COUR DES COMPTES EUROPÉENNE

FR

Communiqué de presse

Luxembourg, le 29 mars 2022

Les organes de l'UE doivent renforcer leur cybersécurité

Le nombre de cyberattaques dirigées contre les instances de l'UE est en nette augmentation. Le niveau de préparation en matière de cybersécurité varie d'un organe de l'UE à l'autre, mais il n'est globalement jamais à la hauteur des menaces, toujours plus sérieuses. En raison de leur forte interconnexion, une faille dans la sécurité d'un organe de l'UE peut en exposer d'autres. C'est la conclusion d'un rapport spécial de la Cour des comptes européenne consacré au niveau de préparation des instances dirigeantes de l'UE aux cybermenaces. Les auditeurs recommandent d'instaurer des règles de cybersécurité contraignantes et de renforcer les ressources de l'équipe d'intervention en cas d'urgence informatique (CERT-UE). Ils ajoutent que la Commission européenne devrait promouvoir une coopération accentuée entre les organes de l'UE, tandis que la CERT-UE et l'Agence de l'Union européenne pour la cybersécurité devraient focaliser leur soutien sur les moins avancés en matière de cybersécurité.

Les incidents de cybersécurité importants ont plus que décuplé entre 2018 et 2021, le travail à distance ayant considérablement augmenté le nombre de points d'accès potentiels pour les cybercriminels. Ils sont généralement dus à des cyberattaques complexes, qui impliquent le plus souvent l'utilisation de nouvelles méthodes et technologies, et il faut parfois des semaines, voire des mois, pour les analyser et s'en remettre. Citons par exemple la cyberattaque menée contre l'Agence européenne des médicaments, avec, comme corollaire, une fuite de données sensibles, qui ont ensuite été manipulées pour saper la confiance dans les vaccins.

«*Les institutions, organes et agences de l'UE sont des cibles de choix pour les éventuels pirates, en particulier pour les groupes capables de commettre des attaques furtives très sophistiquées à des fins de cyberespionnage*», a déclaré Bettina Jakobsen, la membre de la Cour responsable de l'audit. «*De telles attaques peuvent avoir d'importantes implications politiques, nuire à la réputation de l'Union et ébranler la confiance dans ses institutions. L'UE doit redoubler d'efforts pour protéger ses propres organisations.*»

Le principal constat posé par les auditeurs est que les institutions, organes et agences de l'UE ne sont pas toujours bien protégés contre les cyberattaques. Ces entités n'ont pas une approche cohérente de la cybersécurité: les contrôles essentiels et les principales bonnes pratiques dans ce domaine ne sont pas toujours en place et les formations spécifiques, pas systématiquement assurées. L'affectation de ressources à la cybersécurité varie fortement, certains organes de l'UE y

L'objectif de ce communiqué de presse est de présenter les principaux messages du rapport spécial adopté par la Cour des comptes européenne. Celui-ci est disponible dans son intégralité sur le site eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg
E: press@eca.europa.eu @EUAuditors eca.europa.eu

consacrant bien plus de moyens que d'autres de taille comparable. Bien que les différences en matière de cybersécurité puissent, en théorie, se justifier par les différences de profil de risque des organisations concernées et par le degré de sensibilité variable des données qu'elles traitent, les auditeurs soulignent qu'une faille dans la cybersécurité d'un seul organe de l'UE peut exposer plusieurs autres entités à des cybermenaces (les organes de l'UE sont en effet tous interconnectés et ils le sont aussi souvent avec des organisations publiques et privées dans les États membres).

L'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE) et l'Agence de l'Union européenne pour la cybersécurité (ENISA) sont les deux principales entités chargées de fournir une assistance en matière de cybersécurité aux organes de l'Union. Elles n'ont toutefois pas été en mesure de le faire autant que nécessaire, parce que leurs ressources sont limitées ou qu'elles ont accordé la priorité à d'autres domaines. Selon les auditeurs, le partage d'informations laisse également à désirer: par exemple, tous les organes de l'UE ne signalent pas à temps les vulnérabilités et les incidents de cybersécurité importants auxquels ils ont été confrontés et qui risquent d'impacter d'autres organisations.

Informations générales

Pour l'instant, il n'existe pas de cadre juridique pour la sécurité de l'information et la cybersécurité dans les institutions, organes et agences de l'UE. Ces deux domaines ne tombent pas sous le coup de la législation générale de l'UE en matière de cybersécurité, à savoir la directive SRI de 2016 et celle qui lui succédera (la directive SRI 2). Il n'existe pas non plus d'informations exhaustives sur le montant que les organes de l'UE consacrent à la cybersécurité. Les règles communes en matière de sécurité de l'information et de cybersécurité pour l'ensemble des organes de l'UE figurent dans la communication sur la stratégie de l'UE pour l'union de la sécurité pour la période 2020-2025, publiée par la Commission en juillet 2020. Dans son document intitulé «La stratégie de cybersécurité de l'UE pour la décennie numérique» et publié en décembre 2020, la Commission s'est engagée à proposer un règlement établissant des règles communes en matière de cybersécurité pour tous les organes de l'UE. Elle a également proposé d'établir une nouvelle base juridique pour la CERT-UE afin de renforcer son mandat et son financement.

Le rapport spécial 05/2022 «*Cybersécurité des institutions, organes et agences de l'UE – Un niveau de préparation globalement insuffisant par rapport aux menaces*» est disponible sur le site internet de la Cour des comptes européenne. Dans un document d'analyse de 2019, la Cour des comptes européenne avait déjà cerné les défis à relever pour une politique de l'UE efficace dans le domaine de la cybersécurité.

Contact presse

Service de presse de la Cour: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu - M: (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu - M: (+352) 691 551 502
- Damijan Fišer damijan.fiser@eca.europa.eu - M: (+352) 621 552 224