L'ENISA salue l'accord des institutions européennes sur la première directive applicable dans l'ensemble de l'UE relative à la cyber-sécurité et au rôle étendu de l'agence

Après de longues négociations, les institutions européennes sont enfin parvenues à un accord. Celui-ci doit aider les États membres à atteindre un haut niveau de sécurité dans les domaines des réseaux et de l'information qui soit cohérent dans toute l'UE, et qui ouvre la voie à une collaboration plus importante entre ces pays.

La directive prévoit également de renforcer le rôle de l'ENISA en lui attribuant de nouvelles missions de grande importance. L'ENISA considère cet accord comme une étape majeure dans la sécurisation des infrastructures informatiques dans l'UE.

L'ENISA salue l'accord sur la prochaine directive SRI : elle constitue une étape majeure dans les améliorations à apporter à la SRI dans l'UE. Pour cela, la directive SRI prévoit un nombre concret de mesures, dont les plus importantes sont les deux mécanismes de coopération entre les États membres, à savoir le réseau d'Équipes d'intervention en cas d'incident informatique (réseau CSIRT, Computer Security Incident Response Team) devant être coordonné par l'ENISA, et le « groupe de coopération », composé de représentants des autorités nationales compétentes, de la Commission européenne et de l'ENISA. Les États membres doivent également désigner une autorité nationale chargée de traiter les questions de SRI.

Les autres mesures importantes sont la nécessité d'établir une stratégie nationale de cyber-sécurité, et l'obligation pour les entreprises travaillant dans des secteurs sensibles comme l'énergie, le transport, la finance et d'autres, d'informer les autorités nationales en cas d'incident ayant un impact significatif.

Udo Helmbrecht, Directeur exécutif de l'ENISA, a déclaré à propos de cet accord : *« S'assurer de la disponibilité, de l'intégrité et de la confidentialité des infrastructures sensibles et numériques représente un vaste défi pour les acteurs publics et privés. L'ENISA accueille ces nouvelles missions liées à la mise en œuvre de la directive SRI, et continuera d'aider les États membres de l'UE et le secteur privé à améliorer leurs ressources et leur coopération en matière de cyber-sécurité, afin de mettre en œuvre la directive SRI, ce en conformité avec les objectifs du MUN.*

Contexte

La directive relative à la sécurité des réseaux et de l'information (SRI) était la principale proposition législative contenue dans la stratégie européenne 2013 de cyber-sécurité. La stratégie de cyber-sécurité de l'UE consiste en un document de politique publié par la Commission européenne, et détaillant un certain nombre d'étapes que la Commission européenne doit suivre dans le domaine de la cyber-sécurité, dans le cadre notamment d'une coopération entre les États membres, les acteurs privés et publics. Le Parlement doit approuver le texte de l'accord le 17 décembre, et le Conseil le 18 décembre. Les pays de l'UE disposent ensuite de 21 mois pour transposer la directive dans le droit national.

Réseau CSIRT : depuis 2005, l'ENISA gère un réseau d'équipes d'intervention nationales et gouvernementales en cas d'incident informatique, qui a ainsi permis d'instaurer une confiance entre les membres, mais aussi d'échanger des informations.

L'ENISA fournit une assistance aux experts en cyber-sécurité publics et privés de l'UE et les aide à prévenir et à réagir aux crises à venir. L'ENISA organise notamment régulièrement des exercices de crise auxquels prennent part plusieurs centaines de participants. Ces exercices permettent de former les experts, de renforcer la coopération entre eux et de fournir des conseils sur les bonnes pratiques. De plus, l'agence dispense des formations spécialisées sur la gestion de crise, la planification

de crise ou l'élaboration d'exercices. Elle a également réalisé plusieurs études et organisé des conférences internationales sur la coopération en cas de cyber-crise. Le matériel de formation à la cyber-sécurité de l'ENISA a été présenté pour la première fois en 2008, et a depuis été complété et remanié. Ce matériel contient l'essentiel des informations nécessaires pour que les membres du réseau CSIRT puissent mener à bien leurs missions, mais aussi pour garantir la sécurité opérationnelle.

Exercices : depuis 2010, l'ENISA organise 2 fois par an un cyber-exercice à l'échelle européenne : Cyber Europe. Le prochain évènement de ce type aura lieu en 2016.

Article 13a, SCADA-ICS, SNCS : l'ENISA a accompagné les autorités nationales compétentes dans la mise en place d'une approche harmonisée de déclaration en cas d'incident lié aux télécommunications (connu comme l'article 13a du paquet Télécom) et aux prestataires de service de confiance (article 19 de eIDAS). L'agence aide également les États membres de l'UE à développer des Stratégies Nationales de Cyber-Sécurité (SNCS). L'ENISA a par ailleurs élaboré une liste de bonnes pratiques destinées à de nombreux secteurs et services sensibles (par ex. les smart grids, SCADA/ICS, cloud, eHealth, IdO).

Pour plus d'informations sur ce sujet et pour tout contact presse, veuillez contacterpress@enisa.europa.eu, **tél**. +30 2814 409576