Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

Service spécialisé de défense et de sécurité

Le haut fonctionnaire de défense et de sécurité

HFDS
N°2015 -

Affaire suivie par :
Michelle Proquin
Chargé de mission « Plans nationaux »
Téléphone
0155558577
Mél.
Michelle.Proquin
@education.gouv.fr

99, rue de Grenelle
75357 Paris 07 SP

Paris, le 23 mars 2016

Le haut fonctionnaire de défense et de sécurité

à

Mesdames et messieurs les recteurs d'académies, chanceliers des universités,

Mesdames et messieurs les présidents ou directeurs d'établissements d'enseignement supérieur,

Mesdames et messieurs les présidents ou directeurs d'organismes de recherche

Madame la directrice du Cnous par intérim

Mesdames et messieurs les directeurs des Crous

Objet : Rappel de la posture VIGIPIRATE

Les récents attentats de Bruxelles ont rappelé le besoin d'une posture VIGIPIRATE adaptée à une menace particulièrement élevée sur le territoire national.

Les niveaux « alerte attentat » en Ile de France et « vigilance renforcée » pour le reste du territoire sont toujours en vigueur.

Le maintien des efforts particuliers de protection et de sensibilisation est essentiel autour des bâtiments accueillant du public ou lors des rassemblements. Un rappel à la vigilance et aux contrôles est nécessaire.

Les circulaires de novembre et décembre ont rappelé l'ensemble des mesures de sécurité et de préparation indispensables. Les attentats récents ont montré la nécessité de détenir de manière centralisée au niveau du rectorat un état actualisé des différents voyages et déplacements en cours, en particulier à l'étranger, et une capacité de communication avec chacun d'eux.

Vous trouverez en annexe de ce courrier le descriptif actuel de l'ensemble des mesures Vigipirate en vigueur.

Le haut fonctionnaire de défense et de sécurité

Frédéric GUIN

PJ :1

Annexe : mesures VIGIPIRATE en vigueur au 23 mars 2016

Mesures	Commentaires
Activer les cellules de veille et d'alerte et les cellules de crise	Activation des cellules de veille et de crise laissée à l'appréciation des autorités académiques ou des établissements d'enseignement supérieur et de recherche.
Diffuser l'alerte au public	Affichage du logo Vigipirate « Alerte attentats » en Ile de France et « Vigipirate » sur le reste du territoire aux endroits où des mesures de protection renforcées sont mises en œuvre.
Renforcer la surveillance et le contrôle lors des rassemblements	Les efforts de vigilance et de protection doivent porter sur les rassemblements. Maintien des mesures de vigilance et de sécurité renforcées lors des manifestations, scientifiques, culturelles sociales ou festives jugées sensibles, en liaison avec les préfets.
Contrôler les accès des personnes, des véhicules et des objets entrants (dont le courrier) Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	Maintien du renforcement du contrôle des accès dans tous les établissements, sur l'ensemble du territoire national, et plus particulièrement en Ile de France et pour les OIV. Le ciblage, les modalités et l'intensité de ce contrôle sont à définir par le chef d'établissement ou le directeur en liaison avec la préfecture et le rectorat. Cette mesure peut se traduire par le recours à la vidéo surveillance, des rondes de sécurité plus fréquentes. Sur l'ensemble du territoire, une attention particulière sera portée sur les lieux de culte, les écoles confessionnelles et établissements culturels et symboliques sensibles des diverses confessions religieuses. Une attention particulière au contrôle des accès sera portée lors des manifestations pouvant se dérouler dans l'enceinte des établissements pendant les congés scolaires. Ces manifestations doivent être signalées à la préfecture. Les contrôles doivent être visibles et tendre à être systématiques.
Avoir les ressources humaines permettant la cybersécurité	A : Responsabiliser le personnel. 1) En rappelant aux utilisateurs les points suivants : - demeurer vigilants sur les courriels reçus. En cas de doute, ne pas ouvrir les pièces jointes, ni suivre les liens Internet y figurant ; - minimiser les navigations vers des sites Internet n'ayant pas de rapport avec l'activité professionnelle ; - rendre compte aux responsables locaux de la sécurité des systèmes d'information de tout comportement anormal du poste de travail. 2) En invitant les responsables organiques à s'assurer auprès des hébergeurs des sites Internet à protéger d'une capacité d'intervention rapide en cas d'incident affectant l'un de ceux-ci.

Protéger logiquement ses systèmes d'information	B : Protéger logiquement ses systèmes d'information en conduisant dans les meilleurs délais les actions suivantes : • assurer une revue des droits des comptes les plus privilégiés et en assurer une supervision; • contrôler l'application de la politique des mots de passe et renouveler les mots de passe des comptes les plus privilégiés ; • vérifier ou mettre en place les mesures de prévention en matière de déni de service. Base documentaire :Notes d'information du site www.cert.ssi.gouv.fr, notamment : - Note CERTA-2012-INF-001 : Dénis de service – prévention et réaction ; - Note CERTA-2012-INF-002 : Les défigurations de type WEB ; - Note CERTA-2002-INF-002 : Les bons réflexes en cas d'intrusion sur un système d'information ; - Note CERTA-FR-2014-ALE-003 : Vulnérabilité dans OpenSSL. - Note CERTA-2004-INF-001-001 : Protection des sites Internet - Note CERTA-2002-INF-002-004 : Conduite à tenir en cas d'intrusion - Guide du site de l'ANSSI, notamment : - www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_NoteTech.pdf : recommandation pour la sécurité des sites WEB. - www.ssi.gouv.fr/actualité/proteger-son-site-internet-des-cyberattaques. - sécurisation des sites Internet : - www.ssi.gouv.fr/administration/guide/recommandations-pour-la-sécurisation-des-sites-web - attaques par défiguration : - www.ssi.gouv.fr/entreprise/principales-menaces/destabilisation/attaques par défiguration - comprendre et anticiper les attaques en déni de service : - www.ssi.gouv.fr/administration/guide/comprendre-et-anticiper-les-attaques-ddos - conduite à tenir en cas d'intrusion : - www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002 - Notification d'incidents : - www.ssi.gouv.fr/agence/contacts/cossicert-fr "