Réponses du président du comité directeur du CERT-UE, du CERT-UE et de l'ENISA au rapport spécial de la Cour des comptes européenne sur la cybersécurité des institutions, organes et agences de l'UE

1. Synthèse

À la lumière de l'évolution constante du paysage des cybermenaces, la cybersécurité est devenue essentielle et de la plus haute importance pour les institutions, organes et agences de l'Union européenne (EUIBA), qui ont été de plus en plus ciblées par des cyberattaques très sophistiquées au cours des dernières années. Dans le cadre de leurs mandats, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) et l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'UE (CERT-EU) peuvent toutes deux apporter un soutien précieux aux EUIBA en matière de cybersécurité à différents niveaux. La proposition de règlement de la Commission européenne concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et agences de l'UE est un instrument clé dans ce contexte, un instrument que l'ENISA, le CERT-UE et le président du comité directeur du CERT-UE soutiennent fortement.

À cette fin, l'ENISA, le CERT-UE et le président du comité directeur du CERT-UE se félicitent du rapport spécial de la Cour des comptes européenne sur la cybersécurité des institutions, organes et agences de l'UE, qui arrive à point nommé pour aborder le niveau de préparation des EUIBA dans leur ensemble. Le rapport note clairement les rôles centraux que l'ENISA et le CERT-UE peuvent jouer dans ce domaine. Il souligne également le besoin de ressources supplémentaires et de mesures concrètes visant spécifiquement à améliorer la posture de cybersécurité des EUIBA.

Dans cette optique, l'ENISA, le CERT-UE et le président du comité directeur du CERT-UE soutiennent les observations et recommandations clés du rapport, qui sont également alignées sur les propositions législatives de la Commission européenne dans les domaines de la cybersécurité et de la sécurité de l'information pour les EUIBA.

Les commentaires figurant dans la section suivante visent à apporter des clarifications supplémentaires concernant certains domaines du rapport, en particulier en ce qui concerne

le travail pertinent déjà entrepris par l'ENISA et/ou le CERT-UE, ainsi que les mesures envisagées par l'ENISA et/ou le CERT-UE, en particulier dans les domaines du renforcement des capacités pour les EUIBA. En ce qui concerne les recommandations, l'ENISA et le CERT-UE acceptent la recommandation nº 3 (accroître l'accent mis par CERT-UE et l'ENISA sur les EUIBA moins avancés), qui s'adresse spécifiquement à ces deux entités.

2. Principales observations

L'ENISA et le CERT-UE soutiennent les observations clés établies par la Cour des comptes. Ceci étant dit, quelques clarifications supplémentaires sont fournies ci-dessous, en particulier en ce qui concerne les mesures existantes entreprises par l'ENISA et/ou le CERT-UE, ainsi que les plans qui ont déjà été établis pour les activités futures.

Paragraphe 49

En ce qui concerne la demande formelle envoyée par le Comité consultatif sur les technologies de l'information et des communications (ICTAC) au président du comité directeur du CERT-UE en vue d'obtenir des droits de vote au sein du comité, nous aimerions clarifier ce qui suit:

Étant donné les frais généraux considérables que la révision de l'arrangement interinstitutionnel actuel aurait entraînés et parce que les travaux en cours sur le «Règlement concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'Union» avaient déjà abordé la question de la représentation des agences décentralisées, il a été convenu de régler officiellement la question, dans une perspective à long terme, au moyen de ce règlement. D'ici là, comme l'a confirmé le président, les pratiques actuelles se poursuivront et les représentants de l'ICTAC seront toujours les bienvenus pour exprimer leurs points de vue et pour que ceux-ci soient pris en considération, dans toute la mesure du possible et en toute équité.

Paragraphe 66

À la fin de 2021, l'ENISA a établi un plan d'action pour les cyberexercices, qui inclut spécifiquement les EUIBA. Un plan d'action pertinent pour les formations destinées aux EUIBA sera fourni au premier trimestre 2022.

Encadré nº 3

Bien que cela ne soit pas explicitement mentionné en tant que résultats opérationnels, l'ENISA a fourni un soutien opérationnel à divers EUIBA et a coopéré avec eux sur la base de leurs demandes. Par exemple, en 2018, conformément à l'objectif 2.2. Soutenir la mise en œuvre des politiques de l'Union européenne:

- La Banque centrale européenne a demandé un soutien en vue du développement du cadre de test de l'équipe rouge EUROSystème.
- L'Agence de l'Union européenne pour la sécurité aérienne a demandé un soutien pour l'élaboration des objectifs du Centre européen pour la cybersécurité dans l'aviation, pour la sensibilisation à la cybersécurité et pour la mise en œuvre sectorielle de la directive SRI.
- L'Agence de l'Union européenne pour les chemins de fer a demandé un soutien pour la mise en œuvre de la directive SRI pour le secteur ferroviaire, en particulier un soutien pour la mise en place d'un centre sectoriel d'échange et d'analyse d'informations (ISAC) pour les gestionnaires d'infrastructure et les entreprises ferroviaires, ainsi que le renforcement des capacités (organisation de sessions de formation et de sensibilisation).
- L'ENISA a soutenu l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) dans ses efforts visant à améliorer ses compétences en matière de cybersécurité et de continuité de l'activité. Plus particulièrement, l'ENISA a apporté son expertise dans l'organisation d'exercices et l'élaboration de scénarios, et a offert la plateforme pour les exercices de cybersécurité de l'ENISA entièrement développée à l'eu-LISA afin d'organiser un exercice de préparation pour l'un des systèmes informatiques essentiels de l'Union européenne.

Par ailleurs, depuis 2019, l'ENISA dialogue activement avec les EUIBA (par exemple, l'ERA, l'AESM, l'AESA, l'ACER), à l'appui de la directive SRI, sur des activités sectorielles de renforcement des connaissances et de sensibilisation à la cybersécurité, ainsi que sur des initiatives politiques sectorielles connexes en matière de cybersécurité.

Paragraphe 71

L'ENISA a mis au point en 2021 et proposera en 2022 une formation spécialisée sur le thème «Comment mettre en place un programme de sensibilisation et utiliser des exercices de simulation» ciblant spécifiquement les EUIBA. Dans le cadre de leur coopération structurée, l'ENISA et le CERT-UE fourniront également des formations conjointes aux EUIBA en 2022.

Paragraphe 72

Il convient de noter que les exercices de cybersécurité de l'ENISA ont un vaste champ d'application et un large public, y compris les EUIBA. Cette approche permet de répondre également aux besoins des EUIBA, étant donné que ces derniers peuvent largement bénéficier de ces exercices avec les représentants des États membres. Il est à noter que l'ENISA fait participer le personnel technique de l'EUIBA en tant qu'acteurs dans les exercices «CyberEurope» depuis 2016, sous la direction du CERT-UE qui est le planificateur dédié de cette circonscription. Dans le prolongement de ces efforts, l'ENISA prévoit dans sa stratégie d'exercice 2022, dans le cadre d'activités de renforcement des capacités, de promouvoir un nouveau produit d'exercice qui sera fourni avec le soutien du CERT-UE, afin d'offrir aux EUIBA la possibilité d'être formés aux exercices d'auto-évaluation.

3. Conclusions et recommandations

L'ENISA et le CERT-UE acceptent la recommandation nº 3 (accroître l'accent mis par CERT-UE et l'ENISA sur les EUIBA moins avancés), qui s'adresse spécifiquement à ces deux entités.