find errors, whether a simple technical incompatibility, or in a worse

case, a malware. That is why it is extremely important to protect the 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 European initiatives: ERNCIP aiming 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 the Luxembourg governmental actors in cybersecurity, like the CERTs, and their coordination bodies. A new law should increase the importance of cybersecurity and crisis preparedness, as 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, presents the CockpitCI project. He compared the cyber threats on control systems with an F16 jet attacking a WW1 battle field. 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, illustrates the On-Line Risk Prediction System. He recurs to 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 permits to combine several antivirus softwares that perform an in depth scan of any document exchange between a SCADA network and the local IT network, which is often linked to internet. This tool should also be used by security incident analysis teams in order to scan and preanalyse lots of suspicious files.

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

In the after-workshop-discussion, the participants encouraged the creation of complementary competencies for automatic reactions in order to analyse possible sophisticated cyber-attacks in depth. 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 assist control system operators in their 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