La certification de sécurité des réseaux intelligents en Europe : défis et recommandations

L'agence ENISA publie aujourd'hui un rapport sur la certification de sécurité des réseaux intelligents en Europe à destination des Etats membres de l'Union Européenne, de la Commission européenne, des organismes de certification et du secteur privé. Il contient des informations sur les différentes démarches de certifications à travers l'UE et dans les pays de l'Association européenne de libre-échange (AELE). Il décrit la situation spécifique européenne, et présente les défis et avantages d'une pratique de certification mieux harmonisée.

Le rapport a pour objectif de soulever l'intérêt des experts en réseaux intelligents et le soutien des autorités de certification sur les questions ouvertes de la certification de sécurité dans les environnements de réseaux intelligents. Le besoin croissant de certification des réseaux intelligents vient du manque de contrôles sur la chaîne d'approvisionnement en énergie (câbles, panneaux solaires, éoliennes, etc.) introduit par l'automatisation des réseaux intelligents.

Udo Helmbrecht, Directeur Exécutif de l'ENISA, a commenté le projet : *« Les réseaux intelligents et les énergies renouvelables sont très prometteurs pour l'industrie européenne. La certification de sécurité est un outil important afin d'améliorer la confiance des utilisateurs envers la chaîne d'approvisionnement en énergie. Dans ce rapport, l'ENISA fournit des recommandations soutenant les autorités de certification en ligne avec leurs exigences de sécurité nationales, et ouvre la voie vers une meilleure harmonisation des pratiques européennes en matière de certification des réseaux intelligents ».*

Dans ce cadre, l'ENISA fournit les *dix* recommandations suivantes aux Etats Membres et à la Commission européenne :

1. La Commission européenne devrait nommer un comité de pilotage afin de coordonner les activités de certification des réseaux intelligents
2. Le comité de pilotage de l'UE devrait fournir des conseils et un schéma de référence afin de mettre en œuvre une chaine de confiance
3. Le comité de pilotage de l'UE devrait mettre en œuvre un exercice de cartographie parmi les standards et systèmes disponibles utilisés dans l'UE
4. Le comité de pilotage devrait promouvoir la reconnaissance internationale de systèmes tels que le SOG-IS
5. Le comité de pilotage devrait promouvoir une validation correspondant à l'appétit pour le risque impliqué dans chaque cas d'utilisation d'un réseau intelligent

6. Le comité de pilotage devrait faciliter la flexibilité afin de mettre à jour les profils de protection afin qu'ils puissent faire face aux menaces de sécurité actuelles en constante évolution

7. Les Etats Membres devraient utiliser des profils nationaux comme spécifications détaillées des standards internationaux pour couvrir les cas d'utilisations nationales spécifiques ainsi que les test et méthodes de certification soutenues

8. La Commission européenne devrait demander aux comités techniques de créer des profils européens, en collaboration avec les associations européennes du secteur de l'énergie

9. Le comité de pilotage de l'UE devrait encourager la fourniture d'outils à l'égard du cadre de certification proposé, alors que les comités techniques nationaux devraient fournir des outils d'évaluation préalables pour des schémas spécifiques

10. La Commission européenne et les Etats Membres devraient promouvoir la conformité et l'harmonisation en tant qu'avantage économique et mesure de réduction des coûts

Le rapport s'appuie sur les résultats d'un séminaire sur la certification de sécurité des composants de réseaux intelligents organisé en 2012 par la DG-CNECT et l'ENISA à Bruxelles. Le message clef est que l'Europe a besoin de davantage d'harmonisation des pratiques de certification de sécurité des réseaux intelligents, comme moyen de diminuer les coûts de certification. En outre, le rapport est le résultat d'une consultation avec des experts de la certification de sécurité des réseaux intelligents, et a été validé par des experts en sécurité à l'occasion d'un séminaire organisé à Heidelberg en Septembre 2014.

Pour le rapport entier, consultez https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/smart-grid-security-certification/

Pour toute demande, contactez Dr. Konstantinos Moulinos, Officier en Sécurité et Résistance des Réseaux de Communication, ENISA, Expert en sécurité des réseaux et de l'information, ENISA, **Email:** Konstantinos.Moulinos@enisa.europa.eu , **Tél:** +30 2814409629.