COUR DES COMPTES EUROPÉENNE

FR

Communiqué de presse

Luxembourg, le 17 décembre 2020

Les institutions supérieures de contrôle de l'UE mettent en commun leurs travaux consacrés à la cybersécurité

Alors que les menaces liées à la cybercriminalité et aux cyberattaques se sont accentuées ces dernières années, les auditeurs de toute l'Union européenne portent une attention croissante à la résilience des systèmes d'information et des infrastructures numériques critiques. Le compendium d'audit sur la cybersécurité, publié aujourd'hui par le comité de contact des institutions supérieures de contrôle (ISC) de l'UE, présente une vue d'ensemble des principaux travaux d'audit qu'elles ont réalisés dans ce domaine.

Les cyberincidents peuvent être intentionnels ou non et vont de la divulgation accidentelle d'informations à l'ingérence dans les processus démocratiques (y compris les élections) et l'organisation de campagnes de désinformation pour influencer le débat public, en passant par les attaques contre les entreprises et les infrastructures critiques et le vol de données à caractère personnel. La cybersécurité constituait déjà un enjeu crucial pour nos sociétés avant le déclenchement de la pandémie de COVID-19, mais les conséquences de la crise à laquelle nous sommes confrontés ne feront qu'accroître les cybermenaces. Bon nombre d'activités commerciales et de services publics ont dû évoluer et passer à un environnement en ligne, tandis qu'«infox» et théories du complot prolifèrent comme jamais.

La protection des systèmes d'information et des infrastructures numériques critiques contre les cyberattaques est donc devenue un défi stratégique toujours plus présent pour l'UE et ses États membres. Il ne s'agit plus, désormais, de déterminer si des cyberattaques sont susceptibles de se

L'objectif de ce communiqué de presse est de présenter les principaux messages du compendium d'audit publié par le comité de contact des institutions supérieures de contrôle de l'UE et de la Cour des comptes européenne.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

E: press@eca.europa.eu @EUAuditors eca.europa.eu

produire, mais plutôt quand et comment elles vont se produire. Particuliers, entreprises, pouvoirs publics: nous sommes tous concernés!

«*La crise liée à la COVID-19 met à rude épreuve le tissu économique et social de nos sociétés. Compte tenu de notre dépendance à l'égard des technologies de l'information, la prochaine pandémie qui nous guette pourrait bien prendre la forme d'une «cybercrise»»,* **a déclaré Klaus-Heiner Lehne, le président de la Cour des comptes européenne**. *«Nul doute que la recherche de l'autonomie numérique ainsi que celle de réponses aux défis que posent les cybermenaces et les actions extérieures de désinformation continueront à faire partie de notre quotidien et des priorités politiques pour les dix prochaines années. Il est donc essentiel de faire mieux connaître les constatations des audits en lien avec la cybersécurité effectués récemment dans les États membres de l'UE.»*

C'est pourquoi les ISC européennes ont enclenché la vitesse supérieure dans le domaine de la cybersécurité, en mettant plus particulièrement l'accent sur la protection des données, sur l'état de préparation des systèmes face aux cyberattaques, ainsi que sur la protection des systèmes de services publics essentiels. Cette accélération s'inscrit dans un contexte où l'UE entend faire en sorte que son environnement numérique soit le plus sûr au monde. La Commission européenne et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité viennent d'ailleurs de présenter une nouvelle stratégie de cybersécurité de l'UE, qui vise à renforcer la résilience collective de l'Europe face aux cybermenaces.

Le *compendium* publié aujourd'hui fournit des informations générales sur la cybersécurité, les grandes initiatives stratégiques et les bases juridiques pertinentes de l'UE. Il illustre également les principaux défis auxquels l'Union et ses États membres sont confrontés, comme les menaces pesant sur les droits des citoyens européens du fait de l'utilisation abusive de leurs données personnelles, et le risque que les institutions ne soient pas à même d'assurer les services publics essentiels – ou qu'elles puissent ne les assurer que d'une manière limitée – à la suite de cyberattaques.

Le *compendium* s'appuie sur les résultats d'audits récemment réalisés par la Cour des comptes européenne et les ISC de 12 États membres, à savoir le Danemark, l'Estonie, l'Irlande, la France, la Lettonie, la Lituanie, la Hongrie, les Pays-Bas, la Pologne, le Portugal, la Finlande et la Suède.

Informations générales

Ce *compendium* d'audit est un produit de la coopération entre l'ISC de l'UE et celles des États membres dans le cadre du comité de contact. Il est conçu pour servir de source d'information à quiconque s'intéresse à cet important domaine d'action. Il est actuellement accessible en anglais sur le site internet du comité de contact et sera disponible ultérieurement dans d'autres langues de l'Union.

Il s'agit du troisième *compendium* d'audit établi par le comité de contact. Le premier compendium, consacré au chômage des jeunes et à leur insertion sur le marché du travail, a été publié en juin 2018. Le second, sur le thème de la santé publique dans l'UE, est sorti en décembre 2019.

Le comité de contact réunit les présidents de l'ISC de l'UE et de celles des États membres au sein d'une assemblée autonome, indépendante et apolitique. Il constitue un forum permettant d'aborder des questions relatives à l'UE qui présentent un intérêt commun. En renforçant le

dialogue et la coopération entre ses membres, le comité de contact contribue à l'efficacité et à l'indépendance de l'audit externe des politiques et des programmes de l'UE.

Contact presse

Vincent Bourgeais – E: vincent.bourgeais@eca.europa.eu
T: (+352) 4398 47 502 / M: (+352) 691 551 502