Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

2017/0225(COD) - 30/07/2018 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport d'Angelika NIEBLER (PPE, DE) sur la proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité).

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition de la Commission comme suit.

Rôle et le mandat de l'Agence: l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information devrait être renforcée afin i) d'atteindre un niveau élevé de cybersécurité, ii) d'éviter les **cyberattaques** dans l'Union; iii) de **réduire la fragmentation du marché intérieur** et d'améliorer son fonctionnement; et iv) d'assurer la cohérence en tenant compte des résultats obtenus par les États membres en matière de coopération dans le cadre de la directive relative à la cybersécurité («directive SRI »).

L'Agence devrait **respecter les compétences des États membres** en ce qui concerne la cybersécurité, en particulier les compétences relatives à la sécurité publique, à la défense et à la sûreté de l'État, et les activités de l'État dans les domaines du droit pénal.

Les principales missions de Agence consisteraient, entre autres, à:

- soutenir **la coopération, la coordination et le partage d'informations** au niveau de l'Union entre les États membres, les institutions, organes et organismes de l'Union et les parties prenantes concernées, sur les questions liées à la cybersécurité;
- promouvoir des projets contribuant à un **niveau élevé d'hygiène informatique et d'habileté numérique** des particuliers et des entreprises aux questions liées à la cybersécurité;
- **sensibiliser en permanence le public** aux risques liés à la cybersécurité, y compris en favorisant l' éducation, et fournir, à l'intention des particuliers, des organisations et des entreprises, des orientations sur les bonnes pratiques à adopter par les utilisateurs;
- aider les États membres et les institutions de l'Union à mettre en place de **politiques de divulgation coordonnée des vulnérabilités** et des procédures d'examen des divulgations de vulnérabilités par les acteurs gouvernementaux, dont les pratiques et les conclusions devraient être transparentes et soumises à un contrôle indépendant;
- faciliter la mise en place et le lancement d'un **projet européen à long terme** sur la sécurité des technologies de l'information afin de soutenir le développement d'une industrie de la sécurité informatique indépendante à l'échelle de l'Union;
- soutenir la **coopération opérationnelle** entre les États membres, les institutions, les agences et organes de l'Union et entre les parties prenantes en évaluant les systèmes nationaux existants, en élaborant et en mettant en œuvre un plan et en utilisant les instruments appropriés pour atteindre le niveau le plus élevé de certification en matière de cybersécurité dans l'Union et dans les États membres;

- contribuer à l'élaboration d'une **réaction concertée au niveau de l'UE** en cas d'incidents ou de crises transfrontières de cybersécurité majeurs, principalement en soutenant la gestion technique des incidents ou des crises à l'aide de son expertise indépendante et de ses propres ressources;
- organiser au moins **une fois par an**, des exercices de cybersécurité à l'échelle de l'Union.

Organisation et capacités: les députés suggèrent que l'ENISA renforce davantage ses propres capacités et compétences techniques pour être en mesure d'apporter un soutien adéquat à la coopération opérationnelle avec les États membres. À cette fin, l'Agence devrait **renforcer progressivement son personnel** afin de pouvoir collecter et analyser de manière autonome les différents types d'un large éventail de menaces en matière de cybersécurité, procéder à des analyses scientifiques et aider les États membres à réagir aux incidents de grande ampleur. Elle devrait accroître ses capacités sur la base des ressources existantes dans les États membres, notamment en détachant des experts nationaux auprès de l' Agence, en créant des groupes d'experts ou encore des programmes d'échanges de personnel.

L'Agence devrait disposer d'un **groupe consultatif de l'ENISA** composé d'experts en sécurité reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des technologies de l' information des communications (y compris les PME), les opérateurs de services essentiels, les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, les organisations de consommateurs, les experts universitaires en matière de cybersécurité, les **organisations européennes de normalisation** (OEN) et les organes de l'Union.

Le groupe consultatif de l'ENISA devrait fixer les objectifs de son **programme de travail** et le rendre public tous les six mois pour en garantir la transparence.

L'Agence disposerait également d'un **groupe des parties prenantes pour la certification** pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs, le monde universitaire et les autres parties prenantes.

Système européen de certification de cybersécurité: les députés estiment que ce ne sont pas seulement les produits et services qui devraient être couverts par le règlement, mais **l'ensemble du cycle de vie**. Ainsi, les **processus** devraient également être inclus dans le champ d'application.

La certification devrait permettre:

- d'assurer la confidentialité, l'intégrité, la disponibilité et la confidentialité des services, des fonctions et des données;
- de veiller à ce que les services, fonctions et données puissent être consultés et utilisés uniquement par les personnes, systèmes et programmes autorisés;
- d'assurer que des processus soient mis en place pour identifier toutes les vulnérabilités connues et traiter les nouvelles;
- de faire en sorte que les produits, processus et services TIC soient sûrs par défaut et dès la conception;
- de réduire au maximum les autres risques liés aux incidents de cybersécurité, tels que les risques pour la vie humaine, la santé, l'environnement et d'autres intérêts juridiques importants.

Les députés ont suggéré une participation plus forte des États membres et de l'industrie au processus de certification.

L'Agence devrait tenir à jour un **site Web spécifique** fournissant des informations sur les systèmes européens de certification de cybersécurité, notamment les certificats retirés et expirés et les certifications nationales couvertes, et leur assurant une publicité.

Enfin, pour promouvoir l’acceptation généralisée des certificats et des résultats d’évaluation de la conformité délivrés par les organismes d’évaluation de la conformité, les députés ont proposé que les autorités nationales de contrôle de la certification fassent régulièrement l’objet d’un **examen par les pairs** rigoureux et transparent.