www.fsgtnord.org

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

Calendrier BAFA
Cliquer sur l'image

COSPORTS F.S.G.T.
La boutique de votre Comité
Cliquer sur le logo

POSTURE VIGIPIRATE

Mesdames, Messieurs,

La présente adaptation de la posture vigipirate prend en compte une triple menace : la menace terroriste qui se maintient à un niveau extrêmement élevé, la menace cyber, ainsi que la menace représentée par les groupes anarchistes radicaux dans le cadre de la COP 21.

Face à ces menaces, le niveau « alerte-attentat » est maintenu en Île-de-France et la vigilance renforcée continue de s'appliquer sur le reste du territoire national. Les mesures activées à la suite de la campagne d'attentats du 13 novembre restent en vigueur jusqu'à nouvel ordre de même que les objectifs de sécurité définis depuis le mois de septembre : les sites sensibles, tels que les établissements culturels et cultuels, les lieux de forts rassemblements, les transports et les sites industriels sensibles.

Cette posture est activée à compter d'aujourd'hui, 23 novembre 2015, pour être levée le 14 décembre 2015. Les mesures "cyber" sont, quant à elles, en vigueur jusqu'au 18 décembre 2015.

I. Mesures de protection des bâtiments et des personnes

La mesure visant à contrôler les accès des personnes, des véhicules et des objets entrants (BAT 23-01) a été activée après les attentats du 13 novembre et se prolongera au-delà de la COP 21.

Les opérateurs veilleront à appliquer scrupuleusement les mesures de contrôle des accès, présentation d'une pièce d'identité et contrôle visuel des sacs notamment.

Á la suite du déclenchement de l'état d'urgence, l'interdiction des rassemblements de grande ampleur, quelle qu'en soit la nature, sera prononcée, en fonction de leur appréciation, par les autorités préfectorales.

La mesure visant à renforcer la surveillance et le contrôle des rassemblements (RSB 13-01) a été activée après les attentats du 13 novembre et se prolongera au-delà de la COP 21.

II. Mesures de protection des systèmes d'information

Les retours d'expérience à la suite des attentats où de grands évènements mondiaux ainsi qu'une première analyse de la menace, permettent d'affirmer que la tenue de la COP21 représente un terrain favorable au développement d'attaques numériques pouvant perturber son bon fonctionnement ou celui des administrations.

Parmi les attaques les plus probables, il convient de veiller et de sensibiliser les acteurs :
-- sur les risques d'hameçonnage (messages non sollicités contenant un lien redirigeant vers un site ou téléchargeant un code malveillant ;

-- sur les dénis de service sur les sites (indisponibilité, défiguration, intrusion) ;
-- sur les attaques sur les systèmes connectés à internet.

Afin de se préparer à faire face à toute menace ou attaque cyber dans le cadre de la COP 21, la chaîne de cybersécurité est mobilisée.

Il convient de vérifier la mise en œuvre des points suivants concernant :
-- La préparation d'une activation possible de plan de continuité d'activité ; Il s'agit de maintenir à jour les procédures de continuité d'activité en cas de perte temporaire d'un système d'information et de s'assurer que le personnel chargé de mettre en œuvre le PCA est familiarisé avec celui-ci : organisation de crise et personnel qualifié présent durant cette période (CYB 42-01/06) ;

-- Veiller aux bonnes configurations de journalisation des évènements sur vos systèmes d'information critiques Il s'agit a minima de conserver le paramétrage (fréquence, criticité et taille de sauvegarde) adoptée en application de la posture actuelle (CYB 42-01/09) ;

-- La transmission immédiate vers la chaîne cybersécurité de tout incident sur l'adresse ssi@sg.social.gouv.fr

Il est demandé en plus d'adapter et augmenter la fréquence d'analyse des journaux des systèmes critiques. Il s'agit, à minima, d'activer / d'augmenter la fréquence d'analyse des journaux des équipements en bordure de réseau (journaux web, virtual private network, proxies, pare-feux). A noter que les équipes en charge de la supervision doivent être particulièrement attentives aux signaux durant cette période, afin de détecter une intrusion ou une exfiltration le plus tôt possible (CYB 42-01/10) ;

Enfin, il doit être envisagé, en cas de nécessité, de mettre en œuvre les mesures suivantes :
-- Être en mesure de transmettre vers la chaîne de cybersécurité les éléments techniques relatifs à des incidents. Ces éléments doivent pouvoir être transmis au centre opérationnel de sécurité des systèmes d'information –COSSI (CYB 42-01/04) ;

-- Utiliser un réseau déconnecté du réseau usuel (ou un poste dédié) pour communiquer en interne et avec le COSSI. Employer les canaux sécurisés à disposition. En particulier, utiliser des moyens d'échange sécurisés (chiffrement) pour la communication d'informations sensibles (CYB 42-01/20). En cas de nécessité le choix des outils de chiffrement à utiliser sera réalisé en collaboration avec le fonctionnaire de sécurité des systèmes d'information ;

-- Être en capacité de réaliser des filtrages de flux : des équipements de filtrage de niveau réseau (et applicatif) sont pré-déployés en périphérie des sous-réseaux et peuvent être sollicités sans délai. Il faut se tenir prêt à couper les liens des systèmes critiques d'internet, ou, si cela n'est pas possible, à les isoler : flux en sortie (type proxies) ainsi que flux entrants (type virtual private network). Se reporter aux bonnes pratiques et règles décrites dans le paragraphe « guides et référentiels » : points 1, 2, 4, 7, 8 et 9. (CYB 42-01/12) ;

-- Pour les systèmes d'information concernés, se préparer à activer le plan de continuité d'activité. Les différents systèmes d'information liés à la COP 21 doivent être en mesure d'assurer leurs missions même en cas d'attaque par déni de service. Se reporter aux bonnes pratiques et règles décrites dans le paragraphe « guides et référentiels » : points 3, 5 et 6 (CYB 42-02/06).

Guides et référentiels :

Des fiches de recommandations sont disponibles sur le site Internet de l'Agence nationale de sécurité des systèmes d'information - ANSSI - et du site Internet du centre de réponse aux attaques informatiques (CERT-FR).

1. Guide d'hygiène : http://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique
2. Guide des bonnes pratiques : http://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/
3. Déni de service – Prévention et réaction : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-001
4. Sécurisation des sites web : http://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-sécurisation-des-sites-web/

5. Comprendre et anticiper les attaques en déni de service : http://www.ssi.gouv.fr/entreprise/guide/comprendre-et-anticiper-les-attaques-ddos/

6. Défiguration, déni de services : www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateurs.pdf,
7. Cyberattaque, prévention, réaction : www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf
8. Conduite à tenir en cas d'intrusion : www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002
9. Défiguration de sites : www.cert.ssi.gouv.fr/site/CERTA-2012-INF-002

Afin de faciliter le traitement de cette nouvelle posture Vigipirate et la communication à destination des personnels, le détail des mesures relevant du domaine public figure dans le tableau joint à cet envoi.

Le service du HFDS se tient à la disposition des directions d'administration centrale, des conseillers de défense et de sécurité de zone pour répondre à leurs questions éventuelles.

Général (2S) Robert de CRÉMIERS
Haut Fonctionnaire de défense et de Sécurité adjoint
des ministères chargés des affaires sociales