10/09/2010

www.enisa.europa.eu

L'Agence de l'Union européenne identifie les incitations et les défis du partage des informations sur la cyber-sécurité en Europe.

L'Agence de cyber sécurité de l'Union européenne, l'ENISA, c'est-à-dire l'Agence européenne chargée de la Sécurité des réseaux et de l'Information, a lancé un nouveau rapport sur les barrières et les incitations pour le partage des informations sur la cyber-sécurité. Le rapport montre par exemple que les incitations économiques sont beaucoup plus importantes pour les praticiens du secteur que ce que la littérature théorique indique.

L'importance du partage des informations pour la protection des Infrastructures critiques de l'information - CIIP- est largement reconnue par les décideurs, ainsi que par les communautés techniques et celles des praticiens du secteur. L'Agence a réalisé des recherches sur les groupes P2P (poste à poste), par exemple les Echanges d'informations (IE) et les Centres d'Analyse de Partage des Informations (ISAC). Le rapport identifie les barrières et les incitations les plus importantes dans la pratique journalière dans les IE et ISAC pour la CCIP. Cette recherche est différente des autres rapports car elle est concentrée sur les expériences des praticiens du secteur. La documentation provient de trois sources, analyse de la littérature, interviews, et un exercice «Delphi» en deux temps avec des professionnels de la sécurité.

Beaucoup de barrières et d'incitations identifiées dans la littérature sont de faible importance pour les praticiens du secteur et les responsables de la sécurité travaillant dans le domaine des Echanges d'informations. La « véritable » liste des incitations pour les praticiens du secteur est plutôt : incitations économiques (par exemple économies de coûts), incitations de qualité, valeur et utilisation des informations partagées. Les principales barrières au partage des informations sont les informations de mauvaise qualité, une mauvaise gestion et/ou les risques sur la réputation.

L'Agence a mis au point 20 recommandations destinées à différents public cibles, par exemple:

- ✓ Les Etats Membres doivent établir une plateforme nationale de partage des informations et coopérer avec les autres Etats Membres.
- ✓ Le secteur privé doit être plus transparent dans le partage des informations, et améliorer les mesures de préparation basées sur les informations échangées.

- ✓ Les organismes de recherche et les universités doivent quantifier les avantages et les coûts de participation aux plateformes, et réaliser des recherches basées sur des études de cas pour voir où les attaques auraient pu être évitées, ou leur impact atténué.
- ✓ Les Institutions de l'Union européenne et l'ENISA doivent établir une plateforme paneuropéenne de partage des informations pour les Etats Membres et les parties prenantes privées. Le Partenariat européen Public Privé de la Commission de l'Union européenne pour la Résilience (EP3R) est la principale initiative dans ce domaine.

Le Directeur Exécutif de l'ENISA, le Dr. Udo Helmbrecht, a déclaré:

« Le partage des informations est la pierre angulaire pour améliorer la protection des infrastructures critiques de l'information – CIIP, qui est fondamentale pour l'économie et les communications de l'Europe au sein de l'Europe. »

Contexte : Pour obtenir le rapport complet, y compris toutes les recommandations: http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange

Pour les interviews : veuillez contacter le Dr. Evangelos Ouzounis, Expert Senior -Politiques de sécurité des Réseaux : resilience-policies@enisa.europa.eu ou Ulf Bergstrom, Porte-parole, ENISA, press@enisa.europa.eu, Mobile : + 30-6948-460143

Traduction. La version anglaise est la seule version officielle.