Accusé de réception - Ministère de l'Intérieur
076-287600027-20230620-2023-DEL-076-DE
Accusé certifié exécutoire
Réception par le préfet : 03/07/2023

DÉLIBÉRATION N°2023-DEL-076

RÉUNION DU CONSEIL D'ADMINISTRATION DU 20 JUIN 2023

EXTRAIT DU PROCÈS-VERBAL DES DÉLIBÉRATIONS

Le mardi vingt juin deux-mille-vingt-trois à 14h31, s'est réuni le Conseil d'Administration du Centre de Gestion, au siège du Centre, 40 Allée de la Ronce à ISNEAUVILLE, sur convocation de Jean-Claude WEISS, Président démissionnaire, et sous la présidence de Christophe BOUILLON, Président nouvellement élu.

Nombre de membres en exercice : 24 Quorum : 13

PRÉSENTS :

Mesdames Marie-Claude BEAUFILS, Claudine BRIFFARD, Annic DESSAUX, Joëlle DOUBET, Blandine LEFEBVRE, Marie-Françoise LOISON, Françoise UNDERWOOD, Martine VIALA et Messieurs Michel BARBIER, Nicolas BERTRAND, Christophe BOUILLON, Jean CHOMANT, Bastien CORITON, Guillaume COUTEY, Eric HERBET, Laurent JACQUES, Jean-François MAYER, Pierre PELTIER, Jean-Marc VASSE Jean-Claude WEISS.

ABSENTS AYANT DONNE POUVOIR :

- Madame Mélanie BOULANGER (pouvoir à Monsieur Christophe BOUILLON)
- Madame Marie-Agnès POUSSIER WINSBACK (pouvoir à Monsieur Jean-Claude WEISS)
- Monsieur Martial OBIN (pouvoir à Monsieur Jean-François MAYER)
- Monsieur François ROGER (pouvoir à Madame Claudine BRIFFARD)

ABSENT EXCUSE :

- Monsieur Bastien CORITON

OBJET : FONCTIONNEMENT INTERNE – CYBERSECURITE – CELLULE DE CRISE – CREATION – INFORMATION

- **Vu le Code Général de la Fonction Publique,**
- **Vu le Code Général des Collectivités Territoriales,**
- **Vu le dispositif France Relance promu par l'Etat dans le cadre du soutien de l'économie, des entreprises et des administrations à la suite de l'épidémie de COVID-19,**

- **Vu la délibération n° 2022/064 du 10 mai 2022 relative au dispositif France relance,**

- **Vu la délibération n° 2023/015 du 27 janvier 2023 relative à la politique de Cyber sécurité,**

- **Considérant le besoin de structurer la démarche interne du Centre de Gestion en cas de cyber-attaque.**

Monsieur le Président cède la parole à Monsieur Eric HERBET, membre du Bureau, qui rappelle que pour l'exercice de leurs missions, les services du Centre de Gestion ont recours à de nombreuses applications informatiques dont certaines sont transversales (outils de communication et d'échanges de données interservices) et d'autres spécifiques aux activités de l'établissement (applications métiers).

Monsieur HERBET précise que ces outils, développés par des entreprises privées ou établissements publics (GIP Informatique, CIG Grande Couronne), sont générateurs de flux entrants et sortants en lien avec de multiples partenaires externes (collectivités, établissements publics, autres CDG, administrations de l'Etat, candidats aux concours et examens, entreprises et prestataires...).

L'infrastructure informatique du Centre de Gestion a été pensée et dimensionnée pour prendre en compte l'ensemble des informations échangées et traitées quotidiennement. A cet égard, nos équipements, nos logiciels et nos données font l'objet d'une attention particulière, non seulement au regard du règlement général de la protection des données (RGPD), mais aussi sur le plan de la sécurité active et passive.

Dans ce domaine de la sécurité, notre établissement a beaucoup investi ces dernières années, notamment en 2022 ; Il s'apprête en 2023 à renforcer encore ses protections à la suite de l'audit que nous avons engagé dans le cadre du dispositif « France Relance » piloté par l'ANSSI.

Ainsi, par délibération en date du 27 janvier 2023, le Conseil d'Administration a autorisé l'engagement des consultations nécessaires à la souscription de contrats pluriannuels pour des prestations préventives de cyber-sécurité.

Afin de suivre et d'animer l'ensemble des actions en cours et à venir, un comité de pilotage dédié à la cyber-sécurité a été constitué en septembre 2022. Cette instance interne réunit :

- L'élu du Bureau en charge de l'informatique
- Le Responsable du Pôle Moyens Généraux
- La Responsable du Pôle Santé/prévention
- Le Responsable du Service Informatique, avec l'appui du secrétariat de direction
- Le Chargé de Support et Services des systèmes d'information

Monsieur HERBET précise que ce comité de pilotage a pour objectifs principaux :
- De suivre la mise en place des préconisations issues de l'audit de cybersécurité,
- De proposer les actions à réaliser dans le cadre de la politique de sécurité de l'information,
- D'évaluer l'efficacité de la mise en œuvre de cette politique,
- De lancer des plans et des programmes pour maintenir la sensibilisation à la sécurité de l'information,
- D'être consulté en amont de tous projets informatiques des services,
- De s'assurer que les activités de sécurité sont exécutées conformément à la politique définie par le conseil d'administration,
- D'identifier et recommander la manière de traiter les cas de non-conformité,
- D'identifier les changements importants dans les menaces et les vulnérabilités,
- D'évaluer les informations reçues des processus de surveillance,
- D'examiner les informations relatives aux incidents de sécurité de l'information et recommander des mesures de suivi,
- De définir les propositions d'investissement cyber lors de la préparation annuelle du budget.

A l'appui de l'ensemble de ces mesures de prévention, et au regard des investissements ambitieux de l'établissement en matière de protection des systèmes d'information, il est également apparu capital de s'engager dans une démarche de préparation à une éventuelle cyber-attaque.

En effet, quels que soient les protections et les processus de sécurité mis en place, nous ne pouvons exclure cette éventualité. Les enjeux pour le Centre de Gestion, en cas de cyber-attaque, seraient importants ; Ils peuvent se synthétiser en trois points :

- Une responsabilité juridique inhérente à l'impossibilité de réaliser les missions qui sont confiées au CDG,
- Un possible impact budgétaire en cas d'arrêt forcé de l'activité, notamment en ce qui concerne les missions optionnelles,
- Un risque pour l'image et la crédibilité de notre établissement.

Notre démarche de préparation d'une cyber-attaque se veut donc proactive, à la fois anticipative et collaborative ; Elle se décline en deux axes :

1 – la création d'une cellule de crise rassemblant, autour du directeur de l'Etablissement, des membres du COPIL précités ainsi que d'autres personnes disposant des compétences requises pour :

- Repérer et rassembler les indices faisant prendre conscience qu'une cyberattaque est en cours (ou est survenue),
- Ordonner les actions immédiates à mener en cas de cyberattaque afin de la déjouer ou d'en limiter les effets,
- Coordonner les différentes missions à conduire lorsque l'attaque est avérée et qu'elle a produit des effets (communications interne et externe, collaboration avec les partenaires institutionnels, réalisation des obligations légales, organisation du travail en mode dégradé ...),

L'objectif final est d'inclure ces différentes actions dans le Plan de Continuité d'Activité.

2- Le lancement de groupes de travail au sein des différents pôles et services du Centre de gestion, pour élaborer la stratégie de continuité de l'activité en cas de cyber-attaque.

Ces travaux, engagés à compter de mai 2023 avec l'ensemble des services du Centre de Gestion, visent les objectifs suivants :

- Préserver au maximum la continuité de service pour les collectivités affiliées et non affiliées du CDG ainsi que pour leurs agents, par la rédaction de modes opératoires qui viendront se substituer au fonctionnement habituel des services dans l'hypothèse d'une cyber-attaque,
- Limiter les conséquences de la cyber-attaque en termes de retard et report de charge pour les services, en recherchant des solutions préservant le maximum de tâches essentielles,
- Garantir aux agents des conditions de travail acceptables, malgré un fonctionnement en mode dégradé, grâce à l'anticipation et à la réflexion en amont.

Le Plan de Continuité de l'Activité, enrichi des productions des différents pôles, sera présenté au Conseil d'Administration en fin d'année 2023.

Monsieur HERBET indique que, par ces différentes actions et organisation, le Centre de Gestion souhaite se doter de tous les outils nécessaires pour apporter une réponse rapide à une cyberattaque, afin d'en réduire autant que faire se peut les effets sur son fonctionnement et ses agents.

Compte tenu de l'ensemble des éléments exposés, Monsieur HERBET entendu, le Conseil d'Administration prend acte de la création d'une cellule de crise et du lancement de groupes de travail au sein des différents pôles et services du Centre de gestion, pour élaborer la stratégie de continuité de l'activité en cas de cyber-attaque.

Le Secrétaire,
Jean CHOMANT

Pour extrait certifié conforme
Le Président,
Christophe BOUILLON

CENTRE DE GESTION