23/01/2014

EPR07/2014

www.enisa.europa.eu

# L'Agence de cybersécurité de l'UE (ENISA) estime que les Systèmes de contrôle industriels d'énergie, d'eau et d transport désuets et, dépourvus de contrôles de cybersécurité adéquats, doivent faire l'objet de tests de capacité coordonnés à l'échelle européenne.

**L'Agence de cybersécurité de l'UE (ENISA) a publié aujourd'hui un nouveau rapport proposant quelques recommandations sur les prochaines étapes envers la coordination de tests de capacités des Systèmes de contrôles industriels (ICS), souvent désuets, des industries européennes. Parmi les principales recommandations, l'évaluation des ICS figure comme l'une des préoccupations majeures des Etats Membres de l'UE. Elle pourrait être donc abordée à l'échelle européenne selon l'ENISA.**

La technologie de l'Informatique est de nos jours largement utilisée par les systèmes de contrôle industriels (ex.: SCADA) en matière d'énergie, d'eau et de transport. Cette technologie est utilisée pour améliorer l'efficacité, réduire les coûts et permettre l'automatisation des processus. Il est cependant regrettable que celle-ci s'accompagne souvent de mauvaise planification, de manque d'information, de configurations sécuritaires ainsi que d'inclusion de vulnérabilités « jour zéro » à la fois connues et nouvelles, non-découvertes ou non-corrigées dans les systèmes ICS/SCADA.
Les systèmes ICS peuvent durer plus de 20 ans. Ils ont donc toujours été conçus en tant que systèmes indépendants sans exigences de sécurité adéquates.
Par conséquent, ils ne sont pas préparés aux menaces courantes. Combattre les failles de sécurité actuelles exige une compréhension approfondie des questions de sécurité (ex. les vulnérabilités, leurs origines, leur fréquence, etc..). Une bonne évaluation nécessite des outils et des méthodologies spécialisées. L'Agence met l'accent sur l'importance d'une stratégie spécifique afin de définir les objectifs, la mission et la vision pour une Capacité de coordination des tests à l'échelle européenne.

L'étude analyse de quelle façon les actions de l'UE pourraient être coordonnées afin d'atteindre un niveau satisfaisant d'harmonisation, d'indépendance et de fiabilité des capacités d'évaluation de l'ICS, et pouvant de ce fait, influer sur les initiatives en cours. La méthodologie prend en compte la recherche informatique, un sondage en ligne et des interviews de fonds avec 27 experts de l'UE, des Etats-Unis, du Japon, de l'Inde et du Brésil.

**Quelques conclusions et recommandations clés**

Cette recherche a permis d'aboutir à 36 conclusions clés et 7 recommandations pour les secteurs public et privé, en mettant l'accent sur les organismes de l'UE :

- 1. La création d'une Coordination des tests de capacité sous une direction européenne publique et avec le soutien du public concerné, les autorités nationales et le secteur privé européen;
- 2. La mise en place d'un Conseil d'administration fiable et fonctionnel pour faire appliquer la direction;
- 3. La création ou l'implication de groupes de travail spécifiques ;
- 4. La définition d'un modèle financier adapté au contexte européen actuel ;

- 5. La réalisation d'une étude de faisabilité sur les méthodes d'organisation des évaluations ;
- 6. Etablir des accords de coopération avec d'autres organisations impliquées dans les questions de sécurité de l'ICS ;
- 7. La mise en place d'un programme de gestion des connaissances pour l'évaluation de l'ICS.

Le Professeur Udo Helmbrecht, Directeur exécutif de l'ENISA a fait remarqué que : « renforcer la sécurité des Infrastructures d'information critiques et du système ICS est une nécessité incontournable; les risques augmentent et les pirates très expérimentés ainsi que les désastres naturels ont montré les limites des systèmes. Tous les organismes privés et public impliqués doivent sérieusement aborder ces problèmes de sécurité. »

**Pour accéder au rapport complet :**
**Contexte :** Stratégie de l'UE en matière de cybersécurité
**Pour toute demande d'interviews, veuillez contacter :** Ulf Bergström, Porte Parole, ulf.bergstrom@enisa.europa.eu, Portable: + 30 6948 460 143, or Adrian Pauna, Expert, resilience@enisa.europa.eu

*Veuillez noter: traduction. La version anglaise est la seule version officielle*
*www.enisa.europa.eu/media/enisa-en-francais/*
*www.enisa.europa.eu*