PRÉFÈTE
DU LOIRET
Liberté
Égalité
Fraternité

Direction des Sécurités
Bureau de la Protection et
de la Défense Civiles

Orléans, le 26 mars 2024

Madame la Préfète du Loiret

à

Destinataires *in fine*

Objet : **Adaptation de la posture VIGIPIRATE – Urgence attentat**

Référence : Plan gouvernemental VIGIPIRATE du 1er décembre 2016 (édition mai 2019)
Bulletin d'alerte VIGIPIRATE du lundi 25 mars 2024

À la suite de l'attentat de Moscou du 22 mars 2024 revendiqué par l'organisation État islamique et aux menaces terroristes pesant sur notre pays, le Gouvernement a fait évoluer la posture VIGIPIRATE au niveau « URGENCE ATTENTAT », plus haut niveau de vigilance du plan concerné.

La présente posture entre en vigueur immédiatement et jusqu'à nouvel ordre.

Le bulletin d'alerte VIGIPIRATE du lundi 25 mars 2024 et le niveau de vigilance « URGENCE ATTENTAT » adaptent le dispositif de vigilance et de sécurisation en portant une attention particulière sur les mesures suivantes :

- **renforcer la surveillance aux abords des bâtiments publics, éducatifs, sportifs, culturels et cultuels ;**
- **contrôler les accès des personnes, des véhicules et des objets entrant dans ces bâtiments ;**

Tout en maintenant les mesures spécifiques sur les lieux éducatifs, un effort particulier doit être porté sur les évènements et bâtiments cultuels et culturels, notamment en cette fin de semaine.

Concernant la première mesure, j'ai mobilisé les Forces de sécurité intérieure (FSI) pour accentuer les patrouilles aux abords de ces établissements et ai sollicité le renfort de la Force Sentinelle auprès des Armées pour compléter le dispositif.

En parallèle, je demande aux collectivités la mobilisation de leurs polices municipales en coordination avec les forces de sécurité intérieure, notamment pour renforcer la sécurité aux abords des établissements scolaires du 1er degré (écoles maternelles en priorité) et les bâtiments publics des communes.

Concernant la seconde mesure, j'invite les chefs d'établissement à renforcer les mesures de contrôles pour accéder aux bâtiments concernés (contrôle des billets d'entrée, des invitations, des pièces d'identité le cas échéant ; contrôle visuel des sacs ; palpation aléatoire ou systématique en fonction de la sensibilité des lieux ou des évènements).

Le signalement sans délai de tout individu présentant un comportement suspect devra être fait aux forces de l'ordre territorialement compétentes en composant le 17.

Préfecture du Loiret – 181 rue de Bourgogne – 45042 Orléans Cedex 1
tél : 02 38 91 45 45 - site internet : www.loiret.gouv.fr

En complément, **au regard de la menace cyber**, je vous invite à renforcer vos systèmes d'identification des attaques par déni de service distribué (Distributed Denial of Service ou DdoS)[1] et à créer des alertes en conséquence, notamment pour les établissements scolaires.

En parallèle, vous conforterez vos annuaires de crise et vous vérifierez vos capacités à pouvoir communiquer en interne ainsi qu'avec vos bénéficiaires / partenaires dans l'éventualité d'une indisponibilité de vos outils numériques habituels.

Je vous invite à me faire part de toute difficulté rencontrée dans la mise en œuvre des mesures précitées.

P/ la Préfète,
Le secrétaire général,

Stéphane COSTAGLIOLI

1 Une attaque par déni de service vise à rendre indisponible un ou plusieurs services. Un déni de service peut consister à exploiter, par exemple, une vulnérabilité logicielle ou matérielle. L'interruption de service peut également s'effectuer en empêchant l'accès à ce service, par exemple en saturant la bande passante du réseau : on parle alors d'attaques volumétriques. Par ailleurs, une attaque peut solliciter, jusqu'à épuisement, une ou plusieurs ressources d'un service. Il peut s'agir, par exemple, de l'ouverture d'un grand nombre de nouvelles sessions dans un intervalle de temps très court, ou encore d'un nombre trop important de traitements concurrents effectués par une base de données. On parle de « déni de service distribué » (de l'anglais Distributed Denial of Service ou DDoS) lorsque l'attaque fait intervenir un réseau de machines (souvent compromises) afin d'interrompre le ou les services visés.
Toute entité dont l'activité dépend d'une infrastructure réseau connectée à Internet peut être la cible d'une attaque DdoS.

Préfecture du Loiret – 181 rue de Bourgogne – 45042 Orléans Cedex 1
tél : 02 38 91 45 45 - site internet : www.loiret.gouv.fr

Destinataires

Monsieur le Recteur de l'académie Orléans-Tours
Monsieur le Président de l'université d'Orléans
Monsieur le Directeur académique des services de l'éducation nationale

Monsieur le Président de la communauté israélite d'Orléans
Monseigneur l'Évêque d'Orléans
Monsieur le Président du Conseil départemental du culte musulman
Madame la Présidente de l'Église protestante unie d'Orléans
Monsieur le Président de l'Association cultuelle catholique orthodoxe Saint-Avit

Mesdames et Messieurs les Maires
Mesdames et Messieurs les Présidents des Établissements Publics de coopération intercommunale à fiscalité propre
Monsieur le Président du Conseil départemental du Loiret
Monsieur le Président du Conseil régional Centre – Val de Loire

Mesdames et messieurs les directeurs des établissements de santé

Copie :
Monsieur le Directeur interdépartemental de la police nationale
Monsieur le Commandant du groupement de gendarmerie du Loiret
Monsieur le Délégué militaire départemental

Préfecture du Loiret – 181 rue de Bourgogne – 45042 Orléans Cedex 1
tél : 02 38 91 45 45 - site internet : www.loiret.gouv.fr