RÉPONSES DE LA COMMISSION EUROPÉENNE

AU RAPPORT SPÉCIAL DE LA COUR DES COMPTES EUROPÉENNE

Cybersécurité des institutions, organes et organismes de l'UE: un niveau de préparation globalement insuffisant par rapport aux menaces

Table des matières

Le présent document expose, conformément à l'article 259 du règlement financier, les réponses de la Commission européenne aux observations d'un rapport spécial de la Cour des comptes européenne et sera publié en même temps que ledit rapport.

I. RÉPONSES DE LA COMMISSION EN BREF

a) Introduction générale

La cybersécurité est devenue une priorité politique et opérationnelle absolue pour la Commission européenne. La crise de la COVID-19 a intensifié notre dépendance aux services numériques (informatique en nuage, appareils mobiles, intelligence artificielle). Au cours des deux dernières années, nous avons observé une transition massive vers le travail à domicile. Cela signifie que la cybercriminalité et le cyberespionnage, les deux principales menaces auxquelles sont confrontés les institutions, organes et organismes de l'Union européenne, se sont aussi considérablement répandus en ligne. La Commission reconnaît cette tendance. En matière de cybersécurité, elle a fait preuve d'un leadership cohérent et déterminé. Le règlement sur la cybersécurité est entré en vigueur en 2019, et a notamment prorogé le mandat de l'ENISA tout en lui conférant un caractère durable. Ce règlement a également instauré une coopération formelle entre l'ENISA et la CERT-UE (l'équipe d'intervention en cas d'urgence informatique soutenant les institutions, organes et organismes de l'Union). En 2020, la Commission a proposé un renforcement de la directive sur la sécurité des réseaux et des systèmes d'information, qui est sur le point d'être approuvée par les législateurs.

La stratégie de cybersécurité adoptée en 2020 comprenait également trois actions relatives à la cybersécurité des institutions, organes et organismes de l'Union. La Commission a annoncé un règlement sur la sécurité de l'information dans les institutions, organes et organismes de l'UE, un règlement sur les règles communes de cybersécurité pour les institutions, organes et organismes de l'UE, et son intention de fournir une nouvelle base juridique à la CERT-UE afin de renforcer son mandat et son financement de manière à ce que cette dernière dispose de ressources suffisantes face à l'augmentation des menaces, risques et incidents.

Le travail préparatoire de ces propositions a progressé. Bien qu'elles n'aient pas encore été adoptées par le collège, elles devraient l'être pendant le premier trimestre de 2022. Au cours de cette phase préparatoire, les questions importantes faisant l'objet de discussions entre les institutions portent sur la base juridique de la proposition, ainsi que sur la capacité budgétaire des institutions, organes et organismes de l'UE à répondre aux exigences relatives au financement de leurs besoins en matière de cybersécurité, et à satisfaire celles liées à la recherche de ressources nécessaires pour soutenir la CERT-UE, le budget, et en particulier les postes.

Le niveau de préparation à la cybersécurité des institutions, organes et organismes de l'UE présente divers degrés de maturité. Plusieurs de ces entités sont très performantes en matière de préparation à la cybersécurité et devraient continuer à jouer le rôle de leader, en stimulant et en suscitant des progrès ainsi que de nouvelles améliorations dans l'ensemble du paysage de la cybersécurité. Afin de réaliser des progrès mesurables, il est important de reconnaître les niveaux de maturité variables au sein des institutions, organes et organismes de l'UE et de fixer des priorités en orientant les actions d'améliorations en premier lieu là où les lacunes recensées entraînent l'exposition au risque la plus élevée.

b) Position de la Commission sur les observations et recommandations essentielles de la Cour

La Commission accueille favorablement le rapport de la Cour des comptes européenne sur la cybersécurité des institutions, organes et organismes de l'Union. Elle note que le rapport souligne l'importance de cadres juridiques communs pour ces entités concernant la sécurité de l'information et la cybersécurité, destinés à améliorer le niveau global de cybersécurité dans tous les domaines. La Commission relève que les principales observations et recommandations de la Cour ne visent pas la cybersécurité opérationnelle de la Commission en soi, mais son rôle stratégique dans la proposition d'instruments législatifs visant à accroître la cybermaturité des institutions, organes et organismes de l'Union.

Les futurs règlements sur la sécurité de l'information au sein des institutions, organes et organismes de l'UE et sur les règles communes de cybersécurité pour les institutions, organes et organismes de l'UE fixeront les règles communes visant à atteindre des niveaux élevés de sécurité de l'information et de cybersécurité. Toutefois, leur mise en œuvre, dans le contexte organisationnel et opérationnel de chaque institution, organe et organisme de l'UE (en particulier, leurs profils de menace et de risque), restera sous la responsabilité autonome de ces entités. La proposition de règlement sur la cybersécurité disposera de mécanismes de mise en conformité appropriés et proportionnés à l'objectif et au champ d'application des nouvelles règles, sans préjudice de l'autonomie des institutions, organes et organismes.

La Commission préside actuellement le sous-groupe «cybersécurité» du Comité interinstitutionnel pour la transformation numérique (CITN), dont la présidence est tournante (pour une période pouvant aller jusqu'à deux ans). Il convient de noter qu'aucune ressource spécifique n'est allouée aux travaux du sous-groupe: toutes les actions sont fondées sur l'ensemble des efforts déployés par les participants sur une base volontaire.

La Commission approuve l'idée générale d'augmenter les ressources et de renforcer le mandat de la CERT-UE.

Dans cette optique, elle soutient les principales observations et recommandations du rapport. Notre position détaillée est expliquée dans les commentaires supplémentaires de la section III. En ce qui concerne les recommandations, la Commission accepte les recommandations nº 1, points a), b), c), d), e), f) et g), et nº 2, points a), b) et c).

c) Dernières évolutions et prochaines étapes

Une consultation formelle au niveau des directeurs généraux des institutions, organes et organismes de l'UE relative aux projets consolidés des deux règlements (sécurité de l'information, cybersécurité) a été menée, et l'évaluation des retours d'information recueillis est en cours, avant l'achèvement du train de mesures et l'adoption par le collège au cours du premier trimestre de 2022.

II. RÉPONSES DE LA COMMISSION AUX PRINCIPALES OBSERVATIONS DE LA COUR

1. Niveaux de maturité en matière de cybersécurité des institutions, organes et organismes de l'Union

La Commission convient qu'il est important de tenir compte des menaces et des risques lorsqu'il s'agit d'observer le niveau des dépenses effectuées par les institutions, organes et organismes de l'UE en matière de cybersécurité.

De même, en ce qui concerne les ressources humaines, la stabilité des effectifs de ces entités est influencée par un certain nombre de facteurs. Le marché du recrutement d'experts spécialisés en cybersécurité est de plus en plus complexe. Dans de nombreux cas, les règles en matière de ressources humaines ne sont pas adaptées aux profils spécialisés (recrutement, évolution de carrière, formation). En outre, la pression généralisée de l'autorité budgétaire en ce qui concerne les effectifs des institutions, organes et organismes de l'UE signifie que des domaines émergents hautement prioritaires, tels que la cybersécurité, connaissent un manque de postes, notamment dans les services opérationnels internes.

La référence aux progrès en matière de gouvernance et de gestion des risques devrait tenir compte du fait que le contrôle de la mise en conformité passe désormais d'un projet pilote à un déploiement complet Il est donc normal que la couverture soit encore assez faible. Ce projet de mise en conformité est la prochaine étape d'un processus d'amélioration à long terme de la cybermaturité, qui a débuté par la définition d'une méthodologie commune de gestion de risques, la construction d'un outillage commun, le déploiement de la gestion des vulnérabilités, et le suivi, la mise à l'essai et la validation de l'inventaire des actifs. Des progrès ont été accomplis dans cette entreprise de longue haleine, malgré la complexité de la base d'actifs de la Commission, qui compte plus d'un millier de systèmes d'information utilisés par plus de 50 directions générales et agences exécutives.

2. Mécanismes de coopération des institutions, organes et organismes de l'Union

La CERT-UE est une immense réussite dans la promotion de la coopération non seulement entre les institutions, organes et organismes de l'UE, mais aussi au niveau européen, grâce à sa participation en tant que membre à part entière du réseau des CSIRT créé en vertu de la directive SRI. La CERT-UE illustre ainsi comment la coopération et les services de cybersécurité peuvent être renforcés. Les observations de la Cour sur la CERT-UE soulignent très clairement le travail remarquable que cette dernière accomplit face à un paysage des cybermenaces de plus en plus hostile et à un manque chronique de ressources.

En vertu de l'actuel accord interinstitutionnel (AII), les agences décentralisées et les entreprises communes de l'UE sont officiellement représentées par l'ENISA au sein du comité de pilotage de la CERT-UE. En outre, leurs opinions sont relayées lors des réunions du comité de pilotage par un délégué du comité consultatif sur les TIC, qui est autorisé à assister l'ENISA dans son rôle de représentante des agences, mais n'a ni siège officiel ni voix. La question de la représentation

adéquate des agences au sein du comité de pilotage de la CERT-UE sera abordée dans la proposition de règlement, où la composition du comité de pilotage sera complétée par un maximum de trois représentants désignés par le réseau des agences de l'UE, sur proposition de son comité consultatif sur les TIC.

La participation au sous-groupe «cybersécurité» du CITN se fait dans toute la mesure du possible au niveau d'engagement décidé par chaque institution, organe et organisme de l'UE. Des améliorations en matière de partage d'informations sur les marchés publics, qui constituent un sujet important dans le cadre de la task-force 2 du sous-groupe «cybersécurité», sont étudiées dans la préparation du nouveau contrat-cadre relatif à la cybersécurité.

En ce qui concerne l'outillage commun pour des services tels que le courrier électronique et la vidéoconférence, la Commission a déjà mis le système SECEM-2 à la disposition des institutions, organes et organismes de l'Union, utilisé pour le courrier électronique crypté, qui repose sur la gestion efficace des clés et des certificats de cryptage. Par ailleurs, SECABC, un outil permettant le cryptage des courriers électroniques entre les institutions, est en cours de développement; l'objectif est de donner accès à cet outil aux institutions, organes et organismes intéressés à partir de 2022. La vidéoconférence sécurisée existe déjà pour les services dans lesquels sont échangées des informations sensibles non classifiées et peut être étendue à d'autres institutions, organes et organismes de l'UE sur une base ad hoc en gérant l'identité des participants à la réunion. Le partage d'informations sensibles sera également traité dans la proposition de règlement sur la sécurité de l'information (c'est-à-dire au moyen d'un étiquetage et d'un marquage communs).

3. Partage d'informations sur les vulnérabilités ou les incidents importants

Le projet de règlement sur la cybersécurité aborde le fait que les institutions, organes et organismes de l'UE ne signalent pas tous à la CERT-UE les vulnérabilités ou les incidents importants, conformément à la proposition de la Commission figurant dans la directive SRI-2[1]. Le niveau de mise en œuvre dépendra des ressources supplémentaires consacrées à cette question par les institutions, organes et organismes de l'UE autonomes. Les possibilités d'imposer l'usage de ces notifications restent limitées, y compris dans le cadre de la proposition de règlement telle que prévue actuellement, en raison de l'autonomie institutionnelle des institutions, organes et organismes de l'UE. La proposition de règlement sur la cybersécurité disposera de mécanismes de mise en conformité appropriés et proportionnés à l'objectif et au champ d'application des nouvelles règles, sans préjudice de l'autonomie des institutions, organes et organismes.

[1] Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148, COM(2020) 823 final.

III. RÉPONSES DE LA COMMISSION AUX CONCLUSIONS ET RECOMMANDATIONS DE LA COUR

Recommandation nº 1 — Améliorer la préparation de l'ensemble des institutions, organes et organismes de l'UE en matière de cybersécurité au moyen de règles communes contraignantes et de ressources accrues pour la CERT-UE

La proposition de règlement comprendra des mesures spécifiques destinées à accroître davantage le niveau commun de cybersécurité. Ces mesures se traduiront par des plans de cybersécurité, définis et mis en œuvre au niveau des institutions, organes et organismes de l'UE dans leur propre cadre de gouvernance en matière de cybersécurité.

La Commission accepte cette recommandation. En ce qui concerne les sous-recommandations spécifiques, la Commission fait observer ce qui suit:

a) La Commission accepte la recommandation nº 1, point a). Le projet de règlement comprendra des dispositions relatives aux cadres de gouvernance et de contrôle, mis en place au plus haut niveau de l'encadrement exécutif de chaque institution, organe et organisme, afin de garantir une gestion efficace et prudente de tous les risques liés à la cybersécurité.

b) La Commission accepte la recommandation nº 1, point b). Le projet de règlement renforcera la mention de l'approche fondée sur les risques pour la gestion de la cybersécurité en précisant que les actions, les plans de sécurité informatique et la mise en œuvre effective des contrôles essentiels devraient suivre les évaluations.

c) La Commission accepte la recommandation nº 1, point c). Les programmes d'éducation, de sensibilisation et de formation en matière de cybersécurité seront cités dans le projet de règlement comme faisant partie des éléments de référence en matière de cybersécurité.

d) La Commission accepte la recommandation nº 1, point d). D'après notre expérience, bien que des audits et des tests réguliers soient essentiels, ils ne sont pas suffisants pour s'assurer que des progrès sont réalisés. Par conséquent, il convient d'établir des comptes rendus réguliers et de faire preuve de transparence dans le cadre de la gouvernance en matière de cybersécurité visé au point a).

e) La Commission accepte la recommandation nº 1, point e). Le projet de règlement comprendra des dispositions relatives à la communication d'informations relatives aux menaces, vulnérabilités et incidents informatiques importants à la CERT-UE par les institutions, organes et organismes de l'UE.

f) La Commission accepte la recommandation nº 1, point f). La Commission soutient la nécessité d'augmenter les ressources de la CERT-UE. Le texte du projet de règlement comprendra des dispositions relatives à la dotation en personnel et aux contributions financières des institutions, organes et organismes de l'UE.

g) La Commission accepte la recommandation nº 1, point g). Le règlement proposé disposera de mécanismes de mise en conformité en rapport avec l'objectif et le champ d'application des dispositions et proportionnés à ceux-ci, dans le respect de l'autonomie institutionnelle des institutions, organes et organismes de l'UE. Le contenu du futur règlement dépend de

l'issue de la procédure législative et résulte d'une décision prise par le législateur de l'Union concernant la proposition présentée par la Commission.

Recommandation n° 2 – Plaider pour de nouvelles synergies entre les institutions, organes et organismes de l'Union dans des domaines ciblés

La Commission, qui préside actuellement le sous-groupe «cybersécurité» du Comité interinstitutionnel pour la transformation numérique (CITN), approuve les recommandations visant à promouvoir des solutions pour un partage cohérent et sécurisé d'informations sensibles, l'échange systématique d'informations sur les projets de cybersécurité et des cadres et contrats communs en matière de marchés publics concernant les services de cybersécurité.

La Commission accepte cette recommandation. En ce qui concerne les sous-recommandations spécifiques, la Commission fait observer ce qui suit:

a) La Commission accepte la recommandation nº 2, point a). La Commission propose des initiatives et des services techniques au sous-groupe «cybersécurité» du CITN afin de promouvoir et de soutenir l'outillage commun pour le partage d'informations sensibles, notamment dans des services tels que le courrier électronique et la vidéoconférence. Nous notons également que des marquages communs et des règles de traitement communes pour les informations sensibles non classifiées seront traités dans la proposition de règlement sur la sécurité de l'information.
b) La Commission accepte la recommandation nº 2, point b). Les task-force existantes dans le cadre du sous-groupe «cybersécurité» du CITN traitent cette question, qui sera approfondie. Des améliorations en matière de partage d'informations sur les marchés publics sont en cours d'élaboration dans le cadre de la préparation du nouveau contrat-cadre relatif à la cybersécurité.
c) La Commission accepte la recommandation nº 2, point c). Les institutions, organes et organismes de l'UE ont déjà accès à des contrats-cadres interinstitutionnels dans le domaine des TIC gérées par la Commission. La préparation du nouveau contrat-cadre relatif à la cybersécurité sera coordonnée avec le sous-groupe «cybersécurité» du CITN.

Recommandation n° 3 – Centrer davantage l'action de la CERT-UE et de l'ENISA sur les institutions, organes et organismes de l'UE moins avancés en matière de cybersécurité

La CERT-UE et l'ENISA sont destinataires de la présente recommandation.