19/12/2011

www.enisa.europa.eu

Sécurité des Systèmes de contrôle industriels : recommandations pour l'Europe est les États-membres

L'ENISA, l'Agence Européenne de cyber-sécurité, a publié aujourd'hui les résultats d'une étude sur la sécurité des Systèmes de contrôle industriels (SCI). Le rapport décrit la situation actuelle de la sécurité des SCI et propose sept recommandations pour l'améliorer.

Les *Systèmes de contrôle industriels (SCI)* sont des réseaux de commande et de contrôle conçus pour soutenir les processus industriels. Ces systèmes sont utilisés pour surveiller et contrôler divers processus et opérations, tels que la distribution de gaz et d'électricité, l'eau, le raffinage du pétrole et le transport ferroviaire.

Au cours des dix dernières années, ces systèmes ont été victimes de plusieurs incidents notables. Ces derniers comprennent l'attaque "Stuxnet", qui est supposée avoir utilisé des logiciels malveillants pour cibler les systèmes de contrôle nucléaire en Iran, ainsi que la "nouvelle version" de ce logiciel malveillant DuQu. Ces incidents ont suscité de vives inquiétudes sur la sécurité parmi les utilisateurs des SCI.

En 2011, l'ENISA a travaillé sur les principales préoccupations concernant la sécurité des SCI et sur la création d'initiatives nationales, paneuropéennes et internationales sur la sécurité des SCI. Les parties prenantes impliquées incluent des dispositifs de sécurité des SCI et des fournisseurs de services, des fabricants de logiciels/matériels pour SCI, des opérateurs d'infrastructure, des organismes publics, des instances de normalisation, des universités et des services de R&D.

Ce rapport final propose sept recommandations pratiques et utiles pour les acteurs publics et privés du secteur des SCI, destinées à améliorer les initiatives actuelles et à développer la coopération. Les recommandations préconisaient la création de stratégies nationales et paneuropéennes sur la sécurité des SCI, un Guide des bonnes pratiques sur la sécurité des SCI, des activités de recherche, la mise en place d'un banc d'essai commun et des capacités de réponse aux urgences informatiques dans le secteur des SCI.

"Une sécurité réelle des Systèmes de contrôle industriels ne peut être obtenue qu'avec des efforts communs, caractérisés par la coopération, l'échange de savoir et la compréhension mutuelle de ***toutes*** *les parties prenantes impliquées"*, a affirmé Rafal Leszczyna, rédacteur du rapport.

Le Professeur Udo Helmbrecht Directeur Exécutif de l'ENISA a ajouté :

19/12/2011

www.enisa.europa.eu

"L'affaire *Stuxnet a mis en évidence le problème de la sécurité des systèmes de contrôles industriels. Notre étude montre que les parties prenantes ont encore beaucoup à faire dans ce domaine. Nous espérons que nos sept recommandations entraîneront des améliorations considérables.*"

Informations contextuelles : Afin d'améliorer la sécurité des SCI, en avril 2007, le Conseil de l'Union européenne a adopté le Programme européen pour la protection des infrastructures critiques (PEPIC). Le principal élément du PEPIC est la Directive sur l'identification et la nomination des Infrastructures critiques européennes. En parallèle, les problèmes liés à la sécurité des informations en Europe sont gérés par l'Agenda numérique pour l'Europe (ANE) et le Plan d'action CIIP. Les résultats de l'étude de l'ENISA ont été validés au cours d'un atelier à Barcelone, en septembre 2011.

Pour consulter l'intégralité du rapport, veuillez cliquer ici

Pour toute demande d'interview, veuillez contacter : Ulf Bergstrom, Porte-parole de l'ENISA, press@enisa.europa.eu, Portable : + 30-6948-460-143.

Veuillez noter: traduction. La version anglaise est la seule version officielle.

www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu