Conseil de
l'Union européenne

Bruxelles, le 21 juin 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

RÉSULTATS DES TRAVAUX

Origine:	Secrétariat général du Conseil
en date du:	21 juin 2022
Destinataire:	délégations
Nº doc. préc.:	9716/22
Objet:	Conclusions du Conseil sur le rapport spécial de la Cour des comptes européenne n° 05/2022 intitulé "Cybersécurité des institutions, organes et agences de l'UE: un niveau de préparation globalement insuffisant par rapport aux menaces" - Conclusions du Conseil, approuvées par le Conseil lors de sa session du 21 juin 2022

Les délégations trouveront en annexe les conclusions du Conseil visées en objet, approuvées par le Conseil lors de sa session du 21 juin 2022.

ANNEXE

CONCLUSIONS DU CONSEIL

sur le rapport spécial n° 05/2022 de la Cour des comptes européennes intitulé "Cybersécurité des institutions, organes et agences de l'UE: un niveau de préparation globalement insuffisant par rapport aux menaces"

LE CONSEIL DE L'UNION EUROPÉENNE,

RAPPELANT ses conclusions relatives à l'amélioration de l'examen des rapports spéciaux établis par la Cour des comptes dans le cadre de la procédure de décharge[1];

1. PREND NOTE du rapport spécial n° 05/2022 de la Cour des comptes européenne intitulé "Cybersécurité des institutions, organes et agences de l'UE: un niveau de préparation globalement insuffisant par rapport aux menaces"[2].

2. SOULIGNE l'importance et l'urgence de renforcer le niveau de cybersécurité au sein des institutions, organes et agences de l'UE, compte tenu de la récente intensification de la transformation numérique au sein des institutions, des informations sensibles traitées par ces dernières, ainsi que du nombre et de la gravité d'attaques qui ne cessent d'augmenter contre les institutions, organes et agences de l'UE et du niveau de la menace qui les touche.

3. RAPPELLE les conclusions du Conseil européen du 20 juin 2019[3], dans lesquelles le Conseil européen a invité les institutions de l'UE, ainsi que les États membres, à œuvrer à des mesures visant à renforcer la résilience et à améliorer la culture de sécurité de l'UE face aux menaces cyber et hybrides émanant de l'extérieur de l'UE, et à mieux protéger les réseaux d'information et de communication de l'UE, ainsi que ses processus décisionnels, contre les actes de malveillance de tout type.

---

1 Doc. 7515/00 + COR 1.
2 Doc. 8040/22.
3 Doc. EUCO 9/19.

4. RAPPELLE ses conclusions du 10 décembre 2019 sur les efforts complémentaires pour renforcer la résilience et lutter contre les menaces hybrides[4], dans lesquelles il a demandé aux institutions, organes et agences de l'UE de veiller, avec le soutien des États membres, à ce que l'Union soit en mesure de protéger son intégrité et de renforcer la sécurité de ses réseaux d'information et de communication et de ses processus décisionnels pour les protéger des activités malveillantes de tous types, sur la base d'une évaluation globale de la menace. À cet effet, le Conseil a déclaré dans ces conclusions que les institutions, organes et agences, soutenus par les États membres, devraient élaborer et mettre en œuvre un ensemble complet de mesures destinées à assurer leur sécurité, conformément au mandat du Conseil européen de juin 2019[5].

5. RAPPELLE ses conclusions du 22 mars 2021 sur la stratégie de cybersécurité de l'Union européenne pour la décennie numérique[6], dans lesquelles il a souligné que la cybersécurité est essentielle au fonctionnement de l'administration et des institutions publiques, tant au niveau national qu'au niveau de l'UE, ainsi que pour notre société et l'économie dans son ensemble.

6. RAPPELLE ses conclusions du 23 mai 2022 sur la mise en place d'une posture cyber de l'Union européenne[7], dans lesquelles les institutions, organes et agences ont été encouragés à participer à la cartographie des outils de communication sécurisée existants dans le domaine cyber, qui sera examinée au sein des instances compétentes du Conseil et avec les groupes de coopération concernés, tels que le réseau des CSIRT et le réseau UE-CyCLONe.

7. SOULIGNE qu'il est nécessaire de remédier au risque systémique inhérent à l'interconnexion entre les institutions, organes et agences de l'UE, ainsi qu'entre celles-ci et les institutions des États membres, et ceci en dépit de leur indépendance institutionnelle et de leur autonomie administrative.

---

4 Doc. 14972/19.
5 Doc. EUCO 9/19.
6 Doc. 6722/21.
7 Doc. 9364/22.

8. PREND NOTE des observations formulées dans le rapport spécial, à savoir que les institutions, organes et agences de l'UE n'ont pas atteint un niveau de préparation à la hauteur des menaces et ont des niveaux de maturité différents en matière de cybersécurité. EST CONSCIENT qu'il convient d'améliorer le niveau de préparation des institutions, organes et agences de l'UE en matière de cybersécurité, ainsi que les synergies entre eux.

9. ENCOURAGE ainsi vivement les institutions, organes et agences de l'UE à poursuivre la mise en œuvre de mesures de gestion des risques cyber qui assurent un niveau suffisant de cybersécurité, comme le prévoit la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148, afin d'améliorer leur niveau de préparation.

10. INVITE les institutions, organes et agences de l'UE à intensifier à la fois leurs efforts pour se protéger contre les menaces cyber, et leur coopération en ce qui concerne l'établissement de normes et de spécifications cohérentes, en particulier pour les marchés publics, les projets et les services liés à la cybersécurité, et à améliorer l'interopérabilité de leurs systèmes informatiques, y compris en vue d'assurer la communication sécurisée de contenu non classifié.

11. INVITE l'Agence de l'Union européenne pour la cybersécurité (ENISA) et l'équipe d'intervention en cas d'urgence informatique des institutions, organes et agences de l'UE (CERT-EU), dans le cadre de leurs compétences, à intensifier leur coopération pour soutenir les institutions, organes et agences de l'UE en matière de cybersécurité, en particulier en ce qui concerne le renforcement des capacités des institutions, organes et agences de l'UE qui ont un niveau de maturité différent en matière de cybersécurité.

12. PREND NOTE des conclusions et des recommandations du rapport spécial, et RECONNAÎT que le niveau de préparation des institutions, organes et agences de l'UE en matière de cybersécurité, ainsi que les synergies entre eux, devrait être considérablement amélioré. Les institutions, organes et agences de l'UE devraient disposer d'un cadre global de gestion des risques pour la sécurité informatique, procéder à des évaluations des risques et à des audits réguliers, sur la base d'une méthode commune ou bien connue et de normes internationales, et rendre systématiques les programmes de sensibilisation et de formation à la cybersécurité pour le personnel.

13. SOULIGNE également que les institutions, organes et agences de l'UE devraient allouer un budget suffisant pour garantir la mise en œuvre de mesures de protection contre les cybermenaces tout en respectant le cadre financier pluriannuel et PREND NOTE de la recommandation du rapport spécial selon laquelle une entité représentative de l'ensemble des institutions, organes et agences de l'UE devrait être nommée et dotée d'un mandat et des moyens appropriés, pour contrôler le respect des règles communes en matière de cybersécurité.

14. RECONNAÎT que le CERT-EU devrait être informé sans délai des cyber incidents importants des institutions, organes et agences de l'UE et, à cette fin, devrait être doté de ressources adéquates prévisibles et adaptées au niveau de menace actuel et aux besoins des institutions, organes et agences de l'UE notamment en matière de personnel, d'équipements techniques et d'infrastructures.

15. NOTE que la coopération et l'échange d'information en matière de cybersécurité, ainsi que l'interopérabilité des canaux de communication sécurisés entre les institutions, organes et agences de l'UE devraient être renforcés et systématisés. DEMANDE que cette coopération et cet échange d'information incluent aussi les autorités publiques responsables de la cybersécurité dans les États membres.

16. PREND NOTE des réponses de la Commission, de la CERT-EU et de l'ENISA qui accompagnent le rapport spécial.

17. INVITE la Commission à tenir compte des recommandations du rapport spécial et à se montrer ambitieuse lors de l'élaboration des politiques relatives à la cybersécurité des institutions, organes et agences de l'UE et à promouvoir pour davantage de synergies entre les institutions, organes et agences de l'UE.