11/10/2011

www.enisa.europa.eu

L'ENISA, l'agence de cyber-sécurité de l'UE, lance un guide expliquant comment établir des partenariats public-privé (PPP) efficaces pour la sécurité des systèmes d'information

Un nouveau guide contenant 36 recommandations expliquant comment établir des partenariats public-privé efficaces pour la sécurité des systèmes d'information résilients a été publié aujourd'hui par l'ENISA, l'agence de cyber-sécurité de l'UE

Dans l'ensemble de l'UE, l'infrastructure critique de la plupart des États-membres est entre les mains du secteur privé. Par conséquent, l'industrie et les gouvernements doivent collaborer pour fournir à la fois aux citoyens et aux entreprises un accès sécurisé et fiable aux systèmes. En Europe, les infrastructures critiques de l'information (CII) sont fragmentées, non seulement géographiquement, mais aussi en raison de la concurrence entre les différents opérateurs de télécommunication.

Augmenter la résilience des CII est donc fondamental pour l'Europe. Pour répondre à ce besoin, les partenariats public-privés (PPP) ont évolué pour protéger l'économie numérique dans de nombreux États-membres, à des moments différents et selon des cadres juridiques différents. Grâce à cette évolution naturelle signifie, il n'existe pas de définition commune de ce que constitue un PPP. Dans un monde où les menaces à l'encontre des infrastructure ne respectent pas les frontières nationales, le nouveau guide sur les PPP de l'ENISA, l'agence européenne chargée de la sécurité des réseaux et de l'information, contient 36 recommandations expliquant comment établir efficacement un PPP et souligne le besoin d'une compréhension commune à travers l'Europe. Cela est particulièrement important pour le partenariat public-privé européen pour la résilience (EP3R), une initiative de l'Union européenne qui assure la liaison avec les PPP nationaux sur les problèmes de protection des infrastructures critiques de l'information (CIIP).

Le Professeur Udo Helmbrecht, Directeur Exécutif de l'ENISA, a déclaré : « *Il existe le besoin d'une approche globale véritablement internationale vis-à-vis de la cyber-sécurité et de la protection des infrastructures critiques de l'information. Aucun pays ne peut créer de stratégie de CIIP de façon isolée, car les frontières nationales n'existent pas dans le cyberespace. Les PPP font donc partie de l'agenda du Groupe de travail spécial sur la cyber-sécurité et la cybercriminalité formé par l'UE et les États-Unis.*»

Taxonomie des PPP

Le guide de l'ENISA classifie les PPP en matière de sécurité et de résilience en trois catégories : **PPP axés sur la prévention, PPP axés sur la réaction et PPP**

parapluies. Le guide consolide et valide une taxonomie des PPP et révèle cinq éléments principaux à prendre en considération :

- **Pourquoi un PPP devrait être créé ? (portée/menaces)**
- **Qui doit être impliqué ? (couverture géographique/focalisation, liens interdépendants)**
- **Comment un PPP doit-il être régi ?**
- **Quels services et mesures incitatives doivent être proposés ?**
- **Quand un PPP doit-il être créé et autres questions de temporisation ?**

Ces résultats proviennent de 30 questionnaires et de 15 entretiens approfondis avec des acteurs des secteurs à la fois public et privé représentant vingt pays. En outre, le guide décrit et représente graphiquement des PPP des **États-Unis, du Canada et d'Australie**, identifiant les facteurs de réussite essentiels pour le partage de l'information, ainsi que des façons d'encourager la collaboration internationale.

Cliquez ici pour le rapport complet

Informations contextuelles : Communication de la Commission européenne sur la CIIP et l'EP3R

Pour tout demande d'interview, veuillez contacter : Ulf Bergstrom, Porte-parole de l'ENISA, press@enisa.europa.eu, Portable : + 30-6948-460-143, ou Lionel Dupre, Spécialiste de l'ENISA, lionel.dupre@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