JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 315 du 29 juin 2022

Loi du 17 juin 2022 modifiant :

1° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ;
2° la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État ;
3° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ;
4° la loi modifiée du 8 avril 2018 sur les marchés publics.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Notre Conseil d'État entendu ;

De l'assentiment de la Chambre des Députés ;

Vu la décision de la Chambre des Députés du 17 mai 2022 et celle du Conseil d'État du 31 mai 2022 portant qu'il n'y a pas lieu à second vote ;

Avons ordonné et ordonnons :

Art. 1er.

La loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° L'article 2 est modifié comme suit :

a) Le point 4 est remplacé par le texte suivant :

« « infrastructure critique » : tout point, système ou partie de celui-ci qui est indispensable à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population ; » ;

b) Il est inséré un point 4*bis* libellé comme suit :

« 4*bis*. « sécurité de l'information » : sécurité autour des réseaux et systèmes d'information non classifiés installés et exploités par les administrations et services de l'État ; » ;

2° L'article 3 est modifié comme suit :

a) Il est inséré un paragraphe 1*bis* libellé comme suit :

« (1*bis*) Le Haut-Commissariat à la Protection nationale est encore chargé des missions suivantes :

a) attributions dans sa fonction d'Agence nationale de la sécurité des systèmes d'information, ci-après « ANSSI » ;
b) attributions dans sa fonction de Centre de traitement des urgences informatiques, ci-après « CERT Gouvernemental » ;
c) attributions dans sa fonction de Service de la communication de crise, ci-après « SCC ». » ;

b) Il est inséré un paragraphe 1*ter* libellé comme suit :

« (1*ter*) Dans sa fonction d'ANSSI, le Haut-Commissariat à la Protection nationale a pour missions :

a) de contribuer à la mise en œuvre de la politique générale de sécurité de l'information de l'État ;

b) de contribuer à la mise en œuvre, en concertation avec les administrations et services de l'État, des politiques et lignes directrices de sécurité de l'information portant sur les domaines de la politique générale de sécurité de l'information de l'État et des nouvelles technologies de l'information et de la communication ;
c) d'émettre des recommandations d'implémentation des politiques et lignes directrices de sécurité de l'information et d'assister les administrations et services de l'État au niveau de l'implémentation des mesures proposées ;
d) de définir, en concertation avec les administrations et services de l'État, une approche de gestion des risques, en vue de constituer un plan d'évaluation et d'identification des risques concernant la sécurité de l'information et d'accompagner, à leur demande, les administrations et services de l'État dans l'analyse et la gestion des risques ;
e) de conseiller l'Institut national d'administration publique, respectivement, à leur demande, les administrations et services de l'État dans la définition d'un programme de formation dans le domaine de la sécurité de l'information ;
f) de promouvoir la sécurité de l'information par le biais de mesures de sensibilisation ;
g) de conseiller, à leur demande, les établissements publics et les infrastructures critiques en matière de sécurité des réseaux et systèmes d'information et des risques y liés ;
h) d'assurer la fonction d'autorité TEMPEST en veillant à la conformité des réseaux et systèmes d'information classifiés aux stratégies et lignes directrices TEMPEST et en approuvant les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des pièces classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel. » ;

c) Il est inséré un paragraphe 1*quater* libellé comme suit :

« (1*quater*) Dans sa fonction de CERT Gouvernemental, le Haut-Commissariat à la Protection nationale a pour missions :

a) de constituer le point de contact unique dédié au traitement des incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information des administrations et services de l'État et, à leur demande, des établissements publics et des infrastructures critiques ;
b) d'assurer un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et systèmes d'information des administrations et services de l'État et, à leur demande, des établissements publics et des infrastructures critiques ;
c) d'assurer la fonction de centre national de traitement des urgences informatiques, dénommé CERT National, en
    1. opérant comme le point de contact officiel national pour les CERTs nationaux et gouvernementaux étrangers ;
    2. opérant comme le point de contact officiel national pour la collecte et la distribution d'informations relatives aux incidents de sécurité qui concernent les réseaux et systèmes d'information implantés au Luxembourg ;
    3. relayant les informations collectées aux CERTs sectoriels en charge de la cible d'une attaque ou à défaut de CERT sectoriel, directement à la cible.
d) d'assurer la fonction de centre militaire de traitement des urgences informatiques, dénommé CERT Militaire, en
    1. opérant comme le point de contact officiel national pour les CERTs militaires étrangers ;
    2. assurant un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information de l'armée à partir du territoire du Grand-Duché ;
    3. opérant, à partir du territoire du Grand-Duché, une équipe d'intervention spécialisée capable de prendre en charge la réponse aux incidents de sécurité d'envergure liés à ces réseaux et systèmes d'information.