Le Directeur Exécutif de l'ENISA défend devant le Parlement Européen une approche équilibrée de la confidentialité en ligne avec un secteur européen des TIC fiable

"Le défi pour les responsables politiques est de mettre en place une approche équilibrée de la confidentialité, avec un impact minime sur les intérêts des citoyens et du secteur privé", a déclaré Udo Helbrecht, Directeur Exécutif de l'ENISA, à un sommet du Parlement Européen à Bruxelles. La conférence, organisée conjointement par le Comité des Libertés Civiles et la Présidence Luxembourgeoise du Conseil de l'Union Européenne, co-présidée par les Comités IMCO et ITRE, a débattu de la protection de la vie privée en ligne, à travers le renforcement de la sécurité des TIC et des capacités informatiques de l'UE.

L'ENISA s'est réjoui de discussions spécifiques concernant l'adoption de technologies renforçant la confidentialité, la riposte face aux vulnérabilités des logiciels, des matériels et des infrastructures informatiques, ainsi que du développement d'un secteur des TIC fort et dynamique dans l'Union Européenne. L'ENISA espère que la conférence aura un effet stimulant dans le débat politique lié à ces thèmes complémentaires.

Les technologies renforçant la confidentialité, la standardisation et la certification: bases du secteur des TIC

L'utilisation de technologies renforçant la vie privée en ligne, telles que la confidentialité par choix, font partie de l'offre TIC garantissant une plus forte protection tout en restant compatible avec les fonctionnalités de sécurité standard. De plus, les recommandations de l'UE qui concernent le développement de logiciels et matériels sûrs, telles que la standardisation et la certification, qui sont également conçues par l'ENISA, peuvent être promues et appliquées à travers l'UE comme un moyen de répondre aux vulnérabilités.

L'introduction de l'Internet des Objets est un exemple qui démontre l'importance accrue de ces dernières puisque ce phénomène entraine des défis de sécurité qui peuvent être partiellement atténués du point de vue de la résilience des réseaux. Cependant, l'imbrication de l'Internet des Objets et des composantes logicielles et matérielles introduit davantage de risques et de menaces. De ce point de vue, certaines composantes de l'architecture Internet jouent un rôle important. Par conséquent, il est important d'établir un échange de l'information autour des incidents et vulnérabilités ainsi qu'un dialogue parmi les acteurs qui peuvent construire une approche concertée de la sécurité.

Les Etats Membres ont développé des mesures spécifiques pour protéger les piliers critiques de l'infrastructure des TIC de l'UE. Le nouvel accord sur la directive NIS participe d'une coopération de tous les acteurs et secteurs dans la réponse aux défis de sécurité et d'infrastructure digitale (que ce soient les secteurs de l'énergie, la santé, des transports ou de la finance) afin d'assurer un haut degré de sécurité pour les systèmes essentiels, les infrastructures et les citoyens. L'ENISA possède une large expérience dans ces domaines. A travers son expérience, des mécanismes de coopération ont été développés (à travers les CSIRT et la série d'exercices Cyber Europe) qui autorisent les autorités compétentes, avec le secteur privé, à répondre aux incidents (article 13a, TSP) [1]. « Nous espérons pouvoir continuer à améliorer et renforcer notre collaboration dans cette direction » a déclaré Udo Helmbrecht.

L'ENISA met en lumière la valeur ajoutée du marché de la cyber sécurité

Dans ce débat, la valeur ajoutée générée par la cyber-sécurité, qui pourrait atteindre 640 milliards d'euros[2] pour l'économie européenne, a été mise en avant. Le marché de la cyber sécurité est sous-développé en

Europe, avec une valeur estimée à 20 milliards d'euros et un taux de croissance annuel composé de 6%. Ce qui importe, c'est que l'UE parvienne à établir une cyber confiance parmi les citoyens et l'industrie afin de créer un secteur des TIC européen compétitif, renforçant ainsi davantage la position de l'UE.

Pour de plus amples informations sur le sujet et pour les demandes de presse, merci de contacter

press@enisa.europa.eu, Tel.+30 2814 409576

Pour de plus amples informations sur la conférence du Parlement Européen, merci de visiter:

http://www.europarl.europa.eu/committees/en/libe/events.html?id=20151208CHE00191
http://www.stoa.europarl.europa.eu/stoa/cms/home/events/workshops/privacy

1 TSPs (Trust Service Providers). ENISA propose un nouveau schéma de déclaration pour TSP. Article 13a: Art. 13a, de la directive 2009/140 EC, fait partie du Télécom Package et vise à assurer la sécurité et l'intégrité des réseaux de communications électroniques et les services (télécoms). Dans ce domaine, l'ENISA a la responsabilité de la collecte des incidents, des mesures prises au sein des secteurs de télécommunications des Etats membres, et de contribuer à «l'harmonisation des mesures techniques appropriés et a l'organisation des mesures de sécurité en fournissant des conseils d'experts» et par «la promotion de l'échange des meilleures pratiques".
2 Risk and Responsibility in a Hyperconnected World –World Economic Forum
3 Cyber-security market size in Europe – Gartner 2014